Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Wednesday, June 20, 2018

Work Order No.: NRC-3784 Pages 1-357

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

1
2
3
4 DISCLAIMER
5
6
7 UNITED STATES NUCLEAR REGULATORY COMMISSION'S
8 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
9
10
11 The contents of this transcript of the
12 proceeding of the United States Nuclear Regulatory
13 Commission Advisory Committee on Reactor Safeguards,
14 as reported herein, is a record of the discussions
15 recorded at the meeting.
16
17 This transcript has not been reviewed,
18 corrected, and edited, and it may contain
19 inaccuracies.
20
21
22
23

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

WEDNESDAY

JUNE 20, 2018

+ + + + +

ROCKVILLE, MARYLAND

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., Charles Brown, Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Chairman

RONALD G. BALLINGER, Member

DENNIS C. BLEY, Member

VESNA B. DIMITRIJEVIC, Member

JOSE MARCH-LEUBA, Member

JOY L. REMPE, Member

MATTHEW SUNSERI, Member

DESIGNATED FEDERAL OFFICIAL:

KATHY WEAVER

ALSO PRESENT:

HUDA AKHAVANNIK, NRR

ERIC BENNER, NRR

LUIS BETANCOURT, NRO

SUSHIL BIRLA, RES

HAROLD CHERNOFF, NRR

SAMIR DARBALI, NRR

BERNARD DITTMAN, RES

MATT GIBSON, EPRI

TEKIA GOVAN, NRR

MAURICIO GUTIERREZ, RES

JERUD HANSON, NEI

MYRON HECHT, The Aerospace Corporation*

DAN HUDSON, RES

RONALDO JENKINS, RES

DAVID RAHN, NRR

PAUL REBSTOCK, RES

SERITA SANDERS, NRR

RICHARD STATTEL, NRR

BRIAN THOMAS, RES

ANDREA D. VEIL, Executive Director, ACRS

DEANNA ZHANG, NRO

*Present via telephone

CONTENTS

P R O C E E D I N G S

8:33 a.m.

CHAIR BROWN: All right, I'm going to say this again. The meeting will now come to order, now that we've established some order amongst the members here. This is a meeting of -- you want me to start over again, Jose? This is a meeting of the Digital Instrumentation Control Subcommittee. I am Charles Brown, Chairman of the Subcommittee.

ACRS members in attendance are Ron Ballinger, Matt Sunseri, Dennis Bley, Jose March-Leuba, Joy Rempe, and Vesna with a long last name, Dimitrijevic. Did I get it close? I'm working on that one.

We will also be joined today, later, some presentations by NEI and EPRI, Mr. Jarud Hanson and Matt Gibson. I want to confirm that that's correct. Okay, thank you. Designated Federal Official for this meeting is Kathy Weaver.

The purpose of this meeting is for the staff to present and discuss the status of the Digital I&C Integrated Action Plan, revision 2, and current efforts to address common cause failure; 50.59 process for digital instrumentation control upgrades; commercial dedication; updated ISG-06 licensing

process, revision 2; strategic modernization efforts; and an overview of EPRI's digital engineering guide. Those are a lot of items on the plate for today.

So the ACRS was established by statute and is governed by the Federal Advisory Committee Act. That means that the Committee can only speak through its published letter reports. We hold meetings to gather information to support our deliberations. Interested parties who wish to provide comments can contact our offices requesting time after the meeting's Federal Register Notice is published.

That said, we also set aside 15 minutes for spur-of-the-moment comments from members of the public attending and/or listening to our meetings. Written comments are also welcome. The ACRS section of the US NRC public website provides our charter, bylaws, letter reports, and full transcripts of all full and Subcommittee meetings, including all slides presented at the meetings.

Today we will hear presentations from the NRC staff and representatives from NEI and EPRI. The Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions as appropriate for deliberation by the full committee. The rules for participation in today's

meeting have been announced as part of the notice of this meeting, previously published in the Federal Register.

And on to this particular last couple of sentences. All public folks that are in the audience as well as the staff should be aware that comments made by the Subcommittee members themselves individually are their opinions and their opinions only, not of the full Committee. If and when we ever publish a letter relative to these, they will, that issues the full Committee's actual opinions.

They are provided, our comments are provided for staff consideration and therefore their work. Currently, we have received no written comments or requests for time to make any oral comments from members of the public regarding today's meeting.

As always, we have one bridge line established for interested members of the public to listen in. Also, the bridge line will be opened at the end of the meeting to see if anyone listening would like to make any comments.

A transcript of the meeting is being kept and will be made available, as stated in the Federal Register notice. Therefore, we will request that participants in this meeting use the microphones

located throughout the meeting room when addressing the Subcommittee.

The participants should first identify themselves and speak with sufficient clarity and volume so that they may be readily heard. Also, please silence cell phones, pagers, iPhones, iPads, and any other types of new and embellished electronic equipment that you may have on your sole or possession.

We will now proceed with the meeting while I check my cell phone.

MEMBER REMPE: Charlie, I believe Myron's on the line. And Myron, you may not realize it but you're --

CHAIR BROWN: I'm sorry.

MEMBER REMPE: You need to be on mute, because we can hear you shuffling papers.

CHAIR BROWN: No, thank you very much. Myron?

DR. HECHT: Okay, I apologize.

CHAIR BROWN: You can hear me, and we can hear you.

DR. HECHT: Yes, I can.

CHAIR BROWN: Okay.

DR. HECHT: Thank you.

CHAIR BROWN: All right, you will be on mute, correct, unless you want to make a comment.

DR. HECHT: I will be on mute.

CHAIR BROWN: Okay, thank you.

DR. HECHT: Yes.

CHAIR BROWN: Thank you, Joy.

MEMBER BLEY: Can I slip something in, Charlie, before you start?

CHAIR BROWN: Of course.

MEMBER BLEY: I noticed some similarities in language and concepts among the integrated action plan for the modernization of NRC's digital I&C regulatory infrastructure; the advanced reactor vision and strategy document; the licensing modernization project, where we had a meeting on yesterday; and something we haven't formally seen yet, but the Transformation Team's achieving modern, risk-informed regulation.

Along the way, could you point out where you're trying to be tied to these other kinds of documents conceptually and any places where you're really taking a divergent approach from what you see elsewhere?

CHAIR BROWN: Okay, let me wrap this up and we'll get started. We will now proceed with the

meeting, and I call upon Eric Benner, Director, Division of Engineering, NRR, for any opening remarks.

MR. BENNER: Okay, thank you, Member Brown and members of the --

CHAIR BROWN: You got your --

MR. BENNER: I should be on. I have a light on, so.

CHAIR BROWN: Okay, you need to --

MR. BENNER: I just need to speak up, I guess.

CHAIR BROWN: Speak up, correct.

MR. BENNER: Member Bley, that's a great observation you made. As these other activities roll out, we have come to some of the same conclusions. In a number of cases we have not been plugged in, but you know, we have tried to start getting plugged in. Because as you point out, there are some common objectives to these things, so there is a need for greater integration.

So I'll just open by saying we need to do better in that regard. But I thank you for the observation. So I'm happy to be --

MEMBER BLEY: Does it fit with your, the schedule for this project for that to really happen?

MR. BENNER: Well, I think on one level it

does, because we have, you know, we do have some flexibility in different piece parts of this. For subcomponents of what we're doing, you know, we have been engaging.

For instance, ISG-06, we've been working with licensing folks. So while we haven't had an explicit tie to, you know, that activity, we have some common members on the groups who likely have been.

MEMBER BLEY: Fine, I hope that happens. Because it'd be a shame if we end up going in all different directions through these various processes.

MR. BENNER: So I thought you were going to start by saying you noticed some similarities between this presentation and our presentation on May 17. Because those similarities are there also, that, you know, we did a detailed discussion on some sub activities. This is a broader discussion of all the activities in the modernization plan.

So we're here to talk to you about the changes that have occurred in the plan itself over the last year. And we really appreciate, because we've had some scheduling challenges, we really appreciate your support in scheduling all these meetings to support our schedule. Next slide, please.

So here's a more detailed breakdown of

today's agenda. We'll briefly discuss the Commission direction that kicked off all of our activities, the overall IAP strategy, and discuss each of the IAP modernization plans. Additionally, we're going to use this as an opportunity to talk about how we addressed and are addressing some of the feedback we heard in the May 17 meeting. Next slide, please.

So we feel we're making good progress on the IAP activities. We're getting to a point where some products are getting out. We revised the IAP last January. We're in the process right now of revising it in anticipation of a Commission meeting in the October timeframe.

It's important to note that each of these versions of the IAP is a snapshot in time, right. So we, you know, we have the commitment that they are living documents, but we put these snapshots out so people can sort of see what progress we're making.

So, you know, some of this is duplicative of what I said last month, but you know, it goes without saying that our highest focus are on activities that support those near-term upgrades needed by industry. So CCF is the highest technical priority identified by industry and the staff, primarily for upgrades made under 10 CFR 50.59.

So we'll discuss the status of these activities, and just want to note that we did issue the RIS supplement last month, and I believe we provided a copy to the Committee, so.

CHAIR BROWN: Yes, we got a, that supplement one we got. I tried to find the original 2000, 2002-22.

MR. BENNER: We can --

CHAIR BROWN: Somewhere along the line, and every time I thought I had it, it turned out to be reading supplement 1.

MR. BENNER: Okay. I'll get you a copy.

CHAIR BROWN: It's not, I mean, just somewhere if you could just get it to Kathy and have it, and then she can send it to us.

MR. BENNER: Okay, thank you.

CHAIR BROWN: I did have a question relative to that, since you brought it up.

MR. BENNER: Okay.

CHAIR BROWN: Is it, the way I read the other pieces of paper to the supplement, you can't just throw away the original. They --

MR. BENNER: Yeah.

CHAIR BROWN: Somehow go together. So I really haven't had a chance to see how to integrate

those two together, or whether there's differences between the two.

MR. BENNER: Matt, the original pretty much provided a straight endorsement for the underlying NEI guidance document. So the RIS itself I wouldn't say adds much substance. But you know, clearly having the, you know, NEI-0101 as companion to the RIS is important for anyone attempting to use it.

CHAIR BROWN: Okay.

MEMBER BLEY: Is there a, can you briefly explain the logic for having both the RIS and its supplement and the ISG as separate documents?

MR. RAHN: Yes. You're talking about ISG-06?

MEMBER BLEY: Yeah.

MR. RAHN: Okay. This is David Rahn, I work for Eric in the Office of NRR, Division of Engineering. The ISG-06 document is intended to be used as a description of what should be included with a license amendment or license amendment request. The RIS and the RIS supplement is really geared towards performing upgrades under 50.59 processes.

MEMBER BLEY: Thank you. That's what the title says, but thank you.

MR. BENNER: So they've, I was just about

to do introductions, so that's a fine segue. So you know, this is a broad NRC effort. I'm the Chair of the Digital I&C Steering Committee, but I share Steering Committee privileges with Brian Thomas and Bob Caldwell, who is at the side table, and other division managers as we see fit to help on any particular issues.

Each of these modernization plans has an associated working group, and we have members from each of the working groups here today to present their work. Our speakers are Dave Rahn, and I'm sure many of you know Dave.

Dave is in a slightly different role today because we're, my current Deputy is supporting NRO with some management changes they've had. So Mike Waters, who many of you are familiar with, is my Acting Deputy. Dave Rahn, who is typically a member of the Technical staff, is Acting Branch Chief for all NRR digital I&C activities.

So Dave's been doing a great job as a staff member, and in the short time, he's been doing a great member as the Branch Chief, including getting pulled into a more substantive part of this presentation today.

MEMBER BLEY: And Eric, if I can, how do

you envision as you go forward with now four modernization plans, those will have some kind of standalone document on each one that's that modernization plan, and do they get rolled into other guidance eventually? What's the grand view of this thing?

MR. BENNER: Under the IAP, there are sections for each of the modernization plans dedicated. So that is the real documentation of the integrated action plan and the modernization plans. But as you point out, each of the modernization plans has underlying products that are the outcome of those modernization plans.

So yes, all the work, I mean, ultimately I would think the IAP and the modernization plans go away and we wrap that up, and it's the more typical NRC prop docs, whether they be generic communications, rulemaking, you know, those sorts of things that would have object permanence for the kind of changes we're looking to make.

MEMBER BLEY: Okay, toward the end of today, you'll get into schedule some?

MR. BENNER: Yes, I believe we cover.

MEMBER BLEY: Happy to wait for that.

MR. THOMAS: If I can add to that, Brian

Thomas. So we, sorry about that, Brian Thomas. As Eric, yeah, spoke to the individual modernization plans and their products associated with those individual modernization plans.

But essentially the view is that under modernization plan MP 4B, which looks, you know, which is really the examination of the overall regulatory infrastructure of the digital I&C, we will then consider whether or not those products, you know, whether we need to address those products in other venues, i.e., if an ISG for example, like ISG-06, should go into a more permanent or more durable guidance, you know, more durable guidance mechanism, rather than, you know, sit in isolation as an ISG. So that's --

MEMBER BLEY: Which some have sat for as guidance for very long periods of time.

MR. THOMAS: Yes, yeah. So that's the, that's what we envision, that under 4B, we would then do an overall examination of the regulatory infrastructure and decide how to either bring permanency to some of that, some of the guidance and some of the products. Or if they continue, you know, as an isolated document or isolated guidance.

MR. BENNER: Okay, thanks. So just

finishing up some introductions. Other presenters we have today are Mauricio Gutierrez, Tekia Govan, Dinesh Tanejo, Samir Darbali, Huda Akhavannik, Luis Cruz, Paul Rebstock, Rossnyev Alvarado, and Harold Chernoff. And I just dove through that list of names because to point that they represent the offices of NRR, NRO, and Research.

They bring a wide range of experiences to these activities. There are also a number member of the audience who are here to support any questions you may have, who contribute to all the digital I&C modernization activities. So as always, we continue to maintain communications with our stakeholders, including the Committee.

Again, I thank you for your willingness to schedule around our various activities. And we'll continue to communicate with you. And with that, I'm going to turn it over to Dave Rahn.

MR. RAHN: Okay, thank you, Eric. And yeah, let's start with the next slide. So a few years ago, the staff embarked upon proposed rulemaking to codify IEEE 603-2010. Okay, that's better.

In the process of doing that the Commission, oh, looked at our products and they made a determination that they thought that the process we

were under was headed into a conflicting set of requirements from one office desires versus another. So they asked us to reevaluate the program that we were functioning under.

And they issued in February of 2016 an SRM, which is 15-0106. And in that document, they've asked us to perform an overarching review of what we're trying to do with digital I&C and said that, you know what, this is big enough that we thought you ought to be doing this under some kind of an oversight of a steering committee.

And with that, we think you guys ought to really modernize our infrastructure to make it more usable and useful by our stakeholders as well as our staff.

So they directed us to engage in a series of interactions with our stakeholders and outline what are their common problems that we've identified and where, which items should we be focusing on and in what order. And they specifically gave us some overarching principles to follow.

One of those was that any new requirements that, meaning rules and things that are the got-to-haves, must be performance-based rather than prescriptive. And we should be focusing on approaches

that would ensure that licensees would understand what they need to do to comply with all the requirements.

The requirements themselves should be technology-neutral. And the guidance for any specific technology types could be tailored if necessary. So the focus that we're headed on right now is to come up with performance-based requirements, and any specific guidance to address certain types of technologies would be tailored toward those particular technologies.

The other goal they set out for us was to make sure that any requirements that we come up with should be the same for operating reactors versus new reactors. And they also, they told us that along the way, if we identify that there's any particular policy issues that require looking at by them, they want us to raise it early so that they have some time to look into it before we proceed with a proposed rulemaking of some kind.

So those are the overarching principles that we're following. Next slide please.

MEMBER MARCH-LEUBA: So I can focus on what you're saying, on performance-based.

MR. RAHN: Yes.

MEMBER MARCH-LEUBA: What does that mean?

For example, when you say thou shall consider common cause failures when you replace this relay.

MR. RAHN: Yes.

MEMBER MARCH-LEUBA: That's not a performance-based.

MR. RAHN: Well, it's performance in the sense that it requires an evaluation of a proposed design, such that you will have a process by which you can ensure a safety function will proceed to its conclusion in the event of some kind of a common failure. So it's performance in the sense that it requires you to do that evaluation.

CHAIR BROWN: But not do the, excuse me.

MR. RAHN: Yes.

CHAIR BROWN: The requirements already do that. I mean, if you look, my perception is the requirements already do that. If you look at the IEEE 603 and your actions are supposed to go to completion. That's a very performance-based, independence is a very performance-based.

MR. RAHN: Yes.

CHAIR BROWN: There's a whole slew of those in there. So I had the same question that Jose did in terms of what are we thinking about that's different than what they have. I've heard this, been

thrown around like candy at a child's party at a lot of these meetings. I'm not trying to be pejorative.

MR. RAHN: No, I understand. It's an overall performance requirement for designing power plants and nuclear power plants.

MR. THOMAS: Let me chime in.

MR. RAHN: I'm sorry, go ahead.

MR. THOMAS: So, great question. We ourselves are asking that question. We have recognized that we do have, for instance, IEEE 603 that has some performance-based requirements in it. Concurrent with that, I think the transition team and the staff have recognized that even IEEE 603 is very prescriptive.

So from a transformation perspective, there are some thoughts that, even though that may be performance-based, it might best not be incorporated by reference into --

CHAIR BROWN: Why do you think 603 is prescriptive? Independence is prescriptive?

MR. THOMAS: Well, I was --

CHAIR BROWN: If we're going to make it performance-based, we're going to say, Well, you don't have to be independent as long as you trip when you --

MR. THOMAS: And I was, yeah I was

reflecting the views of the Transformation Team. But the digital I&C Committee, what I was about to say is that's a good question. We're asking the same questions about which parts of the regulation are already performance-based but could use some enhancements, which parts of it are not.

And that's what we mean by when we look at the overall regulatory infrastructure, that's part of the evaluation we have to go through. So we're not there yet, it's a good question. I think when we think performance-based, we think an outcome, you know, you achieve a certain safety outcome. We've not yet really --

MEMBER MARCH-LEUBA: What you mean by performance based --

MR. THOMAS: Delved into the regulation.

MEMBER MARCH-LEUBA: Is that your change has to work? I mean, is that what you're saying?

MR. THOMAS: Well, I think when we think performance-based, we're really thinking of allowing licensees more flexibility in how they meet the regulatory requirements. So I said it's outcome-based, but we still have a lot of work to do to really examine.

CHAIR BROWN: Somehow I have difficulty.

In all of the new plants we've reviewed and talked about over the last ten years that I've been here, we've focused, the Committee has anyway, has very much focused in a manner to verify that we've got the fundamentals met, redundancy, independence, deterministic performance, diversity, defense in depth, and control of access fundamentally.

I have a hard time figuring out where and how, I worry about those being compromised. Do we no longer need redundancy? Do we, we only have to be partially independent? We can still have a serial data communication from bistable processor to bistable processor, from division to division?

Because we know, because we're so good at programming, that we know it's not going to cause a problem. Somewhere along the line, this thought process from those four, those five fundamentals, I worry about those getting compromised.

When you looked at, and I think I brought this up in the ISG-06 meeting, those fundamentals are stated very clearly in the first page or so of the paragraphs in the discussion, the description. But yet there's almost very little talked about in the entire rest of the ISG relative to those fundamentals.

So I worry very much about those being

compromised. If that's what we mean by flexibility, that does not seem to be a very good idea, based on the top-level fundamental principles. And that's, when I see these words, that's what I start thinking about, what do we mean and how do you actually execute those when you're talking about flexibility.

MR. BENNER: And we'll, I'll talk for a minute and then I'm going to turn it over to Rich Stattel, he wants to speak. But we're aligned with that concern. I think even the Transformation Team talks about, you know, better articulating at a higher level those fundamental principles, and then allowing different approaches to achieve those.

And I think everyone agrees that, you know, someone who picks up IEEE 603 and uses that as their method for meeting those principles is probably going to be in a good place. There has been a push by different stakeholders to say what about other sets of standards.

So we're going to have to do some homework to look at those other standards to say, you know, do they also adequately demonstrate, you know, meeting those fundamentals. So with that, I'll turn it over to Rich.

MR. STATTEL: Yeah, hello, I'm Rich

Stattel from the I&C Branch. I believe I can shed some light on the direction that we received from the Commission. So what we're talking about is what was in the SRM, direction from the Commission. The background behind that has to do with the rulemaking effort, so during the rulemaking effort.

Now, we agree that by and large, IEEE 603 and our fundamental design principles that we apply are performance-based. But during the rulemaking effort, there were several conditions that were being proposed to be added to regulation, and those were very prescriptive. So in a sense, the Commission was responding.

So in recent years, we've had different efforts, basically trends to prescribe specific designs. So what we mean by performance-based is essentially when we talk about single failure criteria, the criteria is not how to design a system, it's how the system needs to perform in the presence of certain types of failures.

So the direction we received from the Commission, they rejected the proposed conditions and they directed us essentially to stay on course and to keep our regulatory infrastructure as performance-based as it is today.

MEMBER MARCH-LEUBA: So adding a single failure criteria is not performance-based?

MR. STATTEL: It is performance-based.

MEMBER MARCH-LEUBA: It is prescriptive.

MR. STATTEL: But, think of it this way. If I write a regulation that says you must design a system, it must have four channel, four independent channels, it must have cross checking between --

MEMBER MARCH-LEUBA: That is --

MR. STATTEL: You're basically telling the applicant how to design the system in order to meet the single failure criteria. But the underlying criteria, the single failure criteria as it is currently articulated in IEEE 603, is, by and large, is performance-based. It does not prescribe any particular design.

We have licensees who use four-channel systems, we have licensees that use three-channel systems, we have licensees that use one out of two twice logic. So there are many ways to meet the performance requirements that are in IEEE 603.

Like I mentioned, there have been recent trends to try to make the regulation more prescriptive and dictate certain designs. And the Commission has basically directed us not to do that and to retain the

performance-based requirements that are in our current regulatory structure.

MEMBER MARCH-LEUBA: Yeah --

MR. STATTEL: So the change is basically preventing a shift toward prescriptive regulation.

MEMBER MARCH-LEUBA: I'm just concerned that it makes life for the licensees harder.

MR. STATTEL: Excuse me?

MEMBER MARCH-LEUBA: It makes the life for the licensees harder to go that way. But it's a logical position. Because right now we tell them, You're going to have a redundant and diverse system. And that's prescriptive. Now you're saying I'm require your single failure and no common cause failures, and you decide how to do it.

The easiest way to do it is to have redundant and diverse. Just satisfy those two criteria. Now you just let it open a little bit in the cloud.

MR. STATTEL: Well, understand we're really not talking about changes in policy, we're talking about retaining our performance-based regulation.

MEMBER MARCH-LEUBA: Okay.

MR. STATTEL: Okay.

MEMBER MARCH-LEUBA: The way you put it, I think it clarified much better what you meant. Thank you.

MR. STATTEL: Thank you.

MR. RAHN: The next slide, please. So the approach that we're taking to look at this overall architecture of requirements and guidance and standards, we're essentially looking at this from a top-down approach. It's kind of based on feedback that we'd received from our stakeholders as well.

And so what we've been told by our stakeholders is that we, our process would be better, it does accomplish the safety and security requirements that were, set out to achieved, but it would be better if it would enable them to do this in a more timely fashion and perhaps with a little more efficiency.

And that's in the sense of what needs to be provided for a staff evaluation, how timely can we perform a review of that. Is there any duplication of documentation that's needed to be provided? There's a lot of overlap on certain of the documents that we represent or what we considered acceptable practices.

So the overall objective is to take a look at this entire infrastructure, and we'll have a slide

later on this morning that goes into how we're going to do that. And see where we can tailor it, streamline it, make it more efficient and also more timely to do a performance evaluation, I mean a safety evaluation, for the people submitting license applications and amendments.

Yes, go ahead, Charles.

CHAIR BROWN: No, I want to let you finish. I thought, you took a deep breath and I.

MR. RAHN: Yes, so --

CHAIR BROWN: I'll let you finish before I chime in.

MR. RAHN: So we're approaching this from two different aspects. One is a short-term tactical approach. In that sense, we're looking at what could we do in a short-term basis to help kickstart this process, make things a little bit easier for licensees, hit all the highest priority items and create some interim products that they'd be able to start using.

And then we also have a strategic long-term look at this process to say what could we do to make an overarching efficiency improvement in the entire infrastructure.

CHAIR BROWN: I just want to step back for

a moment relative to both Jose's and my interchange with you. The performance-based versus prescriptive, I have, no, don't get me wrong, I have no problem with the performance-based aspect of the whole thing. It's also based on years and years and years of building stuff and delivering it to ships that are operating.

There is a balance between performance-based and prescriptive. There are some things that you would like to be prescriptive because number one, they simplify the regulator's understanding of what the licensee is doing. And it simplifies the licensee's need to do certain things. He doesn't have to evaluate the world's alternatives and justify what he's doing. You have to pick and choose those.

I would use one example that we've argued over incessantly for the last four years or five years, and that's the control of access in these plants relative to external communications, being hardware-based one way. That's very prescriptive.

However, how do you make that performance-based without introducing a significant amount of risk relative to the takeover of networks by hackers?

So there is a point at which the regulator, in my mind, okay, can be prescriptive to ensure a level of safety for the overall plant that is

really, has nothing to do with the basic plant operations. It's just trying to prevent people from getting in, based on the new technologies that we have.

So to me it's a balance. When people say we cannot do prescriptive, I just think you should not, that's like throwing the baby out with the bathwater. You should not do that. So I just wanted to make that.

The one other observation I would make is that IEEE 603 and other documents that we use are piece-part-type documents. They talk about this item and that item. 603 doesn't talk about architecture per se in the big picture. And in reality, the cleanest picture of the I&C world is you have a strong defensive architecture.

Forget what, how you, what the pieces are inside of it and everything else if you have a good defensive architecture. It is a major benefit relative to having to assess common cause failures.

So I just, those, I worry that those concepts and thought processes are getting lost in this drive to provide so much flexibility that there are effectively no real requirements that you can put your thumb on or say no to. So that's my speech.

MR. THOMAS: Thank you, Charlie, and if I may respond. We echo your concern. I want to underscore that there's work to be done on the part of the staff. And when we reflect on what's in the SRM, I interpret it to mean to the extent practicable. So yeah. Enhance the regulations, the regulatory infrastructure with the concept of it being performance-based to the extent practical.

And I agree with you, I mean, there are areas in which it's prescriptive and that's probably well suited. We still have to, as I said, this is work to be done. We still have to examine, you know, the pros and cons of what's in the regulatory infrastructure, what's in the regulations, as well as what's in our guidance.

And have to look at the, you know, the advantages and disadvantages of going in either direction, whether we go in a more prescriptive direction or we go in a more performance-based direction.

So there's still a fair amount of work. It's a very good comment, very good observation, but I do want to underscore that the staff has a lot of work to do under MP 4B. And we'll talk about that a little bit.

But so far, our focus has been on the, as Dave talked about, the tactical work, which is, you know, the narrow term activities that would yield implementable results for the industry. And so this longer term strategy is different criteria that's articulated in the SRM. We do have to examine exactly to what extent those can be achieved and is it worth it, in terms of.

CHAIR BROWN: Let me ask one other question just for an understanding part. ISG-06 license amendments, the RIS 2002-22 is 50.59 simplifying cert? My understanding, based on reading the documents is that the ISG-06 largely is used for wholesale replacements, modernization of reactor trip safeguard systems, etc. Those types of systems.

The RIS is aimed at non-safeguards and reactor trip systems. Now I thought there's a sentence in there, but it wasn't elaborated on. I think that, am I correct in my assumption?

MR. THOMAS: That's nearly true.

MR. BENNER: Yes.

CHAIR BROWN: Like chiller, reflect chiller, controller replacements and motor controls, etc., etc., and all the stuff that goes on. Okay, I just wanted to confirm that my understanding is

correct. Thank you.

MEMBER BLEY: I'm going to interrupt for just a minute. I may disagree with much of what was said, but I sure got the sense that you guys are pretty vague on what performance-based means. And you ought to think that through and get it spelled out pretty well, you know. The most simple definition I know is that you meet measurable or predictable performance requirements.

Now that might be a reliability requirement, it might be a particular accident that you can actually observe that happens. In a sense, though, it's a little like the argument between prevention and mitigation. And if you think about that one, that really depends where you are.

There aren't things are strictly prevention and things that are strictly mitigation. If you're starting at the beginning of before anything goes wrong, prevention is not having the initiating event, the thing that starts a bad scenario. And mitigation is anything that, once you have that prevented.

If you get further along when you're getting out, now with even your stuff's been getting reactor safety, you're out at point where you're about

to melt the core, prevention is trying to stop melting the core and mitigation is what -- if you've already melted the core, you can still prevent a release.

So I think it's the same thing with prescriptive and performance-based. Depending on where you're thinking, things can fall into different pieces. And I think you ought to think this one through.

Single failure criterion is really a way to meet a performance requirement of high reliability. I agree with Charlie, you don't throw out everything prescriptive. I think for me there's no other way to cut that. But maybe you can think of one.

But if our goal is high reliability, we could have a prescriptive requirement that you have single failure proof to make it more likely that you're going to be in that condition. And I think you can argue a good case there.

One that was brought up earlier, if you get down to redundant and you say, I want fourfold redundancy and two out of four logic, that's getting very prescriptive about how you meet these kind of criteria.

So I'd just like to see you get very clear on this, because I heard different things from

different people, and it sounds like a jumble of we're told to do it so we're going to go do it. But I don't know quite what it is.

CHAIR BROWN: I want to echo that, because I didn't mean to come across as four channels of something is necessary. All the plants operated, and I had one out of two, I had two out three, I had two out four. A whole variety in the plants that we dealt with, and they all were there, and you could justify why you did that, just based on various parameters and other operational scenarios.

So I wasn't dictating, I didn't mean to imply from that standpoint. The one other, and I hope you're going to cover this later, the common cause failure thing is just a thorn in the sides of everybody. And there seems to be, BTP 7-19 attempts with I guess a couple of ways to go at that, and you're going to talk about it next.

If one is the diversity, which is, looks like that's the major approach. Every plant we've looked at, it's fundamentally been diversity, not simplicity and the ability to test. Because the ability to do 100% testing is almost, it's not almost, it is impossible on the complex systems that we're using.

But you can, somehow I didn't see in any of the write-ups on CCF or anything else what other approach. There's almost the diversity, the 100% testing is really off the table, and the industry has said that numerous times. I understand their struggle with that bit, particularly with the non-safety systems, you know, chillers and TG voltage regulators, governors, etc., whatever controllers, what have you.

It seems to me somewhere you've got to try to figure out how you make it easier, more flexible for them to start upgrading systems. And use the fundamentals. One of the items you all used in your embedded device thing was the concern about embedded devices, and some of the controllers had come with new stuff. Which, and they're all over the place, they're ubiquitous now in the industry.

Will it flip this thing into the network? It's no longer independent. It's getting hammered by the network all the time. Well, that's, now how do you prevent that? Is that you have to be prescriptive to present that? Is it an architecture issue? The fundamentals that we talk about in terms of redundancy, independence, all that kind of stuff, well, independence was lost in this case.

I'm not saying you need two of them,

that's kind of crazy. You don't control a motor with two controllers. You've got to have, it just doesn't work. So you have to give up something somewhere. And it seems to me right now the regulations have made it very, very difficult for industry to go down this path.

And the embedded device thing can really be attack, or other issues, if you fall back on the principles, which are high level, in terms of, you know, the way they perform. You know, where do they get their data? How independent are they if they if they are influenced by other things? You really should be able to say no, we can't accept that approach.

But if you make them independent, have at it. We won't talk to you anymore. I'm not saying what to do. But it's just you've got to come across something. The CCF thing is eating us alive, and my personal opinion, I think it's being over-used to push back without providing the industry some flexibility. There will be errors, there will be mistakes.

But the bottom line is if the chiller controller doesn't work, you fix it. And you ought to be able to move on. And I don't see that flexibility being passed out to the industry, based on the

discussion we had in the paper given to us.

So that's my next speech.

MR. RAHN: Okay. At our last meeting, I think in May, we did cover a little bit of this when we talked about the RIS supplement. And the RIS supplement, in my mind, you know, for the first time enables more than just 100% testability and required internal diversity for those non-critical, non-RPS, non-SFAS type logic upgrades.

So I think we are reaching towards exploring the use of other types of design attributes. Now, granted we have an agreement on what those design attributes could be. But they're at least opening the door now in our regulatory products that enable licensees to have that flexibility that you're describing.

CHAIR BROWN: I brought it up because it's kind of a tactical issue at this point, as opposed to the bigger picture framework. I'm sorry, I left my microphone off.

MR. RAHN: Let me have a next slide, please.

MEMBER BLEY: That's, some of that discussion reminded me of yesterday when we went through the Licensee Modernization Project's

documents. They have a section on defense in depth in the back of what they're working on. It's the beginning of what might be a nice way to help you think about some of these things.

So I suggest you take a look at that. I don't feel it's really completely figured out yet, but I think it might give you some ways to take some of the things Charlie just said and actually formalize how you look about that and see how much defense we need on some of these particular issues.

MR. RAHN: Thanks, Dennis.

CHAIR BROWN: The other reason for bringing this stuff up, I mean the three others have mentioned a lot of things is to, really want you to understand that I would like to help get this process fixed. And I think Dennis would, and I'm sure Jose has the same feeling. We both have struggled with this stuff, or all three of us have.

And we really want to help with this. We don't want to be an impediment, and we're open to, the reason I threw all these items out on the table early was I wanted you to know at least somebody on the Committee. And I think they both echoed some agreement with it, to some extent, is that we're open to these opening things up so that there's more

flexibility.

But they've got to be the right things, and we don't like seeing things eliminated. No prescriptive, all this, and what does that mean. There needs to be a balance on how do get them there. Okay, that's, just, we're looking to help.

MR. RAHN: Thank you. The framework by which we're proceeding on this integrated action plan is to break this into component topics. And they're kind of organized in a way of which is the most needed, the highest priority, and then structured down to less, less priority. But we've broken it what we call into modernization plans.

Currently we have four major plans, some of which are subdivided into subparts. The first one is Modernization Plan #1, which is this topic of common cause failure that we've been discussing. And what are we doing to enable licensees to have a little clearer guidance on how to proceed to address the issue of a potential for common cause failure in any potential modernization that they do at their plants.

So the first product that we developed, which we covered a little bit in our last meeting, is this RIS Supplement 1, and that product enables licensees to have guidance as to how would they go

about addressing the 50.59 criteria when they embark upon the use of a new digital device where in the past it hadn't been a digital product.

And they've been, in the past, tripping on a couple of the criteria of 50.59. And so the RIS gives them a tool by which they could use what we call a qualitative assessment process that weighs the products of the design attributes that they've included in the design, along with the quality of the design processes that were used and putting the proposed design together. And any relevant operating history that they could rely on to say, hey, this particular component has a good history of being reliable.

So that's one tool, it makes it a little bit easier for them to implement digital under 50.59.

MEMBER MARCH-LEUBA: While we're talking about this, it's going to hurt me to say this in the record, but PRAs can be useful. Everybody around the table is laughing because I normally don't have much use for them. Have you guys considered, as part of this RIS 2002-22, a prescriptive requirement that when you change a relay that was analog and you put now a digital one, you also must include the component on your PRA model?

And evaluate the impact of it and say it has no impact, and therefore you can go ahead and do it. Or wait a moment, I now have a common cause failure because I just replaced 25 of those, and I'm cutting across all my four divisions, or something like that. This is a nice, structured way to do your 50.59.

And it would have to be prescriptive, it would have to be a requirement that if you change a component for someone that is much better but potentially dangerous, you should evaluate the consequences and put it in your in PRA model. And it might be a humongous model, but that would be a useful PRA.

MR. RAHN: Thank you.

MEMBER MARCH-LEUBA: And that's the way I would do it, simply, if I --

MR. RAHN: We haven't thrown it out completely. We have talked about it. A lot depends on the fidelity of the PRA model that exists, and a lot depends on the availability of useful reliability information and relevant reliability information.

MEMBER MARCH-LEUBA: I would put it with a high probability of failure. I would, going with my model, I assign an arbitrary high probability of

failure, an arbitrary common cause failure with components similar to it, and see what happens, and that gives you an idea.

Instead of just judging by looking at your system and hoping that the engineers have sufficient brain process to do the same thing, I'm just throwing it out. Myself not being a PRA guy and always complaining about it, I see a value for this.

MEMBER BALLINGER: Isn't this analogous to licensees using PRA to evaluate maintenance decisions? Same thing. I think they're already doing that.

MEMBER MARCH-LEUBA: What I'm saying is you just don't, not always notice all these secondary effects. I mean the consequences. I write software for a living on a different life.

And you always have this extra line of coding there that is beautiful because it does this new thing. And you don't see the consequences of that line of code. Whereas PRA allows you to look at it more structurally.

MEMBER BALLINGER: But again, my friend Dennis will tell me that different licensees have different qualities of PRA.

MEMBER BLEY: Yeah, but I think what Jose brings up, you know, it's hard to find another place

where you can track how these things interact throughout the plant.

Even if you don't have a good model and something conservative to see what happens, at least lets you know where you could be getting problems, if in fact there is a common cause failure problem or some other linkage among these things. So there aren't many other places where you get that integrated look at the plant.

MR. BENNER: And some of this is a segue, not to get ahead of ourselves. We do have, the Program Offices has been working with Research and outlining some research needs. And one of those research needs is looking at, you know, better use of PRA in this arena.

So I think there's different levels of sophistication. I think there's one level of sophistication that can be done now, like say where you can start just using, you know, a PRA model of, you know, just sufficient quality to say, hey, what are, you know, if I replace some of these components, and I have some failures that cross lines, what does that mean, to help assess the safety significance.

So I think some of that can be done now. There's been some dialog. While the RIS doesn't get

into really consequences, there has been some desire by some members of the industry to talk about, hey, you know the RIS is one step, but there would be a way to look at consequences as a different way to, you know, justify some of these mods.

But I think there is a challenge of these, you know, these models have obviously certain assumptions, they go to a certain level of detail. You know, when you start getting down to the component level and different failure mechanisms, many of those things are not modeled.

So that's why there is, like I said, some research work that we'll talk about a little later today to start probing more where we could make greater use of PRA to help solve some of these problems.

MEMBER MARCH-LEUBA: I'm thinking at our level, we can at least tell the industry that we would give them credit for something like this. By being silent, they're never going to do it because they know they're going to have to go up Mount Everest to get you to consider it. But if we think ahead while we're thinking about the high-level stuff, and hey, this will be useful.

We still don't know what level of detail

you would need, but we would be open to give you credit for it. That will go a long way.

CHAIR BROWN: No, I'm going to have to take charge of the meeting here. We're on slide 6, and the members have literally destroyed the entire timeline for getting through 51 slides by 11:45.

MEMBER BALLINGER: You happen to be one of the members, by the way.

CHAIR BROWN: No, I'm excluded from that because I'm the Chairman. So anyway, I think we've covered a lot of philosophical items which I think were really good to get out on the table early in this discussion. And then I'd like to encourage us, including myself, to try to allow you to at least finish a few slides here before we interrupt again, so.

MR. RAHN: Okay, thank you. So as I mentioned, the RIS supplement that we developed opens the door to the use of certain design attributes that could be used, other than 100% testability diversity. But we want to make sure that we agree on this package of what potential design attributes there are available that are effective.

And so this next MP 1B product that we call is a review of a product that's being developed

through NEI, NEI-1616, which was to have a framework for using design attributes that help address CCF issues. That product is currently on hold while EPRI is doing some reformatting of that document. We may hear a little bit about that later today. But --

CHAIR BROWN: Is EPRI doing that, or is NEI doing it?

MR. RAHN: Well, it's an NEI document, and it relies in part on a product that's partly, has been developed by EPRI.

CHAIR BROWN: Okay. That what they're going to talk about this afternoon?

MR. RAHN: Yes.

CHAIR BROWN: All right, thank you.

MEMBER BLEY: So what do you do if they don't get there?

MR. BENNER: So then we're giving them some time develop that. If it doesn't happen, we're going to have to look at a different approach to coming up with this document. Some kind of an agreement on what design attributes are considered appropriate for addressing CCF or minimizing consequences of risk and things like that.

But you're right, if they don't come up with it, we're at some risk in not having agreement on

that. I do want to say one thing, though, in defense of this. You know, for the past 21 years, they've been making changes to devices and control systems in the plants.

And there are a lot of common knowledge now, a knowledge base, on the part of designers and developers for doing this very thing. They're not all written down in one common document of some kind. But there are design practices that people have been using over the years to things like, you know, eliminate all single failure points, you know, where something can go wrong.

Put in median selects, you know, when you have two or three devices and one of them fails and you can't rely on it anymore. There's a lot of different techniques you can do to enhance the reliability of a system that's being developed. So those things are, they're sort of common knowledge, but they're not all packaged in one place.

MEMBER BLEY: That brings up a, remember when there was an AEOD?

MR. BENNER: Yes.

MEMBER BLEY: They sponsored some work at one of the labs gathering data on digital card failures and trying to define what the failure modes

were and cataloguing all of that. But they only did that for a few years. Is there anybody who's really tracking that now on a coordinated database that's giving you real solid information?

I know this committee had urged seven, eight years ago that it really be a consolidated effort to identify failure modes in the digital systems and especially the things that cross boundaries.

MR. BENNER: I still haven't seen anything convincing there.

MR. RAHN: From a nuclear regulatory, you know, regulatory basis, I'm not aware of anything currently happening. There are industry databases in other industries, but I'm not aware of anything that's being put together for the nuclear industry.

MEMBER BLEY: EPRI showed us something quite a few years ago, but it was a summary of what they knew at the time, and I don't know that that's really continued.

MR. THOMAS: Yeah, so it's part of some of the research -- sorry, like EDD, like CCF, you know. Potential for a non-safety to impact safety, etc., etc. Some of these specific research-focused efforts, which you'll hear about later on today may show

activity under those research --

MEMBER BLEY: I look forward to hearing about that, because we've now got enough of these systems of one kind or another out in the nuclear fleet, we ought to have a pretty extensive database of players.

MR. THOMAS: Different entities that have databases, and that's part of the effort to go back to those databases, INPO being one of them. I think INL also has an extensive database in terms of operating experience and, you know, likes to see --

MEMBER BLEY: They're the ones did that work for AEOD, but I don't know if that's still been going on or not.

MR. THOMAS: I think they still have a database. We need to, this is part of, you know, I keep telling about all this heavy lifting. We've got to do a lot of work that's left.

MEMBER BLEY: This is where we started seven or eight years ago saying, That would be the first thing we really get under control.

MR. THOMAS: That's really the first thing in this effort.

MEMBER BLEY: We look forward to hearing more today, then, so later.

MR. RAHN: And the third portion of this is what we're going to hear from, as soon as I finish speaking, Mauricio will talk to us about progress that we've been made on evaluating our current NRC policy on CCF and whether or not any changes need to be made there.

The next major portion of this is a product that we're working jointly with NEI on in evaluating whether or not there should be some kind of a digital-specific amendment or an appendix to NEI 9607, which is the process on how would one licensee go about determining whether a proposed modification needs prior review by the staff.

So it's all about the 50.59 process. So we anticipate that what, the door, the RIS opened the door to some information on how a licensee could proceed under 50.59. The MP2 process would provide a more detailed framework for how digital I&C modifications could be made under 50.59 in much more detail than the RIS did.

CHAIR BROWN: That would still only apply, that would still not apply to a reactor trip and safeguard systems. Is that --

MR. RAHN: Generally it's not applicable to those.

CHAIR BROWN: I didn't know, I just wanted to know where you were thinking about this MP2 going.

MR. RAHN: Yeah, so the thought process is those that are less safety-significant than things like RPS and SFAS.

MEMBER SUNSERI: So that's an area that I don't quite understand. I mean, 50.59 is, the scope of it is laid out, and we have many, many years of experience using it. How is digital different? Why is it different?

MR. RAHN: Yeah, so --

MEMBER SUNSERI: I mean it doesn't, you're not creating new accidents, doing things not described in the FSAR. How does this differ?

MR. RAHN: So what trips people up is, both on malfunctions and also even introducing new accidents. But malfunctions with different results is a problem, because typically you're going to install something that has, you know has an embedded software in it. The software you cannot guarantee is error-free.

And so you have to make a judgment as to is it reliable enough so that I don't create a new failure mode, and then potentially, you know, invalidate what the current safety analysis says on

how something is going to fail. So that's always been a problem for licensees on how to address basically criterion 6 of 50.59.

But in addition, the likelihood is another issue. In the past, safety evaluations were performed using what was known about analog equipment. Now you're introducing a piece of equipment that might have an embedded failure mode in it that you hadn't planned on.

So how do you go about estimating the hope for a reliability of that component? And it's a tricky way to have to answer those kinds of questions. So the guidance that was put out in this RIS, which will then get forwarded to the Appendix D of 9607, will enable licensees to have a tool that would enable them to answer those questions a little more precisely using a qualitative analysis.

MEMBER REMPE: So to explore what you've said a little more, yeah, okay, it would change the probability of failure, but could it also change the way you've analyzed the situation in a PRA? Because it's an unexpected mode that might not be considered in a PRA at this time. Is that a consideration, to kind of tie it back to what Jose said earlier?

MR. RAHN: You could probably perform some

kind of a qualitative evaluation to do that. To me, the benefit of, if you were going to have PRA as tool, the big benefit to me is identifying, you know, reliability information that shows that this component is highly reliable compared to what's been assumed in the PRA for success path through one of those safety trains.

So, you know, if you can show something is so much more reliable, you know, then potentially you could use the PRA information. But if you don't have confidence in that data, I don't know how you could use the PRA information.

MEMBER MARCH-LEUBA: My recommendation before, my suggestion was not to demonstrate that my new relay is so super reliable. It's that to demonstrate that failure of that relay doesn't cause any serious problem. So I lose the chiller, so what. So for now, I'll have to shut down the plant because I lost the chiller. So what?

MR. RAHN: Yeah, so it's good for informing, it's risk-informing.

MEMBER MARCH-LEUBA: Yeah.

MR. RAHN: But eventually you still have to make the change, and then you have to have a change process for that. The change process we have

available is 50.59. You still got to get through that hurdle.

MEMBER MARCH-LEUBA: Yeah, the beauty of this is that it makes you think that I already changed 25 relays and they're all the same manufacturers, same embedded software. What if all of them fail at once?

MR. RAHN: Yeah, so the RIS describes the fact that you need to understand what you've already changed in the plant, so that when you make a decision as to whether there's potential common cause failure, you have the background information.

MEMBER SUNSERI: So just to pull the string a little bit more on the 50.59 piece that I was bringing up. Essentially what you describe is a situation that I don't see much different than some of the equipment that is installed in the existing plants. So let me give an example.

Some of the reactor protection systems that I'm familiar with are, have cards, right. And these cards are chained together to create a certain logic for a trip function or actuation function. Now, the cards, the individual card may have more than one function in it, and they only use part of it for the particular logic that they want to achieve for this output, right.

So inherently, there could be an embedded function in that card that somebody would have to assess to decide whether or not the 50.59 evaluation was going to pass or need regulatory approval or not, right. So how is that different than software? I mean, so let me then propose it in a different way.

What I heard you saying then is because digital is so complex, people don't know when to say enough is enough on the review and when to stop, so it all goes to meeting regulatory review. Is that the problem?

MR. RAHN: Well, in the example you brought up, typically that particular, if you're going to make a wholesale change of cards of that type, that would probably become a license amendment request, just because of the complexity. So if you were to, you know, I lost the train of thought on the second part of your question.

MEMBER SUNSERI: So if you used the two kind of parallel examples, the one I described versus just a purely digital situation, the question I guess becomes is the digital just so complex that you can't decide when enough is enough analysis to say this thing would not need regulatory approval, or prior regulatory approval, so they just default go to

needing regulatory approval.

MR. RAHN: But the scenario you're proposing is a single card change-out, as opposed to a wholesale system change-out.

MEMBER SUNSERI: Well, and I'm just using it as an example. I mean, so I wasn't saying we're going to change out the whole reactor protection system. But the reactor protection system as a whole in the example I described has cards that have functions on cards that aren't used.

MR. RAHN: Yes.

MEMBER SUNSERI: And so therefore they represent potential embedded things. So if you're going to modify the card, put a jumper here, put change the timer, those would in my mind normally pass the 50.59 evaluation. A licensee could make those changes without NRC approval.

MR. BENNER: Yeah, I think that to try and interject, we on the staff believe there's enough flexibility under 50.59 to allow a range of mods. Industry wants, wanted, continues to want clarity on where that line is, partially because it is a licensee-controlled program subject to inspection.

We have hundreds of inspectors out there, they all have different experiences with 50.59. They

raise a lot of questions. Licensees generally, you know, want what I would call as some cover for what they've done to be able to demonstrate to individual inspectors, hey, I've done a good job in justifying this mod, that I can make this mod under 50.59.

So I think, I'm not going to say that the digital systems are so complex that everyone defaults to it needs a license amendment, but there's enough complexity in the potential failure mechanisms that it opens up a lot of questions when you have individual inspectors looking at it.

So in the time I've been with the program, the focus really has been on helping clarify, like you say, when is enough enough, and when can a licensee profess, you know, good confidence that they've done enough to justify that they don't trigger any of the questions under 50.59.

So I think the flexibility is there, I think this has been, and even the Appendix D, will continue to be a clarifying exercise to give everyone involved, the review staff, the licensee staff, inspection staff, you know, better clarity on when, where is that line of enough evaluation is enough.

MEMBER SUNSERI: Okay, I think that helps me a little bit, thanks a lot.

CHAIR BROWN: We've moved one slide in the last 15 minutes, so we're really getting back on track here.

MR. RAHN: And we stepped through the last two bullets here. The third part is a process by which we can potentially leverage some of the work that's being done in the commercial grade dedication processes to see whether or not a particular component is suitable for use in a safety application. That's our MP3. We call it acceptance of digital equipment.

And the last section is a bifurcated program by which we look at what's the quick short-term product that we can use to help clarify our requirements and guidance for performing license applications and amendments, and also what's the overall framework that we should be heading towards.

And we call that MP 4A and 4B. Later on, Luis Betancourt will talk to us about that. Next slide please.

So where we're at currently is at this SRM that outlines the reporting processes that we've promised to the Commission was issued in, back in October 2016. We are currently at revision 2 of this product. It was issued back in January. I believed we furnished the ACRS Committee a copy of that.

We're in the process of developing revision 3, which will update where we've gotten to so far. It'll also talk a little about a little bit more development we have in the broader framework, the MP 4B section. So we're proceeding along, and as we get a product available for people to share, we'll make that available. Next slide, please.

Yeah, so currently, as I mentioned, rev. 2 has made these particular changes to it that you see on this particular slide. And I won't go into the details on those. Next slide, please.

So what we're planning to do is basically summarize what we've already done so far on the RIS and Appendix D, talk a little bit about where we are, want to head with regard to this NEI-1616 document, which won't have progressed very far by the time we need to issue rev. 3.

CHAIR BROWN: Appendix D and RIS, they're part of NEI-1616?

MR. RAHN: Yeah, the RIS and Appendix D are more specific guidance on how one could tell you whether or not you need to have a prior review by the staff.

CHAIR BROWN: Appendix D, though, is in NEI?

MR. RAHN: Yes, it is.

CHAIR BROWN: Appendix D.

MR. RAHN: Yes.

CHAIR BROWN: The RIS is a separate document.

MR. RAHN: Exactly.

CHAIR BROWN: All right, you go ahead.

MR. RAHN: RIS is our document, basically. Appendix D will be something that we hope to endorse.

MR. BENNER: Likely if we get Appendix D to where it needs to be, the RIS would ideally go away.

CHAIR BROWN: All right.

MR. RAHN: So what I do want to point out on the bottom of this slide here, you know, we're looking at the fact that now there's a transformation paper out there. We've identified that there are some recommendations in the transformation paper that we should be considering as part of our overall long-term framework.

The other issue is that currently we've had some lessons learned from the review of new reactors, and there have been some streamlining in that process already. So we're going to see what lessons learned were performed there to see whether we

could roll those into our long-term plan. Yes.

CHAIR BROWN: Yeah, I just saw the transformation package that came out shortly, maybe a week ago or so, something like that. That's a higher level, all-encompassing?

MR. RAHN: Yes.

CHAIR BROWN: That's not, that's really not going to interfere. Maybe I said the wrong word. You're going to continue with this.

MR. RAHN: Yes.

CHAIR BROWN: And this, your work would end up becoming something underneath the transformation.

MR. RAHN: Yes, yes. We're going to see how we --

CHAIR BROWN: I was worried about two things going along, and now there's somebody else going to be doing the same thing you're doing if we leave the bubble.

MR. RAHN: Of course, there's no action that we can really take until the Commission says something about it.

CHAIR BROWN: That's fine. You've answered my question.

MR. RAHN: Yeah, but we're looking at it

just to, we know it's happening.

CHAIR BROWN: All right, thank you.

MR. BENNER: The digital I&C specific stuff, what we've professed is we will, you know, merge that into the IAP. So there's one thing happening in that arena.

CHAIR BROWN: Okay.

MR. RAHN: And the last item I wanted to mention is as we're proceeding along on this greater framework, we've identified that yes, there's going to be a need for some additional research to support this product. So we're getting revision 3, we hope to give you the first little synopsis of what we were thinking of doing in the research area.

CHAIR BROWN: Okay.

MR. RAHN: Next slide, please. So yeah, the schedule we're headed down is revision 3 is, we're shooting for September. We know we also have the annual reporting to the Commission on our progress on the IAP, which is scheduled for October, and also we're planning another digital I&C Commission meeting in October as well.

MEMBER BLEY: Is there a schedule that goes out beyond this?

MR. RAHN: Not yet.

MR. BENNER: Not for the IAP proper. You'll see we have for under individual activities we're going to discuss, they have their own schedules, which are incorporated.

MEMBER BLEY: That would be the four modernization plans? Okay.

MR. BENNER: Have their own, right. This is just the schedule of the overall IAP update.

MEMBER BLEY: This is just a minor thing I want to toss in since you're, I think you're near the end of this one. And I went back and looked again through the plan, and those words, performance-based, are like buzzwords. There are scattered, it's never defined, it's never clear. It's obvious somebody said, You got to be performance-based. Said, yes, yes, we're performance-based. That needs to be fixed up.

And there's another buzzword that you might not know as modified, technology-neutral in the area of regulation. They are now, they, NRO, in all their documents and in the stuff we've recently read is now using the phrase technology-inclusive. And you've got technology-neutral everywhere in the report, and you probably ought to get consistent with that. I can't tell you why that's better than what

was there before.

MR. RAHN: Thank you.

MEMBER BLEY: I like what was there before actually.

MR. BENNER: We'll pay attention to that.

MEMBER REMPE: David, even though you said wait till rev. 3, you're going to hear about the research, just, high level, what you thinking about? Getting data, or analysis, or what?

MR. RAHN: We're going to cover today, today we'll have some slides on that. We'll hear from Paul Rebstock later on at this morning, if we talk faster.

MEMBER REMPE: If you don't get interrupted.

MR. RAHN: That's right.

CHAIR BROWN: I would make one observation. We moved in the Naval Nuclear Program from magnetic amplifiers to transistors to integrated circuits, to microprocessors to, there was something else I was going to say and I forgot what it is.

(Simultaneous speaking.)

CHAIR BROWN: From 1965 through 1972, so over 18, no, 1978, when I took over the division. So in that 23-year period, we moved completely through

four different -- I take that back. I forgot vacuum tubes. In 1980, we still had vacuum tube source range instrumentation in some of the earlier S5W submarines.

So, and yet our specification stayed the same. So it's amazing, this talking about having technology-neutral or technology, what did you say, inclusive?

MEMBER BLEY: Inclusive.

CHAIR BROWN: Looking at the documents, whether it's IEEE 603, regardless of the year, 1991, 2008, 2018, roughly those documents are technology-neutral and inclusive. They don't tell you what to use, whether you use string or glue.

MEMBER BLEY: I might be a dinosaur, but I never saw a mag amp fail in my time.

CHAIR BROWN: Mag amps were extremely rugged and they worked beautifully. They had to be aligned more frequently than some other things, as wells as the vacuum tube.

My point being is don't get so wrapped up in those words that again you lose track of the endgame, that's all I'm saying.

MR. RAHN: Yeah, your system specifications were at the system level, not the hardware level.

CHAIR BROWN: Back then, we built the first microprocessor-based I&C equipment for the CVN 72 and CVN 73 using the analog combination transistorized integrated circuit reactor protection, the entire plant monitoring system specifications. And then we kind of adapted the outputs. So it's amazing what you can do with the existing stuff if you just go for it.

Anyway, that's, just be careful that's all.

MR. RAHN: Okay. Okay, at this point, yeah, so what I'd like to do, I'm going to change places with Mauricio so I could help him with his slides while we, he'll inform us on our progress on attacking the policy issues regarding CCO.

CHAIR BROWN: Okay, just -- we're due to take a break. We're on slide 11, okay. I want to go ahead and take a break so we don't run too far behind, but we've had a lot of -- I did a quick look through the slides.

We've had a lot of discussion on almost every one of these, and so we should take into account the interactions you've had, and I know you will do an outstanding job. So right now we will --

MR. RAHN: Mauricio and I just had that

same discussion.

CHAIR BROWN: Is that right?

MR. RAHN: So thank you.

CHAIR BROWN: We will recess for 15 minutes and then come back at 10:15.

(Whereupon, the above-entitled matter went off the record at 9:58 a.m. and resumed at 10:21 a.m.)

CHAIR BROWN: Okay, we will restart this whole evolution. We're back in -- you're good now? You're good, okay, back in session. Mauricio, it's all yours.

MR. GUTIERREZ: All right, thank you.

CHAIR BROWN: You're under a lot of pressure.

MR. GUTIERREZ: Thank you for your time today. As you said, my name is Mauricio Gutierrez, I'm the team for the MP 1b and MP 1c teams. The other members on this team are Dinesh Tanejo and Rossnyev Alvarado. What I'd like to do, if it's okay with you, is to skip the next couple of slides. I think we've already given you an overview of what's an MP 1 risk; go on to the next slide.

We've had some discussion on risk 2002-22, Supplement 1 this morning, and in the discussion, I think the information covered on this slide on NEI 16-

16 has already been discussed. Does anybody have any questions before I move on?

Okay, we'll proceed to the next slide, which begins the discussion on activity MP 1c, and this is on implementing the Commission's policy on CCF in digital I&C systems.

The policy on common cause failure is articulated in the SRM to SECY-93-087, and we continue to consistently apply it to address evolving digital I&C technologies. The staff took a look at the policy written in the SRM, and we also looked at our implementation of it. At this time we determined that it's not appropriate for us to propose or request a change to Commission policy. We believe that the policy that is in place provides us with the flexibility needed to implement our current initiatives in digital I&C.

We are currently developing a commission information SECY on future improvements to address CCF. On the next slide, please?

CHAIR BROWN: Your SECY for the update, do you have an idea for the time frame for that? I thought we were supposed to hear about that earlier, but then it got delayed. My mind is trying to backtrack to some earlier information on the upcoming

SECY. So do you have a time frame when you're all going to have that available?

MR. THOMAS: So I believe the planned completion for that SECY up to the Commission in August.

MEMBER BLEY: Brian, your mic.

MR. THOMAS: Yes. The plan schedule is to have that SECY issued to the Commission, I believe, in the mid-August time frame, so it's on a fast track. We have a draft now, which is going through -- we just had an alignment meeting with the EDO on it yesterday. It's just a draft that basically maps out a framework for, what is the message to the Commission?

CHAIR BROWN: Okay, thank you.

MR. GUTIERREZ: Okay, just a little context here. Due to the evolving nature of digital I&C technologies and their implementation in new and operating reactor safety systems, BTP 7-19, which is a part of the standard review plan, has been updated seven times to continue to address acceptable means for protection against potential digital I&C CCF concerns.

The last significant update captured the ISG on CCF that was developed during the 2006-2007 time frame, in coordination with NEI and other

stakeholders.

So the staff has been evaluating all the BTP 7-19 updates, and we've taken into account recent interactions with licensees, inspectors, technical reviewers, and other stakeholders in the implementation, and we're proposing these five points to update our guidance, which is primarily in BTP 7-19 for consistent application of a commission policy moving forward.

The first bullet states that licensees and applicant should continue to address CCF due to software. This is just a reiteration of our position that we think the commission policy on software CCF should continue to remain in place without modification.

CHAIR BROWN: Can I ask you a question on that one? I'm going to slow you down. I've been struggling for a long time with how in the world you address software CCF. It's largely a design issue, if anything, and if I was an applicant or anybody else, I'm not sure I could develop a methodology to evaluate or address software CCF-type issues.

I mean, for the trip systems and safeguards, multiple divisions and independence, fundamentally, is a basic protection. It doesn't mean

a design issue is not in there where you flagged the wrong thing, or you had the wrong subroutine pulled up or something like that. But that has nothing to do with -- it's not a software failure, per se. So what do you expect licensees to do, to do that?

MR. RAHN: I might be able to help with that. The way we address CCF has everything to do with how you evaluate the performance of a proposed digital system. So it's not only the architecture that you set out, like multiple channels, use of diverse devices, and things like that, but it's also evaluating what could be the potential consequences of a common cause failure. So it means bringing it down to the modes of failure that could happen, and then what would be the consequences of that new failure mode, and then what alternatives could there be to ensure that the safety function you're trying to achieve will still get accomplished?

In many cases, that might be relying on other high-quality systems that are in the plant, and/or if there's sufficient independent controls and instrumentation available to the operators, and the ability of the operator to perform any kind of manual action within a reasonable amount of time, given the limitations of what the safety analysis showed. You

would be able to perform some backup capability in the event that there was common cause failure.

CHAIR BROWN: Can I throw something out there?

MR. RAHN: Sure.

MR. GUTIERREZ: Yes, go ahead.

CHAIR BROWN: This was about 10 years ago; our former consultant to the subcommittee, Sergio Guarro, had built a model kind of based on an approach that's been used in human reliability that says, software failure doesn't quite make any sense. Software is software. But what might happen is, if the wrong confluence of conditions occurs, we execute parts of the software that we don't normally execute in ways they aren't normally executed, because you're outside of the range where we've tested, and that could lead to problems.

That was applied in the aerospace business with some modest success. There was a report back -- I think staff sponsored some of that work -- I know it's not been continued. I'm not sure if it ran into problems or what was seen on it, or if any of you remember that. But at least it's a model that, on the surface makes sense. How does it work? I can't tell you.

MR. RAHN: Yes, I agree with that. The principle, though, is that you don't necessarily know what will trigger the event, but presumably if you have multiple channels with the same inherent flaw in every channel, and you subject them to an event of some type that could raise this trigger to cause multiple channels to fail --

MEMBER BLEY: Exactly.

MR. RAHN: -- what you essentially need to do is identify if this event does occur, what alternatives might you have to be able to respond to that event in a way that at least takes credit -- you've pre-arranged this. This is something you'd have to be trained on.

But it would be a way of saying, I've got enough time to respond if I just go over and throw the switch for X, Y, Z system as a capable system-level backup. But all that really means is that, in advance of installing this thing, you need to perform an adequate defense-in-depth analysis and identify what diverse means, or what alternative means you might have available to accomplish the same functions. So it all requires lots of advance analysis and planning and thought to be put into it.

MEMBER BLEY: Well, and if you're not

going to find these things ahead of time, which is hard to do, having a plan is a way out. And the stuff they did with this model in the space industry, they went through extensive records of missions, and they actually found half a dozen cases where they could identify, this is exactly what happened and what led to the problem.

MR. RAHN: Interesting.

CHAIR BROWN: But you do have, if you look at all the stuff, at least over the last 10 years that we've looked at it, if you step back to the fundamentals, you look at each of those divisions, for instance, in trip or the safeguard systems, they are fed by independent sensors. They are not synchronized in any way, so they're processing on a different time scale. They don't communicate with each other, other than at the voting level, and you build in, already in each one of the plants we've looked at, a series of diverse trips with different equipment -- not microprocessors, but other diverse components -- which come under different things.

There's been an analysis that says, Hey, these are the things that operators can't respond to; therefore, we will build in diversity in these other events where we don't have time to do it.

So if those are the fundamental principles that you articulate within even the BTP, relative to your diversity in defense-in-depth, I was looking for what else do you do. Because if you start looking for software design issues, or do you process this routine at the same -- that's an almost impossible situation to calculate or evaluate. I'm just throwing that out from a thought-process standpoint.

MR. RAHN: No, we agree with that, and what you're describing is what we call addressing CCF.

CHAIR BROWN: And we're doing that. That's my version of continuing. I don't think that is onerous at all -- personal opinion -- and it certainly comes up with a pretty reliable system overall. So I just worry that we're going to get some other complex analysis or fancy FMEA, not that that's a bad word, relative to this. It doesn't work for this thing, or if somebody's saying, We're going to do a PRA on the software, I'd die.

MR. THOMAS: And I think that's a perfect segue for why we don't feel any change to the policy is necessary. I would say these guiding principles -- the first is the what, that we still need to address CCFs. The other four bullets are sort of the how, and the how doesn't really get into -- the things we're

looking at are alternatives. It's not going down the path of trying to further refine how we're going to evaluate software proper.

It's sort of a given that while we may be able to do something in that arena, we don't really think that's the fruitful area for proving safety. So we get into bullets, talking about alternatives means; it's really a given, the limitations on testability of software and digital systems. What are the other things you do to provide a demonstration of safety?

CHAIR BROWN: Just as a calibration point; in programs I ran when we were developing this stuff, we literally had a computer mocked-up with the entire plant model. We brought in the exact equipment that we were going to be delivering to the ship. We had the output of the giant computer; that data was converted into emulated sensor signals exactly as with the same components they would be seeing in the ship. Then we tested it for two years. We had the money to do it, but you have 130 guys under water, and it's pretty important to make sure they're safe.

So we tested it, and we still could not make sure that we found all the, what I call design-type errors. There were circumstances, configurations that we would find later and then fix those. But

those types of design errors, you can do it forever, and you just never find them all.

So to me, it's a very, very large experience lesson to be very wary of people promising to find all the problems. Anyway, I'll let you go on. We're now on slide 16.

MEMBER MARCH-LEUBA: I wanted to waste some time on a completely different topic; it's related to software. Everybody knows that whenever you use software systems, that you must have a watchdog. You would never accept the software system without a watchdog. However, the staff doesn't give them credit for it.

MR. THOMAS: Right.

MEMBER MARCH-LEUBA: In my experience, when software fails, it crashes, and the watchdog scrams, and therefore the software may be an economic problem, but from the point of view of safety, 90 percent of the time, the software did fail. You scrammed the system. So you have to think about how to give the licensees credit for the use of watchdogs.

CHAIR BROWN: I will echo Jose's -- if nobody has figured it out, that has been one of the primary focuses of all of the committees' efforts at reviewing all the new plant designs that we've dealt

with over the last 10 years.

In fact, that's where we have insisted on the prescriptive approach of having a hardware-based, independent-from-the-processor monitoring this. And that is not performance based, but is performance based, depending on how you want to look at it.

If somebody says, Oh, we've got a software-based watchdog timer just cranking around, it doesn't do you any good if the sucker crashes.

MEMBER MARCH-LEUBA: My claim is, of course we're required. I mean, whether it's performance-based or not, if you send one without a watchdog, we won't accept it. But we need to be given credit for it.

CHAIR BROWN: Exactly.

MR. THOMAS: So just from an industry perspective -- and I'm going to talk about it a little bit later, not in any great level of detail -- but that's one our considerations.

CHAIR BROWN: It's an architecture preventive --

MR. THOMAS: Right.

CHAIR BROWN: -- issue that you need to have in software systems.

MR. THOMAS: Right. And that's the thing.

We need a watchdog, you can be the watchdog of the watchdog --

CHAIR BROWN: And it's got to be independent of the software.

MEMBER MARCH-LEUBA: We just reviewed APR 1400, and we saw the watchdog. It's an RC-type watchdog. It's an R and C, and there's no way for them to fail, unless you put --

CHAIR BROWN: From a software standpoint, it's not going to fail. It has very simple parts, though.

MEMBER BLEY: It's not even software.

CHAIR BROWN: Right.

MEMBER MARCH-LEUBA: Are you commenting on the same issue?

MEMBER BLEY: No, I'm just going further. I agree absolutely with --

MEMBER MARCH-LEUBA: So I want to go further.

MEMBER BLEY: I think we need credit. On the other hand, if it's effective 90 percent of the time, or even 99 percent of the time from a risk point of view --

MEMBER MARCH-LEUBA: That's asking too much.

MEMBER BLEY: -- that small fraction where it might go the other way with the kind of things I brought up, we can't forget about.

MEMBER MARCH-LEUBA: What I wanted to put in the next thought in your mind; when we reviewed protection systems, we do something which is called analytic redundancy. You assume that the power is going to trip you, but if the power doesn't trip you, the pressure will. Maybe a combination of a watchdog and analytical redundancy may be sufficient. So we need to at least open the door for the licensees to make that argument.

My concern is that everybody is thinking about it, but nobody dares send it to NRC, because they know they're going to be subject to a 10-year review and $5 million. So if we can think of it on a high level and at least open the door. In my opinion, a conditional watchdog and analytical redundancy covers more than 90 percent of the cases.

We can continue with --

CHAIR BROWN: Okay. Move on, Mauricio.

DR. HECHT: This is Myron. Can I interject there?

CHAIR BROWN: Yes.

DR. HECHT: This is basically a discussion

on software failure. System failure, software problems in combination with Charlie's perspective that software doesn't fail. So crash is one of the failure modes; that's what you're dealing with in terms of a watchdog timer. But there are other failures.

MEMBER BLEY: Hey, Myron, can you use the phone instead of the speaker? It's really hard to hear you.

MEMBER BLEY: If you can't, go ahead.

DR. HECHT: Is this better? Okay. I just wanted to say that there are other software failure modes besides just crash, which could be detected by a timeout indication. There are incorrect responses which would be the classical case. Also, delayed responses. So a watchdog timer is one measure; whether it's 90 percent or 30 percent we don't know, because you have to have the empirical data to collect that. That was mentioned earlier, I think, by Dennis, about how we should be collecting information on that.

I also wanted to point out that the issue of system failures due to software is a little bit complex. For example, with respect to timeouts, this can often be caused by internal conditions, the operating system or the run time kernel might just get

itself hung up, and that is probably independent among the different processes, because they're all receiving outputs and inputs at a slightly different time and doing different things. They're not on a common time source.

So I just wanted to say that system failures due to software in general require an empirical basis, really, to start making assertions about reliability or how to give credit for that. It's more complicated than just saying that software always fails due to an algorithm issue or software always fails due to a crash failure mode.

CHAIR BROWN: I don't disagree with that, except, you have to do what you can do, and we ought to go on. Thank you, Myron.

MR. GUTIERREZ: Okay, so I think we covered the last slide pretty well there in stating that there isn't much change between the policy. The intent of that last slide was just to give you a little intermediate information on what will go into BTP 7-19.

And here on the next slide, some next steps are RIS 2002-22 supplement for 50.59 has been issued, and we're in the stages of planning for the BTP 7-19 update. We will review future industry

guidance in the NEI 16-16 when we are re-engaged by NEI. Our plan is to continue forward with the info SECY to the Commission, aiming to complete that in August of 2018.

CHAIR BROWN: You said you're going to update 7-19? Is that a big revision?

MR. GUTIERREZ: Yes.

CHAIR BROWN: It's the first I've heard about a big revision to it.

MEMBER BLEY: So we'll be seeing that at some point?

MR. RAHN: Yes. We haven't started that process yet, but we've recognized that there are aspects. The wording in BTP 7-19, that is kind of restrictive, and it doesn't really differentiate higher-tier safety significant systems from less safety significant systems. So we're thinking of potentially inserting guidance regarding maybe a graded approach.

MEMBER BLEY: That's part of this integrated action plan?

MR. RAHN: Yes, this will be one of the products that comes out of this.

CHAIR BROWN: Okay. I'd just like to put it on the record, we would -- Step 19 is a pretty

extensive, well-relied-upon document, and so we would like to interact with you all when you get to the point, and look to schedule a subcommittee meeting to go over that with --

MR. RAHN: Yes, we're just talking about it right now.

CHAIR BROWN: I got it. I'm glad you let us know. Okay? Thank you. Go on, Mauricio. Sorry for the disturbance there.

MR. GUTIERREZ: That's it for me, so --

CHAIR BROWN: Good.

MR. GUTIERREZ: I'll turn it over to Tekia.

MR. CHERNOFF: My name is Harold Chernoff, I'm the Chief of ROP Support and Generic Communications Branch. I also have a 50.59 program responsibility in my branch, and let me just quickly say I'm glad I'm not saying good afternoon, I'm still saying good morning.

We're not going to take a whole lot of time, but I just wanted to make -- I've been listening to this morning's conversation, and my colleague's valiant efforts to answer 50.59 questions --

CHAIR BROWN: Be careful with your papers, you're hitting the thing.

MR. CHERNOFF: Sorry -- my colleague's valiant efforts to answer some of the 50.59 questions, I want to just reflect on a couple of the comments you made generically. You guys asked the question, what's different about digital? Well, in the sense of 50.59, nothing. It's just another plant modification; you're applying the same criteria.

What's challenging is, it hasn't been done a huge amount under 50.59, and establishing the confidence that certain kinds of changes can be done under 50.59, they won't get wrapped up into after-the-fact enforcement concerns, and that both industry and the agency have a common understanding of where the margins are, where the sides of the road are.

The other thought I just wanted to get out there is the comments that were made about PRA with respect to 50.59. I think, looking around the room, a lot of people like myself have been involved for 30 or more years on this committee probably, and just reflect upon the fact that in the early '90s when people first started to try to apply PRA numerical outcomes to the use of 50.59, the criteria said, An increase in likelihood, an increase in frequency.

And this was a tremendous difficulty, because 10 times 10 times -12 is still an increase,

and that begat the rulemaking that came to fruition in '99 and 2000, where the language was changed and adopted, the language of minimal increase, and as ex-Chairman Reyes said, Well, I know minimal is more than zero and less than a lot.

So we find ourselves still dealing with a little bit of that, but there is specific guidance that already exists in 96-07 and thumb rules in there for using actual numerical PRA results. It can be done for digital; it's done for other things in 50.59 space, and what the RIS did was reinforce also something that was 96-07 already, which was, It's okay to make a qualitative assessment of likelihood and frequencies. It doesn't have to be numerical; it doesn't have to be sourced in a high-quality PRA answer. It can also be qualitative. And that's really the main focus of the RIS, is to give a process by which to make that qualitative assessment.

MEMBER BLEY: Before you leave that; Reg Guide 1.174 has been around for --

MR. CHERNOFF: Absolutely.

MEMBER BLEY: -- quite a while, and that gives you pretty good guidance in a lot of these areas, and it also tells you to use an integrated process that looks at all aspects, not just the

quantitative. I'm sure the committee members already know, but that standard is obviously for licensing changes. It's actually, for 50.59 purposes, you would not have to always necessarily meet those objectives in there. It could be something less than that, and the rules of thumb --

MR. CHERNOFF: But they give you a lot more room than the earlier criteria in --

MEMBER BLEY: But in 99-07 itself there's even more flexibility and rules of thumb about, Am I increasing likelihoods? There's actually some new multipliers that are in there as guidance. So it's even more flexible than 1.174.

With that, I'm going to let Tekia speak to where we are with the proposed Appendix D and where we're headed.

MS. GOVAN: Good morning, everyone. My name is Tekia Govan. I'm a project manager in the ROP and Generic Communications Branch. Our branch was recently assigned to work on Appendix D, so we're coming in with a fresh perspective in looking at Appendix D as we move forward.

The purpose of the proposed Appendix D to NEI 96-07 is intended to provide guidance for licensees to perform the 10 CFR 50.59 reviews of

activities involving digital I&C modifications. There was an agreement between NEI and NRC to hold Appendix D work until the RIS 2002-22 Supplement 1 was issued, and that was issued on May 31st, 2018.

So we're turning our attentions back to this appendix, and we're having a Category 2 public meeting with NEI to discuss any review topics and status on June 26, 2018. From that meeting, the staff will work with NEI to develop a review schedule for endorsement of Appendix D should NEI request such endorsement. The public meeting is the current status as well as the next step for the Appendix D activities.

So at this time I'll open it up for any additional questions related to the Appendix D effort.

CHAIR BROWN: I just had one question on that; we've got 2002-22, which is an NRC document, and we've got Appendix D. Now, is NEI -- are there differences? I hope there are no contradictions between the two. I presume that was the reason for the delay, so that they could make sure and craft Appendix D to not -- or maybe they're going to argue with you.

MR. CHERNOFF: Well, there's some layers here. One of the layers is just resources, both NRC

resources and RFC resources, there was a decision made that we have to finish this supplement, and we were not able, like the Ed Sullivan show, that we were not able to keep all the plates spinning all at the same time with the resources that were available.

CHAIR BROWN: Do you think somebody really remembers the Ed Sullivan show?

MR. CHERNOFF: Yes. So I think it was a reasonable decision to say, Okay, let's pause the work on Appendix D. Now, the second layer is -- and we're going to talk about this in the meeting -- we see an importance of consolidating 50.59 guidance.

I'm not going to get into the tech side of the equation, but we want the 50.59 guidance on everything to be homed in a very small set of documents, so people don't get confused down the road. When I get hit -- catch the beer truck and I'm not here, everybody will know where to go and where to find it.

So that means probably sunsetting things that are out there like the RIS that are out there and incorporating it into the base documents, which would be NEI 96-07, which we've endorsed with Reg Guide 1187. So some combination of the Reg Guide and the NEI document, whether it be Appendix D, which is what

is being talked about right now, but it could be a blend of things in 96-07 or Appendix D or the Reg Guide.

But we take the 50.59 stuff that's in the RIS, we take the 50.59 information that is embedded in NEI 01.01. There's a lot of other stuff in 01.01, but just the 50.59 part of that, and we home it into a consolidated long-term care facility which we think is for the digital subset of that.

CHAIR BROWN: But you're going to keep 50.59 generic, more top level, and just include what you want to do in these other documents, then?

MR. CHERNOFF: Correct. So some of the other things that we need to talk about are, there's some issues that were in the draft and have been in the draft that are trying to solve, in one or two cases, very limited cases, bigger issues, things that have come up beyond just digital -- that's something we need to talk about. Can it be tackled there, or is it better tackled in another forum?

So another bite, another step in progress, is Appendix D. But it doesn't, obviously -- it's only dealing with 50.59, not some of the other technical issues and challenges associated with --

CHAIR BROWN: Okay. Are you finished with

that one?

MS. GOVAN: That is it.

CHAIR BROWN: Can we move on then? Thank you very much.

MR. CHERNOFF: Thank you.

MR. RAHN: So our next presentation is on our modernization project No. 3. Dinesh Tinejo is the lead for this particular group. Unfortunately he's at the IAEA this week working on a new safety standard, so I will pinch hit for Dinesh while he's gone.

What this is all about is, before we embarked on this whole process of upgrading or modernizing the regulatory infrastructure, we did some evaluations of some of our field processes that we've had, resulting from inspections of modernizations that were made by licensees in the field regarding some of the less safety-significant, non-RPS effectuation type upgrades of local safety systems, local control systems.

We had very good guidance on how to use commercial-grade equipment in those applications; however, what we've noticed is that there have been inconsistencies in how a vendor who provides that equipment that the licensee then uses to dedicate for

a safety function -- how he goes about applying the criteria that we have.

We have EPRI NP 5652; we have another document which we follow which is TR 106439. Those documents talk about how you go about dedicating for safety purposes a commercial-grade item.

So some of the feedback we've gotten from inspecting equipment that's been out there and dedicated for service in a safety application has had -- well, let's put it this way: There's a wide variation in the level of quality of those documents defining whether that particular piece of equipment is dependable enough for that service.

So what we'd like to do is potentially leverage what other industries might have been doing in that regard. For example, the oil and gas industries have several applications where there are safety hazards in the plant. They dedicate a particular piece of equipment to perform a risk reduction associated with that safety hazard. Then they have a process by which they evaluate that piece of equipment they're proposing for some dependability criteria. That's a process that has been ongoing now for a good dozen years or so.

There are standards out there that define

the processes. Right now ISA 84 is one of those standards, and it also now has a sister set of documents in IEC space, which is IEC 61508 and 61511. All of these things define how one might go about assigning what we call a safety integrity level associated with the quality and dependability of the piece of equipment they're going to dedicate for that purpose.

So that's happened outside the nuclear field. So one aspect we've seen is, is there some way we can leverage some of that work that's been done of evaluating commercial-grade equipment that's already out there and has already been evaluated for safety purposes and use that as partial satisfaction of some of the critical characteristics that we use in establishing our commercial-grade dedication process?

So we call that acceptance of digital equipment, and that would allow licensees to maybe go to a vendor who is already purposing programmable logic controllers or even smaller components with embedded devices in them, and then allow us to say, Yes, that is of sufficient quality and dependability, and they have testing. There's test reports associated with them. They call them certification reports that refer to these types of reports.

So this is a certification process, so we are embarking on working with NEI, and NEI is working through EPRI. We'll probably hear later on this afternoon from EPRI on some of that process. Matt Gibson is here from EPRI to help describe some of that.

So the thought process is, if we determine that that process is good enough for our use, we would like to pursue that as one means of satisfying some of our commercial-grade dedication requirements. So the process that we're thinking about is, first, we're having EPRI do some evaluations of the certification process itself, and then inspecting certifiers -- these are already-established certifiers -- and looking to see what the potential value added that we could take credit for.

Then we would develop some kind of an NEI document that would describe how to go about using that towards crediting commercial-grade dedication, and then we would endorse that product. So that's the approach that we're thinking about.

So at this point, NEI has already contracted with EPRI, and they're doing research on this right now. They were planning on developing a document which is temporarily referred to as 17-06.

I don't know how far along that's progressed yet, but that would be this guidance document that I'm referring to.

So we are meeting with them on typically a bi-monthly basis until their research is complete, and at that time we will start working on a more formalized version of this NEI 17-06 document.

MEMBER BLEY: Commercial grade dedication makes sense to me. I ran into a problem in the railroad industry 10 or 15 years ago with counterfeit parts, and I've been told that it didn't apply too much to nuclear because of the way we get into manufacturers and everything else, although I've talked to some inspectors recently who have said, It's not true. We're running into trouble even on safety grade.

Will this approach include some kind of way to trying to spot -- because you can't do it visually -- spot counterfeit stuff coming in to the commercial grade products?

MR. RAHN: That piece of commercial-grade dedication is still -- we have a process now that covers this receiving inspection, process, and ways of determining whether there's a counterfeit or fraudulent component.

This effort on MP 3 is more towards, how can we leverage evaluations that have been done by qualified, third-party certifiers to say that a particular PLC or other component has a certain probability of failure on demand, for example.

MEMBER BLEY: But the existing process will cover commercial grade --

MR. RAHN: Yes. We are continuing the existing process for that. This is only a dependability aspect of it.

MEMBER MARCH-LEUBA: On a related question, how is the Appendix B quality control enforced? If I'm a licensee, and I commission a vendor to supply me something, then that vendor becomes an Appendix B vendor.

MR. RAHN: Yes.

MEMBER MARCH-LEUBA: When I buy it off the shelf, there is no such thing.

MR. RAHN: Yes. So what we do is, we have a process that's outlined in a report that we reference in our documents, 106439. In that document, it outlines a process by which you evaluate the quality of the product as it's being developed, and you perform an equivalency of what is the equivalent level of quality that's being performed by the vendor

that matches the quality steps that we have in our program.

Many times it falls short; it doesn't meet every item in our nuclear quality program. But there are additional steps that a supplier could take to say, Over and above what I bought it for, I'm going to perform these additional steps to try to raise it to the equivalent level of quality.

MEMBER MARCH-LEUBA: Yes, but I see Appendix B as being contagious.

MR. RAHN: Yes.

MEMBER MARCH-LEUBA: But there's a procedure to catch the contagion. I can stop it here; I don't need to go beyond.

MR. RAHN: Yes. This is a process we already have. That process is already in existence.

MEMBER BALLINGER: That 106439, could I go look that up?

MR. RAHN: Yes. I believe little a free one.

MEMBER BALLINGER: I just can't type in 106439 --

MR. RAHN: it's free. Okay. So you can go to the EPRI website --

MEMBER BALLINGER: Oh, that's a report

number?

MR. RAHN: Yes, an EPRI report number.

MEMBER BALLINGER: That makes sense, because I've been involved in cases where -- materials-related stuff -- where somebody buys it to a specification, and it's not. And the only way to find out is to actually test it.

MR. RAHN: Yes. So this particular one is more aligned with digital components. It's not all-encompassing; it's kind of geared towards I&C equipment and digital components.

But the goal of this project is to develop an NEI document that describes how one might go about applying this equipment, and then the staff would evaluate that report and then perform some kind of an endorsement.

CHAIR BROWN: Does that certification -- when you do a piece of commercial equipment, and you certify it; you go through that drill, whatever it is -- vendors have a habit of continually upgrading their little packages that they want to sell to us.

MR. RAHN: Yes.

CHAIR BROWN: So that the stuff inside of it, now that you've certified it, does that mean that he has to build it exactly that way whenever you order

it?

MR. RAHN: The certification process -- and maybe Matt can help us with this -- but the certification process includes identifying versions of the components, so there are software versions as well as hardware versions.

CHAIR BROWN: Oh, hardware versions.

MR. RAHN: Right. So you get a certification report from the certifier, and it describes the conditions under which they said, It is meeting the safety integrity level requirements. Among those conditions are, I'm using this version of this, this version of that.

Now, it behooves the user of this component, if he wants to put one of these into service, he's got to verify that the particular certification report matches the component that he's purchasing. Did you have something to add to that, Matt?

MR. GIBSON: I did. I'm Matt Gibson with EPRI. David, you've referenced me a few times in getting me to do this this afternoon, and I just want to make everybody aware that I have planned on talking about this, to have a full discussion on the digital engineering guide, so if anybody has questions we can

figure out how to work that in.

CHAIR BROWN: Okay. I lost the bubble on something; I just asked you a question, and now I'm --

MR. RAHN: Well, you were asking about verification of versions.

CHAIR BROWN: Yes. We had a terrible experience; we tried using laptops to come in and download and upgrade software packages. We decided not to do that when we found that the same version of various stuff in a different manufacturer's laptop, you couldn't do it. It didn't work, so you had to buy the same thing. It had to be exactly what it was before the versions of everything inside of every software, every routine had to be the same. That's a more complicated issue than this.

MR. RAHN: It is.

CHAIR BROWN: But piece parts can be very compromising on this. I understand the version part; you've just got to work on it. Thank you.

MR. RAHN: So this is our progress that we're making, so yes, we've embarked on this. Right now, most of the work is being done by EPRI, and so our plan is, they're going to share some partial results with us as to what they've learned the value added of the certification process. So that's next

month when we're going to meet with them.

We're planning on having some version of this NEI 17-06 document by late this year, early next year -- I'm sorry, early next year. We will then work with them to bring that document to full usability, and then we'll figure out which vehicle we want to use to endorse it with. And that's it.

MEMBER BLEY: Before you quit, since we just had Matt come to the microphone, this EPRI digital engineering guide; have you guys reviewed that? How does that fit into the process? Apparently, we haven't had the chance to look at that.

MR. RAHN: Yes.

CHAIR BROWN: I asked for it, and we were rejected.

MR. RAHN: Yes. There's been some issues regarding what's sharable, and Matt will get into that this afternoon. This is a very big document; it's very broad and kind of all-encompassing about --

MEMBER BLEY: But staff has seen it?

MR. RAHN: No. Well --

MEMBER BLEY: Okay. Staff hasn't seen it yet?

MR. RAHN: The staff has seen a version through our MOU process --

MEMBER BLEY: Okay.

MR. RAHN: -- with EPRI. The technical review staff has not reviewed it. We know that it's existing, through our office of research. We're continuing dialogue with the development of that document; however, we are aware that a portion of some of this product is going to be able to be referenceable in one of the NEI 16-16 versions. So at least a piece of this document, we might be able to credit design attributes.

MEMBER BLEY: If it's out there as guidance for the licensees -- well, I guess you would need to see the product of it. Maybe you don't need to see it all, because it's --

MR. THOMAS: Yes.

MEMBER BLEY: I'm a little concerned about that.

MR. THOMAS: Right. Under the MOU with research, we do get exposed at a working level with what --

MEMBER BLEY: I don't know what exposed means.

MR. THOMAS: We interact with EPRI on what they're doing. We have been -- you'll see this afternoon from the EPRI staff. The research staff has

seen that under the MOU. We have regular meetings with them.

MEMBER BLEY: But it's not something you'll be endorsing?

MR. THOMAS: We are not endorsing it under the MOU; we do review and comment on it, provide comments back to them. But it's not from a standpoint of endorsing it.

MEMBER BLEY: And your program will not rely on it?

MR. THOMAS: Correct, yes.

MR. CHERNOFF: I think that's the key, that --

MEMBER BLEY: That's a funny mic; you have to get real close to it.

MR. CHERNOFF: Okay. Any organization can develop guidance, and the question is, what reliance are they looking for from the regulators? So I think what we have laid out here is, EPRI is going to have one level of guidance; NEI intends to extract elements of that guidance that they would like NRC to rely on and endorse. We'll look at that, and when we get that, we'll render our judgments as to whether that's adequate.

CHAIR BROWN: Okay. At this point, I'd

like to turn this discussion over to Samir Darbali. Rich Stattel, you might want to sit at one of these tables with a microphone, in case he needs any help. You may be able to chime in on something.

MR. DARBALI: Thank you, Dave. Good morning, like Dave said, my name is Samir Darbali. I'm a technical reviewer in instrumentation controls branch in NRR. I'm going to be talking about ISG-06 Revision 2, Licensing Process. I think this is a presentation where we can make up some time, because I'll be brief.

The subcommittee met back on May 17th. The topics we covered were purpose, scope, lessons learned, the review processes in Revision 2, and how the new alternate review process compares to the tiered process.

Next steps: The key portion of this presentation, we want to provide some update to the subcommittee on how we are addressing some of the verbal recommendations from the May 17th meeting.

MEMBER BLEY: Oh, I have to interrupt. The ACRS only makes recommendations in our formal letters; anything you hear at a subcommittee meeting are comments from the individual members.

MR. DARBALI: Okay. That's why I said

verbal --

MEMBER BLEY: They make no recommendations --

MR. DARBALI: So it's a verbal comment; thank you for that. So to save up some time, I'd like to just skip over the next slides. Purpose and scope, we already covered that. Lessons learned, how we've used this, how we've used the piece to improve on the new process. We got some feedback from industry that we're also using to improve Revision 2.

So Revision 1 and Revision 2 both include the tier process. We've made some improvements on that, and we've made some reorganizations to the ISG. But we've mainly kept that tier-review process. Also in Revision 2 we're introducing a new alternate review process for --

CHAIR BROWN: Back up a slide. I appreciate you slipping through this. This is totally appropriate; I'm not disagreeing. But the Tier 1, Tier 2, Tier 3 review process says it focuses on system description and system architecture.

MR. DARBALI: Yes.

CHAIR BROWN: Yet system architecture was absent from Enclosure 2.

MR. DARBALI: Correct.

CHAIR BROWN: And we made that observation, not a recommendation --

MR. DARBALI: Yes.

CHAIR BROWN: -- during the meeting, and you all said you all would address it somehow. So that's what you're going to do.

MR. DARBALI: Yes, I will get back to that.

CHAIR BROWN: One way or the other.

MR. DARBALI: Yes, and the point of putting that bullet together was to clear up any --

CHAIR BROWN: Okay.

MR. DARBALI: -- miscommunication.

CHAIR BROWN: All right, thank you.

MR. DARBALI: So Revision 2 includes a new alternate review process where we provide a safety evaluation earlier.

CHAIR BROWN: Back up a second. Some of the folks were not here for the May 17th meeting, and I'm trying to look for a top-level, quick summary. Tier 1, 2, and 3 were largely -- and correct me if I'm wrong -- were largely platform-oriented, largely. But if you read the ISG, the Tier 1, Tier 2, Tier 3, Tier 1 was if you use an existing approved platform; Tier 2 was if the platform had some deviations that you

were going to use, you had to identify those and fix them; Tier 3 was, Oh, gee, it's a new platform, and you have to expose all your entrails and explain why this one is okay, similar to what you would do with a platform review or approved topical report.

MR. DARBALI: Correct.

CHAIR BROWN: It effectively didn't have an approved topical report. The alternate review process was, you still had a topical report, but -- and now I've forgotten the but.

MR. DARBALI: So it's essentially a Tier 1 review; it could also apply to a Tier 2 review, but essentially a review where you already have a pre-approved topical report platform. The only difference is, you're issuing that safety evaluation during the implementation phase.

CHAIR BROWN: It's before testing?

MR. DARBALI: Correct, that's the key difference.

CHAIR BROWN: Okay, now I'm recalling. Thank you for finding my locator.

MR. DARBALI: Sure. So we can spend a little bit of time on this slide, which basically discusses the key characteristics of a license amendment request using the alternate review process.

Basically, all the necessary and sufficient assigned information is provided in the LAR.

The licensee will describe the vendor oversight plan and appropriate commitments to complete topical report plan-specific actions, as well as commitments to complete life-cycle activities under the licensee's QA programs; they will also be a part of the amendment request.

On the next slide, the alternate review process will rely on license amendment requests containing licensing information and additional regulatory commitments to implement remaining development life-cycle phases by the licensee's QA program after the license amendment has been issued, and the NRC staff may translate some of those commitments into a license condition.

CHAIR BROWN: Yet you issue the license before they have completed factory-acceptance testing, etc.?

MR. DARBALI: Yes.

CHAIR BROWN: So then it's largely reviewed at the end. I guess it gets delivered, but then there's some review that they actually pass the factory acceptance test.

MR. DARBALI: Yes.

MR. RAHN: So who does that? That's not you all. Isn't that the site?

MR. DARBALI: That would be -- factory acceptance tests may be done by a confirmatory vendor inspection, so we'd be working with the vendor inspection folks to make sure that they have --

CHAIR BROWN: You said vendor inspection. You mean --

MR. DARBALI: Our vendor inspection --

CHAIR BROWN: Your NRC -- okay. Your NRC -- NRC's inspection people, okay.

MR. DARBALI: The next slide will provide the differences. So the top portion is the Tier 1, 2, and 3 review. This is common to Revision 1 and Revision 2. You can see where the license amendment request is submitted, and it's done right when a high-level system design is completed by the licensee.

Then we would get that license amendment request. We would then get what we call a Phase 2 submittal, which is more supplemental, detailed implementation information, and we would issue a license amendment after factory acceptance testing. That would then lead to that yellow box, which is optional regional inspections performed at the site.

At the bottom you see the alternate review

process, where the LAR is submitted, and it contains that system architecture description that meets regulatory requirements. The staff would perform their review and any necessary audits. Then you see when the license amendment is issued, which is before implementation testing. Then we have that new orange box which addresses those optional vendor inspections for implementation and testing activities. Those would be confirmatory and based on the license amendment.

MEMBER BLEY: I look at this thing, and I look at the two flow charts in the ISG, and I don't smell a lot of difference. Can you quickly say what's the main reason you do one of these instead of the other, because they look like they're doing the same thing, except maybe the RAIs come in sequential form in the 1, 2, and 3 phase.

MR. DARBALI: The whole concept of the alternative review process came with working with industry. Industry described a concern they have that -- you can see in the middle, all of the life-cycle activities the licensee has to perform before, during, and after the review.

One of the industry's concerns is that they have to spend a lot of resources before they get

that license amendment, and that kind of steers away management from committing money to digital upgrades.

MEMBER BLEY: So they end up doing essentially the same thing; the order is a little bit different.

MR. DARBALI: Right.

MEMBER BLEY: Okay. That kind of fits with what I saw in the flow charts. I wasn't at that earlier meeting, so --

MR. DARBALI: I mean, the licensee would be getting that license amendment earlier. The staff would be making their safety determination with reasonable assurance. Some of those activities that we would be performing during our review would then just move to confirmatory inspections, and we would have license conditions to make sure the licensee performs those activities.

MR. STATTEL: This is Rich Stattel. Just a little additional clarification: The processes are similar, and as you pointed out, the flow charts look very similar, and that's intentional. What we're trying to do is, we're trying to accommodate the licensee's need to have this early license amendment issue. But in a sense, we want to accomplish the same thing.

Another thing I'd like to point out on this particular chart is, it looks like we're doing a lot less activity if you look at the time line, but in actuality, we expect the actual level of effort, the resources required to complete the evaluation, to be very similar, whether it's the top process, the traditional review method, or the alternate review process.

MEMBER BLEY: That's the sense I got from the ISG.

MR. STATTEL: Exactly.

MEMBER BLEY: I'm glad to hear that. This chart is not in there.

MR. STATTEL: Right, and we've been using the Tier 1, 2, 3 processes for a number of years now. That was introduced with the first version of this ISG, and the main advantage of that -- and we've received a lot of positive feedback from the industry -- is that it allows us to perform our evaluation in parallel with the actual development processes --

MEMBER BLEY: And ensure they do the things that you expect them to do, and you would have seen in the Tier 1, 2, and 3 process, through conditions on the license, essentially?

MR. STATTEL: Exactly, and so the

transferal is not just to the inspectors; we're also putting an additional burden on the licensees themselves. So the activities that are performed in the window between completion of design and factory test -- now, this can be a year or two-year window that we're talking about, because design has to be implemented, hardware has to be built, software loaded onto hardware, integration performed, before you get to the point of completing a factory test -- so those activities, the licensee takes on the responsibility of completing those activities and doing them correctly. So our expectation is that we would end up with a similar level of reasonable assurance of correctness of the final product.

MEMBER BLEY: Thanks, and thanks to all of you. That helps.

MR. DARBALI: So back to the comments we got from the subcommittee: The main comment we received was that system architecture doesn't appear to be covered or reviewed under the Tier 1, 2, and 3 review process. During the meeting we explained that we always look at system architecture. So we went back, and we've made the decision that Section D-2, which is only applicable to the alternate review process -- system architecture -- will now be

applicable to both processes --

MEMBER BLEY: Tier 1, Tier 2, and Tier 3?

MS. GOVAN: Correct. So we'll update Enclosure B to show that as well.

MEMBER BLEY: That little X that goes across the enclosure?

MS. GOVAN: Yes.

MEMBER BLEY: And that's still to be done.

MR. DARBALI: So what we're doing is -- you'll see in the next slide that we're going to go for public comment on July 24th; that's our plan. So we're going to making those changes as well as some of the concurrent comments we've received, so those will be incorporated before it goes out for public comment.

CHAIR BROWN: Okay. All right. Now, will you -- it would be nice, when we do the full committee meeting in July, I hope you are intending to cover these as part of the full committee brief as well?

MR. DARBALI: Yes.

CHAIR BROWN: So that makes it very easy for me to write down.

MR. DARBALI: Right. Hopefully by then we will say we already did it. But the idea is to cover the same material we covered in subcommittee and explain how we would address those concerns.

MEMBER BLEY: Well, since you brought up the full committee, are there any other changes you expect to the ISG before that full committee meeting? Or ever? Well, ever is too big a word.

MS. ZHANG: This is Deanna Zhang. I think we have made some editorial changes to address comments we received internally, so you'll probably see some of those changes as well.

MEMBER BLEY: But we'll see the updated version 30 days before the full committee meeting?

CHAIR BROWN: Well, it can't be 30 days, because it's July the -- he's pulling your chain.

MR. DARBALI: The original intention was not to provide different versions, but to explain how we've addressed comments and any changes that have been done.

MEMBER BLEY: Okay. I will take your word that you will have incorporated it. Okay.

MR. DARBALI: The second main comment we received was regarding the four fundamental design principles, and how it wasn't clear how Tier 1, 2, and 3 review addresses them. That section is B-26; so by making Section B-2, System Architecture, applicable to already to Tier 1, 2, and 3, that solved that issue as well. So the description of fundamental design

principles will apply to Tier 1, 2, and 3 review process.

Those were two of the main comments we received. We received several other comments; one of those was regarding hardware configuration control. The ISG itself, whether it's Revision 2 or Revision 1, doesn't really talk about hardware configuration control or hardware configuration management, so we're evaluating how to address it, because I don't think in any internal energy guidance documents, we have a specific I&C hardware configuration control guidance.

A lot of it points to the licensee's configuration management QA programs, where they already do hardware or non-digital configuration management, configuration control. There they say, Oh, for software or for digital, do these extra things. We're looking into this; it doesn't appear that there is a major need to provide specific --

CHAIR BROWN: It wasn't in the initial ISG, if I remember, was it? We had a lot of extensive discussion on that. I don't remember that; my memory -- but that was eight years ago. That was 2010, when we reviewed the first version, and it was issued, I presume, sometime in 2010 formally, after the full contractor meeting when you wrote the letter. It was,

like, April of 2010.

MR. STATTEL: So one of the objectives of the ISG was to basically put a list together of required information. The initial list was about three pages long, and it included documents such as hardware design descriptions, schematics, layout, architectural drawings, things like that.

There was no intentional omission of any of that material. We did reduce that list down to about one page in the new version, but the basic information that we require to support our safety evaluation is still described within the body of the ISG itself. We just didn't break it down to the more detailed level; we didn't feel that was necessary.

CHAIR BROWN: I didn't disagree with that when I saw the new version.

MR. DARBALI: Something we've seen during our reviews and audits, especially of the vendors is, when they software configuration management, they have a configuration status counting document, and that also lists hardware modules. So configuration management of hardware is covered also, in part, by software configuration.

CHAIR BROWN: Your SDOE, or something like that, was covered.

MR. DARBALI: Secure Development and Operational Environment.

CHAIR BROWN: Right, and that was focused on software configuration management, which is appropriate, I would think. All right.

MR. DARBALI: Then the next slide is the next steps. We'll be briefing the full committee on July 11th, and we expect a letter with recommendations.

CHAIR BROWN: You'll get a letter.

MR. DARBALI: We'll get a letter.

CHAIR BROWN: I can't tell you what the full committee will do to me when I prepare my letter.

MR. DARBALI: We're going to be a little crunched on time, trying to address any recommendations in that letter, if there are any, in preparation for public issuance for public comments on July 24th.

CHAIR BROWN: Unless something comes up during the full committee, we've summarized what we thought were the critical items at the end of the subcommittee, which are the ones you've just addressed.

MR. DARBALI: Right.

CHAIR BROWN: And I can't confirm that no

other member will insert some other thing that we'd have to deal with, but I will do my best. Like I say, I can't tell what anybody else is going to say.

MR. DARBALI: We appreciate that.

CHAIR BROWN: Okay? And we do recognize the time frame, and we're trying to make this as painless as possible. I apologize for the delay that we had; there were some extenuating circumstances.

MR. DARBALI: We appreciate that. So after it goes out for public comments, the future activity is to continue engaging utilities in potential use of the ISG in pre-application meetings, and then put the ISG into practice. Then, further into the future, we want to actually incorporate it as permanent guidance in the SRP.

CHAIR BROWN: For information to the members who weren't here, my memory was that they incorporated lessons learned, and as Richard stated, they have used this over the last eight years, and I take it's been useful.

MR. STATTEL: Yes.

CHAIR BROWN: Is that correct?

MR. STATTEL: Yes, that's accurate.

CHAIR BROWN: Okay. Thank you, let's roll.

MR. RAHN: Okay. At this point I'd like to introduce Luis Betancourt and Huda Akhavannik and Paul Rebstock, who will be briefing us a little bit about the technical and strategic modernization efforts. At this point, we might talk in particular about how we are trying to maintain our awareness of these other modernization, transformation -- you name it -- processes that are happening all at the same time.

CHAIR BROWN: And we're now at 11 o'clock. We've done a good job. We're doing well, thank you very much.

MR. BETANCOURT: We'll go fast, but you can slow me down at any time, sir.

MS. AKHAVANNIK: All right, so good morning. My name is Huda Akhavannik from NRR. I'm an MP 4b working group member, and I'm joined at the table with Luis Betancourt from NRO; he's our lead, and also Paul Rebstock from Research, and he's also a working group member. At the side we have Bernard Dittman, who is also from Research; he's also a working group member, and he is also part of the transformation team.

In 2016 the Commission issued SRM-SECY-16-0070, which directed staff to modernize the I&C

regulatory infrastructure. SECY-16-0070 also highlighted integrated action plan, which directed us to develop a regulatory infrastructure that's simpler, streamlined, and agile, with the principles and attributes that are listed below, which I think we're all familiar with by now, but for the record, I'll just read it out loud: performance-based, technology-neutral, consistent, durable, predictable, scalable, unambiguous, safe, and secure.

MEMBER BLEY: By the way, the slides will be part of the record too.

MS. AKHAVANNIK: Oh, okay. So in order to modernize, our first objective is to perform a broad assessment of the I&C infrastructure. So this broad assessment should first identify the current regulatory infrastructure, which Luis will touch on briefly when he presents two slides from now.

The broad assessment should, at a high level, identify the main challenges there are to licensing, to the design principles that are stated in the SRM, and also consider the evolving perspectives that are in the digital I&C environment. On my next slide I'll discuss some of those evolving perspectives, but you've been hearing about them all day.

Other important areas to consider in the broad assessment are: We have to consider a past review experiences; ongoing licensing review and research efforts, which we'll be hearing about from Paul; lessons learned from operating experiences; insights from other safety-critical industries; and international perspectives.

Through this broad assessment, we expect that we'll identify and prioritize options for improvement and then develop a roadmap of action items from those options.

So this roadmap should encompass the four areas, the four communities that we see on the slide: the operating reactors, new and advanced reactors, fuel cycle facilities, and research and test reactors. We expect that, as we identify the challenges and potential options, some of these challenges and options will be common to all the communities, while some may be more applicable to a specific community.

So an example of an item common to all communities could be the treatment of the software life cycle NRC reviews, whereas a challenge that would be specific to operating reactors versus new and advanced reactors. The operating reactors are bound to their current licensing basis, so it may be more

difficult for them to be able to adapt to a new licensing approach.

CHAIR BROWN: Calibrate me; I forgot, again, from the May 17th meeting. This seems to be more broad than what ISG-06 --

MR. BETANCOURT: Yes.

CHAIR BROWN: If I remember, ISG-06 was focused on operating reactors, not new reactors. Is that a correct remembrance? If you don't have the answer, somebody else can answer.

MR. BETANCOURT: I think it can be applicable to both.

CHAIR BROWN: ISG-06 was new reactors as well?

MR. BETANCOURT: I think so. I'm looking -- no? Okay. We'll let Rich clarify that aspect.

CHAIR BROWN: Richard, did you remember?

MR. STATTEL: ISG-06 is intended for operating reactors, and it supports upgrading analog systems to digital systems.

CHAIR BROWN: Digital systems? So I was correct my memory, then.

MR. STATTEL: It's not intended to apply -- this current scope of it, in the graph, does not apply to new reactors; however, when those operators

become operational, then theoretically, new reactors become operating reactors. Then it would apply to them, if they were to make changes to their systems.

CHAIR BROWN: Got it. Okay, thank you very much. Okay, my memory is validated. You can go ahead now.

MS. AKHAVANNIK: So we realize that we're assessing and identifying options in an evolving environment. It's been two years now since the Commission issued SRM improving the IAP, and since that time, as you've heard from the other groups, the tactical efforts have been high priority to address industry's near-term needs. There was a decision made that we should hold on this MP 4 activity until those tactical efforts are completed.

We expect that the completion of the RIS and ISG-06 will address most of the immediate needs for the operating fleet. Right now IEEE Standard 603-2018 is near completion. The IEEE 7-4.3.2-2016 is expected to be evaluated for endorsement, and we had the recent SECY on the transformation team recommendations that is undergoing SRM. So we have to consider pretty much these moving parts as we develop our roadmap.

I will now turn it over to Luis, who going

to begin by discussing the I&C infrastructure.

MR. BETANCOURT: Thank you. My name is Luis Betancourt, and I am one of the working group, at least for this working group, and I will be slowing down for Charlie; I know that that's a comment I receive all the time.

So to start the discussion on some of the initial observations about the regulatory framework you have in front of you, you have a simplified view of our current landscape. As you can see, up at the top you have the regulations, followed by the policy, then the Reg Guides and the associated industry standards.

One of the first things that we did was -- if you go to the next slide -- as part of the broad assessment, was to identify what the current landscape is; how big is it? So we have found that there are three IBR standards within CFR 50.55. Our next step was to establish how many documents are in the current SRP and the DSRS, which are listed on this slide, followed by some of the documents that are applicable to this community, which are also mentioned on this slide.

If you go to the next slide, some of the initial observations that we have found are that the

current regulatory infrastructure, which was established and supplemented over the decades, has addressed many safety concerns and issues as they arise, using basic information and techniques available at the time.

Although the current framework for operating new reactors has been effective in addressing those issues, elements of the framework appear to have room for efficiencies which will make the infrastructure easier to use by the licensees and applicants. Basically we're looking for ways on how we can simplify and make it easier to navigate for both the staff and the applicants.

We're also trying to find ways to be more performance based, rather prescriptive, and try to be technology neutral.

CHAIR BROWN: I will interrupt to say I really kind of disagree that the existing IEEE 1990 -- it's not technology. It is technology neutral for the most part. Very, very broad in most of that stuff. So I kind of disagree with that, and I also feel that if you go through each and every one of these things, it's fundamentally performance based.

I agree with the earlier -- your next slide, that there's a whole potful of standards,

requirements, and other stuff that you need a significant road map to make sure you've complied with everything before you can get anything submitted, which is very, very difficult for industry to navigate.

I'm going to continue to argue that technology and neutrality of this thing is -- I don't think we're in that bad of shape relative to technology neutrality or the performance-based issues.

MR. THOMAS: Yes. I'll chime in here. Brian Thomas; just to revisit some of what we said earlier, I do appreciate that comment. There are some different camps within the community, the I&C community, that share that view. Then there are some that have a different view, of course. Again, that's part of the work that we have to do.

Your observation is well appreciated. As you go to the next slide, we've got to go through all of those regulatory infrastructure documents and look at them from that standpoint. And again, I read what's in the SRN to say, to the extent practicable, that's my terminology. But it means, as appropriate.

Where you need to be prescriptive, we'll make a determination on that. Where there is room, where we can be more flexible and more performance

1 based, we'll make that determination. So that's that
2 assessment that the working group has undertaken, and
3 there's work to be done there.
4 But we do appreciate your inputs on that,
5 and we also do think that it's an effort that we have
6 to expedite to get going, to really understand what
7 the path forward is for the overall regulatory
8 infrastructure.
9 CHAIR BROWN: I just objected to the
10 advertising, that this is, by definition it was, they
11 appear to be more prescriptive than performance based,
12 and not technology neutral.
13 MR. THOMAS: Right.
14 CHAIR BROWN: I agree there's different
15 camps; I have no problem with people having different
16 opinions. They can be wrong if they would like to be
17 wrong; that's perfectly acceptable.
18 The point is, I think you have to ensure
19 the changes that you make don't compromise the ability
20 to utilize new technologies as they come along. I
21 would have phrased it differently, and that you don't
22 look in terms of your improvements, that you don't
23 become prescriptive in areas where prescriptiveness
24 doesn't add any value to it, but that you balance that
25 out. That's not reflected in the way the words are;

that's my only objection.

MR. REBSTOCK: If I could chime in for just a second to give you a little bit of solace on this subject, what we're looking at are top-level objectives. We're not talking about, we're going to take a hatchet and go through all of our documents and chop them all to pieces in order to get this, and force this into every one. This is an objective for things that we change, something to be kept in mind as we develop.

But the question of what constitutes technologically neutral or what constitutes performance based is going to be in very fine details in each individual document. So how it works out is -- I mean, it will work out in the future, as we develop those documents. At this point, it's an objective; it's a concept that we need to be aware of.

CHAIR BROWN: Okay. Paul, I totally agree with that; your phraseology is fine. My problem is fundamentally when I just couldn't agree that this is a blanket statement that we're already in that position. So I just had to get it on the record that this is my perspective, not the subcommittee's, nor the full committee's perspective.

MR. BETANCOURT: Right.

CHAIR BROWN: This is not new to any of the -- you've got a lot of experience with me over the last 10 years, and so I'm maintaining my consistency.

MR. BETANCOURT: Right, so that's the reason I used the word elements in the slide, just to reflect that, because there are some aspects of the framework that are technology neutral. Our regulations are like that, performance based. If you look at the GDCs, it's the same way.

But there are aspects at the guidance level that we believe that we need to do some work. So the discussion that you had, we totally agree with you.

MEMBER REMPE: Before you leave this -- I hate to jump into these discussions, because I know I'm not an expert on it -- but when I was looking at some of the slides that we were given in preparation for this meeting, there was some stuff about the NuScale review, and how wonderful it was, and how you've reduce the RAIs and all this stuff.

Was it not technology neutral? I mean, was it really -- doesn't it kind of give you a flavor that maybe the current system isn't so bad, and that maybe you could build upon this approach as the way to go, instead of that not being the old approach? I

mean, am I on the right track here?

MR. BETANCOURT: I think this is a good slide to talk about this.

MEMBER REMPE: Okay.

MR. BETANCOURT: As part of the lessons learned that we have from both the NuScale and the APR1400 review, we were able to look at both sides. The APR 1400 was able to use the SRP, and the NuScale actually used a structure view of the SRP, which is basically the DSRS for Chapter 7.

Some of the other things that we learned as part of our review was, rather than going from compliance to compliance of all of the regulations, we went on a high level, an architectural level, because it makes sense. It's safe.

So we actually spent a lot of time learning about the technology, learning about the architecture, and then we went back and said, Okay, do they need the regulations?

So the way it was done for NuScale, it was kind of the same way we've done it in the past, but we actually emphasized more establishing, as part of the review, the architecture, and that actually makes it easier for us to make a safety finding. In order for us to continue that momentum, we know that there are

some applications for non-light water reactors that are coming online in the early 2020s, and right now what they have is the SRP. We not that the DSRS, even though that is applicable for NuScale, it can't be applied to anybody else. So we needed to actually take the lessons learned for those two reviews and boil it into what we call the DSRS for Chapter 7, based upon the lessons learned for those reviews.

We have been in close coordination with the advanced reactor community. I think we actually met with them in April or May as part of the advanced workshop. So we have been coordinating with that community as well as our community inside the NRC. I think there was some mention about the appendix, and the differences in there, and that's what was discussed yesterday. We are aware of that, and we are working with the NRC staff to see how we can incorporate that stuff into the new DRS. So we expect to target that somewhere between summer or fall of 2019.

CHAIR BROWN: What does ARS mean?

MR. BETANCOURT: I was going to go there. So we know that the DRS will actually be based upon our current infrastructure, our current regulations. We still don't know whether the regulation may change

or not, based on the comments we get from the Commission's SECY paper. However, that could be something for the longer term, that we can actually take from the lessons learned from the DRS, and if there is a regulatory framework, then that can become part of that longer-term framework. Right now, the DRS is based upon this framework that we have in place.

CHAIR BROWN: DRS is going to be a design review standard --

MR. BETANCOURT: Correct.

CHAIR BROWN: -- as opposed to a design-specific review standard?

MR. BETANCOURT: That's correct.

CHAIR BROWN: I figured that part out. And the ARS is an advanced reactor standard?

MR. BETANCOURT: No, advanced review standard, I apologize.

CHAIR BROWN: Okay. We haven't looked at the NuScale Chapter 7 yet, so I have no idea whether it will work.

MR. BETANCOURT: So wait until September --

CHAIR BROWN: It's coming up in August.

MR. BETANCOURT: I will be here again, so

you will be seeing me again.

CHAIR BROWN: Spear in my chest. I'm just teasing you.

MR. DARBALI: I know, I know. So any more questions on this?

CHAIR BROWN: No, I just wanted to make sure I got on the record that the way it was phrased was not exactly artful.

MR. BETANCOURT: We noticed that. Okay. Let's continue for the sake of time. So as part of the next steps, one of the things that we're going to be doing as a working group is to incorporate the Commission's decision on the transformation team, and then we plan to coordinate with the stakeholders on how to revise the IAP.

CHAIR BROWN: I'm going to interrupt you here. We made the comment earlier; I just saw the first version of some transformation document that was out, and I made the comment earlier that I'm a little about worried about now transformation has this far larger bubble. It's going to just eviscerate -- we're going to totally transform, and we'll just let the licensees -- hope that they're going to provide a system that works.

And I only say that from the context that,

when I came here in 2008, and I sat in on my first digital I&C subcommittee meeting, it was for BSBWR; it might have been for one of the early projects. The licensee presented his digital I&C system, and it consisted of 10 blocks that said, We've got inputs; we'll process it; we'll have outputs, and it will all work fine.

MEMBER BLEY: And it will all be DAC.

CHAIR BROWN: And it will all be -- what was that? Oh, yes, the DAC process. I think I exploded; my head exploded anyway, and I started asking questions, and the response from both the licensee and the staff was, that was all he was required to supply, and that's all we were going to get.

We fixed that. We ended up with what we needed, which was a detailed, architectural description, as well as a design that showed roughly what we've been getting on all the subsequent projects.

So I'm worried when I see this overarching world called transformation, that we eviscerate standards, and we eviscerate the information provided, not just that we can see, but that the staff gets, because you all are ultimately responsible for the

safety of the designs. You shouldn't be -- okay, such that you don't have the proper information to make that determination.

MR. BETANCOURT: So that's what I have on the bullet right below under IAP, Update the IAP Accordingly. We're going to continue to perform the broad assessment, because the transformation team is independent of what we're doing, even though they came to some conclusions. But we don't know if those conclusions are valid or not. So we still need to continue, but we're also planning to wait to see what the SRN has to say, so we can update the IAP.

CHAIR BROWN: The transformation document was very --

MR. BETANCOURT: -- high level.

CHAIR BROWN: It was extremely high level. It was all verbiage and no meaning.

MR. BETANCOURT: Yes. Okay. So let me move on so we can talk about the research that has been so critical for this. I'll let Paul --

MR. REBSTOCK: Okay, this is just a brief overview of the research activities in support of the IAP. I want to point out that I&C and the people in the office of research have been involved in this project from the very beginning. They have

participated in the development of the document that eventually became the IAP, so the people been in it right from the start. This presentation is going to reference specifically research activities, as opposed to general activities of people in the office of research.

Specifically, our research activities are intended to seek or confirm or confront the technical bases that would support changes to the regulatory infrastructure. In some cases we recognize that the results of the research may inform a need for changes to the regulatory infrastructure. That's not the objective, but it's something that could come out of what we do.

The initial set of research activities is driven by user need requests from the NRR. There are some additional areas under consideration, and those may be implemented by means of user need requests, or we have other vehicles that we can use also.

The initial set of user need requests were issued in the third quarter of Fiscal 2018, just this past April through June. There's been pretty close coordination among research, NRR, and NRO, to make sure that the formal requests are written and answered and developed in a way that can be answered and

executed as expeditiously as we can.

Current set of UNR consists of one as it shows on the slide, on risk-informed approach. That is being developed to provide guidance for the development of risk insights to be used in licensing activities, including grading of considerations, depending on safety significance.

Another issue is safety implications of embedded digital devices, and we've talked about those quite a bit already.

CHAIR BROWN: Is part of grading, are you all looking at -- as opposed to having specifics -- what's the process for grading? What's the hierarchy? Is that part of your --

MR. REBSTOCK: Yes, what criteria could you use?

CHAIR BROWN: Okay. So criteria; that's what you would --

MR. REBSTOCK: We want to look at it from a basic scientific and engineering logic standpoint.

CHAIR BROWN: I don't have any problem; I just wanted to see -- there ought to be some criteria that constitutes the ability to -- what does grading mean in these circumstances?

MR. REBSTOCK: Obviously, I mean, some

things need the whole works, and some things of less safety significance, maybe not quite so much.

CHAIR BROWN: Okay.

MR. REBSTOCK: But the criteria in figuring that out will come from us.

MR. HUDSON: I just wanted to introduce myself. My name is Dan Hudson. I'm in the Office of Nuclear Regulatory Research Division of Risk Analysis, and I recently assumed the role of the technical lead for this aspect of the work that's being done.

In response to your question, I would say that we're not coming in with a pre-defined set of categories that we're going to try to bend things into. We're going to be working with 10 CFR 50.69 and the categories that are there as an example, but I wouldn't say that we're constraining ourselves to this as a pre-determined set of categories to work with.

CHAIR BROWN: Okay, so you're not going to stay inside the box; you're going to look if there's other alternatives as well?

MR. HUDSON: We are going to looking at alternatives.

CHAIR BROWN: Okay, thank you.

MR. REBSTOCK: That applies across the board to all the research activities. We don't want

to be constrained to just exactly what we've got now. The whole point is to fix it; find out what's needed and fix it.

CHAIR BROWN: Okay. Thank you.

MR. REBSTOCK: So with the work on embedded digital devices in related emerging technologies, there is some controversy over what exactly constitutes an EDD. Some of us think of it as the microprocessor inside the motor-operated valve actuator; some people think of it as the distributed PLC, programmed logic controller, on complex skid-mounted equipment.

Whatever it is, there are implications for the basic operation and safety of the plant. So one of the problems with these kinds of devices is that the world is evolving very rapidly, so it is very difficult to get applicable operating experience. So what we need to do is find ways to assess the safety of them in the light of that condition.

Applications of EDD can involve new or alternate operational characteristics, and they can have implications in other areas. For instance, there is an example of a relay that had an embedded digital device, a microprocessor built into it. The relays that it replaced worked fine in the environment that

they were in. When you put in the new devices, they were subject to electrical noise, which caused problems. You don't normally expect a relay to be subject to electrical noise, but there they were. So that's something that we need to investigate.

Also, there are communication pathways and interconnections that can be introduced that can introduce concerns related to independence.

CCF, we've talked about quite a lot. One of the objectives of the research we'll be doing is to find ways to mitigate or suppress the likelihood of CCF.

MEMBER BLEY: I hadn't thought much about the embedded devices, but yes, they're in everything now.

MR. REBSTOCK: Yes, my toaster has one.

MEMBER BLEY: Yes, I know. It's nuts. I found one without.

MR. REBSTOCK: Okay.

MEMBER BLEY: What kind of research are you doing in that area? Or planning to do, or hoping to do?

MR. REBSTOCK: The overall objective -- and this is a bit of a heuristic -- you find what you find, and then that directs where you go beyond that.

What we want to do is get our arms around the big picture of what sorts of devices are being embedded, and how we can classify them. We've got an idea of classification on the basis of what they can do.

Sometimes you get a component embedded in a digital device that you don't really know is even there. It does the same thing that the old component did. There's no adjustments, there's no nothing; the operator can't do anything about it. The device can be tested. The overall, outside device can be shown to function properly, and so there's a digital thing in there, and that's the end of the story.

MR. JENKINS: If I may, my name is Ronaldo Jenkins. I'm Branch Chief, Instrumentation Control, Electrical Engineering Branch in the Office of Research. One of the ways in which we're looking at addressing the EDDs is to look at the total categories of different types of components within nuclear power plants. We know what that is. We know that there are relays, there are motor controllers, etc.

So by looking at what's already there and also looking at what could be introduced by way of a replacement, we can then assess the different hazards that might be introduced, in terms of categories. So by knowing what the state of the technology is now,

and also by looking at what could be replaced and is being replaced within nuclear power plants, we can get a handle on what kind of hazards might be introduced.

MEMBER BLEY: I'm just curious, because I hadn't thought about these things much, the configuration control that Charlie brings up, really branching into security. Do any of these embedded devices have the capability -- have you found any with the capability to communicate over the electrical connections that have them hooked up? Even though they're dedicated to this little device, can they talk outside?

MR. REBSTOCK: That's conceivable. We haven't found anything yet. This is just getting underway now. But I would allow for the possibility of, you've got an air conditioning skid -- everyone likes to talk about chillers -- you've got an air conditioning skid that's got a PLC on it, and it may very well have a serial output that goes to the plant computer or goes someplace to do something to transmit information, and that could be a very good thing. But it's also a vulnerability; that's one of the things we're concerned about.

But to answer your question, we're not there yet. That's something that we're aware of as an

issue.

MEMBER BLEY: You introduced all of this with a statement I want to go back to. As a committee, our focus is on the substance and quality of research, not how it's funded. On the other hand, we do a biannual look at research, and the last time I had a look -- I don't know if it's 90 percent, but a preponderance of research is funded by user needs.

You said you have other alternatives to go at that. Can you say anything about the alternatives to user needs?

MR. THOMAS: Yes, and I think, if you recall when we talked about the research program, we also talked about research plans. That's where --

MEMBER BLEY: Plans exist, but they don't have funds.

MR. THOMAS: Right. Well, there are funds. In this case, this is what we are using. But we are not closing the door, if you will, with regard to the potential for other types of issues to be of concern.

MEMBER BLEY: You might find something significant for which there is no user need, but you'll try to find other funding sources?

MR. THOMAS: Exactly, and then we would

enter into a very collaborative discussion, collaborated, coordinated discussion with the program office, and look to see where we could get those funds from.

MEMBER BLEY: Okay.

MEMBER REMPE: So you had research funds to develop a plan; you had user needs. But also, I didn't hear you say any feasibility studies. Has some of this been done as a feasibility study?

MR. THOMAS: There's a potential it could be. That's why we're not -- right now our focus is on getting our resources focused on the tactical work, the interim work, and then some of the other licensing focus, licensing improvement types of work. The resources across the agency have been dedicated to that. And as you said, the research activities have only recently emerged with user needs.

There are funds in the budget specifically to digital I&C and any of these issues, so we currently have funds for the user needs that have been proposed. But other types of safety-related issues come up, or safety-important issues come up, then yes, we would look to see what sort of a program we would undergo to have funds allocated for that work.

MR. REBSTOCK: Okay. We've got another

issue that is currently under development -- the user need hasn't been issued yet -- for looking at the impact of highly integrated control systems. A highly integrated system integrates information from many sources to provide the best possible indication of the state of the plant and execute control and safety functions as effectively as possible.

But the free exchange of information tends to diminish the independence of channels that are supposed to be redundant to one another, and it opens the possibility of undue non-safety influence over safety functions.

The purpose of the effort that -- what we're trying to put together to result in a fourth user need is an effort to review the state-of-the-art approaches within the nuclear industry within the United States and internationally, and also in other safety-critical issues as to how this can best be dealt with.

We think there are ways to do it, and the purpose of the research will be to look into it, not to design the systems, but to identify the characteristics and the critical points that would affect licensing.

Yes, develop the acceptance criteria,

thank you.

CHAIR BROWN: Highly integrated -- I'll just pass on -- I just can't help myself in these circumstances.

MR. REBSTOCK: I could see it coming.

CHAIR BROWN: Well, it's like all other things when you move from one level of technology that you're dealing with to another one, and in 1978, we recognized that we had to start figuring out a way to use microprocessors to utilize them within our overall reactor instrumentation control protection and safeguard systems.

We started that with a first project, which was two of the carriers. They were authorized right out of the blue, and we went out to develop their entire plant configuration using microprocessors. So it went out for bids to the three companies that we dealt with, and the only microprocessor available at that time was a Z80 2.3 megahertz microprocessor, 4-bit microprocessor with almost non-existent internal memory. Everything was done out of programmable, read-only memories that you had that supported them.

So we went out, and we -- because we had no idea how to utilize microprocessors to do anything,

not even to measure stuff; there was no real experience at that time -- we used a spec issued that said -- well, actually we didn't develop a new spec, it was the old analog spec. There were 29 instruments associated with this particular plant: pressure, temperature flow, level, etc., etc.

We put a microprocessor in every drawer, 29 drawers. The vendors came back and said, Oh, that's nuts. We only need four microprocessors. We will integrate off these into this highly integrated system, and we'll do it all with four microprocessors, and you will love it after that. It took almost 4 1/2 microseconds to say, No, we will continue. It's probably the smartest decision management -- in that case, it was myself and two or three of my group heads. We conversed, and it didn't take long to say no. It was the smartest decision we made; it was just a struggle to get through that.

And your point about, you lose independence and everything else; we eventually migrated to integrated systems, but they were integrated on a division basis, largely what we see in the proposals in the new plants today that have been proposed, which was half as successful. But that took -- it was not until the late '80s when we finally

figured we were comfortable enough to not do it on an instrument-by-instrument basis, to maintain that independence and not screw up anything.

But we did. We went from 29 down to 4 divisions, which in each division handled temperature flow, blah, blah, blah, for that set, and then another set of detectors and so forth.

So you've got to be very, very careful when you --

MR. REBSTOCK: I suspect you were very careful as to what things you combined on which processor.

CHAIR BROWN: Oh, absolutely. We had to maintain the functionality of each and every division, had to address everything that the reactor plant needed, based on the overall accident analysis and control functions.

So people get carried away with the new technology, and as the processors and FPGAs and all the other new things -- PLCs, etc., get better and better, faster and faster and more capable, the idea is, Gee, we can really do this cheaper if we combine all this stuff --

MR. REBSTOCK: I can do the RPS and ESFAS on my cell phone easily.

CHAIR BROWN: Exactly.

MR. REBSTOCK: I don't think I want to.

CHAIR BROWN: And I still use my flip phone, so -- I can get a text message on this, so it works. Anyway, that was just -- pardon?

MEMBER REMPE: Before you leave this last slide, can I comment?

CHAIR BROWN: No, we're finished.

(Laughter.)

CHAIR BROWN: Of course you can, Joy.

MEMBER REMPE: What I was wondering is, especially now with your incoming director of research, have you been aware of what the Department of Energy is doing in the LWRS program, as well as the NEAT program, and have you conveyed to them what you're doing in research? If they're not doing anything to help you, you might even convey to them that they maybe ought to be doing something that helps you, because LWRS is sustainability; that's what it stands for.

MR. THOMAS: Right. We are very, very familiar with what is being done under the LWRS. We do have to explore a little further what's to be done in the digital I&C arena, and we have been talking with some of the labs, if you will. We've been going

to digital I&C and cyber security, Sandia, and we do plan to go out and talk with INL.

We've spoken with them in the past, but now it's a more focused collaboration on that.

MEMBER REMPE: Not just the labs; I'd talk to DOE and help them focus, because I think it's something that, even though there's separation, it's our tax dollars, and they ought to be aware of what you've been --

MR. REBSTOCK: Oh, you mean the folks up in Germantown? Yes, we're --

MEMBER REMPE: Yes.

CHAIR BROWN: Going forward, we're much more keenly tuned in to being very specific with the research that we're after, and how they can support us, so that's where we are.

MEMBER REMPE: That's good to hear. Thanks.

CHAIR BROWN: You done, Joy?

MEMBER REMPE: I'm done.

CHAIR BROWN: Okay. No, that's fine. Thank you. You all have done a great job of boosting us back up, almost; we are now at 12 o'clock. Right now, instead of going on into the industry things, we're going to go ahead and break for lunch, and we

will come back at 1:15.

MR. RAHN: Before we go --

CHAIR BROWN: Yes, go ahead.

MR. RAHN: -- I want to make a remark. I captured only one action item, but I wanted to make sure you don't have others. The one item is that we owe you a copy of the RIS --

CHAIR BROWN: The original; I don't have that yet.

MR. RAHN: We have numerous comments and recommendations that I recorded in my notes.

CHAIR BROWN: Well, the only other one was that we wanted to get involved in the BTP 7-19 upgrade as well.

MR. RAHN: I have that.

CHAIR BROWN: I don't think any of these are onerous. We would just like to be involved, and you can coordinate when you get a reply. I know that's not imminent, but we'd like to coordinate when that comes along.

MR. BETANCOURT: There were also the comments regarding what is performance based, what do we mean about technology neutral --

CHAIR BROWN: Well, those are suggestions for when you develop the details on this. You ought

to try to express what you mean by performance-based and technology-neutral, with examples or something. That will give people some help.

Okay? Other than that, we'll take a break, and we'll be back with the follow-up part. Where's Eric? Is he still running this thing? Is he hiding back there? Oh, there you are. No other problems? I'm going to go ahead and break now until 1:15. We'll continue at 1:15. Thank you very much, we're in recess.

(Whereupon, the above-entitled matter went off the record at 12:17 p.m. and resumed at 1:22 p.m.)

CHAIR BROWN: We're back in session. And I'm going to take one minute -- he would like to create for the record -- just to make and correct a statement they made.

MR. RAHN: Yes, sir. Earlier this morning -- this David Rahn, Office of NRR. And earlier this morning I mentioned that we have this project underway between our -- working together on organization to develop a guidance to identify what is a good method for crediting work being done by certifying organizations.

And I think I mentioned at that time that EPRI is under contract with NEI, and that's actually

not a true statement. There is not a contract arrangement. EPRI is an independent organization -- independent research organization, and the work that they are doing is something that is made by a mutual agreement of the members of NEI and members of EPRI. It is not a contract arrangement.

CHAIR BROWN: Okay.

MR. RAHN: That's it. Thank you.

CHAIR BROWN: That corrects the record, and we will now proceed on. Jerud Hanson?

MR. HANSON: Yes, sir.

CHAIR BROWN: With NEI?

MR. HANSON: Good afternoon. Can everyone hear me okay?

CHAIR BROWN: We're good.

MR. HANSON: I'm Jerud Hanson with NEI. I'm going to spend the next few minutes -- in the interest of time, I'll try to move through these slides as quick as I can without talking too fast. But I'm Jerud Hanson with NEI, and I'm going to provide the industry perspective on current status of the digital I&C IAP.

So I'm going over the slides, just going to give -- elaborate on NEI's approach to addressing the modernization plans within the MP, digital I&Cs

impact on sustaining the nuclear industry, some existing digital upgrade examples. I'll be showing a chart on the method NEI is using to track digital I&C IAP MPs, some milestones we have reached, which you have heard a lot of today, and some --

MEMBER BLEY: I'm sorry. What were those acronyms?

MR. HANSON: I'm sorry?

MEMBER BLEY: You're using to track digital something or another. It sounded

MR. HANSON: IAP modernization plans.

MEMBER BLEY: Okay.

MR. HANSON: Digital I&P -- IAP modernization plan milestones.

MEMBER BLEY: Oh, okay. Thank you. Got it.

MR. HANSON: So this is just a more visually appealing slide to show just a high-level overview of what each of the MPs are, our focus on, the dates that we'd like to see these MP, the milestones delivered. And something I always like to mention when I'm giving a presentation is from the industry NEI side. Who is actually responsible for these different MPs in the industry? So we have a lot of help from our stakeholders, some from the utility.

Neal Archambo from Duke, who is helping on the MP 1 efforts. We have Kati Austgen with NEI, who is the lead for the Appendix D effort. And we have Maria Assard and Warren Odess-Gillett from Westinghouse who are virtual loanees to NEI. And also have Pareez Golub, who is leading the ISG-06 effort for Excel.

Every one of these people doing an excellent job. It has been a lot of work over the last couple of years. So any chance I get I always like to highlight that.

Okay. So this slide and the next slide, we're going to look at some SLR charts that I have provided, and maybe asking the question, why are we talking about SLR when it comes to digital I&C?

CHAIR BROWN: What is an SLR? Sorry.

MR. HANSON: Subsequent license renewal.

CHAIR BROWN: Oh, okay. I just would not have associated --

MR. HANSON: This is my other world at NEI. I'm SLR, and I'm also digital I&C --

CHAIR BROWN: Got it. I got it.

MR. HANSON: -- and sustaining. So what this chart shows is a couple years ago in 2016 NEI conducted an unofficial survey just to get a pulse of

how many licensees out there were actually planning to pursue subsequent license renewal applications. And some responded, some didn't, but fortunately we did have a good majority of the industry that did respond. And one thing I want to point out is --

CHAIR BROWN: When you say "industry," does this mean nuclear plant operators? License --

MR. HANSON: Yes.

CHAIR BROWN: -- you know, licensees?

MR. HANSON: Yes, sir.

CHAIR BROWN: Okay, good.

MR. HANSON: So, but these numbers are by plant. They're not reactor-specific. The questionnaire was very generic, I mean, down to the point where some were saying Plant 1, Plant 2, this year, and that year. So it was very generic. So we just went by plants rather than reactors. This is --

MEMBER MARCH-LEUBA: Do you mean unit?

MR. HANSON: Excuse me, sir?

MEMBER MARCH-LEUBA: If it's a two-units reactor, there will be two points in there?

MR. HANSON: No. It's just one nuclear power plant.

MEMBER BLEY: It's by site, then.

MR. HANSON: Site, yes. This is 20 sites.

MEMBER BLEY: Okay. So it's somewhere 20 and 40 reactors.

MR. HANSON: Right. So -- that's correct. So this is 2016. So we waited a couple years. The end of last year we had an excellent year for subsequent license renewal. All the industry and NRC guidance needed to license reactors for operating in 80 years were approved, were published, and we've had our first applications.

So we decided to conduct the survey again to see if the numbers would change, and they did change, not as much as I would have hoped, but there is definitely an increase. So what you're seeing here in this slide is actually an increase of 12 plants. So we have a total of 32 at this point.

So one way to look at this is we have the guidance from SLR is finalized and we actually have two applications in 2018, and there is a very good possibility that we could end up even seeing more on that.

So first year, SLR out the door, we're having a very good year, and we have a total of 32 licensees going all the way up to 2047. So we already have -- most of our nuclear power plants are licensed to operate to 60 years, and they are going to operate

to 80 years.

So having the licensing to get to 80 years' operation is great. But what we've seen in the industry considering the amount of plants we have shut down, or why they have shut down, and the fact that we only have one nuclear power plant under construction, which at least for right now it seems like it is going to come online in the 2020/'21 timeframe, SMRs and advanced reactors are out there but we haven't seen one built yet.

So for the immediate future, subsequent license renewal is the future of the industry. And where does digital I&C plan them? Well, if we're going to continue to operate our plants in the current environment that we are operating our plants, and what we're seeing as far as plant shutdowns, we need to come up with innovative solutions and how to run our plants more efficiently, and to put it frankly, less costly. That is where digital I&C comes in. We need digital innovative solutions, so that we can get as close as we can to guaranteeing that this plants can actually operate to 80 years.

MEMBER REMPE: So has NEI used these numbers? In light of the fact that some plants are shutting down, what percentage of the operating plants

in your survey of 2018 have said they aren't going to go forward with subsequent license renewal? Are these numbers --

MR. HANSON: Okay.

MEMBER REMPE: Can you put some perspective on these -- this plot?

MR. HANSON: So if I were to just do this in my head real quick, I would say that we're looking at -- so 32 power plants, I would say we're probably looking at a good 60 to 70 percent.

MEMBER REMPE: Thanks.

MR. HANSON: And like I said in the previous -- when we did the survey previously in 2016 where we had some sites that said no plans to submit or no plans at this time, we had the same for this survey, but we did just get a little bit more answers.

And then, of course, we had two -- two utilities out there who didn't even participate because they are no longer NEI members. But since one application has been submitted this year, we do have them on here in 2018 -- with the application being submitted.

Okay. So what is in this picture? Well, the one thing I can say about the picture on the left of the control room simulator is I did take that

picture myself along with the rest of the pictures in here. The only one I didn't is this one on the right.

I didn't have a good close-up when I was out at Robinson and McGuire a couple of months ago, but I did to go out to Robinson and McGuire to see some of their digital systems and some of the innovative solutions they have implemented.

So what I want to point out with this picture is when you walk into a nuclear power plant right now, this is what you see. The technology that has been in that plant since the time it was built, you know, in large part around the '70s, and taken into consideration how long these plants could operate, is this what we really want to continue to see going into 2040, 2050, and even beyond?

Take a lot of the younger generation right now, a lot of the kids growing up and going to college, they don't really know life at this point without a cell phone. So we have these computers, these cell phones. Whether we choose to accept it or not, they run a large portion of our lives.

So we have this younger generation of students growing up that way, going into college, and then they come to get a job in a nuclear power plant, 25 years old, they walk in and they see this.

MR. BALLINGER: And look at the bright side. They've upgraded to gold knobs.

(Laughter.)

MR. HANSON: There's a positive in everything. I do believe that.

MEMBER BLEY: Thank you, Ron.

MR. BALLINGER: The plants that we were in had all black ones.

MR. HANSON: So this is the same station. This is Robinson. And they needed another control room simulator. But rather than do another analog control room, they decided to go with a glass top simulator. And, incidentally, in 2018, they won the NEI top industry practice award for innovative practices.

But one thing I want to point out is, you look at the picture to the right, that is a laptop that controls this whole simulator. All done by a laptop. And the glass top simulator, I went up and played with it myself. You can actually turn the knobs like it's an actual knob, or you can just use your finger to turn the knob.

So what they use this for mostly is to augment a lot of the training that gets done in the analog simulator. So, obviously, in the actual

station, it's still the analog. But the students, the operators, can go on and use this to run their own scenarios and do their own training.

But the best part about this is once they have finished with this glass top simulator, they did an evaluation on the cost compared to the analog simulator, if they would have done another one. This came in at only 10 percent of the cost, and it's just as effective.

CHAIR BROWN: But the hand -- the touch and feel is different from --

MR. HANSON: It is. It is different.

CHAIR BROWN: And that was an issue that we were always concerned with, at least in my other program, because there was tactile feel for I have the right switch or I've done this, that, or the other thing with it. And that was fairly critical with our operators on simpler plants, because they had to react very, very quickly. When the submarine is boring holes in the water, and the reactor shuts down, there is a lot of things they have to do.

MEMBER REMPE: So even if you are doing training or simulator qualification for a time-critical action, you can't use this, can you, for justifying the operators can meet the requirements

for --

MR. HANSON: I don't know if they're there yet, as far as --

MEMBER REMPE: I hope they would be.

MR. HANSON: -- using this specific one to qualify. I know they are using the analog system.

MEMBER REMPE: I think they would be using, yeah.

MR. HANSON: But based on the feedback I received while I was at the plant, and I was talking to the people there who -- who run this training center, I didn't receive any feedback as far as what you describe. I didn't.

MEMBER MARCH-LEUBA: The difficult part is looking at the tiles on top and identify the problem, and knowing where to go, whether -- can you go back one slide backwards?

MR. HANSON: Sure.

MEMBER MARCH-LEUBA: Whether you turn the knob like this, or you turn the knob like this, that's really -- the training is the same. They don't move that many switches doing anything. The problem is identifying I'm going to the right place. So 90 percent you are there.

MR. HANSON: Any more comments or

questions on this?

Okay. So this is -- so the picture on the right -- on the left of the system, this is at McGuire and Catawba. Duke Energy spent $150 million between 2006 and 2010 installing this system across both McGuire and Catawba, and this was used to replace the Westinghouse 7300 process control system.

So there are a lot of benefits of this digital control system, but one of the ones I want to point out specifically that really stood out when I was out there talking to him is one of the primary benefits is the ability to automatically control steam generator water levels and low ranges of operation.

So what this required before was some tricky manual manipulation by the -- by the operators that often resulted in reactor trips. But since this was brought online in 2010, they have not experienced one reactor trip as a result of that same problem. This automatically anticipates the issue and addresses it before it becomes a problem.

So talking to the operators and the design engineers with the system -- who have been using it for the last eight years -- they can't imagine life without it at this point. And even the money that it is going to cost Duke Energy to update the software,

the hardware, and you're talking about to do that it's into the tens of millions of dollars just to keep the system updated. It's a price they pay gladly.

This is probably the most impressive system I saw while I was out there across Robinson and McGuire, and this is why I wanted to use them as an example in this presentation.

MEMBER BLEY: That's not the main control room, though.

MR. HANSON: No, it's not. You have me in the picture there. I'm not -- I'm not sitting there at the operator control about to cause a trip.

MEMBER BLEY: You're in the picture?

MR. HANSON: Yeah, I'm in the picture. I'm in the blue shirt over there.

MEMBER BLEY: You've got more hair than either of these guys.

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: You need to be looking at the microphone or she won't hear you.

MEMBER BLEY: Okay. On your last picture, you had a fairly large glass top simulator. We were out at one of the plants -- it was actually Palo Verde a couple of years ago -- and they had a single-panel glass top simulator that had gotten one of them, and

it ran the full software that ran the analog simulator.

And they ended up getting almost 20 of those put around the plant, so any operator any time could go run transients they were interested in and they found it extraordinarily useful for their operating staff.

MR. HANSON: No. I haven't been --

MEMBER BLEY: Even though it's not touch and feel, but they still could run scenarios and track them out.

MR. HANSON: Right.

MEMBER BLEY: And it was pretty neat.

MR. HANSON: I haven't been to Palo Verde, but I have been out to INL where they have the mockup, where they do the training for the Palo Verde operators. It's pretty amazing to see an entire control room made up of touch screens.

MEMBER REMPE: INL is also fun to impress the congressmen with when they come down.

MR. HANSON: Yes, I know. They are definitely good at that.

Okay. So this is a different schedule we use at NEI to track our milestones. And you see we have each one of the MPs on here. For the RIS, 1616,

Appendix D, MP 3, for acceptance of digital equipment, ISG-06, and long-term infrastructure.

The key at the bottom describes the different color codes used. Blue is industry action; yellow, NRC action; green is joint action; and of course red is bad delay. We don't like delays. So you see the different delays there, and for each of them I've put just who is the deciding party for the delay.

So you see in -- for MP 1A, the RIS. We did have a delay at the beginning of the year based on some stakeholder feedback provided on the version, which another public meeting -- another public comment period was made available, the RIS was issued in May. That's an NRC action.

And then going into the middle of summer and all the way into the early fall, the industry is going to be conducting a series of RIS implementation workshops. This will be hosted by Exelon, TVA, Duke, Southern, and STARS. And we're expecting that hopefully by the end of the year we will begin seeing some RIS pilot projects, digital upgrade pilot projects taking place.

MEMBER BLEY: Well, since this is your schedule, and you heard -- you heard the other

discussions this morning, I don't see NEI 16-16 on here, which seems to be a key item.

MR. HANSON: It is. It the second one down. It's the one with the most --

MEMBER BLEY: I just can't read it. There it is. Okay. Thank you.

MR. HANSON: The one with the most red. You'll see --

MEMBER BLEY: I need stronger reading glasses. Okay.

MR. HANSON: For the justification, that's a joint industry and NRC decision based on focusing of priorities and waiting on information by -- for EPRI, looking at Appendix D on hold, joint decision based on essentially the same reason, focusing priorities on getting the RIS out.

Now that the RIS has been issued, we are going to focus our resources on Appendix D. We heard the justification for MP 4B and the schedule on that.

So for ISG-06, one thing I still -- I will say about ISG-06 and the effort that has taken place with that, we have had some challenges in some of the other areas that we're working in as far as MP objectives.

But I have to say, with the group that is

working on the ISG-06 revision, they continue to meet their schedule. They continue to move forward, and I have every confidence that by the end of this year we are going to see Revision 2 issued, just based on what we've seen so far with that effort. So the NRC team and the industry team working that is doing an excellent job.

So, in summary, I would like to reiterate on the milestones we have reached this year. We have the RIS --

MEMBER BLEY: I'm sorry. Before you do the summary, up in the RIS you have the pilot projects going on late this year.

MR. HANSON: Yes.

MEMBER BLEY: And is NEI running those? That's what it looks like.

MR. HANSON: We're not -- that's industry action. That's what --

MEMBER BLEY: Okay. Who is --

MR. HANSON: Not actually NEI.

MEMBER BLEY: Who is the industry? I thought you guys were the spokesmen for the industry, except for a couple.

MR. HANSON: We need to work through the RIS implementation workshops, and we have -- between

this summer and the fall, we have about probably eight of them scheduled.

MEMBER BLEY: Oh, is that right?

MR. HANSON: Seven or eight of them.

MEMBER BLEY: Okay.

MR. HANSON: So we're going to -- what we're trying to do is use the different utility corporate offices, or even some of the stations, to hit every region within the U.S., so that we can get NRC support, participation, and we also are hoping we can get EPRI there.

So we have industry, NRC, EPRI. And when I say NRC, I'm referring to NRC senior leadership as well as regional participation.

MEMBER BLEY: Okay. And the schedule just ends there. Do you expect those to be done by the end of the year? Or do they extend into next year?

MR. HANSON: As far as the RIS pilot projects?

MEMBER BLEY: Yeah.

MR. HANSON: This is just for 2018. We're doing -- this is not just mine. This is what NEI is using across the Nuclear Generation Division now, and we're focusing on the current year. So this is just 2018.

MEMBER BLEY: My question was: do you expect them to be -- the pilot projects to finish this year, or do they continue on?

MR. HANSON: I would say, no, they will continue.

MEMBER BLEY: Okay. Thanks.

MR. HANSON: Any other questions on the chart before I move on? Okay.

So, in summary, I just want to reiterate the milestones we have reached this year. We have seen the RIS, RIS being issued, guidance for the industry on documenting quality of assessments, and the ISG-06 effort remaining on schedule. I see that as a milestone, and like I said, I am confident we are going to see that being completed by the end of this year.

The priority for this year should be continuing our focus on successful RIS implementation, which is supporting the workshops; ISG-06 issuance and completion of Appendix D for 50.59 screening and evaluations.

If we can get those three pieces of guidance completed and issued this year, I see that as a great success for 2018, and just for the digital I&C effort in general for the -- we've been at work at

this for at least three years. We've had some challenges, but 2018 seems to be moving very well, and I'm confident we can reach that success.

And just going back, referring to subsequent license renewal applications, the fact we saw the numbers between 2016 and 2018 growing, and I think they are going to continue to grow, just keep in mind that subsequent license renewal for now is the future of nuclear power in this country. And digital I&C is key to that future. We need to innovate in order to operate more efficiently and be able to operate to 80 years.

MEMBER BLEY: Okay. And, Jerud, I'm still back on your other one, too. The tabletops look like they're going on this month. Is that true, or are they coming in the future?

MR. HANSON: We're planning -- we're in the planning stage.

MEMBER BLEY: You're planning now.

MR. HANSON: Yes.

MEMBER BLEY: Are those going to be with utilities or with the developers?

MR. HANSON: Okay. So it's going to be both. So those who have participated in the drafting of the RIS, providing the comments, who have been most

productive in doing that, they are going to be supporting the workshops as close to 100 percent as possible.

So our primary lead for the RIS in the industry, Neal Archambo, he is preparing the training materials.

MEMBER BLEY: Okay.

MR. HANSON: And the first workshop we are planning is supposed to be at the end of July, and that's by -- being hosted by Southern. And the person who is organizing that, Ray Herb, he has been instrumental in the development of the RIS.

MEMBER BLEY: Okay.

MR. HANSON: So we are trying to maintain that level of participation all the way through.

MEMBER BLEY: But you're hoping they have licensees participating.

MR. HANSON: Yes.

MEMBER BLEY: Okay. Good.

MR. HANSON: Any other questions? Thank you very much.

CHAIR BROWN: Thank you. EPRI?

(Pause.)

MR. GIBSON: I'm Matt Gibson.

MEMBER BLEY: The button is nearest you.

Where it says push.

CHAIR BROWN: Down at the bottom. Now it's on.

MR. GIBSON: It was on a little bit. I wasn't sure how bright it had to be.

I'm Matt Gibson with EPRI, and I just want to thank the Committee for allowing us to come here and discuss EPRI's research in integrated digital systems engineering.

Just to get things started, I know most of you know who EPRI is, but I do want to remind everyone that we are in fact an independent R&D effort. So we try to provide research that is objective and solves the problems that are fed to us from our different stakeholders. And we get problem statements from a wide variety of stakeholders, as we are a nonprofit chartered for public benefit.

We do collaborate with NEI and our members, and we have an MOU with the NRC through Research, and we engage with them regularly.

This is me. I just included this so that you know who I was. You've dealt mostly with my predecessors, Ray Torok and myself Joe Naser some. But they have all, you know, went fishing now. So we're done with them.

(Laughter.)

MR. GIBSON: Or, in Ray's case, he has gone sailing because he's a big sailing nut, and so we haven't -- I haven't seen Ray since he left. I do see Joe periodically once in a while in industry meetings because he loves HFE, as you probably well know, and so he keeps that up.

We're going to talk about the nexus of digital upgrades with plant modernization a little bit. We're going to discuss systems engineering and its benefits, and we're going to do that because the integrated digital systems engineering effort is based on the -- what I would call the formal systems engineering process.

Some of you may be familiar with that; some of you may not. Specifically, to the guide, we want to talk a little bit about the history, the structure, how we got here, the benefits and examples. We're going to discuss two key elements of this, cybersecurity integration as well as risk integration.

EPRI has a plant modernization plan. Some of you are familiar with Rob Austin. You've probably seen him once in a while. He has now taken over as our lead -- EPRI lead for plant modernization. He has a special project to do that. This is their overall

plan, if you will, the different elements of it.

As you'll see, the digital upgrades and the ability to inform regulatory change are a key element of it. But also, especially for most of our stakeholders, there is a business element for this, too. You know, power plants have to survive as businesses as well as being safe. And so for our research, we try to figure out how you can do both of those things.

I'll pause here and say that systems engineering, you know it as a modern technique. What I want to say here is that --

MEMBER BLEY: If you're really old.

(Laughter.)

MR. GIBSON: The thing is that over time utilities in particular, and vendors as well, have had ad hoc engineering processes. So while we have a lot of regulation and we have good practices and various other things, that has never been really synthesized into a process that achieves predictable results.

We see that regularly. You know, all morning you guys have been talking about different regulatory elements of various sorts, guidance you want to give to licensees. Well, you've got to think about what happens after they get that guidance. What

do they actually do with it?

And you also talked a little bit about performance-based. Well, to do performance-based you have to perform something. There has to be a process that takes those requirements and performs something and has an outcome. And, unfortunately, maybe our industry has not been good about developing those processes in the past.

And so what we're trying to do here is to move that needle. A few years ago, I'd say about four or five years ago -- well, it was four years ago I guess it will be -- we started out looking at the systems engineering concepts. We have a report, 3002008018, that captures that R&D. And we went out and we benchmarked a lot of people. We looked at how it actually did work.

Vendors, many of them control system vendors by the way. I'm not talking about people who do nuclear work. I'm talking about people who do work in the oil and gas, aerospace, transportation, those kind of issues. How you actually get these systems designed, developed, and out the door, what process do you use? This is the process they use, systems engineering. It's very iterative.

So we validate the efficacy for nuclear by

taking those and looking at how we should be doing things as well. And there is no reason we shouldn't.

We've taken these research results and tried to integrate them into a usable methodology. And I will say -- and you guys talked about this a little earlier -- the DEG itself is not scheduled for publication until November of 2018. So this is an early look. The finished document is not there.

But I do want to say that it is -- we have used the systems engineering process to design and build the system engineering procedure. Counting our MOU engagements with the NRC's research, we've done 26 focus group and feedback exercises with different stakeholders, vendors, utilities, again with Research, to get their input.

So what problems do you see that need to be solved through this effort? That has been integrated. So it's coming down to a completely finished document. Our Draft A has been out for review. We've got those comments back. We have addressed those.

Draft B will go out very soon, and we will be providing Draft B to NRC Research for their comments. You know, if they want to give some -- some technical comments, we will consider any of those that

we get.

The key element with the digital engineering guide is that it tries to bring a lot of disciplines together. You'll see that as we talk about it a little further.

There is also a key element we discovered doing this is their silos. I was real interested, and when you first started out this morning I think, you know, you observed that there was some apparent integration between activities within the staff. And if you take that a step further, it truly is -- should be able to get it for all of us -- is integrate more of what we do.

Now, as a long-time practitioner in utilities, I will tell you that every time a regulation comes out, the utility spins up a new process for it. So now you've got 900 people in a 1,000-megawatt plant.

Those things haven't been integrated adequately, and they have a lot of different processes that they are using to try to do all of these different vertical technical activities, measure the I&C a little bit, it's taking in a vacuum when it shouldn't be. It should be part of the integrated engineering process. Risk, other things, cyber we

will talk about a little bit. It should be all integrated together. But there is no process to do that, so this will seek to make this a holistic process that folks can use, be risk-friendly.

And, you know, the U.S. utilities are apparently going to be first adopted. Now, remember, this is not a U.S.-specific thing. So we have international members. So we've talked about this same process with our Chinese members, our UK members, our other European members, our Middle East members. So this is ringing -- this has some resonance for them as well, especially our UK members who are sequenced into a safety case-style regulation. So this fits that very well for them.

V model -- some of you may have seen this in software documents somewhere in the past. This is actually systems engineering construct. See this diagram in the lower left-hand corner? I know you can't -- it's not important you be able to read it, but just the idea of it. That's -- that diagram and this diagram are identical. The only difference is you stretch the diagram into a V model to make it a little more attractive I guess is the best way I'll describe it. It's the same -- the same diagram.

These diagrams contain the different

levels of abstraction. What you do is you design a system and the feedback loops. One of the takeaways from this one is the integrated system engineering model also -- it doesn't supersede, but it integrates your traditions of an SQA, makes it all put together.

Why is that? Well, if you look at the modern -- all the IEEE especially, the current versions, they used to say software engineering. Now they say software and systems engineering. And we read -- when we read the current standards and we look at their prefaces, they talk about how over time they expect all of these to come together fully.

The IC is a little further along. You'll see most of the IC standards are well integrated where they get -- software is integrated fully into the system design along with the hardware.

Composition and decomposition is also an area where we think the system engineering process gives clarity to what you're doing. We also talk about our systems very monolithically as if a whole system is a system that does a system thing. The reality, they're systems within a system within a system.

And the understanding where you are in your composition and decomposition help you understand

what you should be doing, because, you know, as we talk about to people, the whole world is a -- is it the Russian dolls that are all -- you know, one went inside the other? Well, that's what it is. That's what the world is.

And so systems engineering, unless you visualize how to handle that, because you get the little doll out of the middle, you're talking about a different thing than you are all of the dolls put together at the top.

So when any entity, whether it's a vendor of a utility, a utility, or even a regulator potentially reviewing these, knowing where they are in this level can inform how they should be looking at the results.

So, again, it's due November 19. It's pretty far along. The guide is laid out in 12 chapters; 1 through 3 are the framework. We'll talk about each one of these a little bit more.

There's a graded approach, and that is also something that is very needed because the grade that -- we need to grade what these activities do based on some criteria. And as you can see here, we have chose configurability, consequence, and the applicability of the activity.

Systems engineering is much like a gear change. You'll see in the small diagram there in the -- in the left it is an iterative feedback approach. It's an important thing to understand because if you have something that has low configurability -- I think Dave Rahn was talking about, hey, how about the little bitty digital device, you know, something with low complexity; in this case, low configurability because we define it a little more -- not just say complexity, but we have criteria for configurability.

If that's low and its consequence -- structural consequence is low, you spin this once, maybe once and a half times, and you come out of this loop with all of the information you need to make design and safety decisions, if things are more complicated, if it's a high kind of figurability like a full-blown RPS or SFAS, or if the consequences are high, and there's things that have high consequence and are low configurability regardless, this graded approach allows you to spin through this iterative approach until you've got the right answer.

MEMBER MARCH-LEUBA: You're familiar with the famous casino heist where they rob a casino via the aquarium tank?

MR. GIBSON: I've heard of it. I'm not

that familiar with it, though.

MEMBER MARCH-LEUBA: They penetrated the thermostat on the aquarium, and through that they got into the whole system.

MR. GIBSON: That's right. That's right.

MEMBER MARCH-LEUBA: Using the system, the aquarium thermostat would have come out as --

MR. GIBSON: Yes. You'll see right in the left-hand corner there is a hazards analysis. And we will talk about how those hazards analyses work.

MEMBER MARCH-LEUBA: I looked ahead at that slide, and I --

MR. GIBSON: Okay.

MEMBER MARCH-LEUBA: -- keep in mind the aquarium because --

MR. GIBSON: Okay. Well, you can bring it back up. We'll talk about the fish then.

MEMBER MARCH-LEUBA: How come -- how could the aquarium thermostats ring in your --

MR. GIBSON: Well, in the hazard analysis methodology we'll talk about a little later -- we call it HAZCADS -- it really adopts a boundary approach. So if you were looking at the thermostat on the aquarium, I'm just -- I'm ad libbing because I don't really know that much about your aquarium example.

But let's say I can visualize an aquarium, I can visualize a thermostat, and I can even visualize a thermostat just hooked to the internet where somebody can check it. And even leveraging that, one of our researchers, maybe some of you know him -- Sam Harvey? He is the -- I think he used to work for TVA. He's a big aquarium guy, has a giant 600-gallon aquarium.

He's got PLCs and all this stuff down in the bottom to take care of the salinity and all this kind of stuff. And he could watch it from home or on the road. He can be on the road, on his cell phone, and he can see the fish, he can see his -- all his parameters for his fish tank. And so who knows? Somebody -- the same guys could get into his thing and blow his fish up and, you know, who knows, right?

But if you apply the hazard analysis process that we have developed -- when you do boundary analysis, you will discover the thermostat, you will discover its value to the particular function, you will see all of its interfaces, and you can make a hazard judgment on whether that interface presents a hazard, because, remember, in this process, you are integrating all of the hazards, including the cybersecurity hazards, into one integrated process, so

you'd see it, and hopefully you would say, "Somebody might want to use this," because it's a support system basically, right? You know, it's a diversionary tactic, right, I guess is what they use it for -- for the fish tank.

In the casino heist --

MEMBER MARCH-LEUBA: He wasn't there. In the lobby.

MR. GIBSON: He was in the lobby. But it was a diversionary tactic, to make the fish malfunction, right?

MEMBER MARCH-LEUBA: Oh, no, no, no. They got into the thermostat and through there got into the network.

MR. GIBSON: Oh, well, there you go. See, this would have --

MEMBER MARCH-LEUBA: And installed a --

MR. GIBSON: -- detected that, too. If this thing was connected to other networks, you would do a data flow and a control flow, and you discover all of that and you say, "We ain't having this."

MEMBER MARCH-LEUBA: They stole all the database from the casino.

MR. GIBSON: That's right, that's right.

MEMBER MARCH-LEUBA: Through the aquarium

and my -- my claim -- and I want you to think about this -- is when you do the hazard analysis on the aquarium, you will come out the same now, very low. We don't have to worry about it.

MR. GIBSON: In this case, not necessarily, so we'll talk about that a little bit.

MEMBER MARCH-LEUBA: And you hinted a little bit about cybersecurity. Those high school kids are really good, especially the ones in Serbia or where was it they were -- the ones in Yugoslavia? You're not dealing with those guys. You're dealing with the top of the line security officers in a foreign country that have been trained to the limit, because those are the ones attacking your plant. They are the same kids.

MR. GIBSON: We understand that. We understand we have state --

MEMBER MARCH-LEUBA: Macedonia, right?

MEMBER SUNSERI: Matt, so I don't think you'd get any argument from anybody that these are the -- what needs to be done. I think it seems to me the hang-up is, how do we do these things? Are you going to get into that?

MR. GIBSON: I will.

MEMBER SUNSERI: Okay.

MR. GIBSON: Chapter 4, your systems engineering, which basically implements the red circle and the spinning that you see. There's topical guidance Chapters 5 through 12 that cover, as you see here, procurement, human factors, your data communications, cybersecurity, plant integration design, testing, configuration management, and obsolescence.

So that you understand the architecture a little bit, the DEG, as it is, is regulatory, right? It tells you how to do stuff. So it will depend on you, in a given regulatory environment, taking your regulatory requirements and sensitizing them into requirements that you can actually execute on and then feeding them into the system.

So if you have -- if you have a regulatory requirement that says you always paint your containment building blue, that becomes a requirement that gets fed into the process, because, remember, one of our big gaps we have between what we want to do in any requirement space, whether it be regulatory, functional, or business, is translating that requirement into action and results. So that's a three-step process, requirements, action, results.

This guide is positioned in the middle and

the end to take those requirements, convert them into action, and give you results. So what we will do -- and for any of our members, U.S. included -- will be a mapping document that whatever it happens to be at the time just moves around a little bit.

But we in the fall, after this is published, will go through the regulation and show where -- how that regulation -- you know, if you were doing requirements based on those regulations, how they would fit. We're probably not going to take on separate staff guidance that you might have like the Reg Guides, and things like that, but we will go at the regulation level or, you know, other things that are considered regulations and say, "Here is what you've got to do," you know, GDCs, that kind of thing.

And so that will help a U.S. utility use this to see how they might have to take and synthesize their regulatory requirements into their process. And I've personally done this with 603 on projects I've done, and it has worked pretty good.

So it's standards-based, and if you have your speaker notes -- I know I gave you -- it's in a -- in a thing you have, if you've read them -- the whole list of standards that we have synthesized into this guide, our main one being ISO; ISE; IEEE 15288,

which is systems engineering; 12207, which is the hardware -- excuse me, the software -- it's addendums, if you will; and then 15289, which tells you what types of information items need to be captured to document what you do.

These are all international standards in a sense. They're also U.S. standards, if you want to see them that way, because we're international.

Most of these standards are really good.

MEMBER BLEY: You didn't just refer to these. You integrated them into your --

MR. GIBSON: Right. That's the point we wanted to make.

MEMBER BLEY: Unless they change, you're going to have to go back and figure -- somebody in the future is going to have to go back and figure out --

MR. GIBSON: That's fine.

MEMBER BLEY: -- what the --

MR. GIBSON: You would have to do change analysis to see if whatever change was done to the standard would impact what we've done. That's true. And so this is a living thing. We visualize it, you know, should the industries -- well, EPRI will do it for the most part, but, you know, we will get feedback on people using it, you know, depending on how big a

population isn't using it, and then periodically, you know, work on it to synthesize it back.

NEPA has a big list, you know, because one of our favorites is the IEC 61508. We take the little audited stuff in there and we synthesize a lot of stuff into this. The configurability concept comes from there. It is successfully used in a lot of safety applications.

This is the -- this is the integrated digital systems engineering overview, if you will. What you'll see is the list of all of the topics that we address in the guide.

Now, a lot of these topics, you know, you saw the list of topical areas don't have their own chapter. Some of them were actually done in Chapter 4 as part of systems engineering process, such as architecture, analysis, requirements engineering, are all done as part of Chapter 4, which does that.

As you talked earlier, hazards analysis, single-point vulnerability, CCF, are fed in as requirements and synthesized into architectures and results and for people to implement.

Graded approach. Now, the DEG is activity-based. So, first off, we decide what activity the person has to do or should do based on

what we're calling risk. And I will be circumspect about talking about what we mean by risk.

Risk being the undesired result. We're using consequence and these other words in their dictionary definition. So, you know, we're not necessarily talking about just radiological consequence, although that is included.

The process we have we really look at, although I show it this way because the risk metric is technology configurability, it gives you the likelihood. The more configurable, gnarly -- let's put it that way -- something is, the more likely it will have a problem.

This has its roots in the systematic ideas you see in IEC 61508. We also do potential consequence of error. We build this because we use this risk metric to decide what activities are required, and when we do an activity, what documentation/information items are required, all graded approach.

Now, process-wise, we don't -- we do it a slightly different order. We do technology configurability first. Then we do applicability because we've got to learn about the device first before we can tell if it's applicable to any

1 particular activity, and then your potential
2 consequence is done last.
3 Rigor is a well-used word, and not well
4 understood by most people, or they have their own
5 idea. We define rigor as assurance methods that
6 reduce the likelihood of an error. So when you say
7 you want high rigor, what you really mean is you want
8 someone to do something that reduces the likelihood
9 you are going to have an error. And that's the way we
10 define rigor in here.
11 MEMBER MARCH-LEUBA: Back to the aquarium
12 example, in addition to rigor, you need people with a
13 real red hot, with bad ideas, because nine of out ten
14 people, we knew their aquarium thermostats are green
15 on the review, and it has absolutely no consequences.
16 It's not configurable. All you can do is watch the
17 temperature on the poor fish. It tends to be a
18 threat.
19 MR. GIBSON: Well, you know, I think what
20 I need to do is go watch this movie and see -- follow
21 up about how hazard analysis and these other processes
22 would have detected if the thermostat was a risk. I
23 mean, people do that all the time. Professional cyber
24 people and risk people will look for these educations,
25 they look for these data flows. That's how you detect

them. We can talk about that a little later.

You do interface analysis, you do data flow analysis, you do control flow analysis, and you will find that -- you will find that thermostat every time. If you just look at the thermostat and think, not a problem, you won't find it. But this process is not what you're used to.

MEMBER MARCH-LEUBA: It has to be integrated.

MR. GIBSON: Yes. It has to be integrated.

MEMBER MARCH-LEUBA: And it has to be with people with bad ideas.

MR. GIBSON: Otherwise, it does -- and what we find as we go through these is that once you integrate them, you get a lot of synergy in people's knowledge about things. And it starts -- it starts paying off.

I will also say that there's something about -- so the -- there is also a capability maturity model aspect to this. The day you start doing this, the initial practitioners will not be as good at it as they will be after they use it for a few years. So we have to understand the capability maturity model climb that we do as we integrate these things. So it won't

be like overnight, you know, it happens.

So just to give you a quick overview of the graded approach, you know, we do configurability first, and there is parameters here. We won't go into a lot of the details unless you want to.

Build to activity -- because once we know the configuration, then we know what activities apply. If it has no network configuration, if our thermostat is completely air gapped between everything else, it's just sitting there and you can only adjust it by the local knob, the network analysis is not required, right?

Because you've done interface analysis, you know it's not hooked to anything else, there it sits, and you have to consider your physical security aspects of that knob, but not your network. So applicability happens after configurability analysis happens.

Then we do consequence screen. We are in the middle of refining the consequence screens because we want to keep the amount of consequence -- right now we have two consequence levels, high and not high, because as we look at what we would normally do, the result was it's not practical to have a lot of discrete granularity in your consequences because they

don't drive differences in what you do.

It's kind of like if it's consequential, that's the part we want to use. If it's lower consequence, not high in other words, then we have less. But, remember, we're not doing everything based on consequence.

We also have configurability, and we combine those two to give us the ideal -- what kind of activities we should do and how much rigor we should apply and what kind of documentation we should produce. So that's the idea of it.

The DEG, besides a text because it has these things in words and processes, we also visualize them in a swim lane. So you will see the various roles that are addressed. Your maintenance role, your operations role, your engineering role, and your project management role. And you see the project or the plant life cycle, if you will, here.

And this swim lane in one diagram gives you a feel for all of the things you have to do and in what phase you have to do it in. So if you were to look at the DEG in its final form -- each chapter, each activity, not each activity, but basically on a chapter level there is one of these swim lanes.

And at a glance, you can see -- tell

whether or not you're going to do a lot of work in the conceptual phase or more work in detail design or in installation.

Chapter 4 -- we've talked about this already -- is iterative. But also, it performs or confirms things. So let's say, for instance, some things that you want to check here have already been done. Let's say you've been fed a hazard analysis by somebody else who has already done that, some other thing. As you go through here, you can take those pre-prepared or separately prepared artifacts and look at them.

Let's say if you have a vendor do some of this. You can bring those in and analyze them. One of the first things we do is do a division of responsibility. The idea is for the -- for the operational stakeholder to be -- fully own this. So if they farm it out to a vendor, they will asking the vendor to follow the same process.

And so the division of responsibility, though, is key because some things the owner/operator has to do, and some things can be farmed out to a vendor. But, regardless, it is still this process, so you have to keep up with who is doing what.

Requirements development comes next, your

hazard analysis, including CCF, your mitigations. Your architectural development comes out of that, because once you know your requirements, you've done your hazards, you begin your architectural development, and these are not necessarily in this order -- hard in this order because, remember, it's iterative, so you're doing kind of these in a circle.

You do your functional allocation. You decide if a human is going to do it, which system is going to do it, if the human doesn't do it. Your verification/validation, your testimony, and your transition to O&M phase are all addressed here.

Now, the other chapters also enlighten those things in more detail. So if you look at Chapter -- final Chapter 5, and we will want you to get a copy as soon as, you know, we're ready. Maybe even Draft B we can send to -- because we'll send it to the -- to the Research and say, "No, we don't have any problem in showing it to you all."

What you will see is each one of those topical areas also provides additional input, and those topical areas will reference --

MEMBER BLEY: Is that the current draft, or is that the one coming in November?

MR. GIBSON: November.

MEMBER BLEY: Okay.

MR. GIBSON: Well, it might be before November. We hope to finish it up very soon. We probably won't publish it until November, just because of EPRI's internal QA and a lot of this stuff.

Some real-world examples. So if you were replacing a digital recorder, so -- this is pretty straightforward, so where would you start? Well, you know, most of your binding technical requirements you already have because you're replacing a recorder. You already know what its IO is. You know what its function and procedures are. You know those things.

So those existing requirements come into you from above in the composition/decomposition, and then you have to decide on things. And this is the part you have to do in this particular activity down here in the blue.

You're going to decide your parameter values, your bench evaluation, you'll refine your parameters, you'll specify configuration. We'll go through it in the other diagram -- binding technical requirements, decide your parameter values, you do bench evaluations, you have a feedback loop where you refine your parameter values. You specify your configuration, you configure, install, and validate.

That's the loop.

And it's not much to this because this is the recorder, right? You already know what you're going to hook it to. It already does a function. This is probably in procedures already. So it's really a sort of narrowly defined thing. So you operate it in a narrow definition.

You can consider desktop simulation if you want. If you do a lot of these, you can take this design and reuse it for more than one recorder, which makes it very efficient. You can do model number optimization. Let's say this is an XYZ model recorder, and you've already done all of this one time. You can have a template for that model, and then you can start with that. So depending on, you know, how much you use that specific model.

So let's continue with this. This is a popular question. There is stuff inside that thing. You know, there's chips and CPUs and software and all kind of stuff. What's inside of that particular device has been done by other people. It's likely to have been done by somebody using the systems engineering process.

So in this scenario, what you're doing is you're evaluating what you're getting from a recorder.

And that recorder's function -- and when you do the hazard analysis of what that recorder does and its malfunctions turn out to be a certain thing because you agree you're doing a boundary, flow, and connectivity analysis.

You treat these lower-level things as -- you know, you're not trying to control the design of the internals of that recorder. What you're trying to do is understand what you're getting in the context of how you're using it.

So some of these concepts are taken from IEC 61508. This is -- dash 3 is the software one. If you're going to pick up a copy, you know, you'd find it interesting. It has seven sections. It's a big document. Two, three, and six are really interesting because two and three are the hardware and software and, you know, how to do all of that stuff, and six is how you put the two together.

We'd like to illustrate this because the fixed programming language, which is one of the levels of configurability that 61508 has in it, is the types of things we do for this recorder.

The inside of that recorder, however, has been programmed with a full variability language, like, you know, C or whatever. And so that's at a

different level of the onion in which you're operating in. So you treat that as a black box and you access coming into your area.

A lot of good models for how to do that within DEG, the hazards analysis being the key, you know, and your other analyses helping you out with that, especially your CCF. You wouldn't do that for everything, but if it was a high consequence you would.

This is our second example, a little more complicated. You start a little higher in your V model because now not -- less things are given to you. You have to develop more stuff because you don't have it.

At your conceptual and what we -- this is the contextual design stage, but you can use that as a common design if you're going to put in multiple ones of these systems. So you can stop about the 30 percent.

So if you visualize going through the systems engineering process multiple times, and go through it maybe three times for a complex system, then you can kind of pop this. And you use those learnings and those discoveries and use them again for a similar system.

In each case, you finish the design, so you can stop this thing, and then you point and capture the results you get as a template. That's what we call a common design. And you finish up with detailed design.

This last example is -- shows you where you might say a typical thing in the plant where you're doing a software change, just not a design change. It's an implementation fix, like a bug fix. It's not -- it's doing something it's not supposed to, but you know what it's supposed to do, but it's not doing it.

You're now down in the -- in the implementation basically. You hear a lot of people talk about software doesn't break, but software does malfunction. And what you'll see in the -- when we do analysis of failures, most software is a failure of implementation. You may design it. You're design -- the word design means your intent, right? Your intent is for something to be a certain way.

In software, design and implementation tend to mix, and a lot of people, you know, talk about design when they really mean implementation. So you can have a very well done design requirement for software. You can have documentation even that says

software works a certain way, what I mean for it to do.

Cryptographic algorithms are a good example. Those are well published, well API-ed, and documented, and people get them and then they write code to implement them. And they mess up, and those bugs are what provides stuff -- vulnerability to those cryptographic algorithms, not the designs, because the designs are mathematically proven.

So in this case, you know, make a change and you're going to regression test it and declare it good. So it becomes confirmatory. So it's all through this process you usually do something or you confirm that something has been done.

We've talked about this a little bit already, that this process integrates your SQA and your hardware. And because it's iterative and does both things, it eases the requirements for these traditional software life cycles that are waterfall based. This is a lot more -- if you ever heard of agile, this is a lot more agile.

But you're not delivering a product to -- the final product during this agile process. You're just doing intermediate stages of development.

The U.S. industry does plan, our

understanding, to use this DEG. So they are busily making plans. I think Jerud mentioned earlier there is training being done for the RIS package. And so we want to try to synchronize with that, so we can -- when he mentioned EPRI might be there, we want to synchronize that so we can do the training -- do at least initial training on the DEG and the NISP 004 at the same time you do the RIS training or the industry does the RIS training.

Because this will be key to have -- people having a process where they actually do the RIS, because the RIS itself is not implementable. There has to be a process to implement it.

See if there is anything else on there on that is useful. Just the idea that, you know, these are procedures, these first two, these are things the industry gins up to use this. EPRI's part of this is the DEG and our other primary references, which are referenced by these procedures as a process.

Some of you are familiar with the standard design process. That's an initiative the industry did to standardize design engineering throughout the industry and with vendors. It's done and being implemented.

The DEG is going to be an addendum to

that, so it will be part of every mod. So if it's digital, it will get the DEG path.

And the point with this is that the DEG, digital engineering guide, actually does more things than the classical design process does, because it starts a little earlier in the scoping phase and ends a little later in your operations and maintenance.

We'll finish up with the topical areas that are integrated. So EPRI has a process called a technical assessment methodology, published Rev 0 back in 2016, will publish Rev 1 in August.

Our early adopters are Vogtle 3 and 4, Barakah, and Horizon Nuclear in the UK.

This -- the TAM is designed from the beginning to integrate into the engineering process. So it integrates cyber into engineering, basically treats cyber as a hazard that has to be dealt with.

So you'll see, you know, we start out with components. You transition to relationship sets, then address the site, overall site control methods. We also have a process where you can map the results to a regulatory body, so from the U.S. like a map in either 0809 or 571.

What it does for the industry worldwide is to standardize how you go about assessing for a cyber

vulnerability and how you go about documenting it. That's a real issue because right now everybody is all over the place. There is 1,000 guidances that have not been synthesizes in the real world. This is what -- this is what this does, it synthesizes them in the real world.

There is the international standard, IEC 62443, on cyber. You know, our European and Chinese members are very interested in that. This is compatible with that, as well as 0809 and 571.

We have the integration ongoing with the supply chain in 2018. You can use this methodology -- I know the NRC uses the terminology SDOE, secure development and operational environment. The TAM can be used to assess SDOE to determine what the vulnerabilities of that SDOE are and what control methods have to be used.

The second bullet here, I mean, the one I've highlighted we just talked about. Right below it says leads the transition of sustainable engineering-based cyber assessment and mitigation methodology. I don't know how much you guys follow actual cyber practitioner issues, but right now in almost every case the problem with cyber has been moved all the way to the end user for the most part.

Let's look at the NRC's regulations. This is worldwide. The licensee is responsible for cyber. Period. In reality, though, cyber has to start in the design phase and be dealt with there, and then follow through. And so that makes this sustainable because it reduces the operational burden.

The TAM is efficient because it only basically touches a problem one time. You start looking for -- you do attack surface analysis. I'll go back to the -- to the aquarium. When you do the attack surface of that network, you would have found that connected thermostat and all of what was there, and you would have said, wow, this is not good.

This process identifies actual vulnerabilities. So it's not really a control catalog. Let's start with -- that will tell you you have to do all of this. It says go look for your vulnerabilities first. Spend your time doing that.

It develops what we call exploit sequences. Think of them a lot like your PRA people, like a cut set. This is all the things in this exploit sequence that has to happen to you for a result to happen. So that's the way we express it. We do control flow analysis that could help us with that.

Then we identify the most effective mitigations. So we don't use a lot of unnecessary mitigations, only the ones that have a high efficacy that can actually solve the problem.

We score, too. And by scoring the exploit difficulty, we now are able to risk-inform this because the exploit difficulty is a surrogate for a mathematical probability. It's a qualitative measure.

So if something is very difficult to exploit, then its likelihood is -- of happening is very low. If it's very easy to exploit, there's a likelihood of having very high, if I got that straight. Sometimes when I say that I get it backwards, but you get the picture.

We can leverage non-traditional methods. It's important for especially non-traditional devices. Unfortunately, a lot of cyber has its origins in IT. Well, a lot of this stuff, especially as technologically really boils and there's a lot of new stuff that kind of -- that is connected network-wise, but it's a lot different than what it was just a few years ago.

This process allows you to identify normal system features and use them as a security control. So if your fan has a lot that says when anybody makes

a change to it, or it a right-protect bit that is intended for configuration control, you can put those in the mix and say, can I leverage these for security? And take -- and use them as part of your hazard analysis and part of your mitigation strategies.

And all of these techniques really hinge around protecting-detecting and responding-recovery because sometimes detecting and recovering are more effective than absolute protection.

And for active protective measures, there has to always be detection anyway. You have to detect it, so you can act on it for active protection.

Modular -- a system is designed so it can be used by different people in different places at different times, and it can cumulatively result in the final result. This helps us with vendors. It helps us with new plant construction where they have to do certain things at certain times, and then have to wait several years before the rest of it is done. It's modular. Allows for that to happen.

See what else is here. It can be used for services as well. This model can be used -- it says anything because it's timeless, attack surface, exploit sequences, hazards, probabilities. Sound familiar? To a lot of people it is.

Risk-inform and cyber methods. Well, risk-informed cyber, we have to recognize that cyber is a qualitative thing because it involves software for the most part, so it's hard to tell you if you've got a bug or not ahead of time or what level that might be. There is also the element of the threat itself, variabilities and capabilities, intent, all that kind of thing.

So it ends up being a quantitative problem. And so this is where exploit difficulty comes into play, and it's why PRAs have a hard time. I mean, you know, anybody -- PRA person knows that if you -- you can screen a component out of certain PRAs if it has a high reliability. That's what I understand. That's what I've looked at.

Well, if you do that, possibly you haven't considered safe modes that the PRA assumed weren't there. And now that it's at the digital thing, and it has a cyber implication, it can have a hazard otherwise.

So for this, what we do is we blend -- well, I'll get to that in a minute. I was just making a point in this slide as we have to take this slightly different than your PRA, because we have to have this qualitative measure, this risk metric that is a

function of your exploit difficulty and your plant-level consequences.

You can get some plant-level consequences out of your PRA. Some. Others, like your generation risk -- and this is used for other things, so let's say your security access control system, malfunctions in that, those are from different consequences.

Consequences to your emergency preparedness posture, those are all things this thing can do that aren't part of your PRA.

MEMBER BLEY: Matt, the other people who have been here today have been talking about doing tabletops and pilot projects with licensees participating. Two questions. One is, have you done any of that? And, two, when your version comes out in November, or whenever it comes, will it have some fully worked-out examples from nuclear power plants in it?

MR. GIBSON: The answer to that is yes, in all cases.

MEMBER BLEY: Super. Look forward to seeing it.

MR. GIBSON: Let's go back to this slide. Remember, the TAM itself is two years old, or a little better. Vogtle is already doing it. So is Barakah,

and Horizon is gearing up to do it. So there is significant run time at Vogtle.

Now, in addition to that, we've done workshops with utilities, but also in the development of our HAZCADS, which I will go to next. Sandia Laboratories -- I'll get to that. Sandia Laboratories has been one of our collaborators on bringing the STPA model into this, and I'll talk a little bit about that synergy.

We did that -- for two years we have done these to try to work out the interface. So these are not -- I guess that's a good kind of point. Nearly all of this EPRI research -- sometimes we get picked on, "Oh, EPRI is slow." The reason we're slow is because we have to validate that what we're saying is good. And for high TRL, high things that we say are ready to be used by the industry, we have to have mocked them up, tried them, got pilots done.

Pilots, though, in the strictest sense, we avoid somewhat. We use structured events. Sometimes when we try to do pilots -- let's say somebody is going to do a mod, and so we'll try this out. Well, the mod takes three years before it gets through and gets installed. Well, we can't wait that long.

So we do simulations --

MEMBER BLEY: But you have had the licensees actually doing the --

MR. GIBSON: Yeah.

MEMBER BLEY: -- analysis. Okay. That's what I was after.

MR. GIBSON: Yeah. Yeah. We've had vendors doing the analysis, too. I didn't show it here, but several vendors are doing it, too.

We have a model that we use. This is sort of a universal model. Over the top you see where you develop your exploit sequences. These are your -- your different initiators. Let's put it that way. These are your vulnerabilities that caused the hazard to be actualized or your causal events.

They come across the top. Your exploit difficulties is a measure of how hard that is to achieve. Across the bottom you'll see HAZCADS used. That's your plant-level consequence analysis, and we combine those into, you know, qualitative risk. There's cut sheets, cut sets, they integrate those.

Why is this important? Because what we're trying do to is reduced the plant sensitivity to changes in the threat. Because another thing that is causing plants to be whipsawed is if somebody announces a vulnerability, what will that matter?

You've got to be able to get an answer to that question really quick, because otherwise, if you do have a problem, you fix it; if you don't have a problem, you need to ignore it -- or not ignore it, but you need to disposition it, right?

So this process allows that happen in the sense that you've pre-analyzed classes of vulnerabilities. So usually what you do is you get wind of a vulnerability. You just decide if it already fits one of the classes that you mitigated, kind of like a CCS class in a lot of ways. They have a lot of similarities. And if it does mitigate that, you're done, because you've already anticipated it and you've protected yourself.

For instance, let's say a buffer overflow. You hear about those a lot. Well, all buffer overflows are kind of alike, so if you put in mitigations for buffer overflows in general, every buffer overflow that comes out, all you have to do is do a quick check to see if it's the same as all of the other ones you anticipated, and you move on. You don't have to do an extensive analysis of it every time.

That's what we're talking about reducing sensitivity. It's the same thing with the digital in

large. The DEG looks at discovering -- and it's through its design and its hazard analysis as such -- the things that will cause a problem, the initiating issues.

The assurance methods drive the likelihood. You know, if you have something that is just having a high likelihood to occur because it has a high configurability, you'll use enhanced assurance methods.

Use HAZCADS for this, too, because you're doing your hazards analysis, and now you have a qualitative risk measure that you can use for whatever you want to use in your plant that help you judge where you stand on any of these hazards that are digital related but come into fruition.

Let's talk about HAZCADS. It's also due in December, but we've been working on it four years. This is -- this has been a hard baby to birth because we had to come up with -- these concepts we got to pretty early, but we had to do a lot of simulation and internal tabletops.

We've got new scales. Mr. Betancourt is not here, but we've got new scales, STPA risk assessments that they submitted under NDA, so we could look at them. And we use those to you know, try out

this stuff with their -- with their -- we have Korean members who are trying to use STPA as well, not necessarily HAZCADS per se but the root method here.

And we learned a lot. We learned that the STPA method, which is -- really has kind of four parts, we can get to the third part, one through three, pretty easy, because that involves modeling your hazard and getting your hazard -- hazardous actions identified.

The real problem becomes in the last phase, where you have to identify all of the causal amounts. What we find is, unless you have a specific process for a specific kind of cause you're looking for, whether that would be a cyber hazard or a CCF hazard, or whatever, it makes it really hard to do, because, you know, if you're looking at every possible causal effect, so what we see is there is, you know, a series of specialized analysis tools that you do in the fourth step that gets you to the integrate results.

And in this case, HAZCADS gets you all the way there and then it passes you off to a cyber, a common cause failure, single-point vulnerability, safety analysis, or an EMI/RFI process that has been constructed to flange up with the STPA process.

Let's see what else is good here. We integrated with fault trees because we already have fault trees in our PRAs. So what we want to do is be able to start with -- at whatever PRA information, not the probabilities, but the fault trees themselves and event trees and integrate them so that HAZCADS included all of that. So we do that. Even though we don't use the probability, we ingest that.

And HAZCADS will be one of the tools in the EPRI Phoenix tool set when it's -- it will probably in 2019 early when we do that. So every utility will have HAZCADS. They can enter this data, they can do the analysis, they can capture it and integrate it with the PRA, they can use it to inform their design.

So the DEG will get these hazards analysis through this process, or similar processes. You know, we can still readily feed PRA into it, various safety analyses, and single-point vulnerability analyses that are out there.

So we're talking about risks. And the EPRI Guide 5326, which has this long title, Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems, very -- very good report we have.

NEI has used parts of that in their NEI 1616, more deterministic parts. One of the things we realized as we moved on into doing regular -- you know, more hazard analysis research, as well as developing the DEG, is that our -- this particular document has -- suffers the same problem some of our other documents do. They are sort of a potpourri of things you can do, but it doesn't tell you what to do exactly as far as a methodology.

So one of the things we are doing, and we'll start Revision 1 of this in 2018, finish up hopefully early -- early to mid-2019, we're going to take the material in this document and we're going to shift it into a process so it can be used with the DEG.

So the revision is you will come in, you will do a hazard analysis of your system to determine what your actual hazards are, and then you be able to take your preventative and limited measures and you will be able to apply them to those hazards. No hazard, no P&L, right?

I mean, so if you have that hazard, you can apply the P&L. So the P's & L's will become not things, you just must do these things; they will become templates that help you understand how to

figure out what real P&L you have to do to actually mitigate the real hazard you have.

So most of the same material we organized. It will definitely address the risk part as far as, you know, now that you know or now that you have your P's & L's, how that hazard analysis play into your PRA and your safety analysis? And vice versa, you know.

If you have a low -- it brings this process into a degraded approach in the DEG. So if you have a low consequence device, if you have a low configurability device, small hazard surface -- let's use that word now instead of attack surface -- small hazard surface, there's less you have to do.

We are going to update some of the terminology to match IEC 61508, because it's pretty good stuff. It's used all over the world, and so it's compatible with what we do here. It's just synthesized, and it won't say do in accordance with 61508 or synthesize 65108.

I think this might be my last slide. Yep. I'm doing pretty good. You guys are -- you're incredibility quiet for whatever reason. But anyway, the -- maybe I've overwhelmed you with all of this, but I'm not sure.

One of the learnings we are getting out of

this -- and David Rahn touched on it when we talked about the seal research we're doing. We're trying not to really release a lot of preliminary data, but I will tell you that right now we've got almost -- well, last I had a good count it was a billion hours of reliability data. That might be a little bit higher than that now, maybe times two or three.

What we've had to do is sign a lot of NDAs. Our legal has been really busy. Because we've got to get the real data from the OEMs or the certifiers to find out what is going on.

Well, what we really -- the learning that is probably something really important to take away is we think instead of just generally talking about CCF, you need to split it up into three parts, because we think the platforms themselves, like if you go buy a PLC in a brown box from whatever vendor, and it's still certified, he is not going to have a problem with it.

I mean, it's being looked at, tested, and the number of installed bases of those PLCs are phenomenal. There's thousands, if not hundreds of thousands of them in the field, and they have all this data being reported back to them because they've got to keep their seal certifications up. They've got all

of that.

So if you bend the actual the likelihoods of a CCF, there is likely not going to be a problem with your platform. You're just waiting your time looking at all of the internals of that.

Where the real problem starts is when you get up into integration. That's when you hook them together. You know, Charlie mentioned about, well, what happens if somebody serially connects two trains together? Well, that happens in the integration phase when you start hooking these pieces parts up and saying -- your architecture, let's put it that way -- your architecture begins in the integration phase, and that's where your problems start.

Now, integration can be kind of the same. So there can be the same integration in a lot of places, just not as much as the actual platform. And you get the applications, and those are usually unique for that particular plant installation.

So you're likely to have -- any kind of reliability problem is likely to manifest in the integration and even more so in the application.

I'll give you a good recent example. I won't name the plant, but they put in a system that had triplicated inputs. They tested it. Great. It

did all the right stuff. They brought the plant up and the plant tripped. Now, why?

Because they got the set points wrong or the scaling wrong on all three of those triplicated inputs because they did not properly analyze the plant functions that would cause the flow or whatever to be higher than our set point. That's an application problem. That's where all of your common cause failures come in. Most, not all. But that's where the majority of them are.

And another integration -- the least amount of them are in the platform. That's what we're discovering as we do analysis on this. So I thought we'd share it with you during this. Even your analog systems, the key common cause failure there is you make a mistake in your set point calculation, and you put the same one in every one of them, and they're all bad, common cause failure.

But it had nothing to do with the system. It had to do with the human above that, right? So your common cause failures for any systems start at application, most likely, come down, platform, least likely. At least that's what the data we're looking at seems to indicate.

Questions?

CHAIR BROWN: Don't look at me for questions.

MR. GIBSON: Well, Charlie, come on, man. I wanted love from your today. And I didn't get -- come on.

(Laughter.)

CHAIR BROWN: I'm still trying to figure out how you're going to apply this for the circumstances which we've dealt with. And I saw the academic approach. I don't -- that's the wrong word from the systems engineering that I was struggling trying to figure out how I was going to apply this to the application of -- that the NRC is dealing with for the commercial -- how do I program this into and utilize it to pull up and evaluate some commercially certified device, you know, for them to use?

You know, how -- I mean, you've got all this data, but how -- they are sitting over here, and they're waiting for somebody to say, "Hey, we're going to go use this." How do you get it -- that certified -- certification?

MR. GIBSON: Well, David mentioned our research in seal, which is not really what I've been talking about, but, you know, we can digress into that.

The objective of research is to see if you can. But, remember, we're not done with that research. It could turn out that you can't. And if it is, we'll say that. But our premise is that the -- if you want to commoditize safety-related stuff in nuclear, you have to look really hard at how it has been commoditized in other safety industries, like petro chemical, transportation, because they do. They combine safety-related stuff out a catalog from multiple vendors at competitive prices.

Platforms. They still have to do the integration. They still have to do applications. So what we're aiming for here is to see if the certifications issued by these accredited certifiers, which they have the safety plan and the analysis of all of the 61508 parameters, which are very extensive, many of them are systematic in nature, cover actually in better detail than what we do in nuclear actually once you -- I challenge you to go get 61508, read it cover to cover, and then we can have a long discussion.

But the point being is if you're certified to that, well, yeah, but, you know, let's figure out how we get -- books on tape maybe. Oh, I know what -- I'll narrate for you. How about that?

(Laughter.)

MR. GIBSON: But, anyway, the -- what you get out of that especially is all the effort of people worldwide, because everybody is using this kind of technology for things that kill people immediately. Real bodies going to the morgue, right?

So a lot of them are betting their entire companies on this, on these things. Their insurance companies, which is another interesting thing, a lot of these people who use these systems have to be insured by private insurers, and the insurers are taking hard looks at the effectiveness of these programs.

Can we harvest that, right, that ecosystem, so that you can out and buy these seal-certified things and use them, and the thing that you would do with that -- it's at a platform level. The thing you do at that point is ensure that the functional capabilities of that system are what you want. I mean, does it scan, does it respond in the times you want?

Remember, the seal certification certifies that it will do what it says it does. You have to decide if what it says it does is what you really want, and that's the next level, integration in an

application.

Well, if you can get a seal-certified device, how much more looking at it do you really want to do? You need to figure that out, if that's possible. Because that really cuts the cost and time, both for the utilities, the vendors, and the regulator in reviewing these things.

So we're working on that. We're -- we've got a whole host of questions from the staff because we asked them, which is our normal custom, what technical problems do you need us to look at that would make this viable? And we're busily trying to figure that out.

We're integrating with the certifiers, we're looking at how they do things, we're looking at how they themselves are accredited, you know, who accredits them, how often are they audited.

You know, so then we're trying to correlate the systematic quality methods that they certify with the actual reliabilities they achieve. That's the process. So at the end of the day, we can prove that. We'll publish that report, and then the industry will have to make a decision about if that's something they can -- they can live with.

No, not this one. This is a separate

report. Let's not conflate the sealed one with the DEG. DEG is an implementation thing. So let's say, for instance, the separate report we're talking about that David mentioned earlier, and seals, is -- we can come back and talk about that sometime at length if you'd like.

Saying it turns out this way proves that you can buy safety-related platform components off the shelf at various level of capability, including what you call EEDs, use them by checking their certifications and looking at their -- the paperwork that comes with them that has already been third-party certified, and using them and now concentrate on your integration and your application. And that's where you need to spend all your time. We think that might turn out. If it does, that's what that will be.

Now, if you were -- if that were to become to be the case, then in the DEG process you could go through that and use your requirements to make a black box. And you could have a complete design without picking the hardware. As long as you bounded the requirements for the hardware, you then pick it and install it at any point, and that really helps people who have long design cycles. They can design it and then they can pick the hardware right at the end.

And in 10 or 15 years when that equipment is obsolete, they can replace it with another seal-certified device that meets those same requirements, or they can go through a process of updating their requirements and other things and using that.

CHAIR BROWN: Well, you don't have to convince me. You have to convince the people who are going to use it.

MR. GIBSON: Of course.

CHAIR BROWN: So let me go -- let me see, where am I? I forgot where I am in the process. Comments from the room, and then I've got to go to the phone, and then I'll do us in the -- and Myron. Is there anybody back here who would like to make any comments so far, anything from the entire day?

Hearing none -- it would be nice if I had my microphone on. I'll say this again. You couldn't hear me. I take it the answer is no. Is there anybody -- hold on a minute.

DR. HECHT: Charlie, can I ask a question?

CHAIR BROWN: Go ahead and do it because I'm heading off to get the public comment here in a second. So go ahead.

DR. HECHT: Okay. Yeah. I heard that. I wasn't quite sure if the timing was appropriate.

CHAIR BROWN: That's fine.

DR. HECHT: With respect to this last slide, I just wanted to say that I've seen something similar, or we've seen something similar, when you talk about defense systems and talk about, really, a large amount of --

CHAIR BROWN: Myron? Myron, Myron.

DR. HECHT: Yeah.

CHAIR BROWN: There is more static than I can shake a stick at on your phone line. Are you on a speaker or on a handset?

DR. HECHT: No, I'm on a handset. I'm on a handset.

MEMBER MARCH-LEUBA: Can you put the previous slide on?

CHAIR BROWN: Are you talking about the green triangles? Yeah.

MEMBER MARCH-LEUBA: Myron, can you start from the beginning? We couldn't hear you very well.

CHAIR BROWN: Yes. Speak softly.

DR. HECHT: Okay. Is this better?

MEMBER MARCH-LEUBA: Yes.

CHAIR BROWN: Keep trying. Yeah, go ahead.

DR. HECHT: Okay. So I guess if I speak

softly then it comes through.

CHAIR BROWN: Maybe.

DR. HECHT: Is that correct?

CHAIR BROWN: It's very crackly. So just go ahead and give it a shot.

DR. HECHT: Okay. I wanted to point out that the integration area is causing a lot of the problems and something that we have seen. However, this also -- and I think we've seen it in the defense industry.

It's also a function of how complex the platform is. Do you have any data on that?

MR. GIBSON: So our configurability metric is -- if we have data, I mean, it's not like I have, you know, billions of megabytes of it, but when we -- when we looked at system -- the characteristics of system complexity and we -- we've tried to stay away from more complexity because it has too many meanings.

So we looked at the different characteristics that would indicate complexity, like number of interfaces, number of configuration parameters, use of high-level languages, you know how many -- is this thing capable of being programmed to do cat videos, or is it constrained to only doing one

thing? Those are the characteristics of complexity that we looked at to come up with the configurability metric.

And so we think that captures this complexity, and so the amount of -- the amount of effort, let's say, that you put into it proportionalizes to that.

So I don't know if that answers your question, but that's how we approached it here. We did that through analyzing systems and, you know, getting input from different places. You know, it's not like we, you know, have a big database of data. So that -- did that help with how that came out?

DR. HECHT: Okay. So what you're saying is that's the more complex the integration platform, the more errors you found.

MR. GIBSON: Yeah. Yeah.

DR. HECHT: Okay.

MR. GIBSON: Well, the more integration, the platform itself tends to be highly reliable because, like this diagram is saying, the platform itself, the component -- platform components, in their normal way of being configured, are normally very high-volume commodity items, even for safety. I mean, not as high as cell phone, but, you know, there's

thousands -- not tens of thousands in the field. They've got error reporting and all of that.

We don't see -- we don't see problems with the platforms. We see problems starting with the integration, people hook them up wrong, they make different -- bad decisions about their architectures, about, you know, segmentation and isolation, all of that. And then they start having problems.

And also, they take a platform and can make it complex. For instance, typically you buy a platform in a nuclear plant, you might buy a platform and turn it into a two- or three- or four-train super-system, right? But what you really bought is three or four platforms and hooked them together in some way at the integration level.

You integrated those platforms together, and then you put applications on it. When you do that, that's when your complexities begin. I mean, your -- like the English would say, the bespoke things that you do that are customized start at the integration level, because the software that is in the platform, the libraries and operating systems and things like that, have high commodity reliability, if you will.

The ones that when you get into

integration, that's when people start making mistakes. They've only done -- they've only done it a few times. They have not tested it fully, blah, blah, blah. They have not done a hazard analysis on it. You know, they don't know what it could do, what it's hooked it. Then, finally, the applications are even worse because that's where you get your bugs, like programming all three trains of something with a bad set point. That's when that happens.

DR. HECHT: Thank you. If I could ask one more question on the DEG in general. Have you attempted to align it with the NRC requirements, the SRP or the ISG or the RIS 2002-22 Supplement work?

MR. GIBSON: No.

CHAIR BROWN: Very straightforward answer.

DR. HECHT: Okay.

MR. GIBSON: But -- I do have to leave a but. What we do try to do is, remember, what we're trying to as an independent organization is do independent thought, right? It's hard to do independent thought if you're trying to make your research match something that already exists, because you have no opportunity to move the needle further down the road, right?

What we do, however, do is we look at how

this would be used to meet regulation-level requirements, so like 603 and things like that, and we think it's in pretty good shape. When you get like say -- BTP 7-14, or whatever it is, or 19, let's say 14, too, I mean, it has a waterfall method.

Clearly, you know, we're not doing a waterfall method, but that's staff guidance. That's not in the regulation. So why wouldn't what we're saying work better if everybody else in the plant is using it already, right? See that's the kind of thing we're facing here.

So, you know, we -- we try to make sure it works because our members wouldn't want us to create something that would be entirely undoable, right? But at the same time, it has to -- it has to be technically sound.

DR. HECHT: Okay. All right. Thank you.

CHAIR BROWN: Okay? All right. Thanks, Myron.

I've finished with the audience. Is -- the public phone line is open. Would somebody say something? It's supposed to be open. Cathy? I thought it was open. I'll try this again. Is there anyone on the public phone line? If so, please say something.

PARTICIPANT: I can hear you.

CHAIR BROWN: Okay. Does anyone on the phone line have a comment that they would like to make? Okay. Hearing none, Cathy, you can close the phone line. I'll go around -- oh, would you like to say something? Raise your hand. Stand up. Don't forget to give your name.

MR. BIRLA: Sushil Birla, technical advisor in the NRC. Charlie, you asked earlier -- you made a comment earlier that the thing that Matt presented seemed to be a theoretical framework.

CHAIR BROWN: I've lost that one. That was back in the very beginning. Oh, that Matt --

MR. BIRLA: Yeah.

CHAIR BROWN: Oh, that Matt -- oh. That's the way it -- that's the way it came -- that's my understanding based on -- as he went through the slides. It seemed to be more of a theoretical framework to get to something.

MR. BIRLA: So, Matt, can you tell them about the early -- I wouldn't -- we called it pilots, but you've done some testing of the systems engineering process.

MR. GIBSON: Well, you know, I have another life before I went to EPRI, so I've used this

method extensively in my own practice as a control engineer in power plants.

I mean, everybody, it's not theoretical. You phone is built this way. Your car is built this way. Your plane is built this way. We just copy whatever people are doing. It's not really rocket science or theoretical.

MR. BIRLA: Yeah. The defense industry uses that process quite a bit. Most of the data, too, is based on it. And it integrates hazard analysis, and the hazard analysis approach he is talking about has been used in other industries. Plus, that EPRI report of 2015, there are some plant test cases in there, too. So not all that theoretical.

CHAIR BROWN: Okay. Well, that's -- we're out of the public comments, since you're a member of the NRC right now. But, fundamentally, you're just providing us some data of what is available for the staff and others to use.

MR. GIBSON: Exactly. That's what I --

CHAIR BROWN: So we appreciate that particular approach to doing things to see what people are thinking about using. I didn't mean to imply -- maybe I did mean to imply -- it appeared theoretical to me, because I have not -- it has been about 20

years since I had anybody look at something from a systems engineering standpoint, because I have been out separately, not in an organization where we did that.

But the -- I guess my only thought was that if it would have come across -- and he pointed that you all had done some work. I didn't see any specific example where you walked your way through applying the process and coming out with some conclusions.

You made a statement that the platforms are reliable because they're reliable that there was -- you have a lot of data. Well, whatever that is. So I have mixed feelings on platforms. Little platforms, if you want to call them that, you're just taking small devices to say run a chiller as opposed to a bigger platform that is used -- to be used in a reactor trip or safeguards train in a division are different.

MR. GIBSON: They are.

CHAIR BROWN: And they -- they bring far more data in, and they utilize far more complex algorithms, which then require certain additional things that you do in your programming to ensure that you stay on track as you process it.

So there is a wide range of what you call platforms, as you would refer to them. So I don't know, fundamentally, I appreciate the -- you know, the presentation, just to see what is potentially useable. You really have to get to the folks who want to use it, so that the information can be presented to us that that's how they're doing stuff and why it works.

MR. GIBSON: We do. And part of our MOU is we provide training or workshops for research and whatever, you know, regulatory staff, and we'll do that for this, too. Our TAM, as was mentioned earlier, you know, we came and gave them the staff workshop training on that, so they understand it fully. We'll do it for this, too. Just to further what you're saying, I mean, so people understand what these are and how they work.

CHAIR BROWN: Okay. All right. Now let me go -- let me finish the closeout process here. Ron, I'll start with you.

MEMBER BALLINGER: Thank you. This is not my area, so I have to spend a lot of time doing a lot of reading. So this is my I think fifth or sixth time around, so I actually understand a number of what you're saying. So I appreciated the presentation a lot.

By the way, if you don't want to spend 3,500 bucks on IEC 61508, there is an article called An Introduction to Functional Safety and IEC 61508, which you can read and come up to speed on this in a hurry. I found it last night. So I don't have 3,500 bucks and I'm not going to spend 3,500 bucks.

(Laughter.)

MEMBER BALLINGER: For one lousy CD, $3,500.

MR. GIBSON: We're talking about a multi-billion dollar --

CHAIR BROWN: I just -- this is our resident expert on finding obscure references to things we can look at.

MEMBER BALLINGER; It wasn't very obscure.

CHAIR BROWN: Matt?

MEMBER SUNSERI: Thanks to everyone for their presentations, the staff, NEI, EPRI, very high level of detail. So I -- my comments are that I believe the level of safety that we will achieve will depend on the applicants' and licensees' ability to do the sort of things that we have heard about today. So I will be very interested to see the results of some of these what I'll call tabletop, pilot, implementation kind of activities that are going on to

see exactly how effectively people can do these things that we're asking them, because I know we said that there has been some experience doing it in commercial industries, but not commercial nuclear industry, as I understand.

So, you know, look forward to those results because at the end of the day we need something that is better, not just different, than what we are currently doing.

Thank you.

CHAIR BROWN: Okay. Jose?

MEMBER MARCH-LEUBA: Yeah. I do have an opinion on this one.

CHAIR BROWN: Which one, the whole meeting or on the --

MEMBER MARCH-LEUBA: Oh this topic as opposed to people that claim not to know anything about it.

CHAIR BROWN: The EPRI -- the presentation we just had.

MEMBER MARCH-LEUBA: Yes.

CHAIR BROWN: Yeah. Okay. Thank you.

MEMBER MARCH-LEUBA: So, number one, I want to separate two topics. First, cybersecurity, separate it completely from performance.

Cybersecurity is extremely important. We are under attack by professional actors that are a lot smarter than I am and that you guys are. And so you have to assume that the guys that are doing the attack know 100 times more than you do, so cybersecurity is not part of my next comment. This has to be taken seriously.

With respect to the performance of plant protection systems and controls, flying at 40,000 feet, I think that we are doing it. I think that we are grossly overdoing it. There has to be a simpler way to get this thing done.

Two, software fails. I write software for a living, and I know my software fails all the time. But how here it fails catastrophically, and I think we are making the -- perfection the enemy of the good enough. And we should be able to install digital controllers on chillers with having to go through a three-year review.

And so, basically, the bottom line is on performance-based plant protection systems and on controllers, my impression is we are overdoing it. There should be a simpler way of doing -- of getting this done.

CHAIR BROWN: Thank you. Joy?

MEMBER REMPE: No additional comments, but thanks for the presentations.

CHAIR BROWN: Vesna?

MEMBER DIMITRIJEVIC: I have -- thanks for presentation, first. It was -- there was so much material, and I had also a feeling when I was listening to your presentation, that it is sort of theoretical.

But you said to Dennis' questions that you have some examples for applications, and they will be included in the guide.

So I noticed through your presentation that you listed that for this TAM, or technical assessment methodology, that utility adapters at Vogtle 3 and 4 and United Arab Emirates, Barakah, right, those are -- do we have as bad examples from the operating plants in United States which you are going to present as examples? What are the examples you are going to include in the guide?

MR. GIBSON: The examples in the guide are examples on actually doing it. All right? So it's not going to say XYZ plant did this or, you know, whatever. It will walk you through actually an example of how you would do it, a worked example. Let's look at it that way.

The things I saw you -- showed you the examples that we did in the DEG have all been done at utilities during our workshops. Every one of those are actual real-world examples of real people's mods that we went out in the field and did with the DEG and went through it with the licensees with a real mod -- those are all real mods -- and come out with these results and it captured, you know, lessons learned from that.

So those things -- kind of things will be in the DEG as worked examples.

MEMBER DIMITRIJEVIC: So then EPRI will be able to see like the risk-informed cybersecurity or common cause or something like that? Because I, as a PRA practitioner, I will be very curious to see something like that, you know, maybe these risk metrics apply to this graded approach. I mean --

MR. GIBSON: So to be clear, when the TAM Revision 1 comes out, you will be seeing a worked example about using your -- any kind of risk metric you have to combine -- excuse me, consequence metric you have to combine it with the exploit difficulty. Remember we talked about exploit difficulty? Well, the TAM itself develops the exploit difficulty. It says here is kind of how likely this is to happen

based on how hard it is to do.

So you can take that as a worked example, and it will give you an example of a couple of other sort of consequence processes that tell you what the consequence will be.

HAZCADS, which won't be out until November, will also have examples about how to use that with cyber, CCF, and the rest of them. So there will be worked examples in these to show you that. But they are -- they're not all one product. I mean, you know, they're integrated but they're not all one product. But you will have worked examples in them that you yourself could do if you wanted to. We'll even train you if you want.

MEMBER DIMITRIJEVIC: Well, that would be really curious, and I would be curiously looking -- to look at these examples. I really -- I really understand the limitations of the PRA, the existing plans to be applied for something like that, and I also with a pleasure listened to the Jose example on the aquarium.

It would be very difficult to have this well-designed theoretical process actually happened to identify such a vulnerability. So I think the examples would be very useful in this process.

MR. GIBSON: So, as a matter of fact, the HAZCADS, which we already have grasp of, we're working -- we've had some late-breaking things we want to reintegrate into it, so it will be, you know, a couple of months -- well, a month or so probably before we're ready to do widespread graphs of these.

But it has worked examples. We took a feedwater control system at an unnamed plant, and we did -- fully did it. We also took at Sandia the system that they use to do their cyber plant --

MEMBER DIMITRIJEVIC: So a fully designed --

MR. GIBSON: -- fully did the HAZCADS process on and got results. So we used something -- we did those two in our worked examples and they're in a document now. So --

MEMBER DIMITRIJEVIC: Just have to wait and see. You said it will be out in November, right?

MR. GIBSON: I won't pretend that this stuff is not cutting edge from a nuclear point of view. It is used by other people, and part of what our research says is these modern techniques really can have a place in how we solve these problems if we're willing to, you know, have an open mind and figure out how to do them.

There is also the element of training and retraining utility and vendor staff to the extent that we use them. At some point -- and we've got to look at the elephant in the room on that some, too. Because these other -- right now, if we go this way, we can go to aerospace and other industries and petrochemical and hire people that already know how to do this, really. I mean, would just come and say, "Oh, yeah, I've seen this before. Let's just get busy with it." Because they do it all the time.

The existing utility engineers, though, are going -- this is going to be a lift for them. I mean, it will be.

MEMBER DIMITRIJEVIC: Well, I can see one of the very successful risk-informed applications in the new plants, which is the risk-informed ISI, and their matrix looks exactly like yours. I mean, the high, you know, division.

However, my -- I am very clear what are the, you know, consequences there, because they come from the PRA and core damage, and I am very clear about likelihood is there, because it's associated with pipe failure probability and degradation. In this matrix, I have a very tough time understanding likelihood versus consequences because they are not

really precisely defined.

MR. GIBSON: Well, there is more precision in the actual documents. So when they actually come out, you -- you know, you can examine a copy, and we would welcome your technical feedback on it, actually.

MEMBER DIMITRIJEVIC: All right. Thank you.

CHAIR BROWN: Jose?

MEMBER MARCH-LEUBA: Thank you. I forgot something because it came from this morning, and it has been a long day. I wanted to mention something else about this performance-based requirement that came from the -- from the Commissioners. Maybe we need to write something on our letter about it.

CHAIR BROWN: Well, we're not writing a letter. This is an information brief.

MEMBER MARCH-LEUBA: But we will eventually have a letter.

CHAIR BROWN: I have no idea.

MEMBER MARCH-LEUBA: We will. The IAP -- we will. If not, we can always write a letter without having to agree.

CHAIR BROWN: We can always do that, but right now there is -- the IAP changes, is a living document. It is very much living right now.

MEMBER MARCH-LEUBA: Okay. Performance-based is a really good goal. But when you think about all the problems we're getting into, most of them get solved by redundancy, diversity, and throw in a little defense-in-depth for good measure.

CHAIR BROWN: Exactly.

MEMBER MARCH-LEUBA: So if you have a diverse system, and in one of them your software fails, you still have the other one. It is very difficult to postulate random failures of system in two diverse systems.

And that really solves a lot of your problems. So even though it's a good goal to have performance-based, let's not forget -- I mean, let's impose a requirement, redundancy, diversity, and a little defense-in-depth. And that will solve most of the problems, will simplify the reviews, will simplify everybody, and everybody will be happy because you can actually get things done. If you want to make it perfect, you just won't get it done.

Thank you.

CHAIR BROWN: Very useful. Thank you. No, I appreciate that.

Okay. Having exhausted comments from our exalted member base, I would like to thank the staff

for very engaging interactions today. I thought they were -- the discussions on the IAP and the discussions on what we mean by this, that, and the other thing were very productive. And the back and forth on many of these issues I think was useful for everybody in -- over the long term.

So, and I thought the staff did a very good job of doing that, and explaining and getting some of the points across as to where you were going.

I personally do understand the complexity of what you're dealing with. This is -- I'm like Jose in many, many ways. I do -- although he would probably like to reject that comment, I totally agree with him. We have got a process in place that works today, has produced systems that have not generated adverse consequences.

I can't think you can point to any of the specific bad occurrences that we have had over the last 60-something years and postulate that it was because of our methods and the systems we have put in place to protect the plants. So I -- when I made the comment about throwing the baby out with the bathwater, I was -- that was not just throwing the words out. That is very heartfelt.

I agree totally with Jose relative to when

you have systems where you are redundant, you are independent, you have diverse systems that are backing up stuff, that it's really hard to postulate anything.

I had one common cause -- potential common cause failure in my 35 years in the naval nuclear program with a relay, where the manufacturer actually -- the relays would stick after a while if they were in a warm environment inside of a cabinet.

There were at least 15 or 20 of these in every one of about 50 cabinets. And in operation over 20 years, we had one of them stick because they didn't clean the iron after they annealed it -- or quenched it, rather.

And so it had a little residue and the armatures would not come off, and something would happen that I'm not going to talk about that was very untimely. It only happened once, and it was a very -- once we found the cause, it could have been brutal. But we never had two of them fail at the same time.

So common cause failures, you have to look at them, but you have to not beat yourself to death over them also, and that's -- I totally agree with. I think we've gone -- we're really working it overtime in some circumstances, maybe in most circumstances.

Anyway, that's my final thought. I was

1 going to go ahead and we will adjourn the meeting.

2 (Whereupon, the above-entitled matter went

3 off the record at 3:24 p.m.)

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

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

Integrated Action Plan for the Modernization of the NRC's Digital I&C Regulatory Infrastructure

Staff Briefing to the Advisory Committee on Reactor Safeguards Digital Instrumentation and Control Systems Subcommittee

June 20, 2018

Discussion Topics

- Key Messages
- Commission Direction
- Integrated Action Plan (IAP) Strategy for Digital I&C Modernization
- MP #1 - Protection Against Common Cause Failures (CCF)
- MP #2 - Considering DI&C in accordance with 10 CFR 50.59
- MP #3 - Acceptance of of Digital Equipment
- MP #4 - Assessment for Modernization of the I&C Regulatory Infrastructure

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

Key Messages

- Making progress on Integrated Action Plan (IAP) activities
- Focused on developing regulatory products to support near-term upgrade needs identified by industry
- First implementable result targets safety-related upgrades under 10 CFR 50.59 (i.e., RIS supplement)
- Next priority is revised licensing process (ISG-06)
- Staff will continue to pursue broader modernization efforts (initiated in October 2017)

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

Commission Direction on Digital I&C

(SRM-SECY-15-0106 & SRM-SECY-16-0070)

- Develop an integrated strategy under the oversight of a senior management steering committee to modernize the DI&C regulatory infrastructure
- Engage stakeholders to identify common priorities, problems, and potential solutions to address them
- New or revised requirements should be performance-based, rather than prescriptive
- Focus on acceptable approaches to comply with the requirements
- Requirements should be technology-neutral; Guidance for specific technologies should be tailored if necessary
- Same requirements should apply for operating and new reactors
- Evaluate potential policy issues; present any issues that are ripe for consideration to Commission prior to any rulemaking

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

IAP Strategy for DI&C Modernization

- Objective: Modernize the digital I&C regulatory infrastructure to enhance the NRC's capability to be more timely, efficient and effective in ensuring safety, and provide a consistent and predictable regulatory process
  - Tactical - Continue to prioritize and implement the regulatory activities needed to provide regulatory clarity and support industry confidence to perform digital I&C upgrades (MPs #1-3 and MP #4A)
  - Strategic - Assess and implement broader modernization of regulatory infrastructure (MP #4B)

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

Modernization Plans

- **Modernization Plan (MP) #1 – Protection against Common Cause Failure**
  - MP #1A – Regulatory Issue Summary (RIS) 2002-22, Supplement 1
  - MP #1B – Review of NEI 16-16
  - MP #1C – Implementing Commission Policy on Protection against CCF in DI&C Systems
- **MP #2 – Considering Digital Instrumentation & Controls in Accordance with 10 CFR 50.59**
- **MP #3 – Acceptance of Digital Equipment (Commercial Grade Dedication)**
- **MP #4 – Assessment for Modernization of the Instrumentation & Controls Regulatory Infrastructure**
  - MP #4A – ISG-06 Revision
  - MP #4B – Broader Modernization Activities

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

IAP Milestones

- SRM Issued October 15, 2016
- Revisions 0 and 1 to IAP prepared Fall of 2016 through Spring 2017
- First ACRS IAP briefing was on May 17, 2017
- Annual Update Paper per SRM--October, 2017
- Revision 2 to IAP—Issued Jan 2018
- Revision 3 Version being prepared now—Scheduled for Sept 2018

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

Revision 2 of IAP

(Collective changes since May 2017 ACRS meeting)

- Primarily updated schedules for each of the Modernization Plans
- Adjusted to reflect continued work on RIS 2002-22, Supplement 1
- Adjusted to reflect development of an update to ISG-06
- Described progress on new Appendix D to NEI 96-07
- Outlined in greater detail the development longer-term activities

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

Plans for Revision 3

- Potential Updates & Changes
  - Continue follow-up activities associated with RIS and ISG-06 (training, workshops, public comments)
  - Continue work on Appendix D, NEI 16-16 and Commercial Grade Dedication
  - Define longer-term activities beyond MPs #1-3
    - Transformation Paper initiatives (SECY-18-0060)
    - Advanced Reactor Framework
    - Outline Proposed Research Activities

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

IAP Schedule

- Stakeholder Meetings: July/August 2018
- Issue Revision 3 to IAP: September 2018
- Annual Commission Paper: October 2018
- Commission Meeting: October 2018

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

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

MP #1 Protection Against Common Cause Failure

Mauricio Gutierrez RES/DE/ICEEB
Dinesh Taneja NRO/DEI/ICE
Rossnyev Alvarado NRR/DE/EICB

Advisory Committee on Reactor Safeguards
DI&C Subcommittee Briefing
June 20, 2018

Key CCF Activities

- **MP #1A** – RIS 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute (NEI) Guidance in Designing Digital Upgrades in Instrumentation and Controls Systems"

- **MP #1B** – Review of NEI 16-16, "Guidance for Addressing Digital Common Cause Failure"

- **MP #1C** – Implementing Commission policy on protection against CCF in DI&C systems

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

RIS 2002-22, Supplement 1 Purpose and Scope

- Clarifies NRC's previous endorsement of NEI 01-01 for 10 CFR 50.59 upgrades
- Clarifies the use of qualitative assessments used to determine that CCF is sufficiently low
- "Sufficiently low" is based on assessing design attributes, quality of the design process and operating experience
- Not applicable to major Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) upgrades

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

NEI 16-16 - Purpose and Scope

- Originated in support of industry response to NRC's activities on Protection Against Common Cause Failure
- NEI 16-16 provides engineering guidance for industry to address CCF concerns. The guidance includes defensive measures that can be credited to address CCF, in addition to those in the current NRC guidance (i.e., branch technical position (BTP) 7-19) for both operating and new plants
- Based in part on the design measures in Electric Power Research Institute (EPRI) Technical Report (TR)-3002005326, "Methods for Assuring Safety and Dependability when Applying DI&C Systems"

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

Implementing Commission Policy on CCF in DI&C

- Staff will update guidance documents to ensure the Commission policy in SRM/SECY-93-087 continues to be consistently applied and addresses evolving DI&C technologies
- Staff is not proposing nor requesting a change to Commission policy
- Staff is developing a Commission Information SECY on future improvement efforts in addressing CCF

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

Updating Guiding Principles

- Licensees and applicants should continue to address CCFs due to software
- A D3 analysis for reactor trip system and ESFAS to address CCF concerns continues to be required. This analysis can be either a best estimate (i.e., using realistic assumptions) or a design basis analysis
- Clarify the use of a graded approach for a D3 analysis for less safety critical systems
- Clarify the use of alternate means to address CCF concerns
- Clarify the use of certain design attributes to address CCF concerns

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

Next Steps

- Hold stakeholder interactions

- Apply staff clarifications in all activities for regulatory guidance and endorsement activities
  - RIS 2002-22 supplement for 50.59 Issued
  - Standard Review Plan (SRP) and/or BTP 7-19 update
  - Review of future industry guidance (e.g., NEI 16-16)

- Provide Info SECY to Commission (August 2018)

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

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

MP #2– Review of the Proposed Appendix D to NEI 96-07

Tekia Govan, NRR/DIRS/IRGB
Harold Chernoff, NRR/DIRS/IRGB

Advisory Committee on Reactor Safeguards
DI&C Subcommittee Briefing
June 20, 2018

Proposed Appendix D to NEI 96-07

Purpose and Scope

- Intended to provide guidance for licensees to perform 10 CFR 50.59 reviews of activities involving digital modifications

Status and Next Steps

- Appendix D work was delayed, by mutual agreement with NEI, until the issuance of RIS 2002-22, Supplement 1
- Category 2 public meeting with NEI to discuss review topics and status – June 26, 2018

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

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

MP #3– Acceptance of Digital Equipment

Dinesh Taneja, NRO/DEI/ICE
David Rahn, NRR/DE/EICB
Acting Branch Chiefs

Advisory Committee on Reactor Safeguards
DI&C Subcommittee Briefing
June 20, 2018

Acceptance of Digital Equipment Purpose and Scope

- Improved guidance for acceptance of commercial grade digital equipment for safety-related applications
- Evaluate use of Safety Integrity Level (SIL) certification per IEC – 61508 data to supplement commercial grade dedication (CGD) of digital equipment per 10 CFR 50 Part 21
- NEI to submit guidance document for NRC endorsement based on EPRI research on Safety Integrity Level (SIL) certification process to credit identification and validation of dependability characteristics of digital equipment

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

Acceptance of Digital Equipment Overview

- NEI has asked EPRI to research the SIL certification process and 3rd party certification entities
- NEI has initiated drafting NEI 17-06, a guidance document for acceptance of digital equipment for NRC endorsement
- NRC is actively participating in this task by performing informal acceptance review of the draft NEI 17-06
- NRC will initiate formal review of NEI 17-06 upon submittal for endorsement, which will include audits and inspections of 3rd party SIL certifying entities

Acceptance of Digital Equipment Status and Next Steps

NEI expects EPRI to complete research	4th Quarter CY 2018
NEI to share interim EPRI research results	July 2018
Submit NEI 17-06, Rev. 0 for NRC endorsement	1st Quarter CY 2019
NRC initiates review of NEI 17-06 and related audits and inspections	1st Quarter CY 2019

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

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

MP #4A– Draft ISG-06, "Licensing Process" Revision 2

Samir Darbali, NRR/DE/EICB
Richard Stattel, NRR/DE/EICB
Deanna Zhang, NRO/DEI/ICE

Advisory Committee on Reactor Safeguards
DI&C Subcommittee Briefing
June 20, 2018

ACRS Subcommittee Briefing

(May 17, 2018)

- The staff briefed the ACRS DI&C Subcommittee on:
  - Purpose and Scope of Interim Staff Guidance (ISG)-06
  - Lessons learned from using ISG-06, Revision 1
  - The Review Processes in Revision 2
  - How the Tier 1, 2, 3 Review Process compares to the new Alternate Review Process
  - Next steps

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

ACRS Subcommittee Briefing (Cont'd)
(May 17, 2018)

- The Subcommittee provided verbal feedback to the staff. The main comments focused on:
  - How System Architecture and the Fundamental Design Principles are addressed on the Tier 1, 2, 3 Review Process

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

ISG-06 Purpose and Scope

- Defines the licensing process used to support the review of licensee amendment requests (LARs) associated with safety-related DI&C equipment modifications in operating plants and in new plants once they become operational
- Provides guidance for activities performed before LAR submittal and during LAR review. The NRC staff uses the process described in the ISG to evaluate compliance with NRC regulations
- ISG-06 makes reference to, and is to be used in conjunction with SRP Chapter 7

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

ISG-06 Rev. 1 – Lessons Learned and Industry Feedback

- ISG-06, Rev. 1 has been used to review the Diablo Canyon Plant Protection System DI&C LAR (ADAMS Accession No. ML16139A008), the Hope Creek Power Range Neutron Monitoring System LAR (ADAMS Accession No. ML17216A022), and DI&C topical report reviews.
- The concepts of tier labels and review phases are useful
- The "one-stop shop" approach of Revision 1 created challenges:
  - Duplication of SRP Chapter 7, Institute of Electrical and Electronic Engineers (IEEE) Std 603 and IEEE Std 7-4.3.2 guidance
  - References to Regulatory Guides and other documents became outdated
  - Revision 1 focused more on specific documents, instead of the information needed to make the required regulatory findings

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

ISG-06 Rev. 1 – Lessons Learned and Industry Feedback (Cont.)

- The Tier 1, 2 and 3 Review Process could be further improved/streamlined
- Industry has expressed concerns with ISG-06, Rev. 1:
  - Significant resources are required for procuring, developing, and testing a full digital I&C design <u>before</u> the license amendment is issued
  - Several review criteria topical areas were repetitive
- Staff lessons learned, and industry feedback on Rev. 1 informed the development of ISG-06, Rev. 2

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

ISG-06 Revision 1 .vs. Draft Revision 2

- Both ISG-06 **Revision 1** and **Revision 2** include a Tier 1, 2, 3 Review Process, which focuses on:
  - Use of a Pre-Approved Platform Topical Report
  - System Description and System Architecture
  - Review of Software Design, Implementation and Test Plans and Processes
  - Review of Implementation and Test Results Information

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

ISG-06 Revision 1 .vs. Draft Revision 2 (Cont'd)

- ISG-06 **Revision 2** introduces an Alternate Review Process, which focuses on:
  - Use of a Pre-Approved Platform Topical Report
  - System Description and System Architecture
  - Review of Software Design, Implementation and Test Plans and Processes
  - *The Implementation and Test Results Information will be subject to inspection*

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

Characteristics of a LAR Using the Alternate Review Process

- The LAR would provide the necessary and sufficient design information to demonstrate regulatory compliance
- The LAR would describe the licensee's Vendor Oversight Plan that ensures the vendor executes the project consistent with the LAR and the requirements of the 2015 version of NQA 1, Part II Subpart 2.7 on Quality Assurance Requirements for Computer Software for Nuclear Facility Applications
- The LAR would include appropriate commitments to complete plant specific actions that are included in the referenced topical report
- The LAR would include appropriate commitments to complete lifecycle activities under the licensee's quality assurance (QA) program

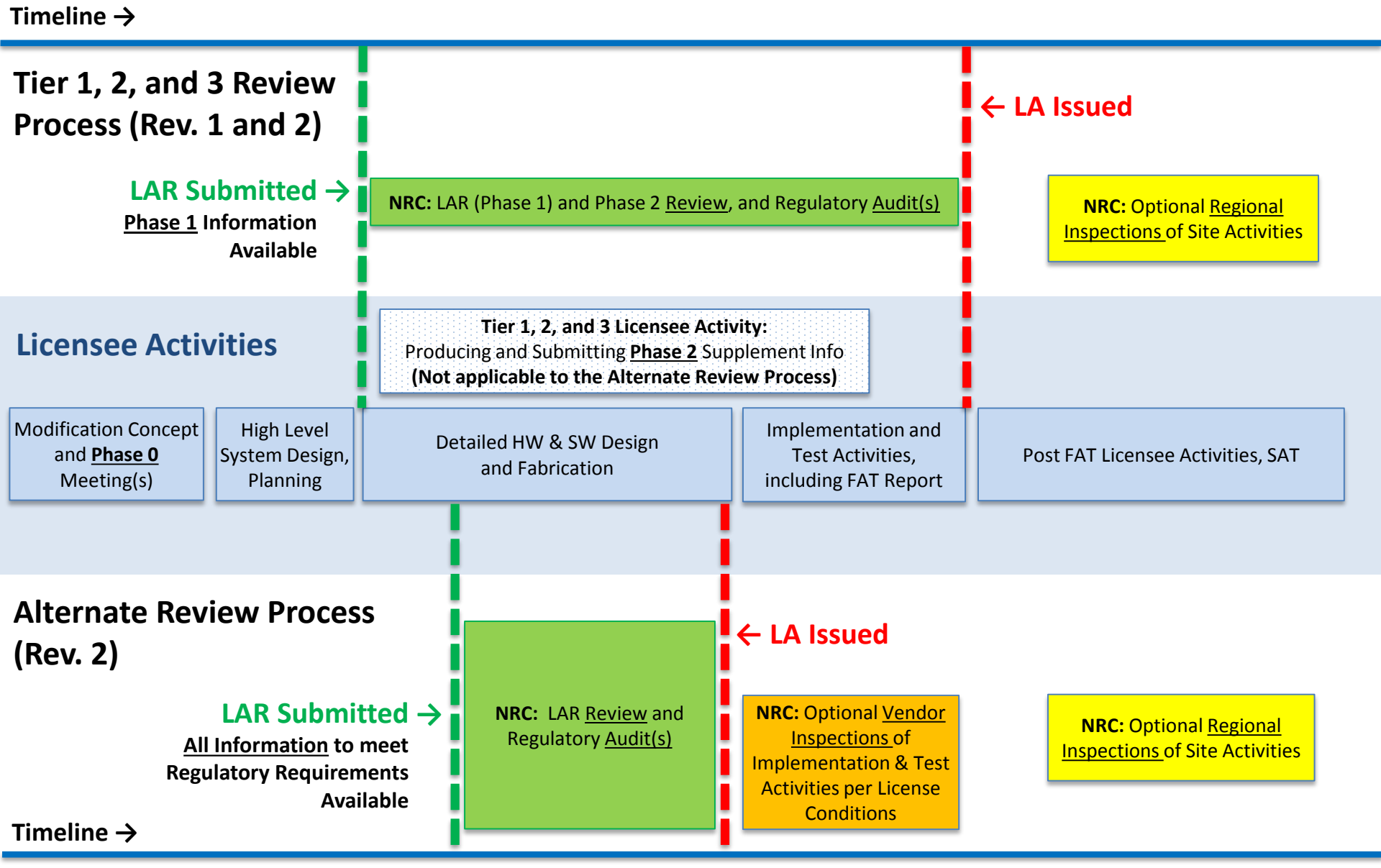
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Alternate Review Process: Licensee Committments and License Conditions

- The Alternate Review Process relies on the LARs containing licensing information and additional regulatory commitments to implement remaining development phases by the licensee's QA program, after the license amendment is issued
- The NRC staff may likely translate some of the regulatory-significant commitments into license conditions, as part of the approval (e.g., factory acceptance testing)

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

Comparison of Licensing and Oversight Activities



ACRS Subcommittee Comments

(May 17, 2018 Briefing)

- System Architecture – the ISG doesn't show how System Architecture is covered/reviewed under the Tier 1, 2, and 3 Review Process.
  - Section D.2 is now applicable to both Processes, and Enclosure B is being updated accordingly.
- Four Fundamental Design Principles – it is not clear how the four fundamental design principles are applied to a Tier 1, 2, and 3 Review
  - Section D.2, which contains the sections on the fundamental design principles, is now applicable to both Processes.
- Hardware Configuration Control – the ISG is silent in regards to configuration control and configuration management of hardware.
  - The staff is evaluating how to address this concern in the ISG

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

Next Steps

- ACRS Full Committee Briefing on July 11, 2018
- Issue the draft ISG for formal public comment on July 24, 2018
- Engage utilities in pre-application meetings
- Exercise ISG and incorporate into SRP

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

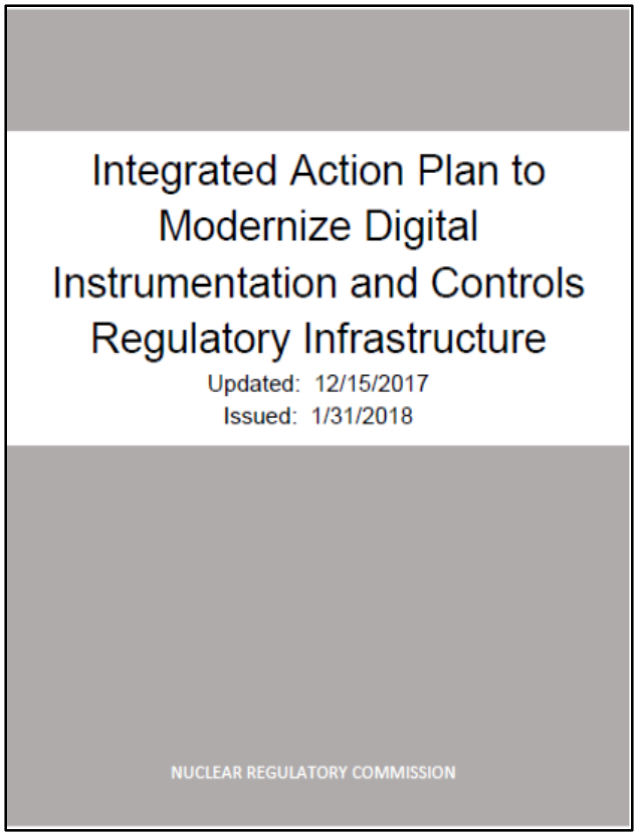
MP #4b Broader Modernization Efforts

Luis Betancourt, NRO/DEI/ICE
Huda Akhavannik, NRR/DE/EICB
Paul Rebstock, RES/DE/ICEEB

Advisory Committee on Reactor Safeguards
DI&C Subcommittee Briefing
June 20, 2018

The Commission Directed the Staff to "Modernize"

- Integrated Action Plan
  - SRM-SECY-16-0070
- Regulatory infrastructure
  - "…simpler, streamlined, and agile I&C regulatory infrastructure…"
  - Principles/attributes, e.g.,
    - Performance-based
    - Technology-neutral
    - Consistent, durable, predictable, scalable
    - Unambiguous
    - Safe and secure


Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure

Updated: 12/15/2017
Issued: 1/31/2018

NUCLEAR REGULATORY COMMISSION

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

Broader Modernization

(Purpose and Scope)

- Objective - Broadly evaluate the current overall I&C regulatory infrastructure and the supporting technical bases and consider other important areas beyond those identified in the tactical activities (e.g., past review experiences, ongoing licensing review) to identify and prioritize the improvements to modernize the regulatory infrastructure over the longer term in light of evolving approaches to I&C
  - Develop a roadmap to modernize the I&C regulatory infrastructure

- The scope of this effort includes four areas:
  - Operating reactors
  - New and advanced reactors
  - Fuel cycle facilities
  - Research and test reactors

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

Evolving Environment

Previous Environment (2 Yrs. Ago)

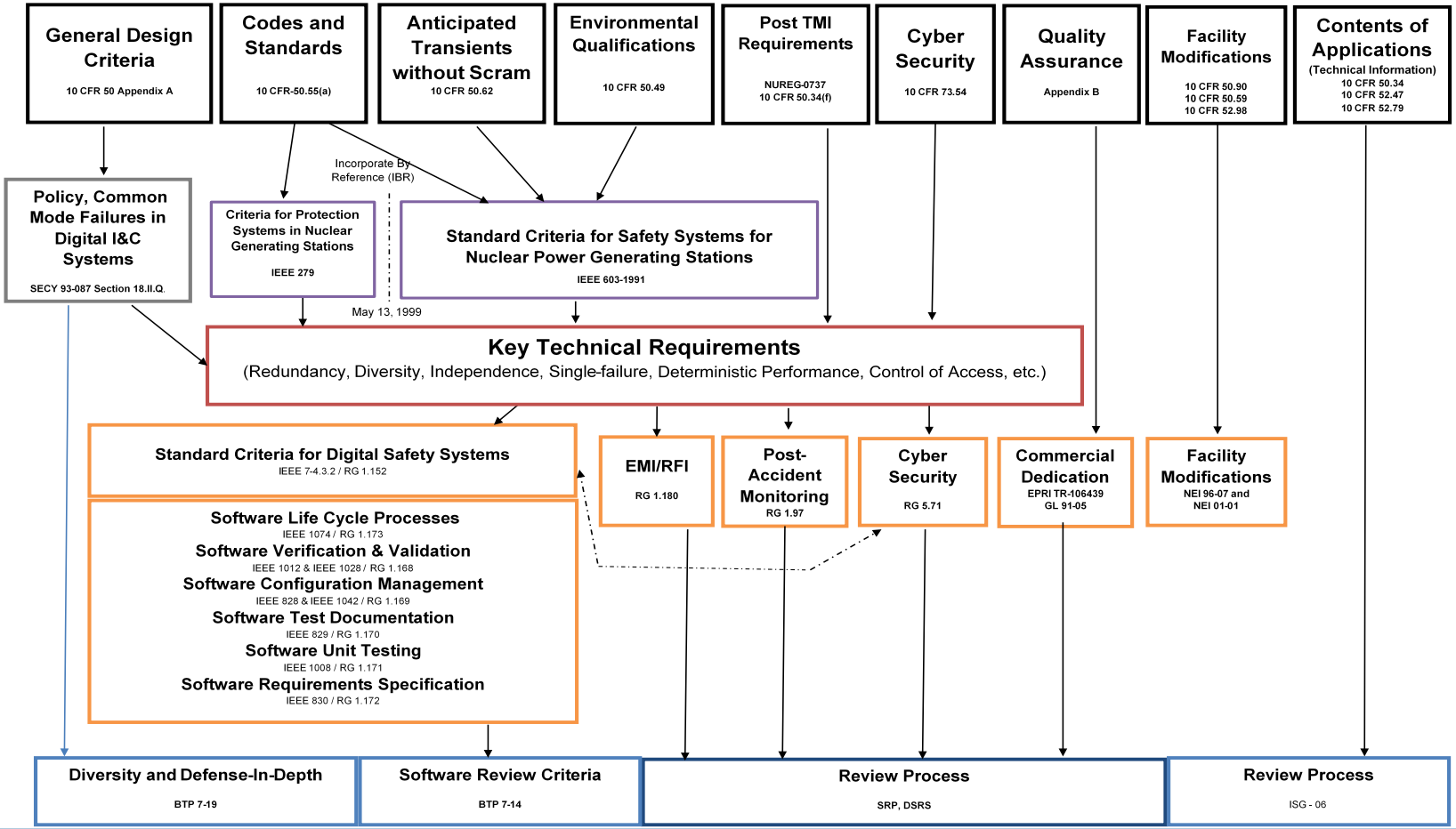
- Commission issued SRM-SECY-16-0070 approving the IAP
- Started tactical efforts to address near-term industry's needs
- Hold on strategic activities until completion of tactical efforts

Today's Environment

- RIS and ISG-06 address many of the immediate needs for the operating fleet
- IEEE Std 603-2018 near completion
- Evaluate endorsement of IEEE Std 7-4.3.2-2016
- Transformation Team's Recommendations (SECY-18-0060)

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

Our Regulatory Framework



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

Scope of MP #4B Assessment

- There are three standards IBR in 10 CFR 50.55a(h):
  - IEEE Std 279-1968, IEEE Std 279-1971, and IEEE Std 603-1991
- SRP Chapter 7
  - 27 RGs referenced in SRP Chapter 7 that endorses 32 standards
  - 17 BTPs referenced in SRP Chapter 7
  - 3 Generic Communications referenced in SRP Chapter 7
  - 14 NUREGs referenced in SRP Chapter 7
  - 52 other documents referenced in SRP Chapter 7 (e.g., EPRI Reports, IEEE, and ISO stds not endorsed)
- NuScale DSRS Chapter 7
  - 19 RGs in DSRS Chapter 7 that endorses 17 standards
  - 3 Generic Communications referenced in DSRS Chapter 7
  - 7 NUREGs referenced in DSRS Chapter 7
- Other Relevant Documents
  - 7 ISGs (most of them superseded)
  - 27 NUREGs
  - 11 SECY Papers
  - 14 Topical Reports
  - 3 RILs

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

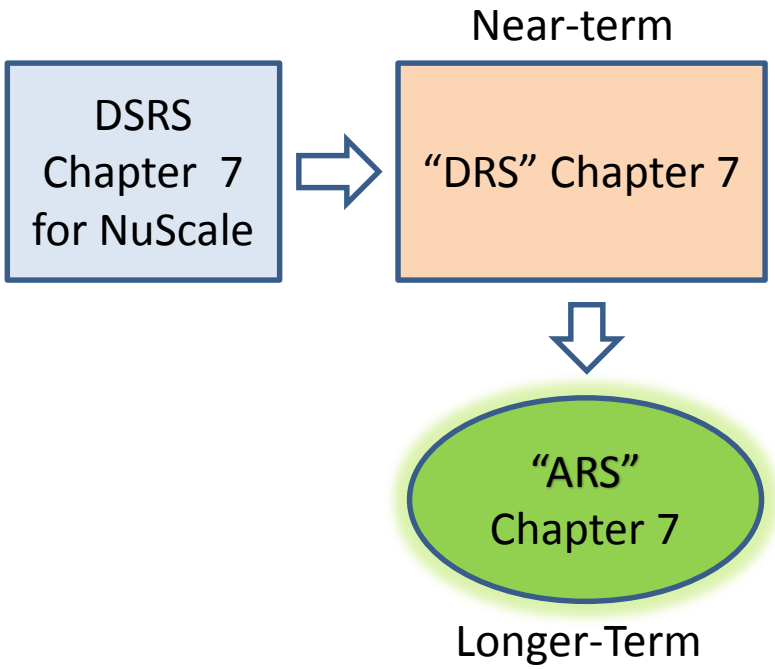
Initial Observations

- Although the current infrastructure for operating and new reactors has been effective in maintaining safety and security, elements of the framework appear to:
  - Have room for efficiencies which would make the infrastructure easier to use by licensees/applicants
  - Be more prescriptive rather than performance-based
  - Not be technology-neutral
- The I&C regulatory infrastructure is not optimal for non-LWR designs—it is largely based on 10CFR Part 50 and applicable Appendix A GDCs

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

Lessons From New Reactor Reviews

- Lessons learned from NuScale and APR1400
- New initiative started
  - Create new, improved guidance for future design reviews in a timely manner
  - Building on DSRS
- Target Issuance by Summer/Fall 2019



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

Next Steps

- Incorporate Commission's Decision on Transformation Team recommendations
- Coordinate with stakeholders when revising IAP
- Update IAP accordingly
- Continue assessing possible improvements to I&C infrastructure
- Coordinate with the advanced reactor community on draft DRS development
- Coordinate research activities in support of modernization activities

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

Research Activities to Support MP4B (Strategic Modernization) Objectives

- Research activities began 3rd FY Quarter 2018
- Research activities will focus on the *What* and *Why* (Technical Basis) for any proposed regulatory infrastructure change.
- Current research projects (driven by user need requests) include
  - Risk-informed approach to enhance the regulatory infrastructure
  - Safety implications of Embedded Digital Devices (EDDs) and related Emerging Technologies (ETs)
  - Impacts of CCF on DI&C system design

(*Note: Other areas are under consideration)*

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

Research Activities to Support MP4B (Strategic Modernization) Objectives

- Objective in all cases:
  - Develop Technical Bases to support evaluation criteria
  - Develop recommendations for evaluation criteria and infrastructure improvements
  - Ensure technology neutral focus
  - Support consideration of risk-informed approaches
  - Support consideration of performance-based outcomes
- Specifically, the research approach for each project will:
  - Identify and review approaches being used by international regulatory organizations and safety critical domestic regulatory organizations (e.g., IRSN, ONR, FDA, FAA)
  - Analyze the technical suitability of any proposed approach for the use in the nuclear industry to address safety issues
  - Assess the regulatory applicability of any proposed approach and provide recommendations to modernize the regulatory infrastructure

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

Questions?

Break

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

Acronyms

ACRS: Advisory Committee on Reactor Safeguards

APR1400: Advanced Power Reactor 1400

ARS: advanced review standard

BTP: branch technical position

CCF: common cause failure

CGD: commercial grade dedication

DI&C: digital instrumentation and control

DRS: design review standard

DSRS: design-specific review standard

IEC: International Electrotechnical Commission

EDD: embedded digital device

ET: emerging technology

EPRI: Electric Power Research Institute

ESFAS: engineered safety features actuation system

FAT: factory acceptance test

GDC: general design criteria

HW: hardware

IAP: integrated action plan

I&C: instrumentation and control

IBR: incorporated by reference

IEEE: Institute of Electrical and Electronics Engineers

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

Acronyms

ISG: interim staff guidance

ISO: International Organization For Standardization

LAR: licensee amendment request

MP: modernization plan

NEI: Nuclear Energy Institue

NRC: U.S. Nuclear Regulatory Commission

NuScale: NuScale Power, LLC

QA: quality assurance

RG: regulatory guides

RIL: research information letter

RIS: Regulatory Information Summary

RPS: reactor protection system

SAT: site acceptance test

SIL: safety integrity level

SRM: Staff Requirements Memorandum

Std: standard

SW: software

TR: technical report

ACRS Update on DI&C IAP: Industry Perspective

Jerud Hanson
Nuclear Energy Institute
Washington, DC

June 20, 2018

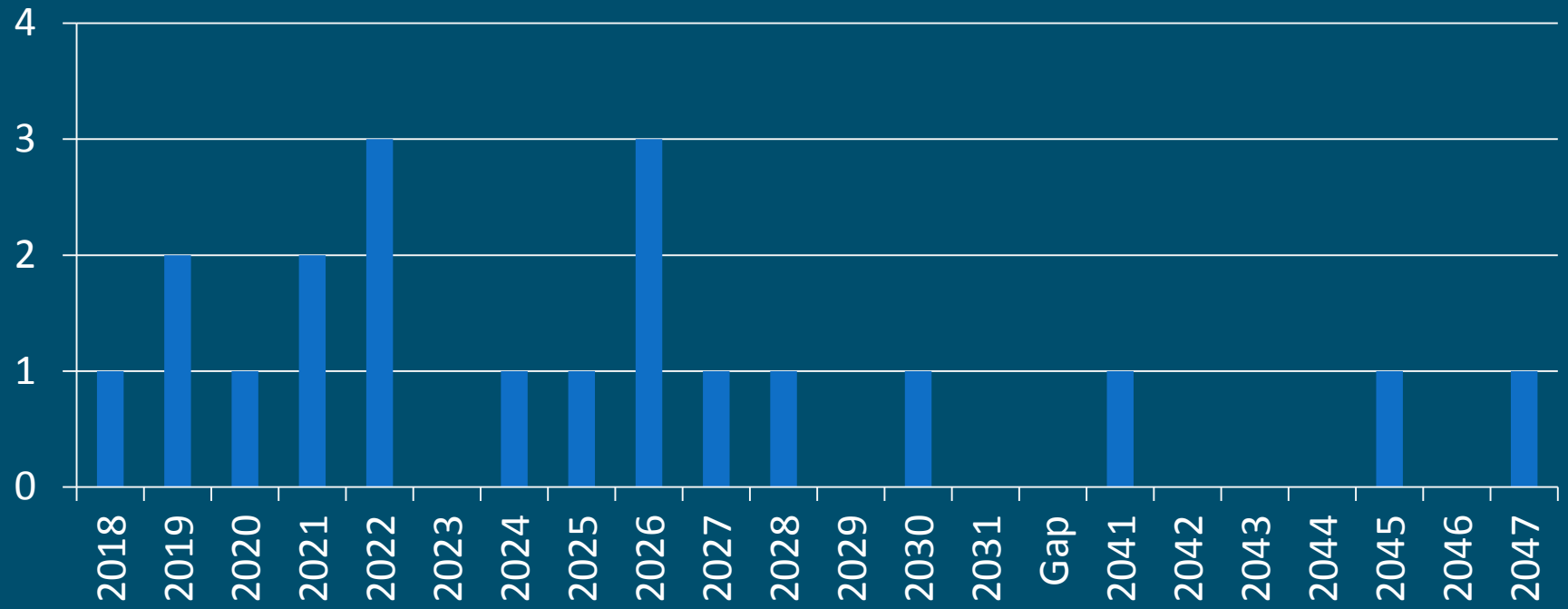
DI&C OVERVIEW

- IAP Modernization Plans (MP)
- Digital's impact on sustaining the nuclear industry
- Existing digital upgrades
- Industry timeline & objectives
- Milestones reached
- Recommendations

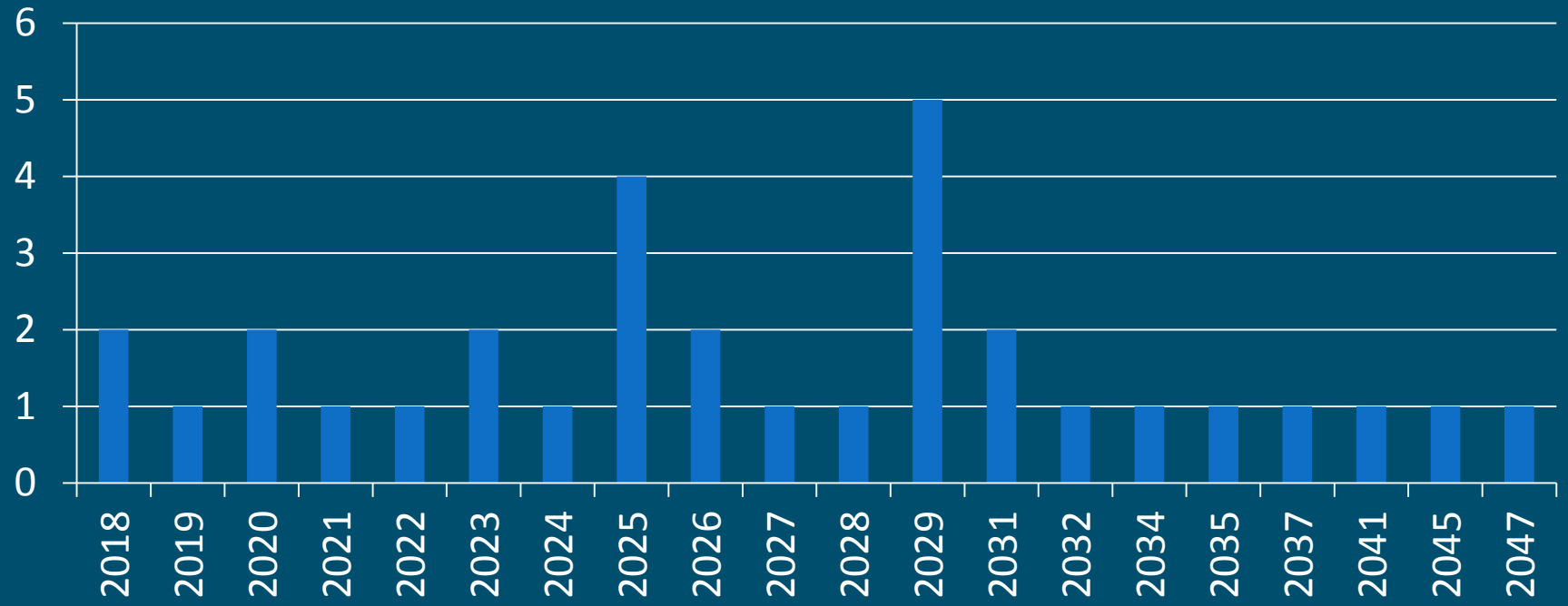
Digital I&C Modernization Plan (MP)

MP1A: RIS Supplement-1 to 2002-22 (Jerud Hanson/Neil Archambo)	MP1B: NEI 16-16 "Addressing Common Cause Failure (CCF)" (Jerud Hanson/Neil Archambo)	MP2: NEI 96-07, Appendix D "Supplemental Guidelines for Digital I&C 50.59" (Kati Austgen)	MP3: NEI 17-04 "Acceptance of Digital Equipment via 3rd Party Certification" (Maria Assard*)	MP4A: Revision to ISG-06 "Digital License Amendment Requests" (Pareez Golub**/Warren Odess-Gillett*)	MP4B: Infrastructure (Long Term) (Warren Oddess-Gillett*)
Final Document Issued 2Q2018	Deferred Pending Completion of RIS & Appendix D	NRC Decision to Endorse 4Q2018	EPRI Results in 3Q2018 Decision to Endorse 2018/2019	NRC Issuance 4Q2018	2018/2019

SLR INDUSTRY SURVEY – 2016 RESULTS



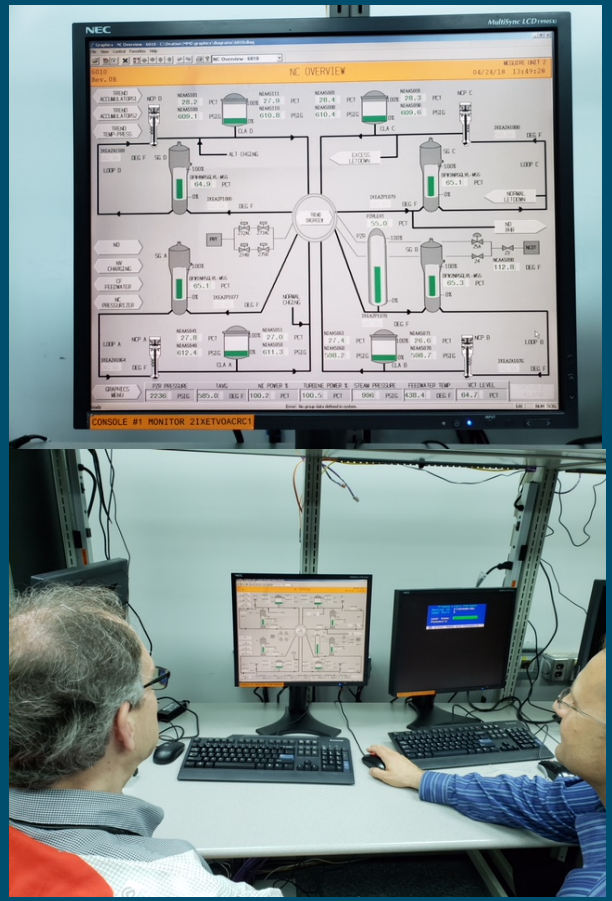
SLR INDUSTRY SURVEY – 2018 RESULTS



DI&C Analog Systems Today

DI&C Robinson Nuclear Station Glass Top Simulator – 2018 NEI TIP Award Winner

DI&C McGuire/Catawba Nuclear Station Ovation DCS



NEI DI&C IAP Schedule

	NEI DI&C IAP Milestone Chart 2018										
	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
MP1A: RIS	RIS Issuance Delayed by NRC due to stakholder pushback- Additional Public Comment Period			RIS Issuance	RIS Focused Q&A Workshops				RIS Pilot Projects		
MP1B: NEI 16-16	On Hold Pending RIS & Appendix D Completion/Implementation (Joint industry/NRC decision)							Revisit Need of additional CCF Guidance & Completion of EPRI Research			
MP2: NEI 96-07 Appendix D	On Hold Pending RIS Completion (Joint industry/NRC decision)				Reach Alignment on NEI 96-07 Appendix D		Submit App D	NRC Endorsement of NEI 96-07 Appendix D			
MP3: Acceptance of Digital Equip.	EPRI Research on SIL Certification									NEI development of NEI 17-06, Rev. 0	
MP4A: ISG-06 Revision	Internal staff review & comment - submitted to ACRS I&C subcommittee			ACRS I&C Mtg	Tabletop	ACRS FC & Prepare ISG for FRN	ISG-06 Public Comment	Incorporate public comments and prepare ISG for publication			ISG-06 Rev. 2 Published
MP4B: Longterm Infrastructure	Kickoff delayed until NRTT SECY is issued (NRC decision)				MP4B Public Kickoff	Future Industry/NRC actions based on kickoff meeting					

Key	Industry Action	NRC Action	Joint Action	Delay

DI&C SUMMARY

- Recent milestones
  - RIS issuance May 31st
  - ISG-06 remains on track for 2018 issuance
- Priority for 2018 should be continuing focus on successful RIS implementation, ISG-06 issuance and completion of Appendix D for 50.59 screening and evaluations
  - Completion of all three MP milestones = Success for 2018
- Number of SLRAs anticipated in this country is growing
  - SLR is the immediate future of nuclear in the U.S.
  - DI&C is key to success of SLR and the industry

QUESTIONS?

ELECTRIC POWER RESEARCH INSTITUTE

Integrated Digital Systems Engineering:

Overview of the EPRI Digital Engineering Guide

Advisory Committee on Reactor Safeguards

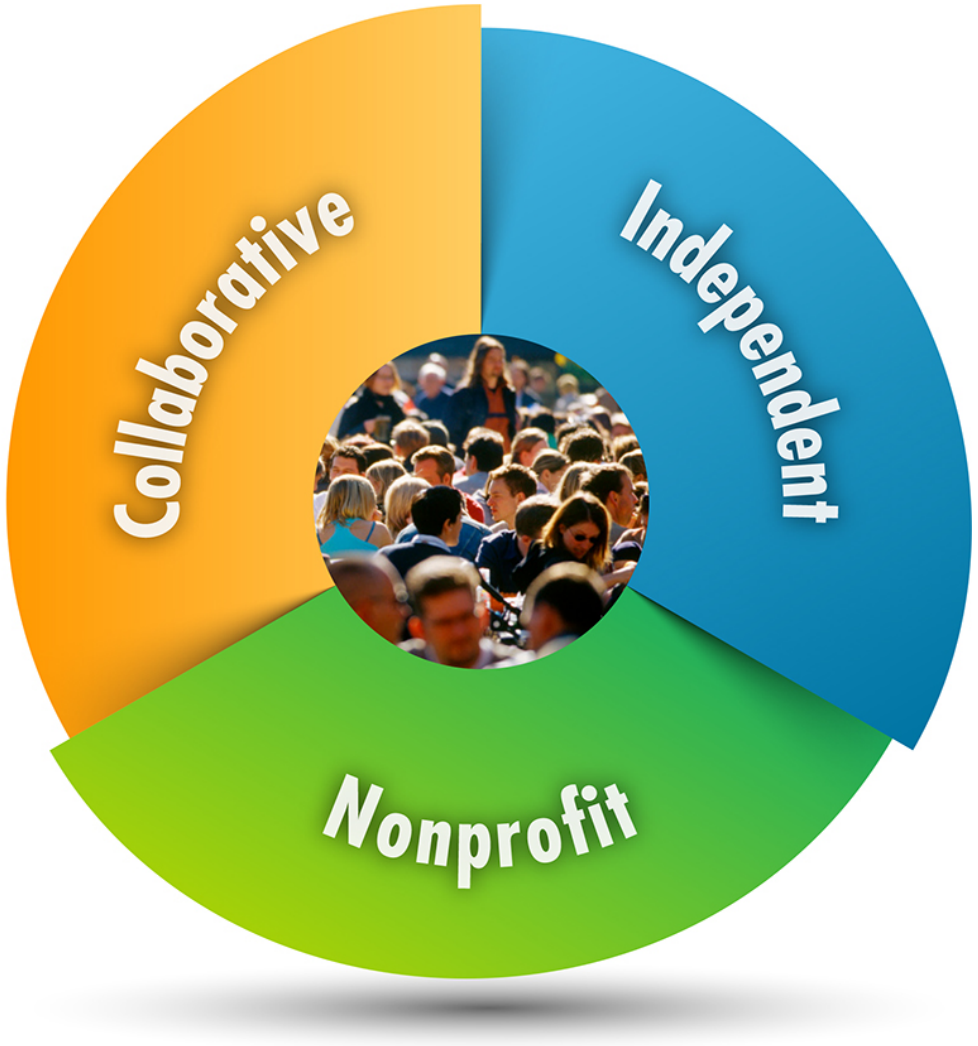
June 20th 2018

Matt Gibson, P.E., CISSP

Technical Executive- EPRI

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Three Key Aspects of EPRI



Independent

Objective, scientifically based results address reliability, efficiency, affordability, health, safety, and the environment

Nonprofit

Chartered to serve the public benefit

Collaborative

Bring together scientists, engineers, academic researchers, and industry experts

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Introduction

Matt Gibson:

Licensed Professional Engineer- (Control Systems),
CISSP- (Certified Information Systems Security Professional)

- EPRI- 2013 - Present
- Duke/Progress Energy- 1982-2013
  - Fleet Process Systems Architect- 2002- 2013
    - *NUSTART Digital I&C, HFE, and Cyber Security Lead AP1000*
    - *Duke/Progress Legacy Fleet Digital I&C Modernization Architect*
    - *Design and System Engineering, Technology Assessment and Integration*
  - Nuclear IT/OT Manager- Robinson Plant 1994-2002
    - *Business and Digital I&C Systems*
    - *Telecommunications*
    - *Software Quality Assurance(SQA) and Cyber Security*
  - Digital I&C/Computer Technician and Specialist – 1982-1994
    - *System Development and Maintenance*
- Electronic Warfare Specialist – US Navy 1975 - 1982

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Agenda

- Nexus of Digital Upgrades with Plant Modernization
- Discuss Systems Engineering and its Benefits
  - How it will be used EPRI Digital Design Guide
- Present and Discuss the Digital Engineering Guide
  - History
  - Structure
  - Benefits
  - Examples
- Discuss Cyber Security Integration
- Discus Risk Integration

© 2018 Electric Power Research Institute, Inc. All rights reserved.

The Modernization of Nuclear Plants

VISION

Achieve economic viability of nuclear power through RADICAL and TIMELY transformative innovation & modernization, including:

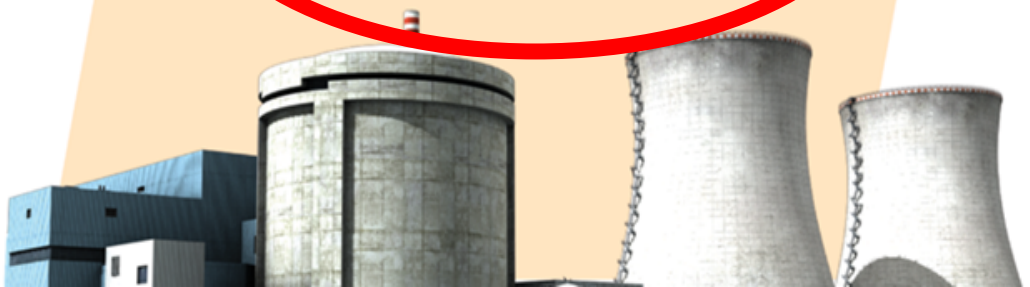
- Business Process Transformation
- Monitoring
- Analytics
- Automation
- Integration

GOALS

Achieve local market economic competitiveness through cost reductions

COMMON ENABLERS

- CIM — Common Information Model
- Agile Business Processes
- Connectivity
- Common Integrated Tools/Applications
- Digital Upgrade
- Inform Regulatory Change



FUNCTIONAL AREAS

- Operations
- Radiation Protection
- Emergency Preparedness
- Maintenance
- Security
- Outage Management
- Engineering
- Work Management
- Warehouse & Supply Chain
- Chemistry
- NDE
- Training

EPRI ELECTRIC POWER RESEARCH INSTITUTE

© 2018 Electric Power Research Institute (EPRI), Inc. All rights reserved.

Systems Engineering

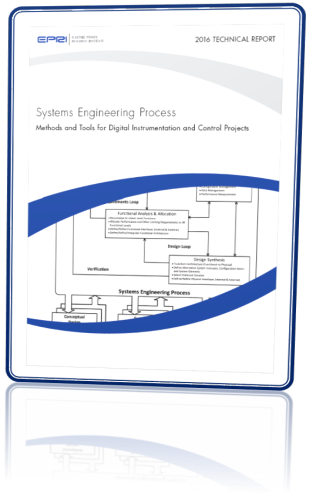
A Modern Engineering Process for Digital I&C

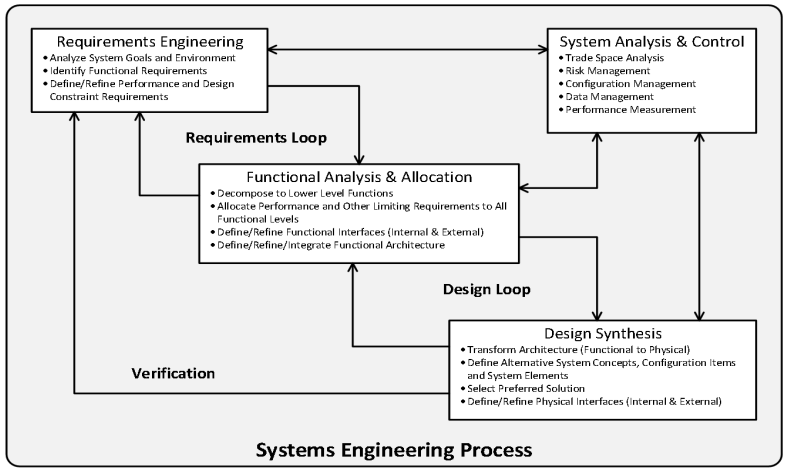
© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI Systems Engineering Initiative

- EPRI has develop Systems Engineering (SE) insights with recent R&D.
  - Concluded with: *Systems Engineering Process: Methods and Tools for Digital Instrumentation and Control Projects. (3002008018)*
  - Validated the efficacy of the SE process for nuclear
  - Included benchmark of non-nuclear users

Systems Engineering(SE) Methods -EPRI 3002008018





- Results from this research are now being integrated into a useable methodology.
  - Evolved into the "Integrated Digital System Engineering" strategy.
  - The EPRI *Digital Engineering Guide* (DEG) is schedule to publish in November 2018, 3002011816
    - Consolidates related topical disciplines into a holistic process, using a core SE methodology
    - Contains "risk friendly" processes that allow local risk methods to be integrated
    - US utilities are first adopters with a DNP initiative to use the DEG via an industry standard procedure, NISP-EN-04

© 2018 Electric Power Research Institute, Inc. All rights reserved.

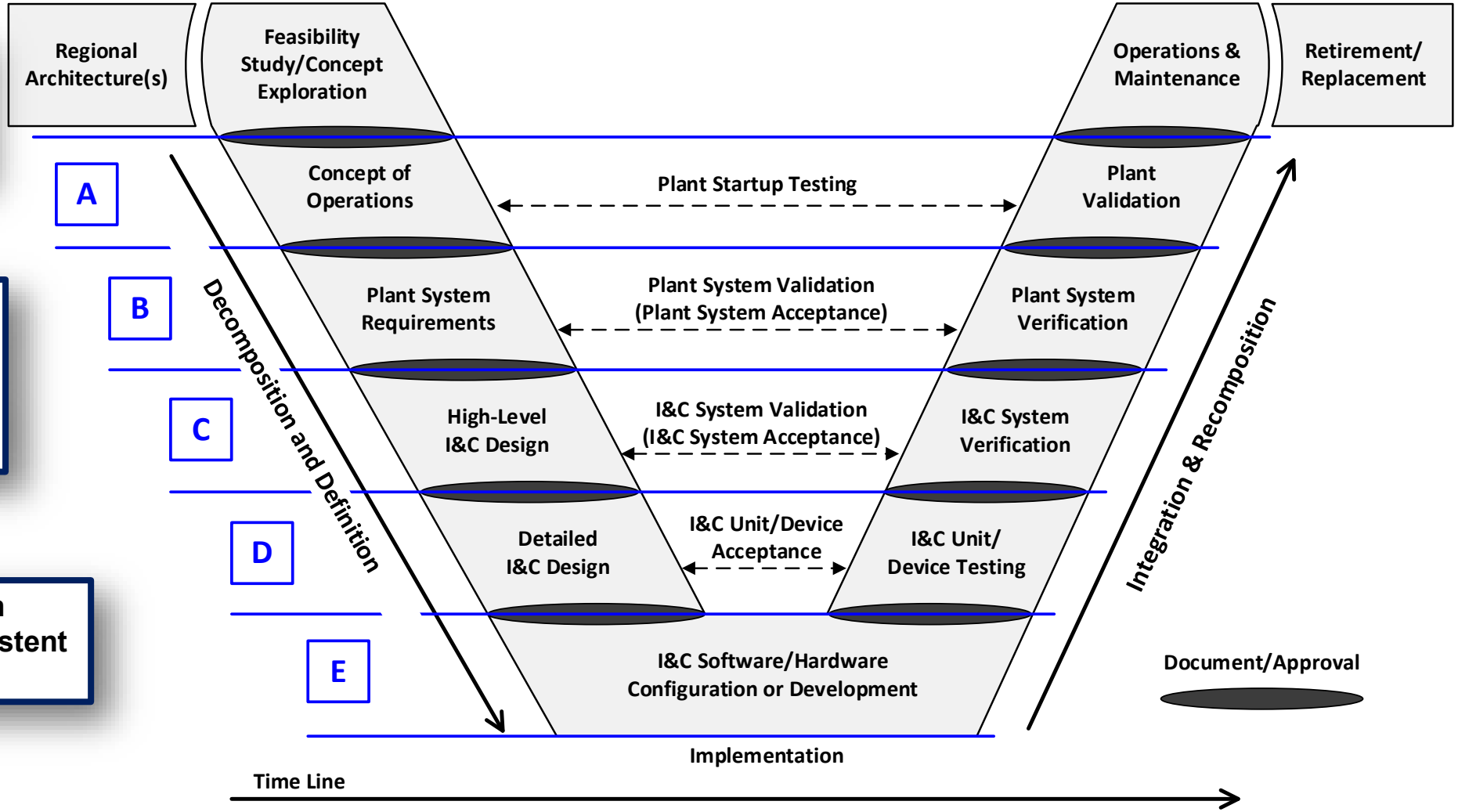
Systems Engineering "V" Model

Model Includes all components including Software.

Separate SQA not needed.

A facility change can enter at any level of this model, but engineering activities depend on information from at least one level above the change

Decomposition and Recomposition guide the level of effort to be consistent with the level of the change



© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Digital Engineering Guide
3002011816
November 2018

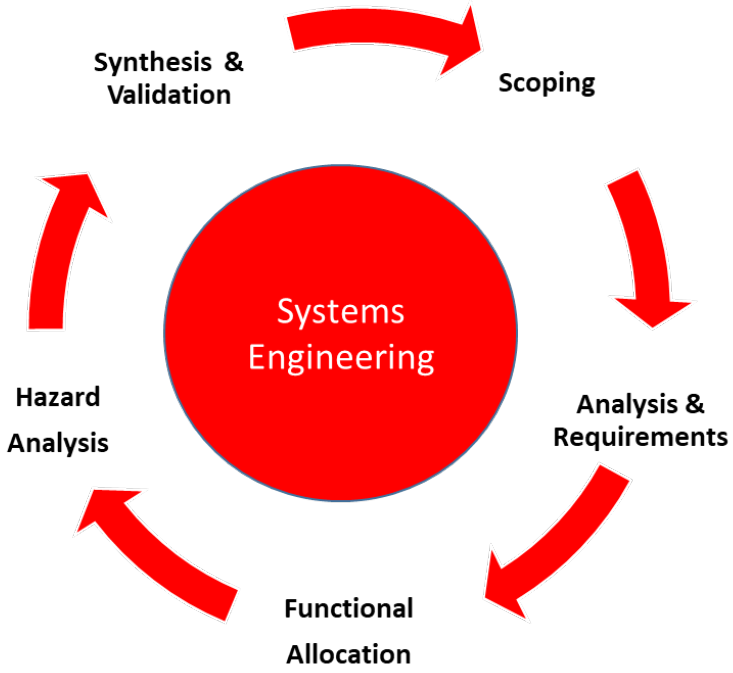
A Practical Systems Engineering Process for Digital I&C Engineering

© 2018 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

EPRI Digital Engineering Guide (DEG)

- **Chapter 1 thru 3 Framework**
  - Graded Approach
    - Configurability determination
    - Consequence determination
    - Activity Applicability determination
    - Structured Information guidance



- **Chapter 4 – Systems Engineering**
  - Modeled after EPRI 3002008018 and ISO/IEC/IEEE 15288:2015
  - **Synthesizes various ISO/IEC/IEEE standards.**
  - Chapter 4 is the foundation for all remaining chapters

- **Chapters 5 thru 12 – Topical Guidance**
  - Procurement
  - Human Factors Engineering
  - Data Communications
  - Cyber Security
  - Plant Integration Design
  - Testing
  - Configuration Management
  - Digital Obsolescence Management

© 2018 Electric Power Research Institute, Inc. All rights reserved.

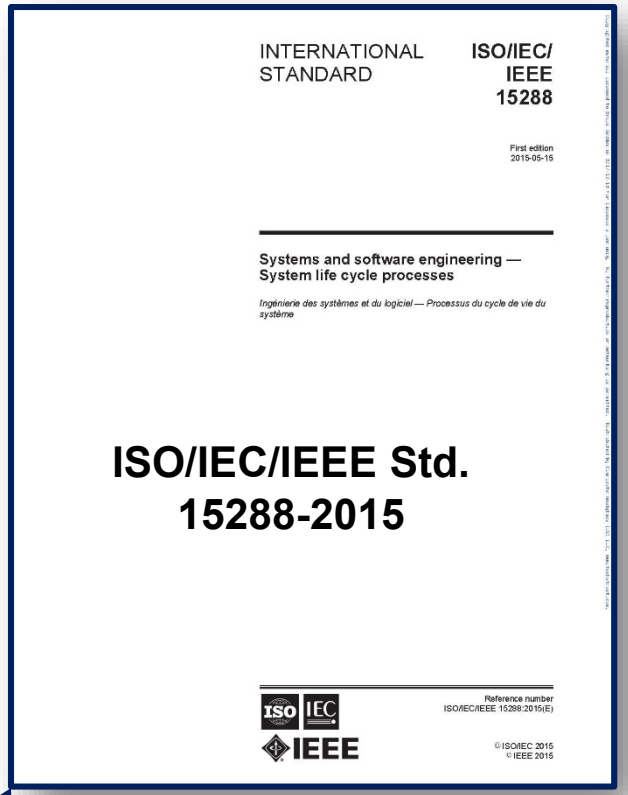
Regulatory Mapping Guides

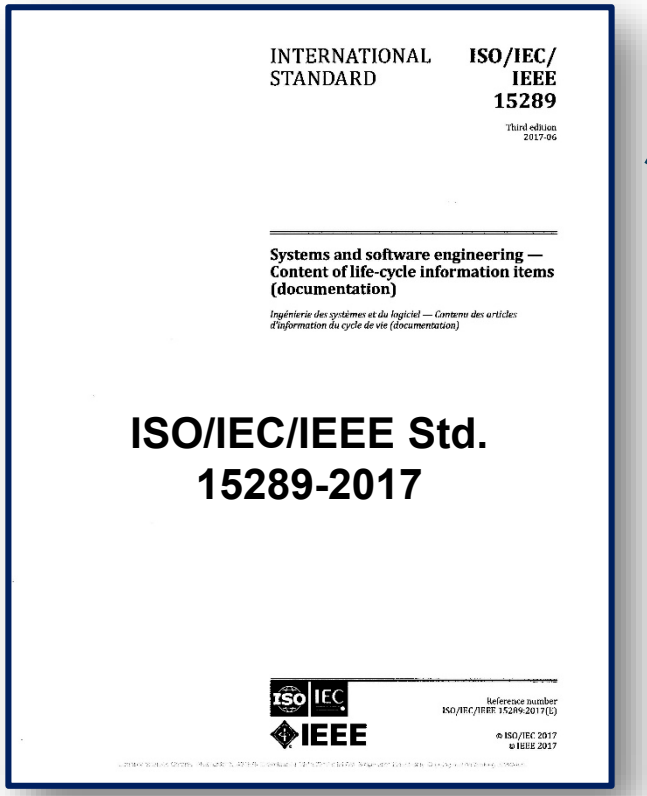
- A series of separate companion reports, one for each region
  - Separate reports allow for each one to be updated independently as needed.
  - This idea is proven in the Cyber Security Technical Assessment Methodology-TAM (EPRI 3002008023).A separate companion report (EPRI 3002010676) provides a template for mapping TAM results to NEI 08-09 security controls.

- The DEG mapping guides will maps the DEG activities or tasks/deliverables to regional regulations (NRC rules in US, ONR in UK, etc.)

© 2018 Electric Power Research Institute, Inc. All rights reserved.

“This document ***specifies the purpose and content*** of all identified systems and software life-cycle ***information items***…”





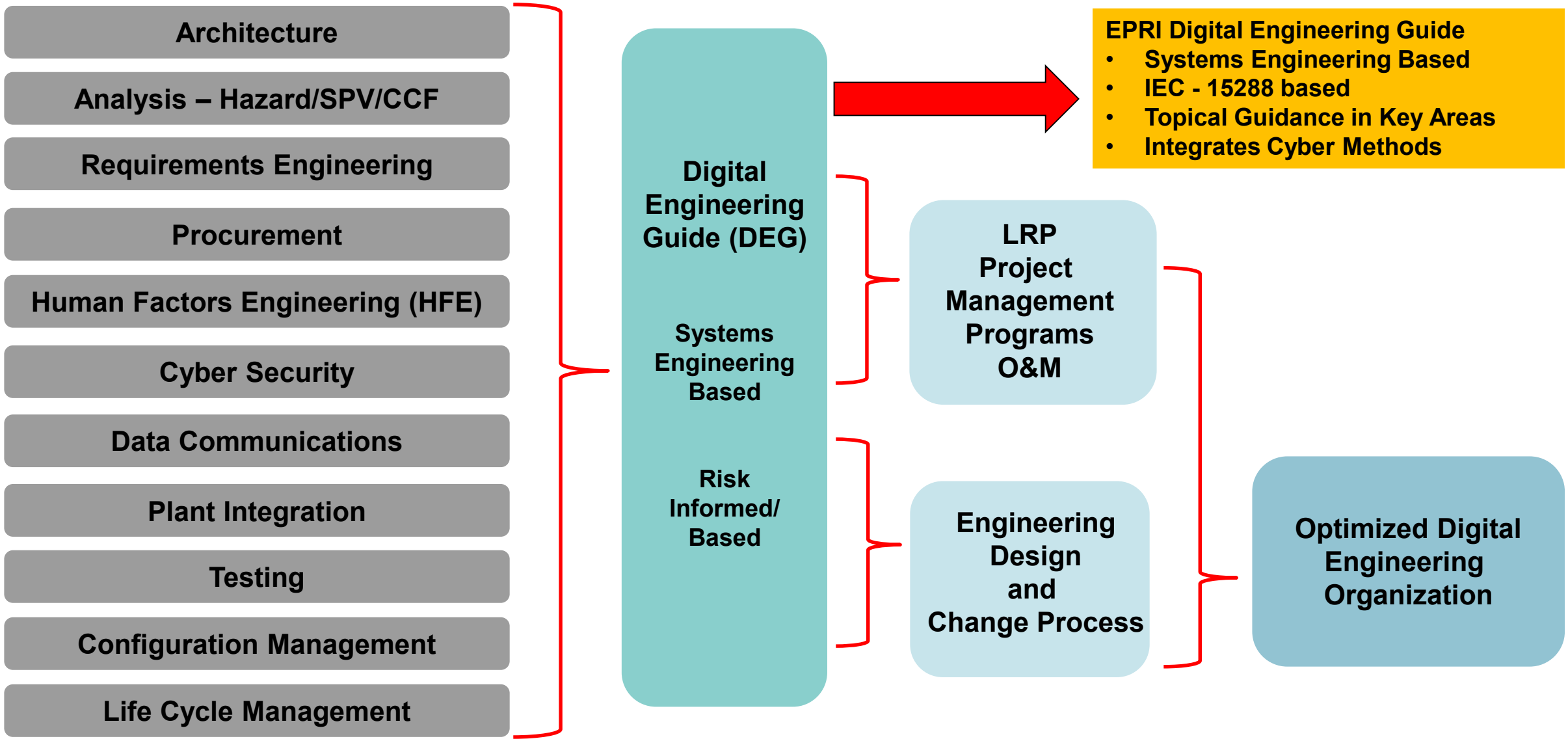
“This International Standard ***does not detail information items*** in terms of name, format, explicit content and recording media. ISO/IEC/IEEE 15289 addresses the content for life cycle process information item (documentation).”

“ISO/IEC 12207:2008 (IEEE Std. 12207- 2008) does not always specify when software information items are to be prepared, ***nor does it identify information item contents***.”

Standards are Synthesized into Actionable Guidance

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Integrated Digital Systems Engineering

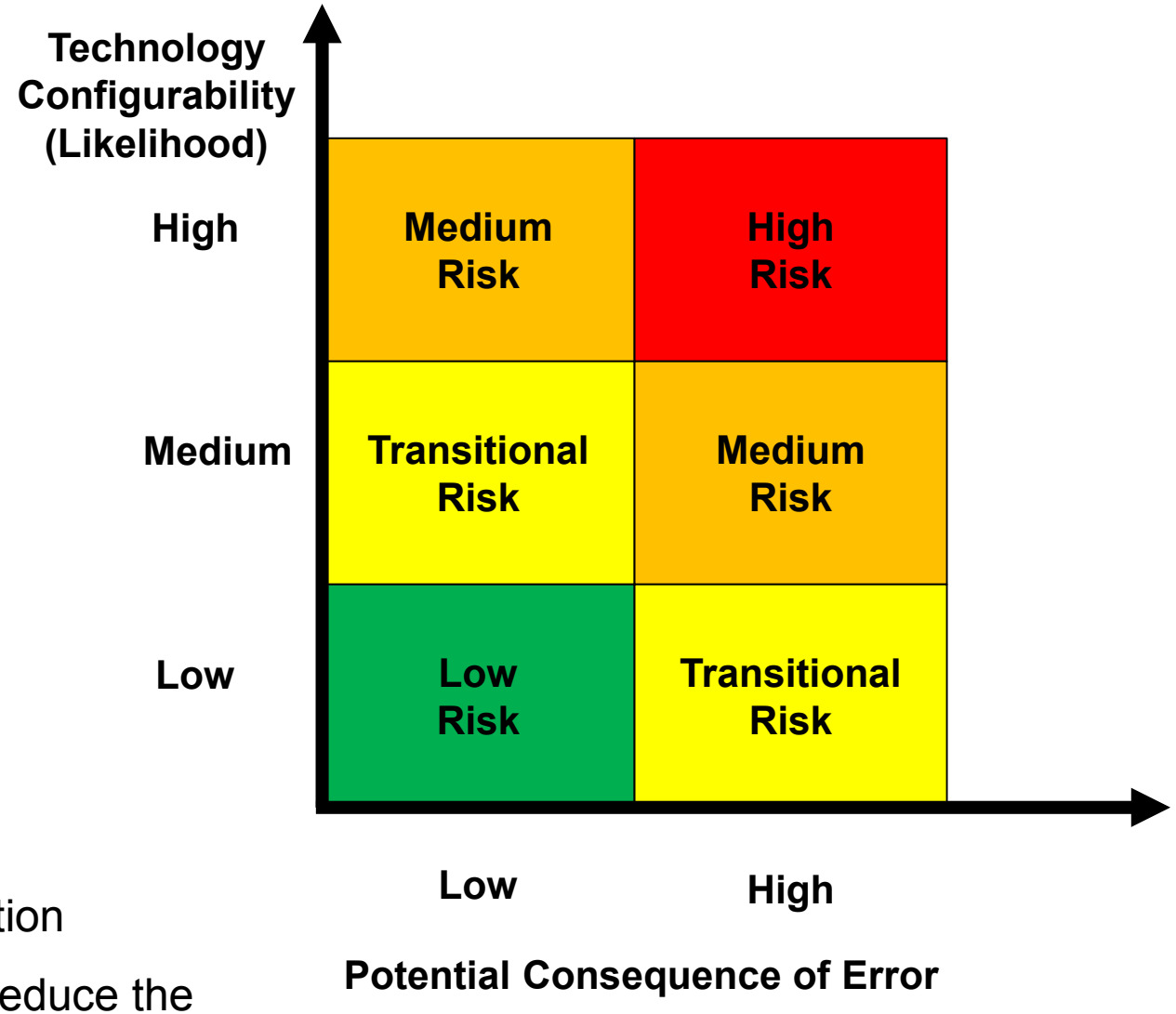


© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

DEG Graded Approach

Applicability



- **The DEG is Activity Based**
- If Applicable then…….
  - Consider Risk
  - Drives level of Activity Rigor and Documentation
  - Rigor is defined as assurance methods that reduce the likelihood of error
  - Activities can be completed <u>without documentation</u>

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Graded Approach

- **Step 1: Configurability Screen**
  - **Low** (A Few Settings)
  - **Medium** (Wide Range of Settable Parameters)
  - **High** (Custom Application Software)

ATTACHMENT 7
Page 1 of 1

Configurability Grading Criteria

Programmable electronic equipment (PEE) shall be classified as "high configurability" if one or more of the following criteria are satisfied:

- PEE applications are developed by or for the end user via a Full Variability Language and/or a Limited Variability Language.
- The PEE is a collection of module types that can be interconnected in a physical architecture that is synthesized from system design criteria and an application-specific functional architecture.
- Using engineering tool software, application-specific modules are developed such that the modules can be interconnected in a physical architecture that is synthesized from system design criteria and an application-specific functional architecture.
- Application-specific operator, maintenance, or engineering workstation displays are user configurable via engineering tool software that provides a library of display objects and/or a method for developing display objects, and a method for developing workstation displays.
- Application-specific control functions are user configurable via engineering tool software that provides a function block library and a method for developing control logic. The engineering tool software may also provide a method for developing or programming custom function blocks.

PEE shall be classified as "medium configurability" if none of the "high configurability" criteria are satisfied and one or more of the following criteria are satisfied:

- PEE applications are developed by or for the end user via a Fixed Program Language.
- The PEE is user configurable by setting one or more parameter values within a range defined by the product vendor. Parameter values are set using the product faceplate and/or a data communications port connected to a mobile device provided with configuration tool software supplied by the product vendor or a third party.
- The PEE is user configurable by removing an internal device, assembly, or circuit board and replacing it with a different version.
- The PEE is user configurable by loading a different version of firmware via a data communications port connected to a mobile device provided with configuration tool software supplied by a vendor or a third party.
- The PEE is user configurable via hardware settings, such as dip switches, jumpers, potentiometers, etc.

PEE shall be classified as "low configurability" if it does not satisfy any of the "high configurability" criteria or the "medium configurability" criteria.

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Graded Approach

- **Step 1: Configurability Screen**
  - **Low** (A Few Settings)
  - **Medium** (Wide Range of Settable Parameters)
  - **High** (Custom Application Software)
- **Step 2: DEG Activity Applicability**
  - Activity Not Applicable – Technology/Function does not exist
  - Activity Conditional – See each DEG Section Guidance
  - Activity Required

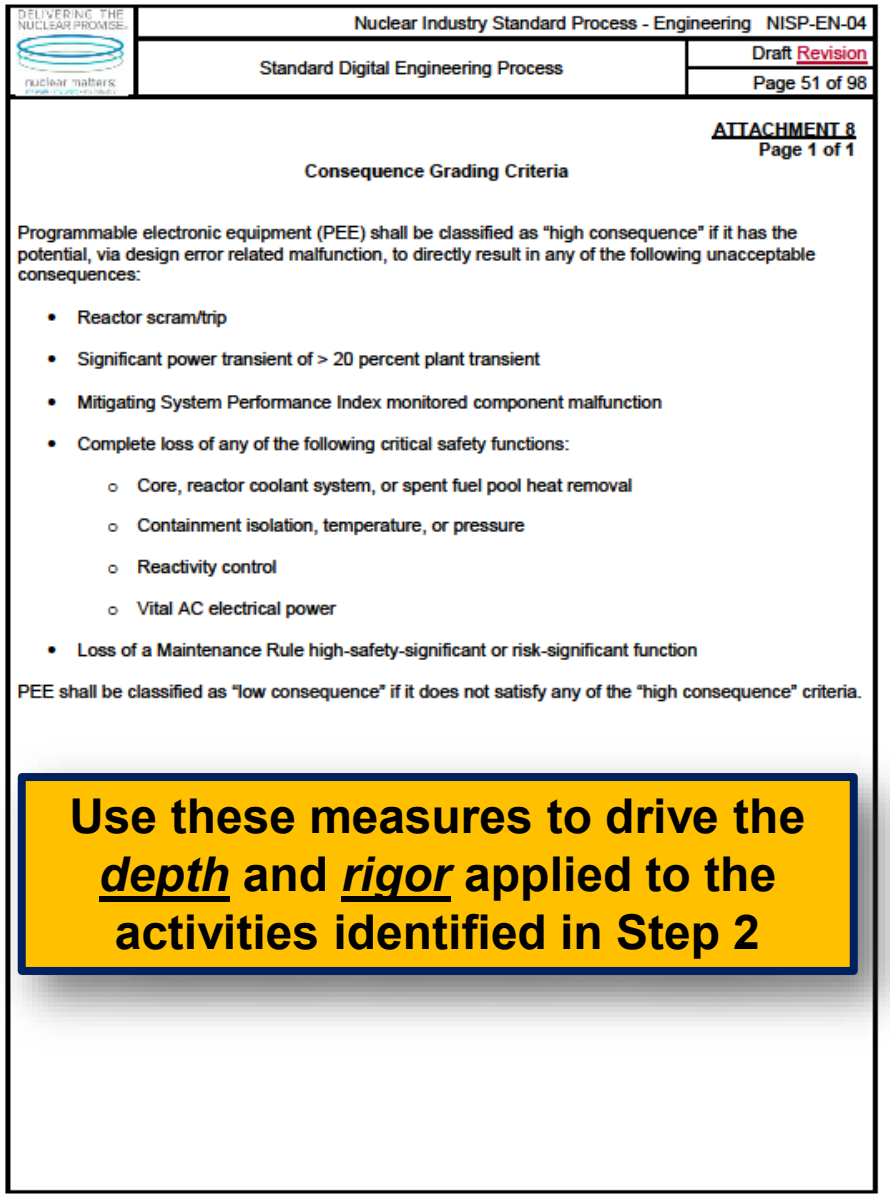
Project	Replace L&N Paper Recorder with Yokogawa DX2000 Common Design Package - Indication Only, No Data Communications				
Digital Engineering Guide Activities		Configurability			RE/RS Decision
		Low	Med	High	
3	I&C Programs, Plans and Lifecycles				
3.1	I&C Program Management				
3.1.1	I&C Strategic Plan	N	C	R	Common Design Package
3.1.2	Equipment & Vendor Selection Criteria	C	C	R	Yokogawa DX 2000 /xx/yy/zz/aa/bb
3.1.3	HFE Program Plan		C		per HFE checklist and/or DEG Chapter 7
3.1.4	Cyber Security Plan		C		Applicable
3.2	Standard Design Process				
3.3	Systems Engineering Process				
3.3.1	Vee Model Activities		R		Yes - see EPRI example
3.3.2	Process Model Activities		R		Yes - see EPRI example
3.4	System Development Lifecycle (SDLC)				
3.4.1	Development Activities in the Generic SDLC		C		No
3.4.2	Verification & Validation Activities in the Generic SDLC		C		No
3.5	Graded Approach				
3.5.1	Technology Configurability		R		See configurability screen
3.5.2	DEG Activity Selection		R		This screen
3.5.3	Risk Reduction		R		See DEG section guidance
3.6	Vendor Oversight				
3.6.1	Develop Vendor Oversight Plan	N	C	R	if 3rd party qual/CGD
3.7	Technical Transfer				
3.7.1	EPRI Computer Based Training	C	C	R	Yes
3.7.2	EPRI Classroom Training	C	C	R	Yes
3.7.3	Vendor Training	N	C	R	Read the manual
4	Analyses				
4.1	Initial Scoping Phase				
4.1.1	Perform Problem/Needs Analysis		R		Obsolescence driven
4.1.2	Develop I&C Insights from Existing Analyses	C	C	R	HRA or SFA
4.1.3	Perform Operating Experience Review		R		Yes
4.1.4	Develop Hazard Analysis Plan	N	C	R	No
4.2	Conceptual/Common Design Phase				
4.2.1	Develop or Confirm Preliminary Hazard Analysis	C	C	R	No formal FMEA, but document failure mpdes in the package
4.2.2	Assess CCF Susceptibility		R		if in multiple division - and include CCF P/Ls to the extent possible in c
4.2.3	Perform CCF Coping Analysis (if needed)		R		if susceptible
4.3	Detailed Design Phase				
4.3.1	Develop or Confirm Detailed Hazard Analysis		R		see 4.2.1
4.3.2	Identify & Resolve Single Point Vulnerabilities (SPV)		C		TBD
4.3.3	Resolve Remaining Hazards		R		see 4.2.1
4.3.4	Verify Hazard Analysis Results		R		verify results of 4.2.1
4.4	Planning Phase				
4.4.1	Update PRA		C		application-specific
4.4.2	Validate Hazard Analysis Results		R		see 4.2.1
4.5	Installation/Testing Phase				
4.5.1	Validate Hazard Analysis Results		R		bench test
4.6	Closeout Phase				
4.7	Operations and Maintenance Phase				

For each activity in the DEG, this form provides suggested applicability by configurability category. However, RE/RS have the final decision.

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Graded Approach

- **Step 1: Configurability Screen**
  - **Low** (A Few Settings)
  - **Medium** (Wide Range of Settable Parameters)
  - **High** (Custom Application Software)
- **Step 2: DEG Activity Applicability**
  - Activity Not Applicable – Technology/Function does not exist
  - Activity Conditional – See each DEG Section Guidance
  - Activity Required
- **Step 3: Consequence Screen**
  - **Low**: Does not meet High Consequence Criteria
  - **High**: Meets Risk and Impact thresholds for High Consequences



DELIVERING THE NUCLEAR PROMISE. nuclear matters

Nuclear Industry Standard Process - Engineering NISP-EN-04

Standard Digital Engineering Process

Draft Revision

Page 51 of 98

ATTACHMENT 8
Page 1 of 1

Consequence Grading Criteria

Programmable electronic equipment (PEE) shall be classified as "high consequence" if it has the potential, via design error related malfunction, to directly result in any of the following unacceptable consequences:

- Reactor scram/trip
- Significant power transient of > 20 percent plant transient
- Mitigating System Performance Index monitored component malfunction
- Complete loss of any of the following critical safety functions:
  - Core, reactor coolant system, or spent fuel pool heat removal
  - Containment isolation, temperature, or pressure
  - Reactivity control
  - Vital AC electrical power
- Loss of a Maintenance Rule high-safety-significant or risk-significant function

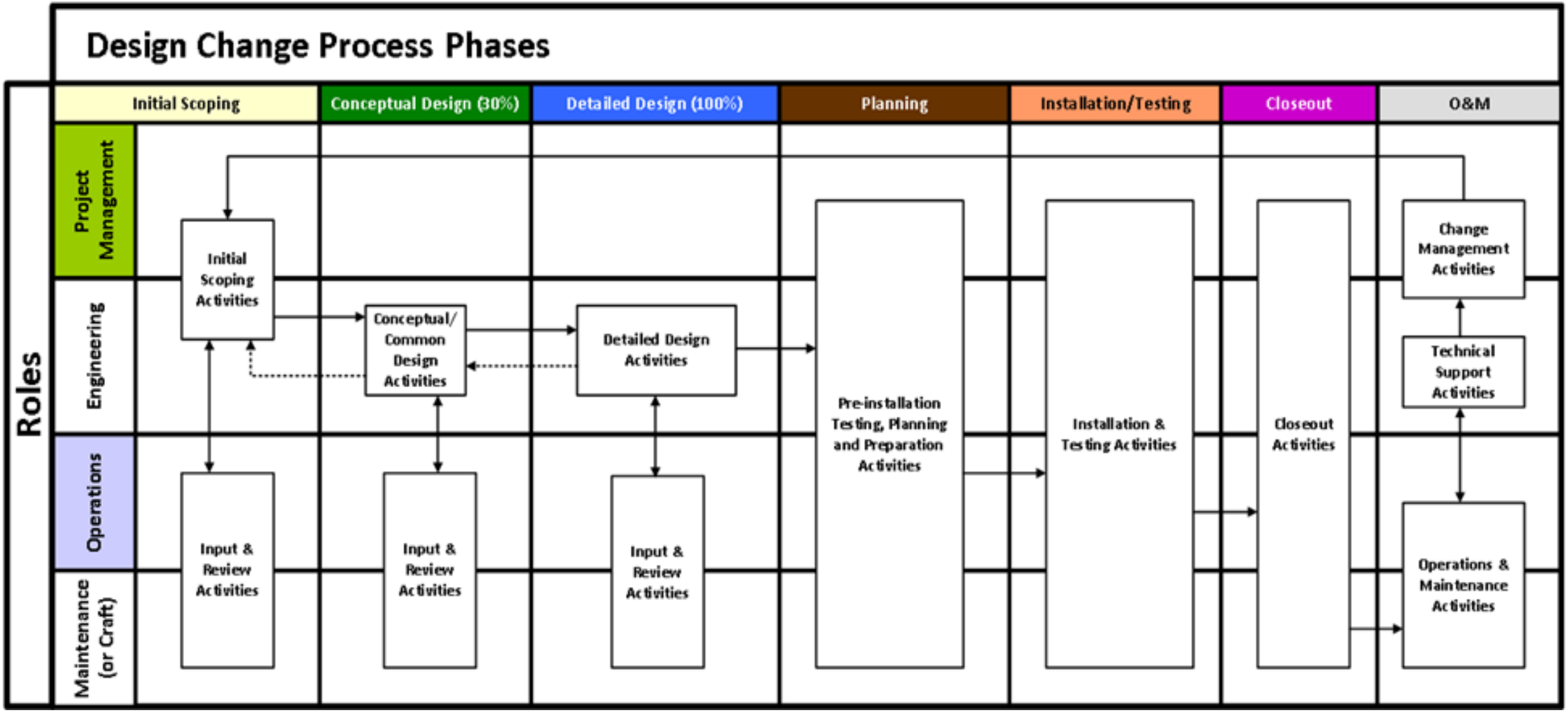
PEE shall be classified as "low consequence" if it does not satisfy any of the "high consequence" criteria.

Use these measures to drive the *depth* and *rigor* applied to the activities identified in Step 2

© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

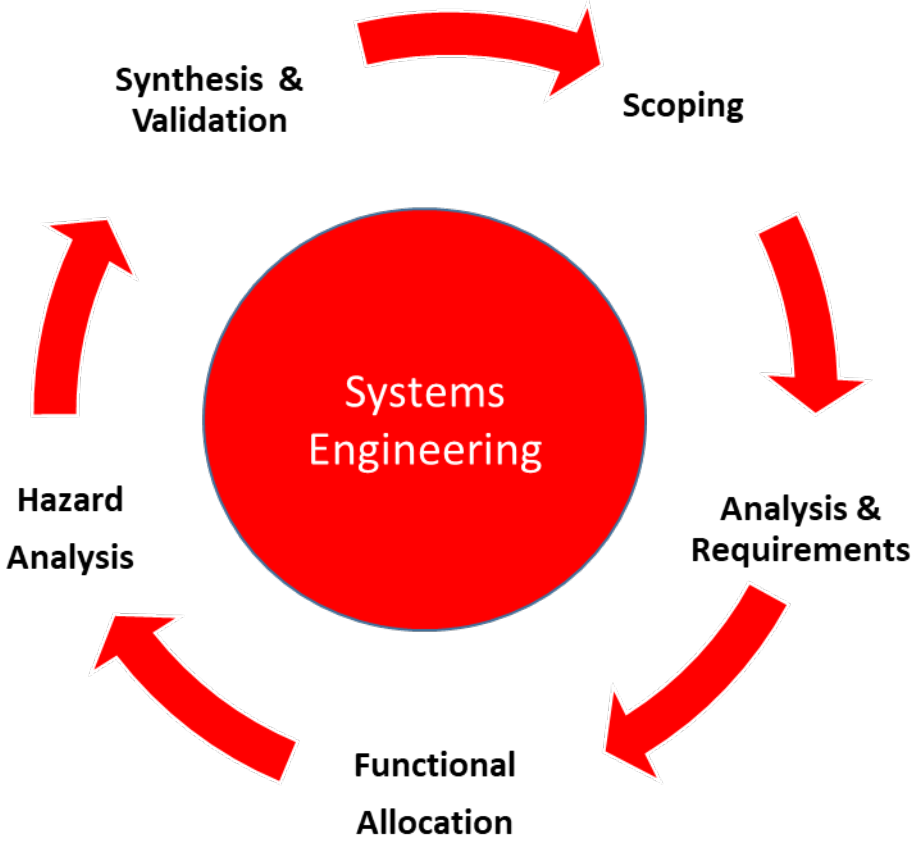
DEG Swimlane Visualization



© 2018 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Chapter 4 – Systems Engineering



- Phase Based using Perform/Confirm method
- Iterates through the SE process for each phase in a <u>non-liner fashion</u>
- Includes links to the topical chapters
- Iteratively converges on the final synthesized design
- Addresses:
  - Division of Responsibility (DOR)
  - Requirements Development
  - Hazard Analysis (including CCF) and Mitigations
  - Architecture Development
  - Functional Allocation (including Human/System Allocation)
  - Verification and Validation
  - Testing
  - Transition to the O&M Phase

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Digital Engineering Guide

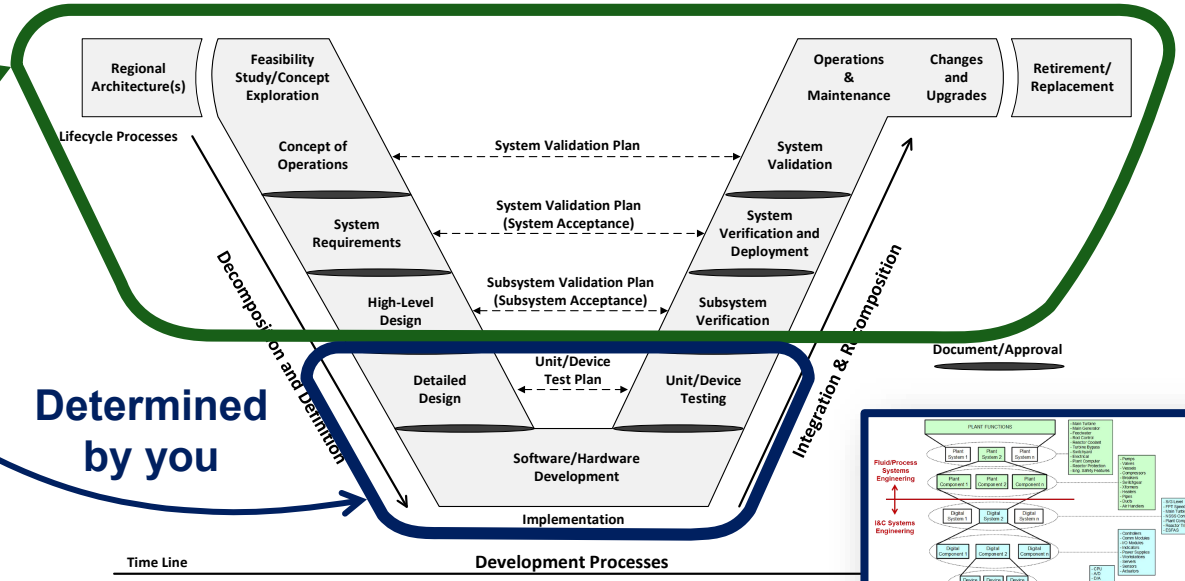
Real World Examples

© 2018 Electric Power Research Institute, Inc. All rights reserved.

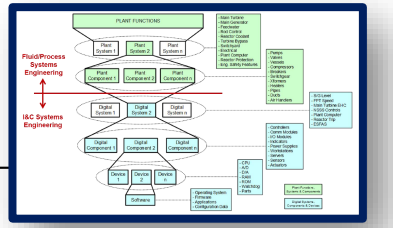
SE Process Example 1

1. Bounding Technical Req’ts.
2. Decide Parameter Values
3. Bench Evaluation
4. Refine Parameter Values
5. Specify Configuration

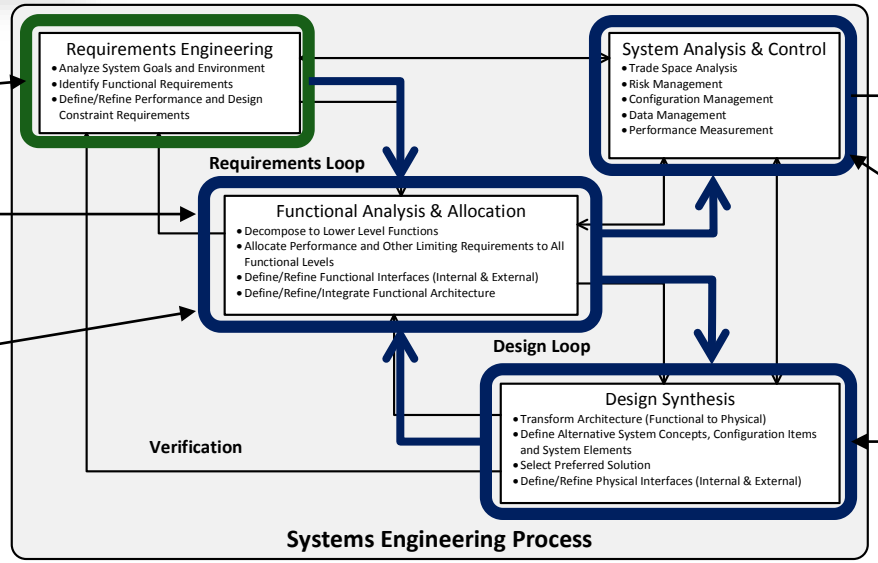
Predetermined by the plant and plant system designs.



Determined by you



1. Bounding Tech. Req’ts.
2. Decide Parameter Values
4. Refine Parameter Values



Configure, Install & Validate

5. Specify Configuration

3. Bench Evaluation

Also Consider:

1. Desktop Simulation
2. Reusable Style Guide
3. Model Number Optimization

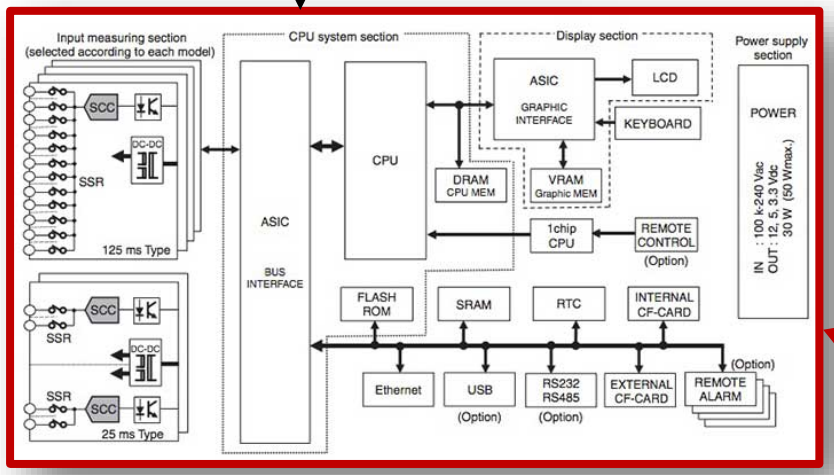
© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

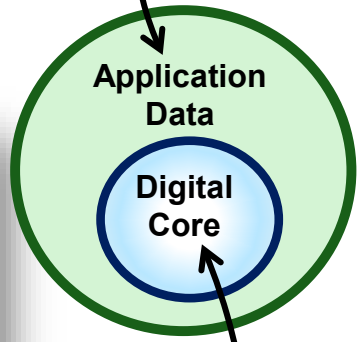
SE Process Example 1 (cont.)

1. Bounding Technical Req'ts.
2. Decide Parameter Values
3. Bench Evaluation
4. Refine Parameter Values
5. Specify Configuration

Fixed Program Language*



*per IEC 61508-3

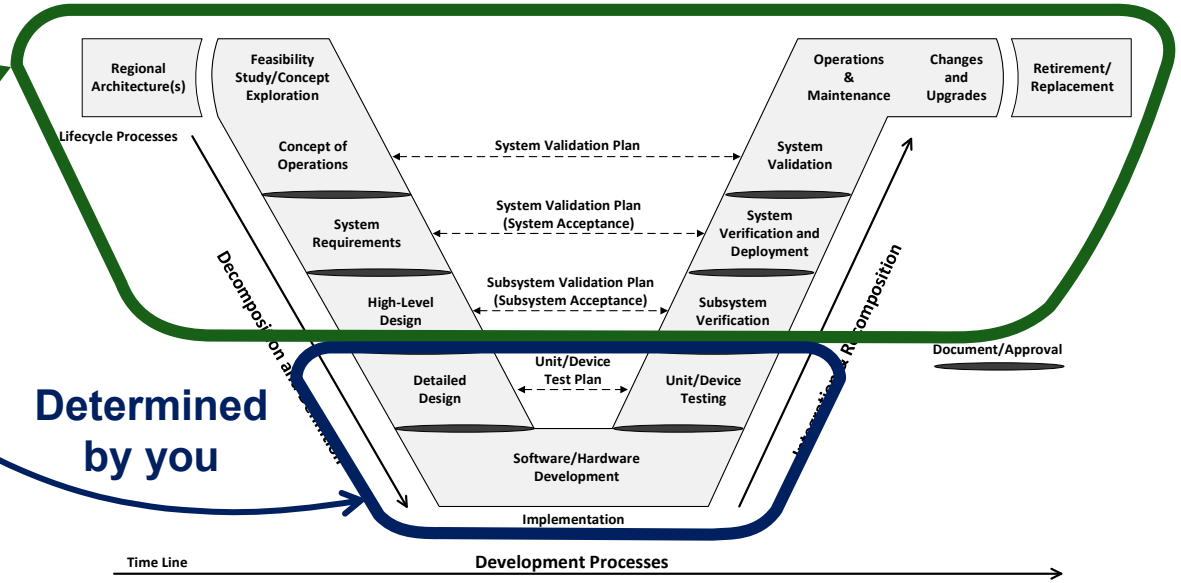


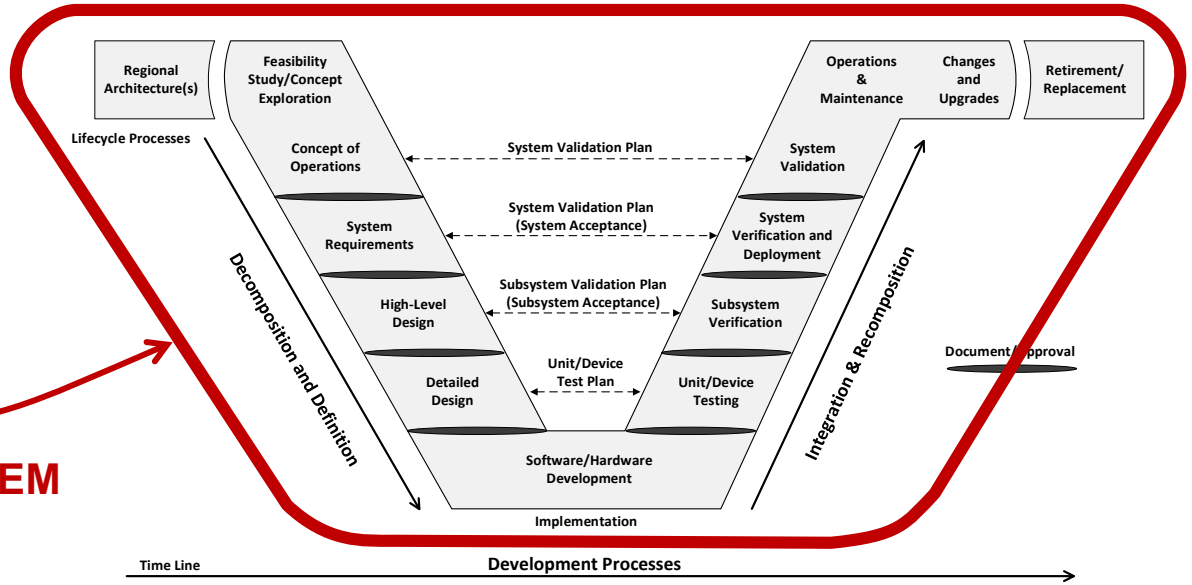
Full Variability Language*

Predetermined by the plant and plant system designs.

Determined by you

Performed by OEM

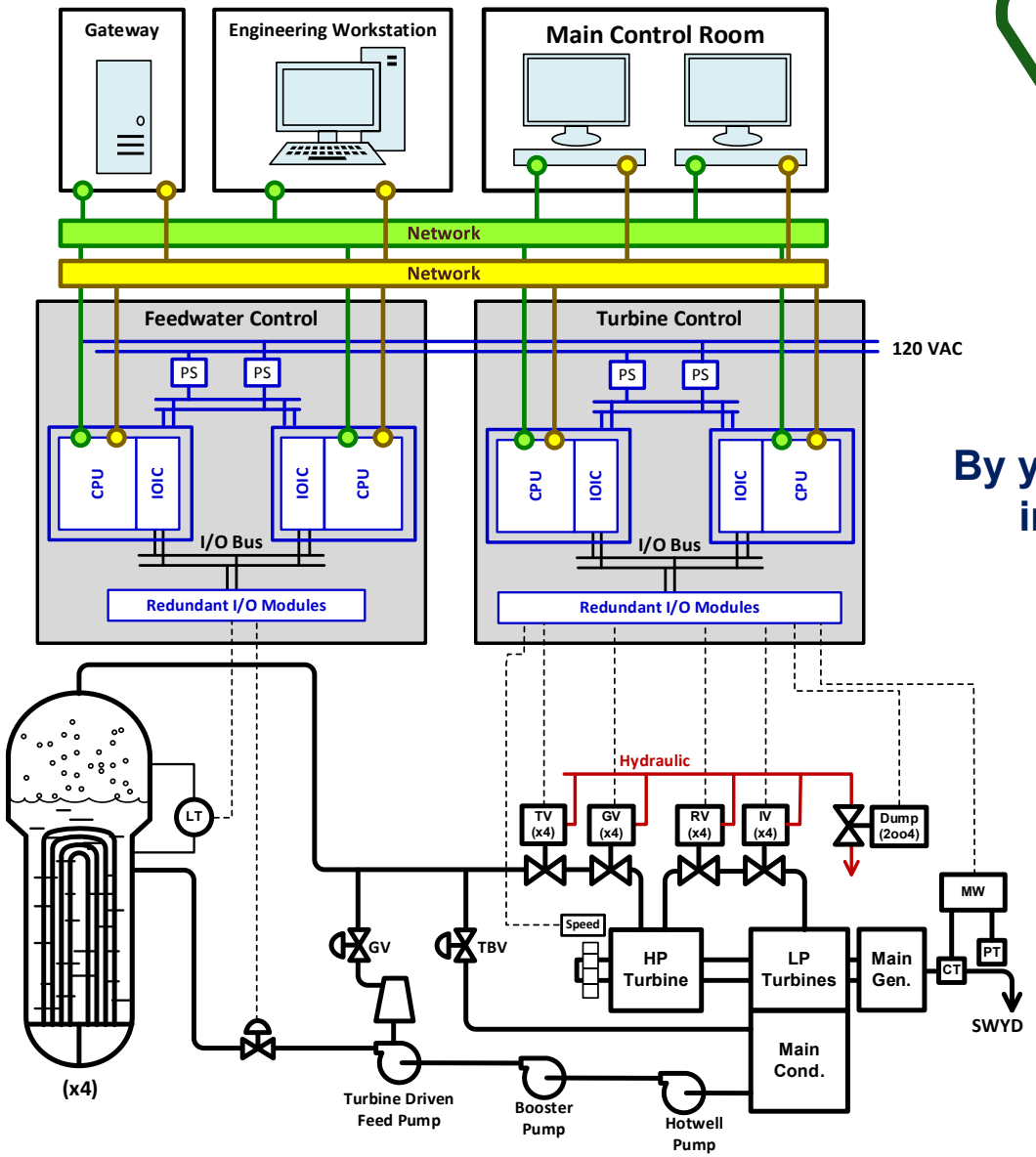




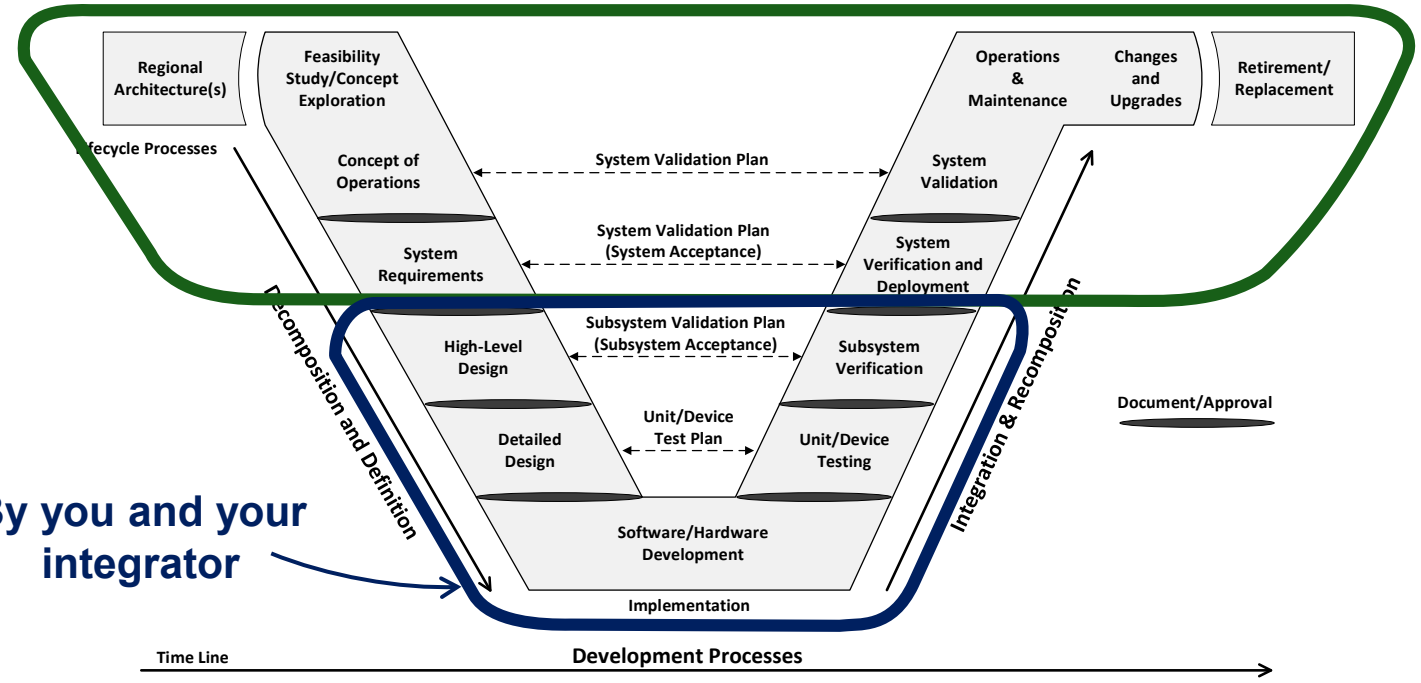
© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

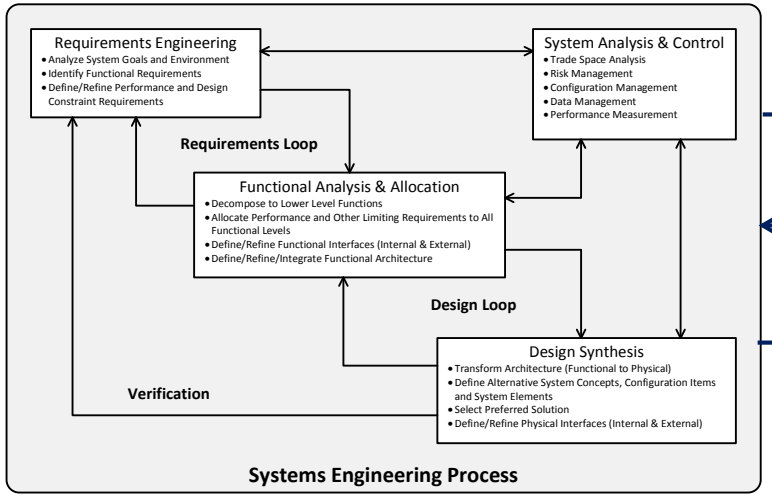
SE Process Example 2



Predetermined by the plant and plant system designs.



By you and your integrator



Common/ Conceptual Design (30%)

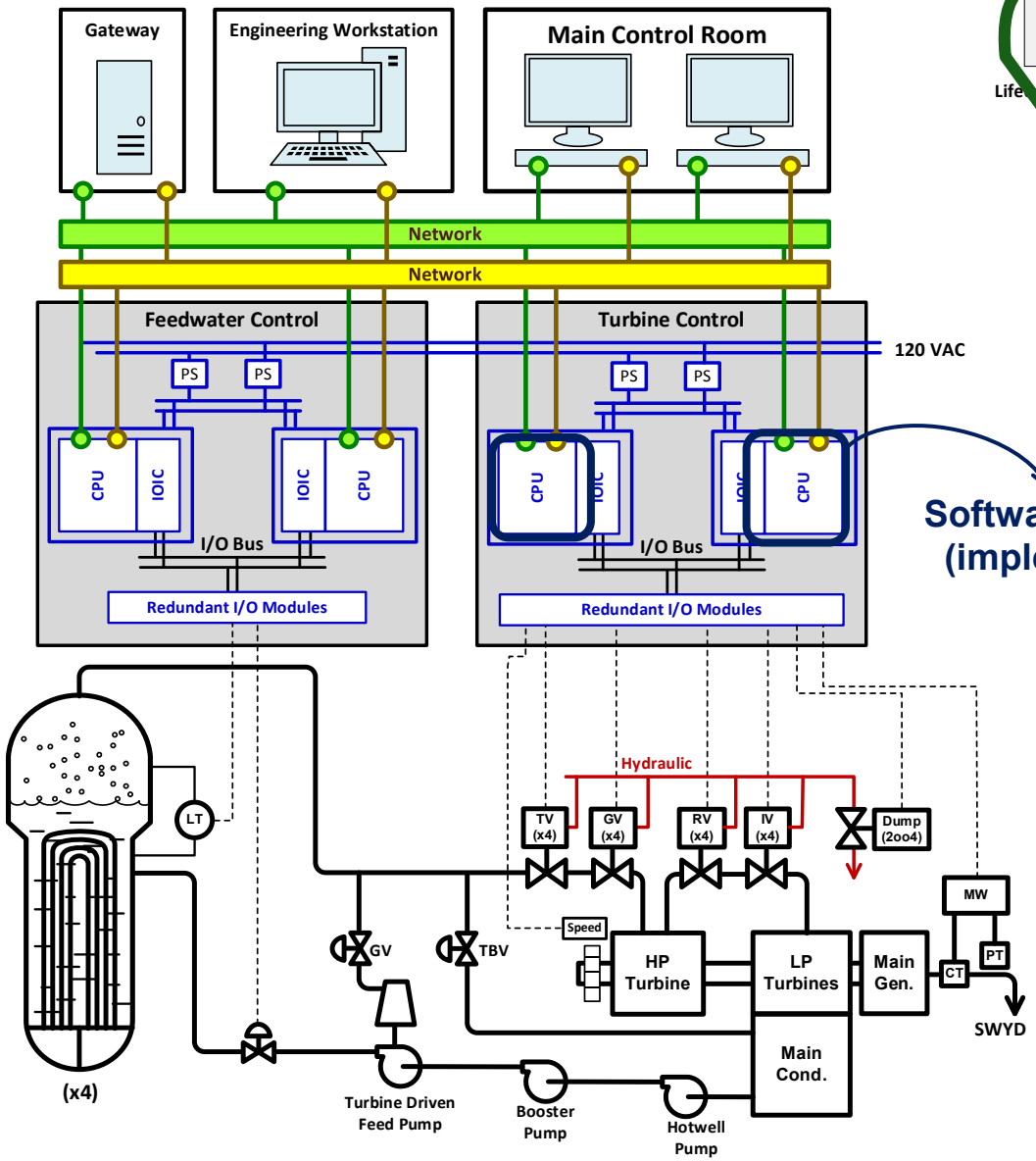
Detailed Design (100%)

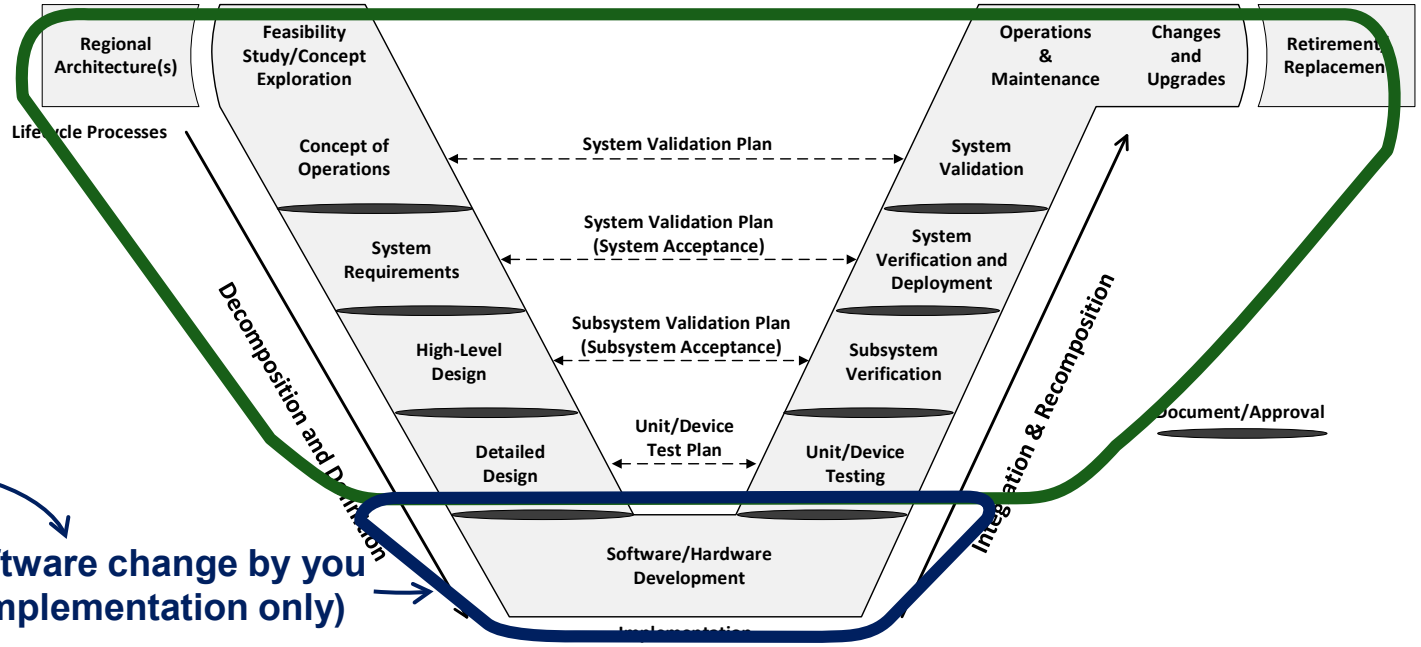
© 2018 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

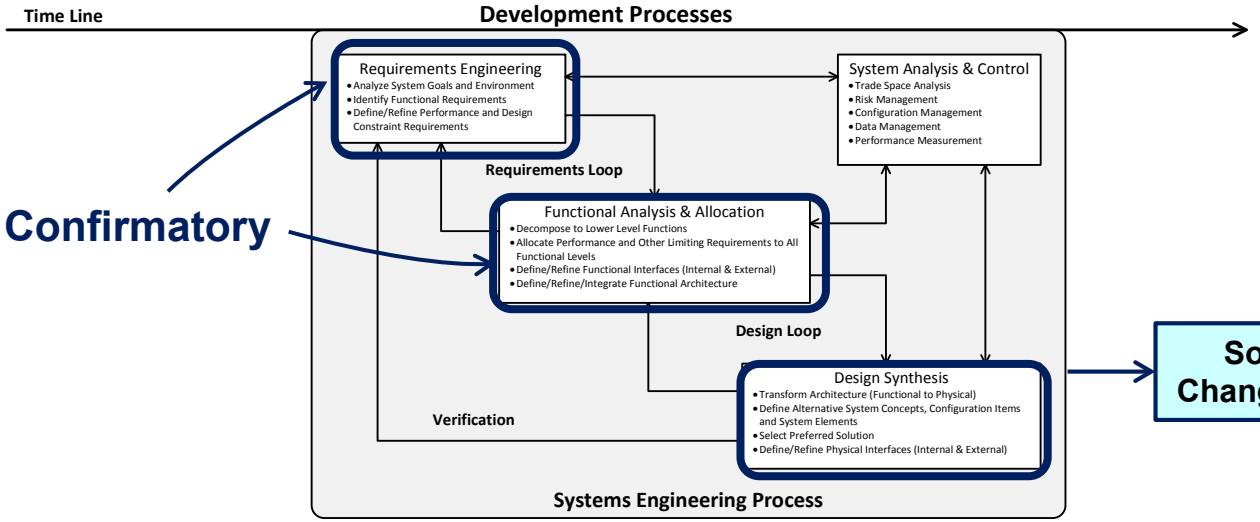
SE Process Example 3

Predetermined by the plant, plant system, and I&C system designs.





Software change by you (implementation only)



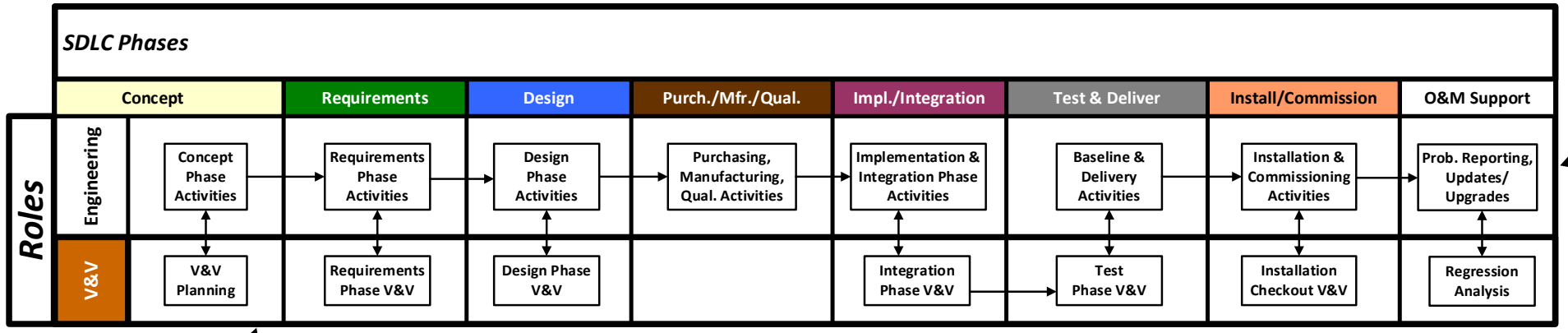
Confirmatory

Software Change (100%)

© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Systems Engineering Model evolves SQA

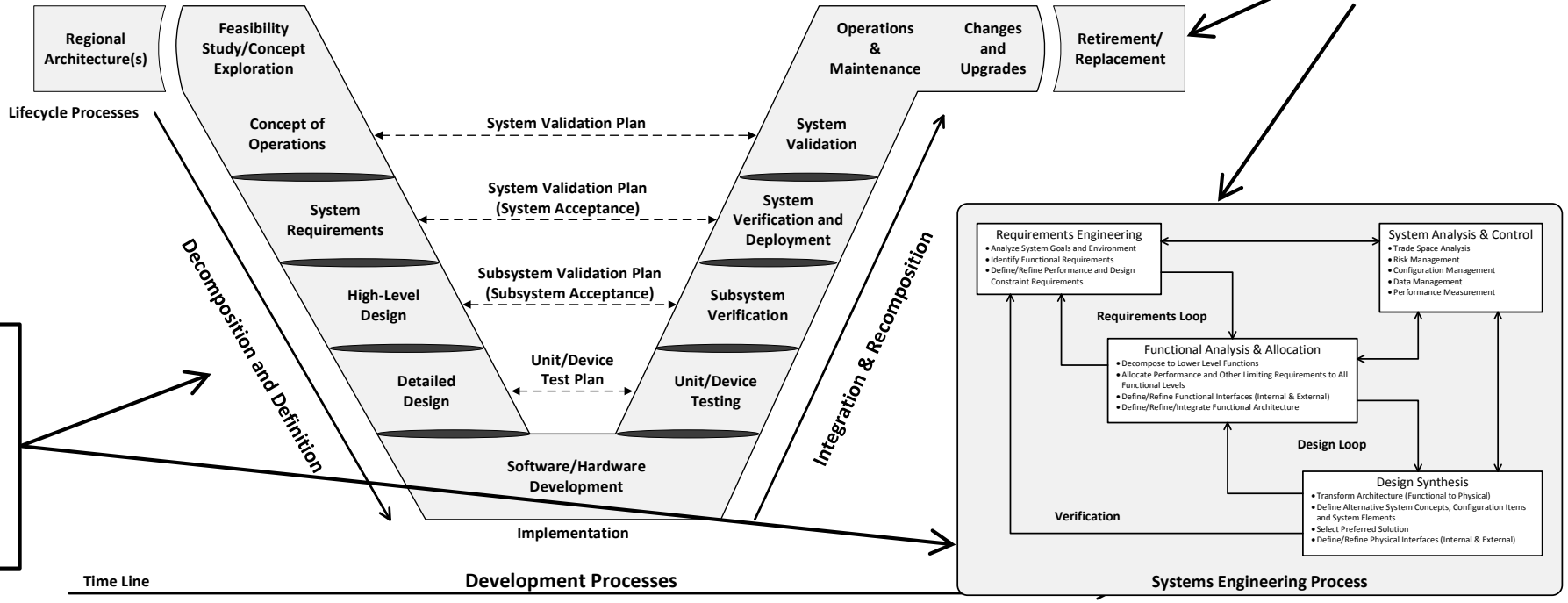


Traditional SDLC Only

Systems Engineering

A linear, gate-driven system development lifecycle (SDLC) process described in IEEE Stds.

An iterative process that promotes system architecting, decomposition, discovery, refinement, and recomposition, described in EPRI 3002008018

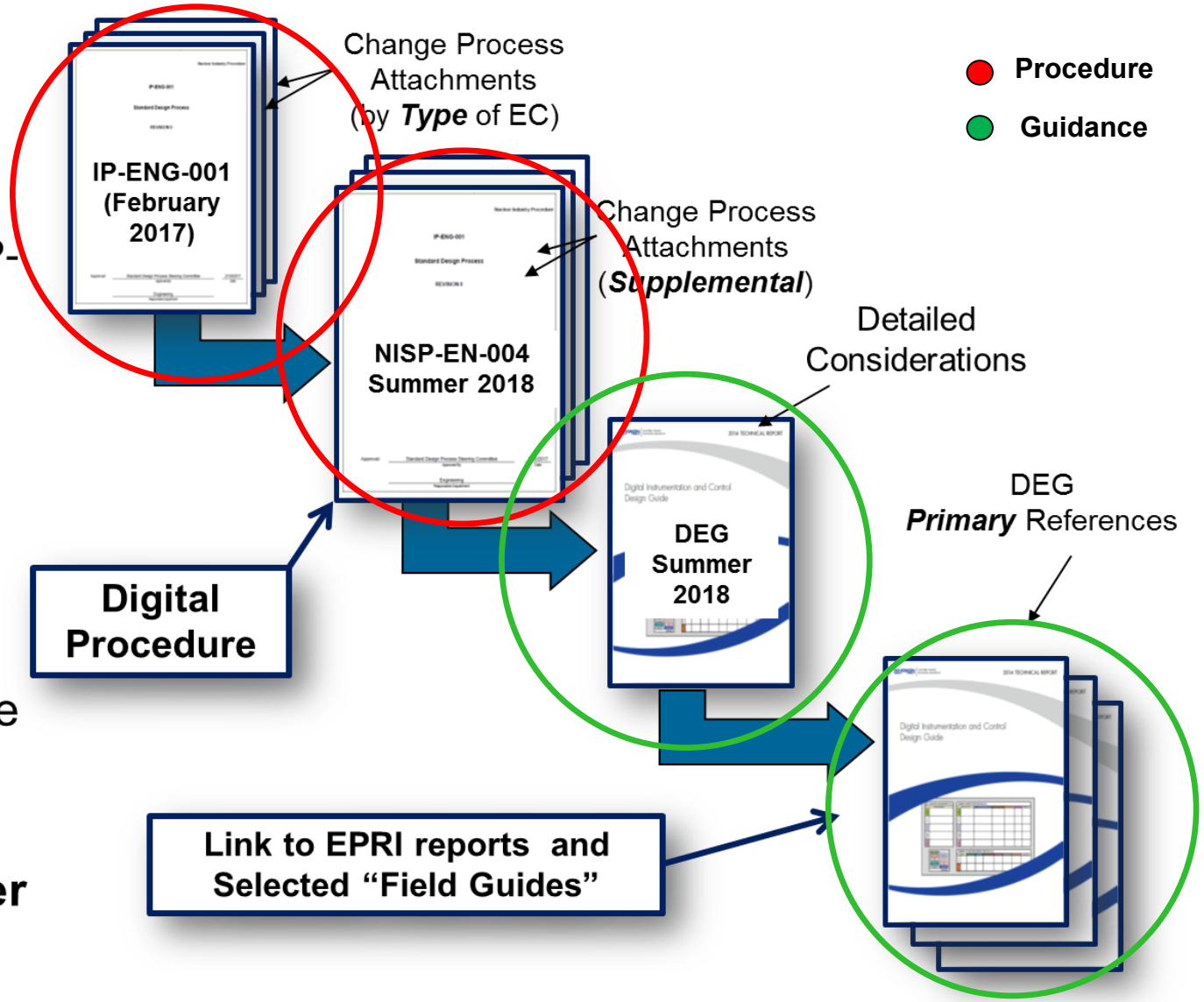


© 2018 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

US Industry Plan to Use the DEG

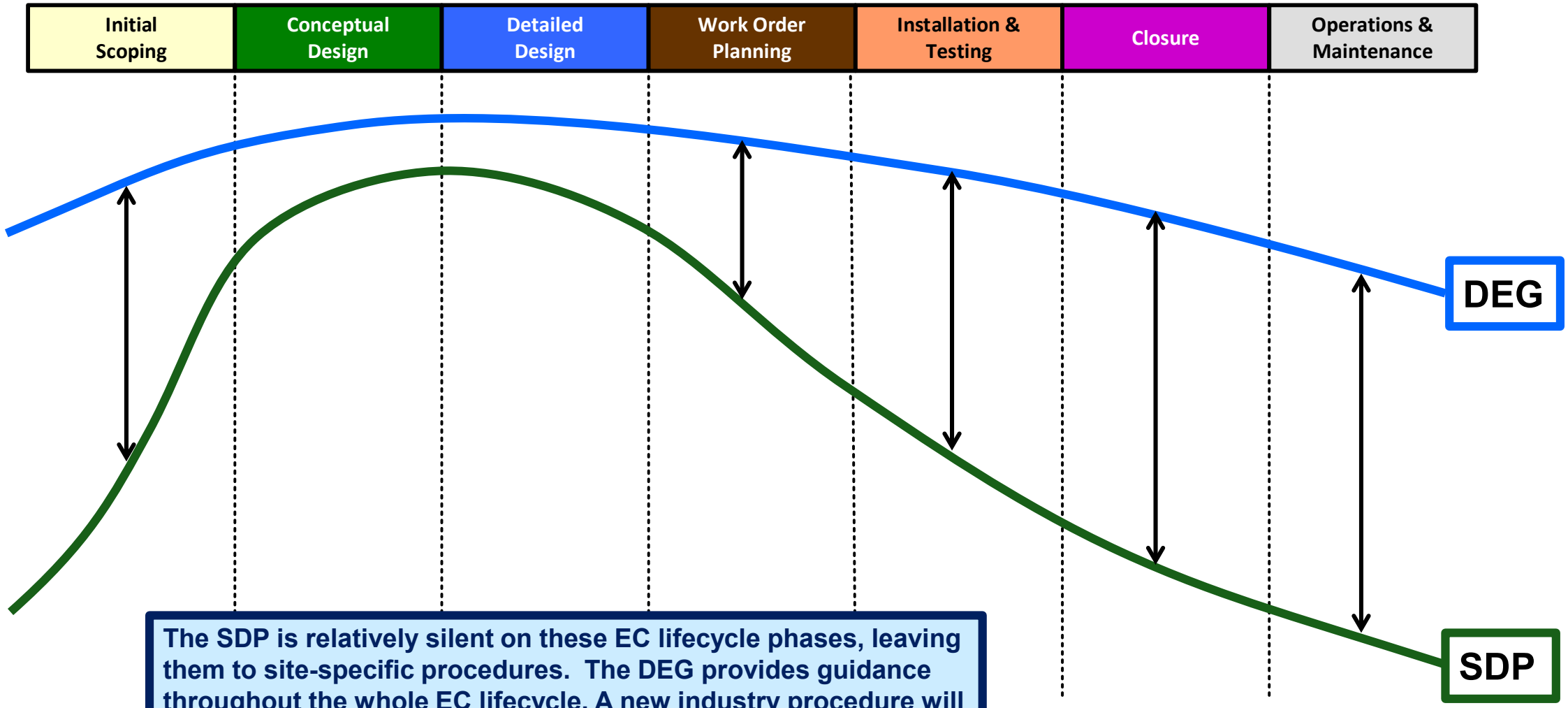
- IP-ENG-001 remains the Package Development Process
  - But revised (a little) to recognize NISP-EN-004 activities
- NISP-EN-004 is the Digital Specific Topical Procedure
  - Same process attachments as IP-ENG-001, tailored with DEG-specific supplemental information
  - Provides the user with "what to do"
- DEG still provides detailed guidance on design considerations, "skill of the craft", and primary reference
- **Digital Training and Tech Transfer completes the framework**



© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Relative Depths of SDP and DEG Guidance



The SDP is relatively silent on these EC lifecycle phases, leaving them to site-specific procedures. The DEG provides guidance throughout the whole EC lifecycle. A new industry procedure will provide the "glue" between the SDP and the DEG.

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Topical Area Perspectives

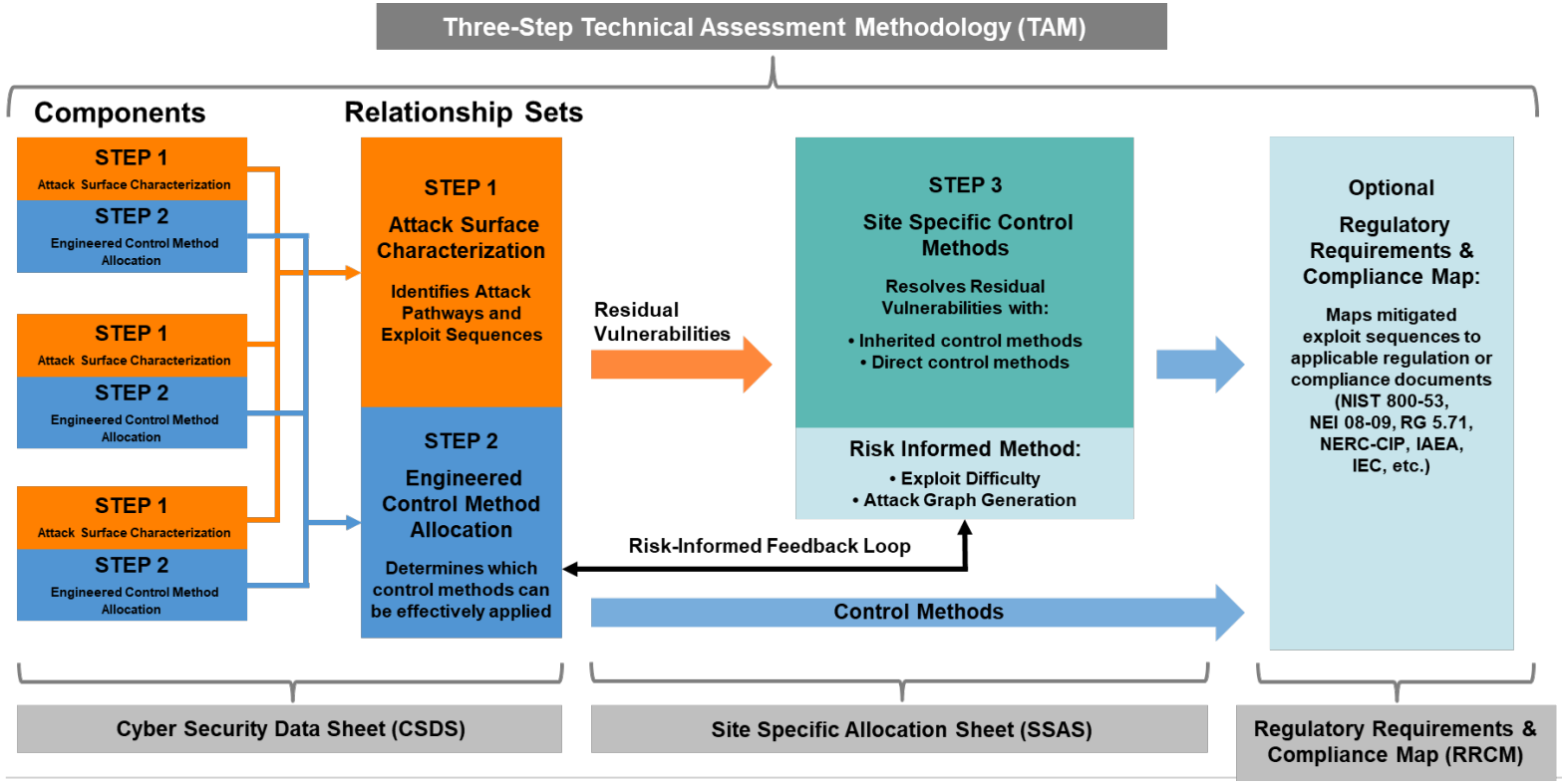
Cyber Security/Engineering Integration
Risk and Reliability/Engineering Integration

© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI Technical Assessment Methodology (TAM)

- TAM published Oct 2016
- Early Utility adopters
  - Vogtle 3&4
  - Barakah(UAE)
  - Horizon (UK- under consideration)

- Revision 1 scheduled for August 2018
  - EPRI Product ID: 3002012752
  - Compatible with most existing standards and regulation including IEC 62443
  - **Integration with Supply Chain Fall 2018**

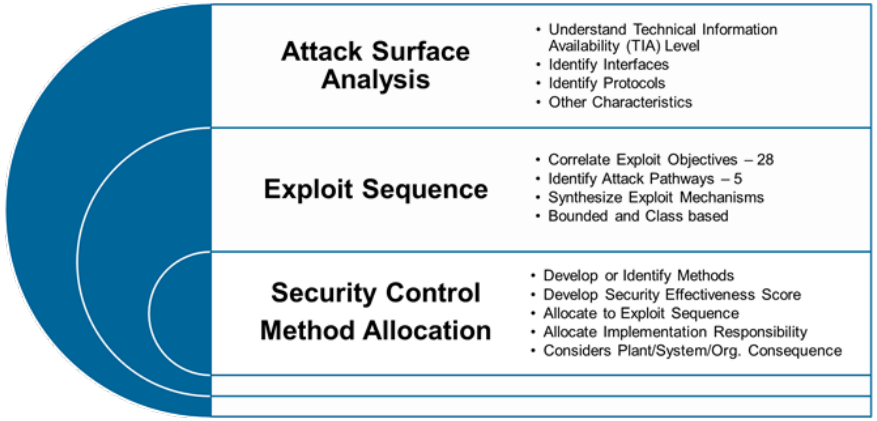


- **Designed to integrate into the overall engineering and design processes, including the DEG.**
- Leads the transition to sustainable engineering-based cyber assessment and mitigation methodologies.
- Standardizes the assessment methodology and documentation

© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI Technical Assessment Methodology (TAM)

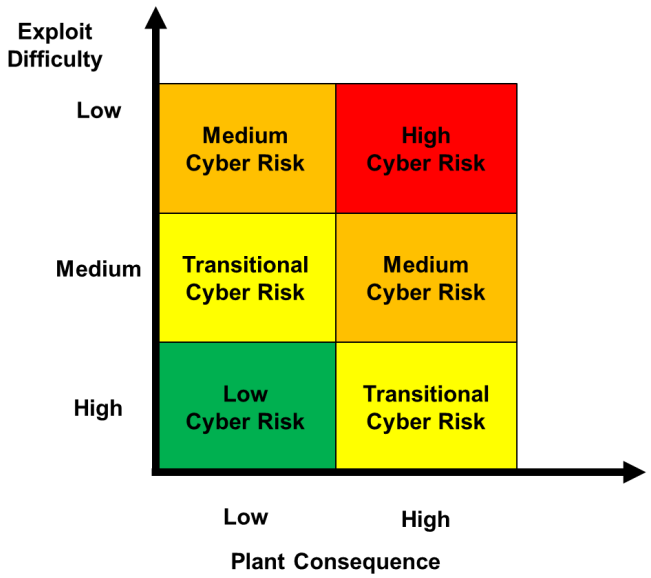
- Key Features
- Efficient and complete
  - Identifies actual vulnerabilities and exploit sequences via data flow and control flow analysis
  - Identifies the most effective mitigation
  - Scores the exploit difficulty for use with consequence and risk methods becoming risk informed
- Leverages non-traditional control methods
  - Identifies normal system features that can be used for security functions (e.g. Maintenance Logs)
- Modular
  - Can be executed by different organizations, in different places, and at different times.
  - Modular results can be combined through Relationship Sets to achieve holistic outcomes.
  - Can be used anywhere. From within the supply chain through operational commissioning, Including the constriction phase.
  - Can be used to assess services as well.



© 2018 Electric Power Research Institute, Inc. All rights reserved.

Risk Informed Cyber Security Methods

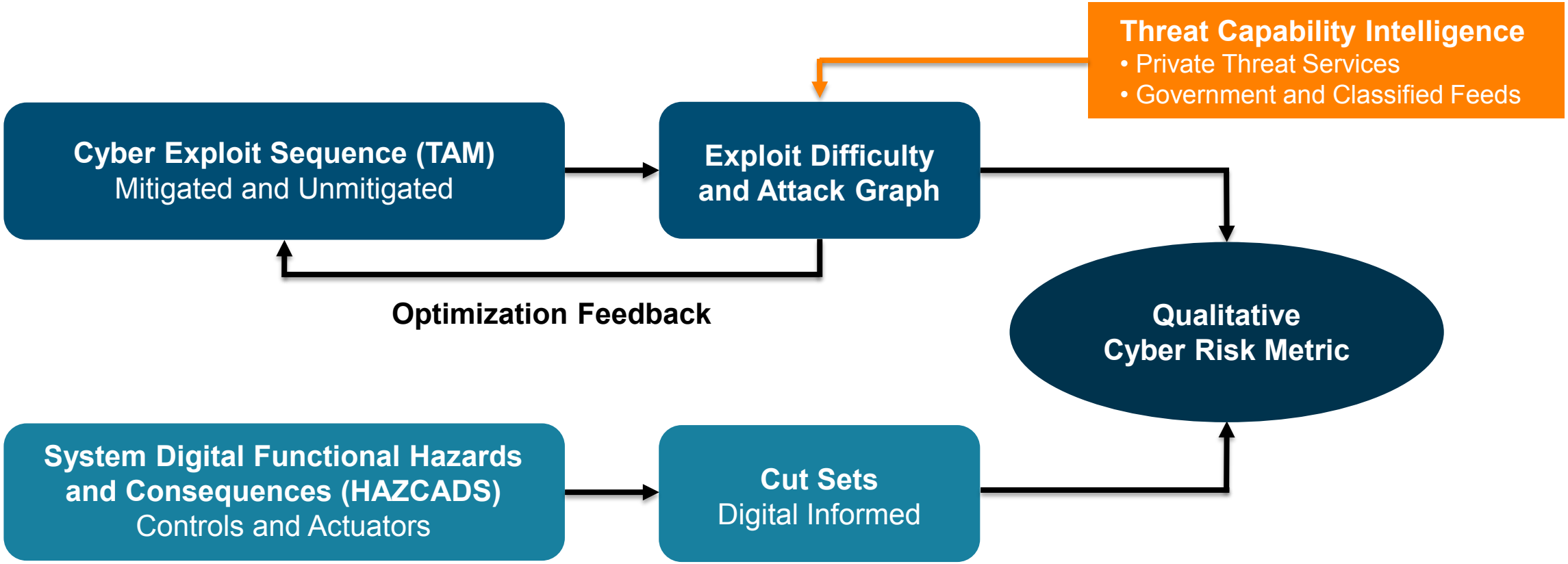
- A qualitative approach is needed given the software based nature of cyber vulnerabilities and threat variabilities.
- Method uses exploit difficulty vs. equipment failure probabilities
- Traditional PRA approaches lack the insight and completeness required to provide an accurate or complete cyber risk.



- **Industry Benefits include the ability to:**
  - aligns resources with actual risk
  - reduce cyber vulnerability mitigation cost
  - limit cyber mitigation to a sustainable but effective scope
  - provide consistent cyber risk determinations
  - improve digital risk insights generally
  - Integrates with broader Risk Informed Initiatives, (i.e. 10CFR50.69)

© 2018 Electric Power Research Institute, Inc. All rights reserved.

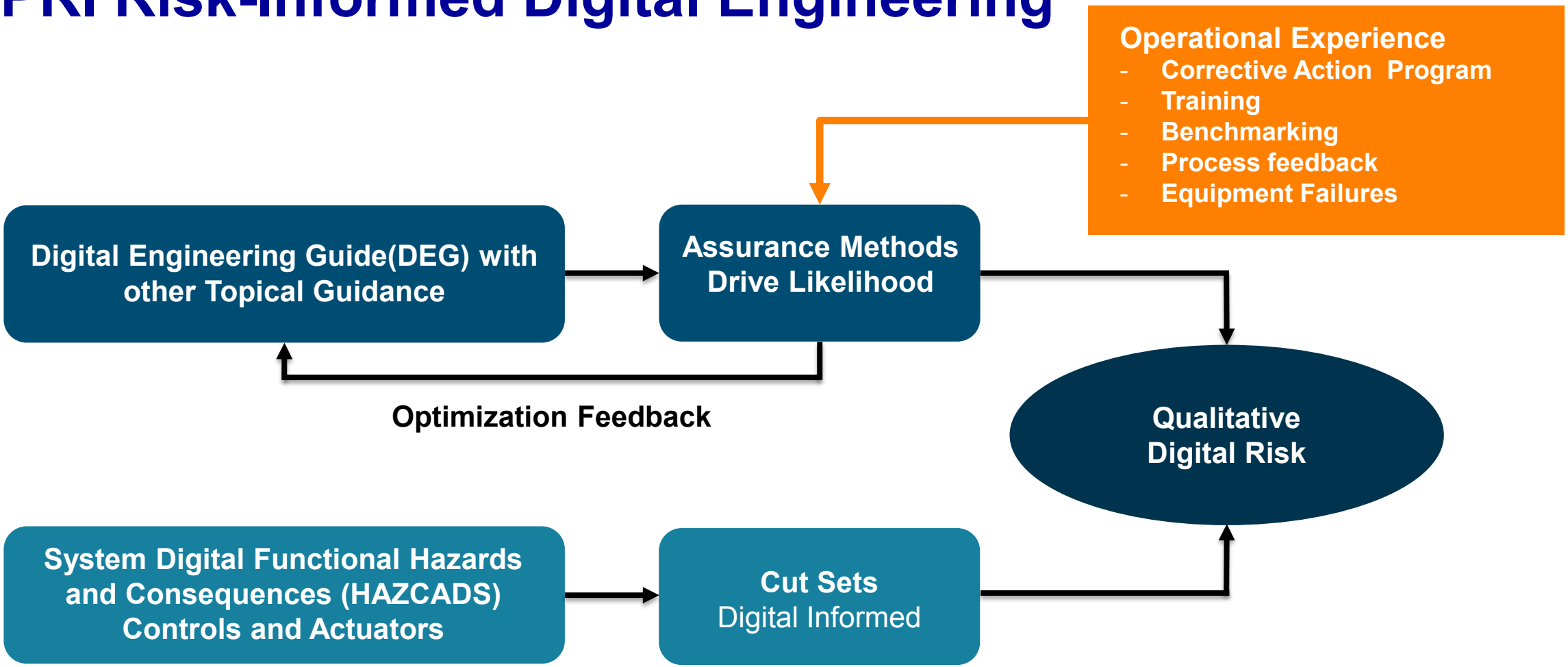
EPRI Risk-Informed Cyber Security Process Model



Effective vulnerability mitigation based on analyzed consequences informed by threat capability intelligence can dramatically REDUCE THE SENSITIVITY of a nuclear facility to changes in the threat environment.

© 2018 Electric Power Research Institute, Inc. All rights reserved.

EPRI Risk-Informed Digital Engineering



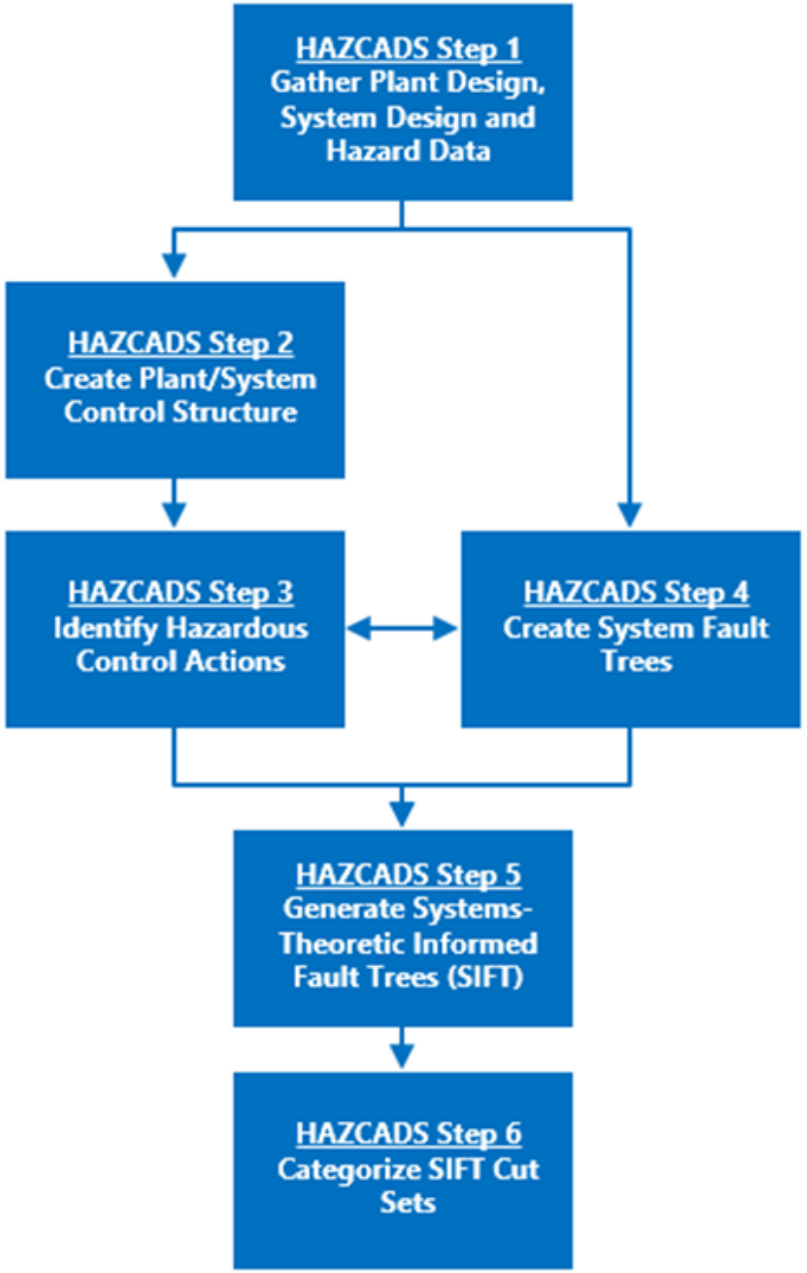
Effective Digital Hazard Identification and Mitigation can dramatically REDUCE THE SENSITIVITY of a nuclear facility to problems with Digital Technology introduction.

© 2018 Electric Power Research Institute, Inc. All rights reserved.

HAZCADS (Dec 2018 > 3002012755)

- Hazard and Consequence Analysis for Digital Systems(HAZCADS)
- **Derivative of Hazard Analysis Methods for Digital Instrumentation and Control Systems -3002000509**
- Uses System Theoretic Process Analysis(STPA) and Fault Tree Analysis(FTA)
- Discovers and Analyzes Plant/System Level Hazards that are related to digital technology
- Qualitatively informs mitigating design and operational features and controls

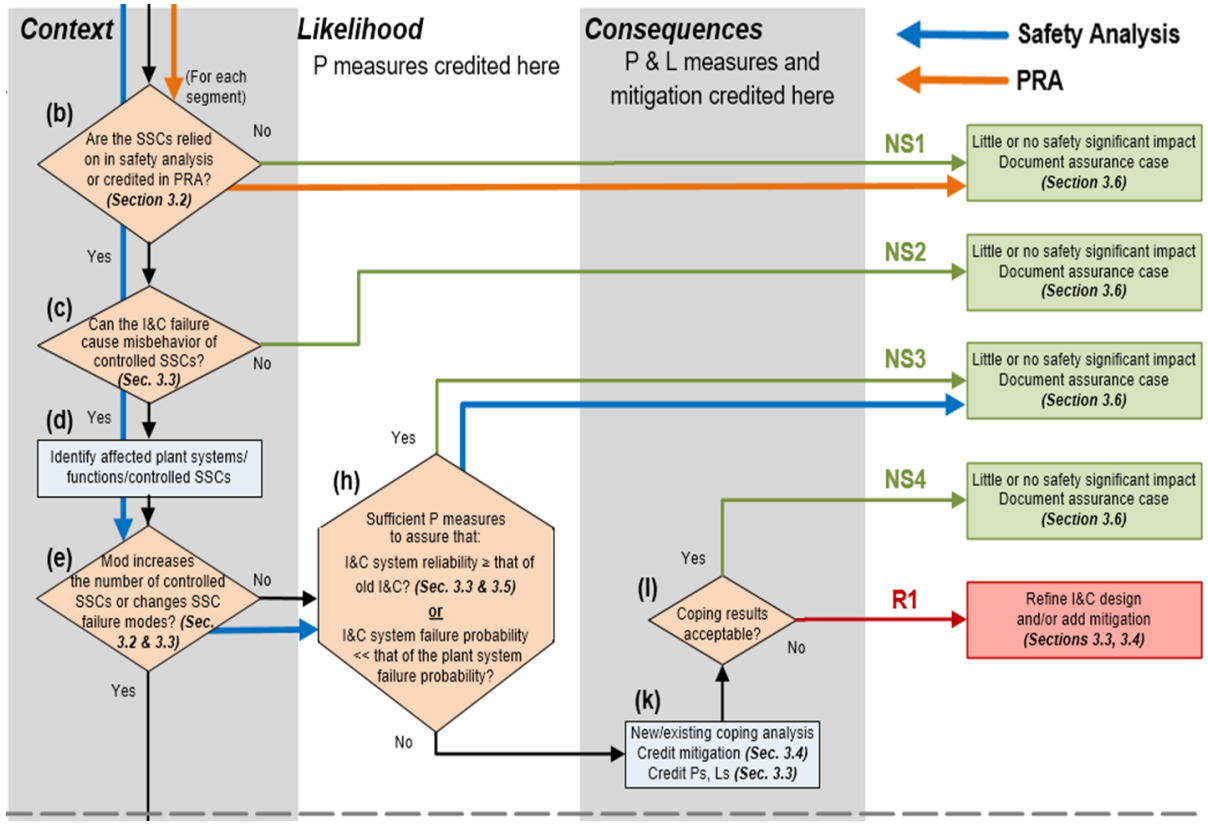
- **Used for:**
  - **Cyber**
  - **Common Cause Failure**
  - **Single Point Vulnerability**
  - **Safety Analysis**
  - **EMI/RFI**



© 2018 Electric Power Research Institute, Inc. All rights reserved.

Common Cause Failure Guide (CCF) Update

- **EPRI 3002005326** - *Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems* (June 2016)
  - Realization that the *complete* risk informed CCF method should be refined and utilized.
  - Potential to become a key element in risk Informing Digital I&C.
  - Revision 1 planned for 2018/2019
    - Shift to a Hazard Based Risk Method
    - P&L measures will become prototypes
    - Update Terminology to match IEC 61508
    - Integrated into Digital Engineering Guide

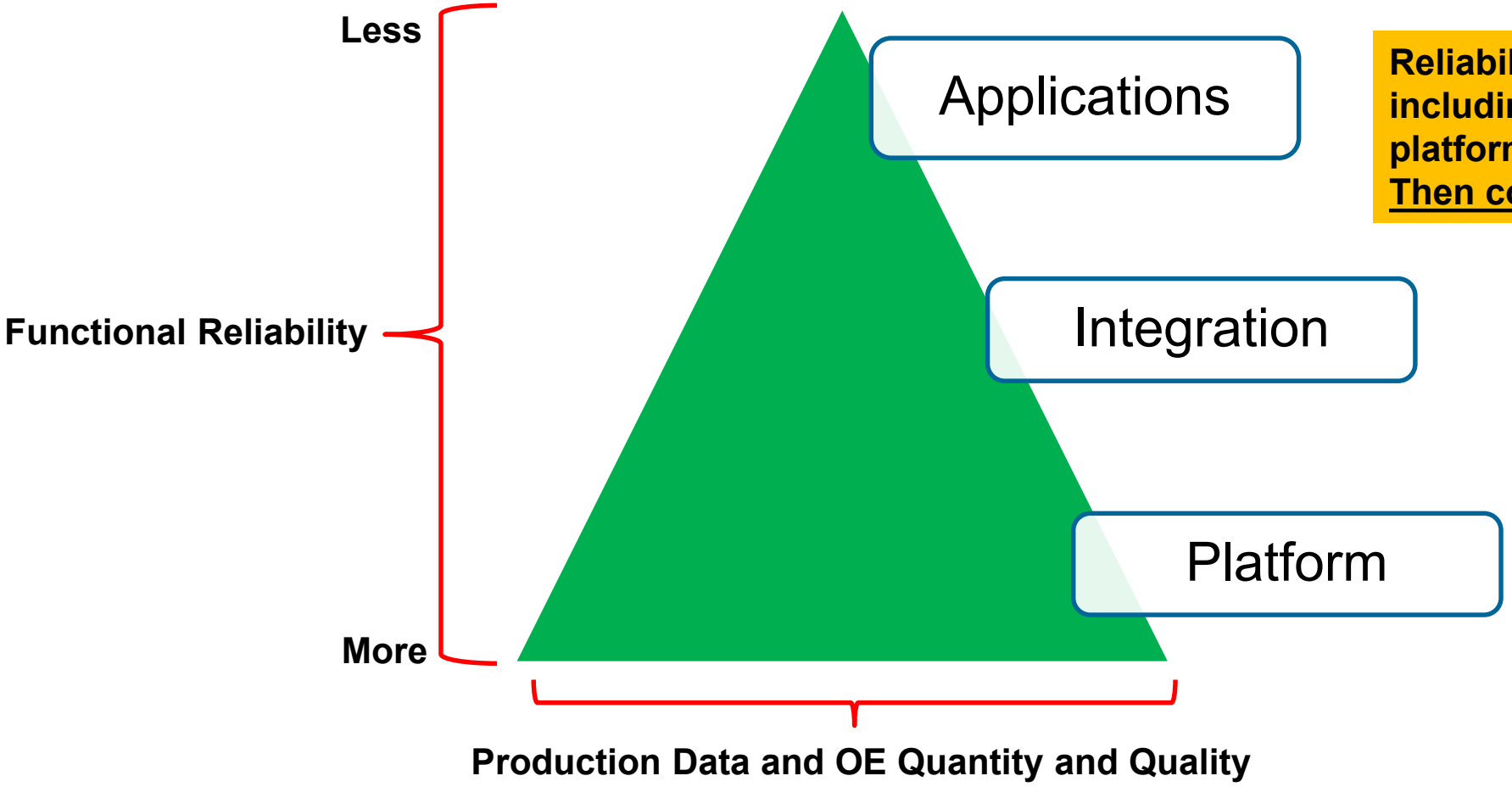


- **Integration of Hazard/Risk methods**
- **Develop to a field usable Methodology**

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Platform vs. Integration vs. Application Reliability

- Emphasis on Platform issues likely misplaced.



Reliability, especially software reliability, including CCF, should be segmented by platform, Integration, and application. <u>Then considered separately</u>

© 2018 Electric Power Research Institute, Inc. All rights reserved.

Questions

© 2018 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity

© 2018 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE