Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Open Session

Docket Number: (n/a)

Location: teleconference

Date: Wednesday, September 7, 2022

Work Order No.: NRC-2076 Pages 1-89

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1716 14th Street, N.W.
Washington, D.C. 20009
(202) 234-4433

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, as reported herein, is a record of the discussions recorded at the meeting.

This transcript has not been reviewed, corrected, and edited, and it may contain inaccuracies.

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

698TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

WEDNESDAY

SEPTEMBER 7, 2022

+ + + + +

The Advisory Committee met via videoconference at 1:30 p.m., Joy L. Rempe, Chairman, presiding.

COMMITTEE MEMBERS:

JOY L. REMPE, Chairman

WALTER L. KIRCHNER, Vice Chairman

DAVID A. PETTI, Member-at-Large

RONALD G. BALLINGER, Member

VICKI M. BIER, Member

CHARLES H. BROWN, JR., Member

VESNA B. DIMITRIJEVIC, Member

GREGORY H. HALNON, Member

JOSE A. MARCH-LEUBA, Member

MATTHEW W. SUNSERI, Member

ACRS CONSULTANTS:

DENNIS BLEY

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

P R O C E E D I N G S

(1:30 p.m.)

CHAIRMAN REMPE: Okay, folks, it's 1:30 p.m. on the East Coast. So this meeting will now come to order.

This is the first day of the 698th meeting of the Advisory Committee on Reactor Safeguards. I'm Joy Rempe, Chairman of the ACRS. Other members in attendance are Ron Ballinger, Vicki Bier, Charles Brown, Vesna Dimitrijevic, Greg Halnon, Walt Kirchner, Jose March-Leuba, Dave Petti, and Matt Sunseri. I note we do have a quorum. Today, the Committee is meeting in-person and virtual.

The ACRS is established by the Atomic Energy Act and is governed by the Federal Advisory Committee Act. The ACRS Section of the U.S. NRC public website provides information about the history of this Committee and documents such as our charter, bylaws, Federal Register Notices (audio interference) at least the meetings that are open.

The Committee provides advice on safety matters to the Commission through its publicly available letter reports.

The Federal Register Notice announcing this meeting was published on August 10, 2022. This announcement provided a meeting agenda as well as instructions for interested parties to submit written documents or request opportunities to address the Committee.

The Designated Federal Officer for today's meeting is Ms. Christina Antonescu. A communications channel has been opened to allow members of the public to monitor the open portions of the meeting.

The ACRS is now inviting members of the public to use the MS Teams link to view slides and other discussion materials during these open sessions. The MS Teams link information was placed in the Federal Register Notice and agenda on the ACRS public website.

Periodically, the meeting will be open to accept comments from participants listening to our meeting. Written comments may still be forwarded to the Designated Federal Officer.

During today's meeting, the Committee will consider the following topics: Proposed New Regulatory Guide 1.250, Dedication of Commercial-Grade Digital I&C Items for Nuclear

Power Plants; and, two, SHINE Memoranda Review and Deliberation/Report Preparation.

A transcript of the open portions of the meeting is being kept, and it's requested that speakers identify themselves and speak with sufficient clarity and volume so they can be readily heard. Additionally, participants should mute themselves when not speaking.

Before we start today's meeting, I want to take some time to highlight a couple of items. First, one of our staff members has received a significant recognition. Senior Staff Engineer Mike Snodderly has been awarded an NRC Meritorious Service Award in recognition of his exemplary performance, initiative, and dedication to the NRC's Operating and New Reactor Safety Programs. Mr. Snodderly received this award for his lasting contributions to technical support issues facing ACRS.

Most recently, he worked with ACRS members to implement novel ways for the Committee to establish and meet an aggressive review schedule for the NuScale design certification application. His efforts enabled the ACRS review to be completed on an unprecedented schedule.

In addition to his technical support work with the Committee, Mr. Snodderly also served at Commission staff level and as branch chief during his 32-year NRC career. Mr. Snodderly exhibits a proven level of superior performance and strong leadership that is a credit to himself and the agency.

I also want to express our appreciation to Members Halnon and Ballinger, along with ACRS staff members Weidong Wang, Chris Brown, and Mike Snodderly, for our well-organized visit to Region II, the Byron Station, and the SHINE facility. These visits help us better perform our duties as ACRS members and I've missed the years when the pandemic prevented them.

At this time, I'd like to ask other members if they have any opening remarks.

Not seeing any, I'd like to ask Member Charles Brown to lead us through our first topic for today's meeting. Charlie?

MEMBER BROWN: Okay, thank you. I'm going to try to provide a slight summary of the last meeting, since it's been a while, and a little bit of a calibration on how these two things fit together.

Currently, the commercial -- you've got Topical Reports, which make formal declarations, and NRC reviews and they approve them. And it can be for whatever it is, whether it's a commercial item that's been tested, and whatever it is, you all can approve that.

Right now, there is a -- then their commercial certification is done under Reg Guide 1.164, which references some EPRI documents and Topical Report, which I will mention in there, and that Topical Report generally characterizes critical characteristics and attributes as being physical performance and dependability.

And, therefore, the commercial certification is reviewed trying to satisfy those three main functions.

And that's kind of an arbitrary categorization, the way they put them together. They presented that last time.

Dependability is the hard one. The first two, you can kind of test and do things. The last one is a little bit more cerebral, the way I view. It's not as easy to prove dependability as it is to test something.

The Reg Guide 1.250 is an effort to now

utilize an international standard, which develops something called safety integrity levels one through four, and that if the certifying -- I'm not going to get into the dedication bodies and all that.

If it comes to that process, now it is available for people to use and they are proposing to accept that as the -- what's the word? I forgot the words now. Satisfying the dependability category or characteristic, okay?

So, when we reviewed this last time, we didn't have the IEC or we couldn't find it. So I was able to get that this time.

I hope none of the rest of you tortured yourself by trying to look at it.

So anyway, the object now, we went through that, so the effort here now, it says, follow 1.250 and they meet these SIL type requirements for whoever they're getting the stuff from.

In other words, if they get a computer card that's been used in numerous projects, everybody says it's reliable, we don't have to do anything.

They accept that as the certification

for the review of the application of the stuff in the nuclear power plants. I may have overstated it, but I think that's close enough.

So, that's what they are now going to rephrase or redo this time. We made some comments last time and I didn't -- I saw what you all had proposed.

I'd like to say I remember every one of them. I did this two weeks ago. And they're going to present that in a summary package.

And I have a few questions at the end so as we don't disturb the flow. Did I get most of that right? Okay.

And we've got both the staff and NEI will be presenting, for your information.

MR. BENNER: Okay, so thank you, Member Brown, Chairman Rempe, and members of the Committee. Can you hear me?

MEMBER BROWN: A little closer.

MR. BENNER: People usually don't say I don't talk loud. So, but that characterization is accurate.

I'll step it back just a little bit, because way in the past, nuclear power plants typically would purchase components from what we

call Appendix B supply. All Appendix B --

MEMBER BROWN: I forgot that part, I'm sorry.

MR. BENNER: No, no it's a good -- it's a good clarification.

MEMBER KIRCHNER: Could you identify yourself for the reporter?

MR. BENNER: I'm sorry. Okay. This is Eric Benner, the Director of the Division of Engineering and External Hazards at NRC's Office of Nuclear Reactor Regulations.

So those suppliers were called Appendix B because it refers to the part of the NRC's regulations that contain our quality assurance requirements, 10 CFR 50, Appendix B.

But over time, there have been fewer and fewer suppliers who wish to go through all the challenges of providing things to that quality standard.

So that begat the creation of what we call commercial grade dedication programs, which is what Member Brown was talking about.

We have guidance that has been in place for a while for how licensees can do this dedication process.

Essentially, make their own determination that components meet the quality assurance standards of 10 CFR 50 Appendix B.

As that has become more prevalent, there have been these generic entities that have taken on some of those responsibilities so that individual licensees didn't have to do all those steps themselves.

So like I said, we've had guidance in that area and time marches on. As we've talked about, there are, in those criteria are expectations for determining the dependability of those components.

As time marched on, there's this IEC standard that has the safety integrity levels that gets part of dependability of components.

So, this effort and this regulatory guide is basically a roadmap of how licensees can use that SIL certification within their commercial grade dedication programs to satisfy the dependability characteristic standards.

DR. BLEY: Eric?

MR. BENNER: Yes.

DR. BLEY: This is Dennis Bley.

MR. BENNER: Hey, Dennis.

DR. BLEY: Have we -- have we gathered any careful analysis of how commercial dedicated components have performed compared to those that go through the old process? Reliability parameters or things like that?

MR. BENNER: I'm going to give more of a process answer and see if anyone jumps in to help me.

Even for commercial grade dedicated items, the licensees have reporting requirements under 10 CFR Part 21.

And under those reporting requirements, if there's a belief that components have different failure mechanisms, that gets reported and gets transmitted to different entities.

I mean, I used to be in what is now called the Operating Experience Branch, MOR, and we look at all those reports as well as other failure reports, and I can just say anecdotally that we didn't see any what I would call weaknesses overall in this commercial grade dedication process.

I think at the end of the day, the licensees have the responsibility. In some ways, on one level it's better because the licensee who

is the responsible entity for operating that facility now is taking on the responsibility to say, yes, this component meets these quality standards that they're held to.

So, like in any process, we find design defects. We find different flaws and everything.

But I think overall we would say the commercial grade dedication process has been a huge success.

DR. BLEY: Okay. I appreciate the process comments and I'm sure they're all correct.

We do have large databases now, equipment, reliability, and it just seems like somebody from industry or maybe OpE at NRC ought to tease that data apart and see if we see any differences.

I know we're using plant--specific data when we look at the theories for plants, and that kind of takes care of it all, but I think the larger question probably deserves an answer.

And I suspect the answer would make us feel good.

MR. BENNER: And we certainly will

take that back and see what kind of data we can tease out in that regard.

So that was the end of my expected remarks. And with that, if there are no other initial questions, I'll turn it over to Dinesh Taneja who is going to be giving the main part of our presentation.

MEMBER BROWN: Can I make one observation that I forgot on my input? When I said Reg Guide 1.164 was the kind of umbrella that they operate, 1.164 represents the EPRI document, and that EPRI document covers all types of equipment, not I&C.

There's a Topical Report also in every document that's funneled in that covers dedication of the electronic, digital electronic components, programmable components.

So it's kind of a two-piece. 1.164 is not all electronics. It's everything. Mechanical, all kinds of general stuff.

And this other part now is in there to cover the other stuff. So if you hear the two things, they're not -- they're not both the same.

One deals specifically with – they mention it in the slides, so that's why I brought

it up now. Thank you very much, Dinesh.

MR. TANEJA: Good afternoon, Member Brown and Chairman Rempe. My name is Dinesh Taneja. I am the I&C Technical Reviewer in NRR NRC Branch.

And I've been actually working on this particular topic since 2016, since we were directed by the Commission to modernize the digital, the INC regulatory infrastructure.

So one of the tasks that I've identified was to see if we can leverage this SIL certification process which has really matured over the last 15-20 years into the commercial grade dedication process. Next slide, Meraj.

Next slide, please. So, in this activity, a number of people that have worked with me and supported me in trying to get this Reg Guide where we are today, Mike Eudy's managing this Reg Guide process, Bernie Dittman that worked with us for a couple of years has retired since, David Rahn, he's on the line with us, he has supported this activity from my branch, and I have Greg Galletti and Ayo on the vendor and QA branch that have been instrumental in development of this activity.

And Jonathan Ortega, he's left us to

go to DOE but he was also instrumental in developing this. Next slide, please.

So I think I can go through the material that I covered back in the Subcommittee meeting, which was on July 21, or I can just cover what's happened since.

So it's really, if you have any questions, you can get me deeper into it, but I'll probably just summarize what we did during the Subcommittee meeting and the feedback that we took back that resulted in our documents.

So next slide, please. So the scope and purpose, I think we probably discussed that. This Reg Guide is really endorsing the NEI 17-06 Revision 1, which is the process or the guidance on how to utilize the SIL certification into the commercial grade dedication activities.

Now, NEI has been working on that document as part of the IAP activity since 2016 and we have been basically participating in a way that we have been providing constantly feedback to NEI on development of NEI 17-06.

So part of the endorsement is endorsing the portions of the IEC 61508 standard that really focuses on these critical characteristics of

dependability.

Now, like Member Brown mentioned, that the standard is like a six- or seven-part standard. It's a pretty big standard. And it covers a myriad of things.

And so, but for the purposes of our – we are doing a limited proportion of utilization of the standard. So that portion is being endorsed by this Reg Guide as well.

There is the ISO IEC 17065 standard that really is a framework that, like, in this case, the certifying body, which is a third party that does the certification activity, this is the framework that they work under.

It's like their web program that they abide by when they're doing this work, providing reliability, repeatable performance of the certification.

And also the relationship, describe the relationship of this specific Reg Guide, the Reg Guide 1.164.

That is the guidance on how to do commercial grade dedication on any commercial item that has a base in a nuclear facility.

And the EPRI TR 106439, I have put

together a timeline slide based on the feedback that we got during the Subcommittee.

And a lot of the questions that we were getting were really related to why are we doing this now and all that sort.

It's fully respective of commercial grade dedication. So I'll go through that. That's near the end of my presentation, which will probably link how all these documents are linked together that we tried to basically establish at length in the record. Next slide, please.

So I think I've already covered the background of it and all, how we came about working on this document.

And on this slide, what I would point to is that it was not a first of its kind effort. I think there was a precedence.

We had previously endorsed NEI 1405, which was a process for procuring commercial grade laboratory calibration and test services.

And so we kind of followed that framework on how to utilize this third party commercial grade processes into a -- I want to call like an Appendix B type of activity.

And, other than that, what I think what

we talked about on this slide has already been discussed. So, next slide, please.

So I'll cover a little bit of historic perspective of these EPRI standards. And this one thing here that I want to point out is that in 2016, when this task was identified under the IAP, the Integrated Action Plan, as part of the modernization of the IAC infrastructure, regulatory infrastructure, EPRI started a real effort, and this is an EPRI document 3002011817, it's the efficacy of the SIL process.

But this research was undertaken by EPRI to take a look at the -- can this SIL certified component and what do they do as part of the certification?

Can that be utilized into the nuclear arena? And I think some of the work that's done under that, NEI's presentation that I just sneaked in, they'll probably go into a little bit of the detail on how they utilized that, leveraged that research work in putting together NEI 17065.

That was another item. So the MP #3 was a task that was identified under the IAP. All right.

So as part of this activity, what else

we did was that in the ANSI accreditation, ANSI National Accreditation Board, I think that's what ANSI stands for, ANAB is the one that does what they call the -- they use the word accreditation body, right?

So they accredit the certifying bodies, right in the USA. In the USA, for example, Exida is one of the certifying bodies that does SIL certification.

And ANAB, which is the national accreditation board, annually goes in and audits their activities to make sure that they are complying with ISO 17065 and they are doing the work in accordance with that.

So, part of this development activity, the NRC staff took this opportunity to observe. We did that over three cycles.

We observed and conducted audits of Exida and we provided some of our feedback which they accepted, and they actually enhanced their accreditation audit activities as a result of that.

What else is on this slide I highlight? Yes, and also –

MEMBER HALNON: Can I ask you a quick question?

MR. TANEJA: Yes, sure.

MEMBER HALNON: This is Greg Halnon. When you looked at the accrediting, actually, the accrediting has several aspects to it.

One of them is compliance in process but it also has outcomes. Was operating experience heavily looked at in that accrediting?

In other words, went through the process and looked at failures in the industry to come back and say, is that anywhere possibly connected to inadequate certification?

MR. TANEJA: So, the other thing is certification of the certifying body, whether they are performing the activities in accordance with their procedures, plan and procedure that's in compliance with the ISO standard.

And also, one of the initial key facts that we gave them, that they were pretty strong on looking at the processes, the accreditation body.

But what they call it is looking at the actual technical work. They did not really dig into it much deeply.

Actually, what do they do? They really look at a component, SIL certification in

accordance with the IEC 61508.

MEMBER BROWN: That's ANAB that you're talking ab out?

MR. TANEJA: That's ANAB.

MEMBER BROWN: Okay, so --

MR. TANEJA: That's really --

MEMBER HALNON: They pressed them to take a look at the technical outcomes, not just the process compliance, but with the technical outcomes.

MR. TANEJA: Right, exactly. And I think they took our feedback and they modified their checklist.

MEMBER HALNON: Okay.

MR. TANEJA: That includes some of those items as part of their ongoing audits.

MEMBER HALNON: Good. Thank you.

MR. TANEJA: All right. Next slide, please. So the regulatory bases for this Reg Guide are the things here for 21.3, which really allows for commercial grade dedication of off the shelf items, which is basic components in the nuclear power plants and facilities.

And all these activities have to be performed by under an Appendix B program or by what

we call is a dedicating entity that has an Appendix B program influence.

And that is all laid out in our regulation. What is dedication? What's the definition of dedication?

And, briefly, what it really says is that it's an acceptable way of using a component, a commercial component, as a basic component for what it's been dedicated. What is boils down to is once thou shall identify the critical characteristics of the component and thou shall verify those characteristics.

And it plays out full process and how you go about verifying those characteristics. And so there is no real guidance that are developed in basically making sure that it's done consistently across the board.

But those are the basic regulations that -- so one thing here that I would point out, the Reg Guide -- hm?

CHAIRMAN REMPE: I don't know if you want to do it now or later, but you mentioned the items that already exist.

MR. TANEJA: Right.

CHAIRMAN REMPE: And so, there's no

reason to think that if anyone would follow this new Reg Guide, they wouldn't adhere to other existing guidance, whether it's a branch technical position or an ISG.

I mean, all of those things still exist and they'd have to adhere to it as they perform this dedication process, right?

MR. TANEJA: Correct. Correct. So I think what this Reg Guide does is it supplements the existing guidance, right?

CHAIRMAN REMPE: That's what I took away from my read on it, but I'm not an expert in this.

MR. TANEJA: Yes.

CHAIRMAN REMPE: I want to make sure that you were agreeing. And frankly, the other Reg Guide, the 1.164, it doesn't list every single guidance that has to be followed, and yet it's not been a problem. They still were recognizing that this had to -- they had to adhere to this.

MR. TANEJA: Yes.

CHAIRMAN REMPE: Just checking. Thanks.

MR. TANEJA: So I think what I was going to point out is that the draft of the Reg Guide

that we had here during the Subcommittee meeting did not have the direct base as the Appendix B, Criterion VII.

I think the markup that we gave you, we added that Criterion VII to the regulatory bases of the Reg Guide. So that's one change that we did make. Next slide, please.

So, nothing really -- we did not have to -- the changes that we made as a result of the Subcommittee meeting to the Reg Guide were not at the level that we needed to go back for public comments.

So the public comments that we discussed during this Subcommittee meeting and how we dispositioned them and any impacts to the Reg Guide were already incorporated in the draft guide that we shared at that time.

So nothing has changed since the -- and we did not have to go back and ask for public comments and there are no new comments.

So I think really there is, unless there is any interest in the comments that we got from public, we dispositioned them adequately, and any impact to the Reg Guide, we incorporated them and we did not really have any follow-up on that area.

MEMBER BROWN: I presume the main one you put in there was the 10 CFR Appendix B addition.

MR. TANEJA: Criterion VII.

MEMBER BROWN: Which was a quick summary about documentary evidence, et cetera.

MR. TANEJA: Yes. Next slide, please. I think the next few slides, I probably want to skip that. Let's skip down to the historic perspective. I think that was a lot of the questions that we got during the Subcommittee -- next slide -- were all about why are we doing this and what we are doing here and --

MEMBER BROWN: Can you back up for one minute?

MR. TANEJA: Yes.

MEMBER BROWN: Back up a slide just for that --

MR. TANEJA: Sure.

MEMBER BROWN: My take on your position when I went through, and correct me if I'm wrong, but were largely process oriented, not necessarily technically oriented, and it's reflected in what I see.

You've got to do it. You can't extend the time period about which you

recertify. You've got to follow the endorsements. You've got to have certain things. But it's process oriented, it's not just technical requirements are this or that.

MR. TANEJA: Yes. These are clarifications.

MEMBER BROWN: I've got it. Thank you.

MR. TANEJA: So our regulatory positions are not exceptions. What happened is, we endorsed Rev. 1 of 1706. So when we received the Rev. 0, we provided a set of comments to NEI, which they incorporated.

So, really, Rev. 1 addressed all of our concerns. But here, I think these are more like highlighting the areas that I think one was a little vague of the periodicity of doing the oversight. They said it's got to be done at least hours, and that's one of the clarifications.

And the other was that make sure that the certificates that you do get, I think we hear that there are some counterfeits out there on the market, that you really need to pay attention to the generalness of those

documents.

If you're going to utilize a certificate, make sure that it is a good one, not just some entity.

So I think those were just kind of safeguards, those that needed clarification. Okay, so, next slide, unless you have any questions.

So these were the five public comments that we go and their dispositions. Nothing new there. So, next slide.

So here, I think is where I think probably we'll answer most of the questions that were raised during the Subcommittee meeting.

And the information that I have here really is coming from Reg Guide 1.64's endorsed document.

Those are the EPRI document that we endorsed. Has a pretty good history of where the commercial grade dedication of items and services.

And what I did is I've taken the parts that are of interest to the -- from the regulatory framework.

It covered a whole lot of -- gamut

of things, that document, but I just captured a few.

So this effort really goes back to the '70s when there was -- Appendix B suppliers were disappearing and during the heydays of the nuclear, there were people that were disappearing and the concern was can we take these commercial items and what do we do with them, right?

These commercial grade item discussions started back then when we didn't have Appendix B suppliers.

In '76 the first standard that came out was the ANSI 18.7 that was endorsed by the NRC as Reg Guide 1.33, which addressed the end user of the commercial off the shelf item.

So, in '78, Part 21 basically was revised. That required a commercial grade dedication before it could be used as a basic component.

It became a regulatory requirement in '78 that if you're going to use it as a basic component, thou shall dedicate it, right? In '88, EPRI 5652 issued that really provided a methodology of how you go about doing commercial grade

dedication.

In '89, NRC issue a generic letter, 89-02, that conditionally endorses NP 5652. Next slide, please.

In '91, generic letter 91-05 was issued. And that basically pointed to 10 CFR Appendix B, applicability to commercial grade dedication process. But that's really going to be how it imposes the QA requirements onto the process itself.

So in '94, EPRI issued TR 102260, a supplemental guidance to the NP 5652. But these two documents, the NP 5652 and EPRI TR 102260, the Rev. 1 of that is the front vision that they gave it a new document or that endorsed by Reg Guide 1.164. That is in a pre-document --

MEMBER BROWN: That's not the 106 -- whatever the number is.

MR. TANEJA: That document, they gave it a new number which basically is a division one to this, and NP 5652. So what they did is this is a supplemental guidance, right? The NP 5652 and the supplemental guidance, revision one to that, became the new EPRI doc.

MEMBER BROWN: And that's 106439

you're talking about?

MR. TANEJA: No.

MEMBER BROWN: Or is that the 22 --

MR. TANEJA: That's a document that we endorsed by Reg Guide 1.164. Okay, that's the 3002002982. Right. Yes, that's why it's so confusing and I thought I'd put it in a timeline because there's just so many different documents and so many things happening, right?

So in 1996 is when EPRI 106439 was issued. Now, this document is the one that actually provides guidance on how to do commercial grade dedication of digital items, the PLCs and the computerized items and the digital devices.

And this is where it supplements the EPRI 5652, right? And in the new standard, this is called out in section 14.1 of the EPRI guidance document.

This section focuses on the digital under that document. So the EPRI TR 106439 was endorsed by the NRC by a safety evaluation in 1997. In 2011, a second paper was generated.

So we have these bunch of documents, so the issue must have been there, right? The staff issued a paper saying that, hey, we should have

a record on commercial grade dedication process.

Right? Because we are noticing these by generic letters and safety evaluations. So that's really where the development of the Reg Guide 1.164 effort was initiated. Next slide, please.

So in 2014, EPRI issued the 3002002982. That is, and it's a mouthful, that division 1205652, and a supplement supporting document here, 102360.

And in 2016 is when the modernization, project number three, that was identified as part of the IAP effort, Commission direction for modernizing the I&C infrastructure.

And that effort that was identified was how can we leverage the I&C 61508 into the commercial grade dedication activities?

Like I said earlier, concurrent with that, EPRI started their research work, and I think in EPRI's presentation, in their presentation I think they'll go over that a little bit, how they use that research and do that.

In 2017, Reg Guide 1.164 was issued that endorsed the EPRI 3002002982. In 2021, December, is when we received NES 1706 Rev One for endorsement. And today we are in front of you

trying to get this document endorsed via Reg Guide 1.152.

So it has had a long history. It's been evolving, but the nuclear industry has been dedicating this item for a number of years now.

And my personal experience with dedication of digital items goes back to the early '90s when we dedicated single loop controllers that were made by, I forget now, I think Fisher Porter or somebody like that and then (audio interference) that were digital recorders that replaced pen and paper.

And they were commercially dedicated back in the early '90s, so those efforts – and we used this guidance in EPRI 106439 in performing those dedication efforts.

But that's my presentation. Are there any questions? I'd be more than happy to entertain them. And I have, I think, hopefully, people online with me, Greg was there, QA branch, so any questions.

MEMBER MARCH-LEUBA: This is Jose.

MR. TANEJA: Yes.

MEMBER MARCH-LEUBA: Just for my education, as you say in your presentation, the

whole thing was started in the '70s when people couldn't buy spare parts, right? Has this evolved now? So if I'm designing a new reactor from scratch, can I use commercial parts for the guide? Or is this only -- is this only for spare parts or can I build a new reactor with them?

MR. TANEJA: Well, our regulatory framework doesn't distinguish between a commercial part or an Appendix B supplier part. What it says is that if you are going to use a commercial off-the-shelf as a basic component, thou shalt dedicate it and thou shalt follow this process of dedicating it.

So a dedicated item by de facto means it's equal to an item produced under Appendix B. It's as good as that.

MEMBER MARCH-LEUBA: So I could design a brand new reactor --

MR. TANEJA: Just using commercial parts, if you dedicate it.

MEMBER MARCH-LEUBA: Right. Okay. Thank you.

MR. BENNER: Now, there's a pragmatic aspect that I could go someplace and buy a vessel and then say I'm going to dedicate it. But I just

don't envision that being how a reactor vessel comes to play. So I think it's for this to be an avenue, it's because there is a commercial -- like, breakers. I mean, it's stuff that you just buy commercial grade. I mean, I think there's still going to be plenty of major components in any new power plant that are going to be -- the only reason they're going to be there is if there's an Appendix B supplier making that.

MEMBER MARCH-LEUBA: The guide is focused on Digital I&C. They still have commercial parts or commercial -- so I&C components that would be very difficult to go under Appendix B?

MR. BENNER: Yes. Well, I wouldn't say difficult. It's just, is there a market there? I mean, to get that be certified as an Appendix B supplier, you subject yourself to NRC inspections and other things.

And I think there's just not enough customers that these vendors want to do that. They're like, hey, I got commercial stuff that I sell to all these highly safety significant industries and it's good enough for them.

So, nuclear, if you want to use mine, you have to find a way to get my stuff. I'm not

going to come to you.

MEMBER BROWN: I was going to try to provide some perspective on that. Because most of you all would probably assume I'm not great on what I would call all third-party type stuff.

I mean, but from an experience standpoint in the electronics world, I'm not talking about pipes and valves and gears and stuff like that, which are big parts that you can do things with, there's thousands of parts on a computer-based module, PLC, and that's aside from the million chips we've got inside the microprocessor, inside the logic in it.

And you can't test all of it. There's just no way to do it. You're faced with stuff in the military world with MILSPEC, military specification, parts.

There, there's a big market. A lot of ships, a lot of army units, a lot of stuff goes out in the field. There's a lot of stuff that gets built all the time.

So when you build a transistor for an integrated service or a log unit or any piece of equipment that's going into the field, they'll build 10,000 pieces on an assembly line.

They'll test 100. And if no more than three fail, the whole lot passes. I just picked a number out of there, but that's the ballpark.

That's what you live with in the electronics world. So I appreciate this approach because I think that's what we're facing largely.

We need to go out and find out are these parts that people are using, PLCs whatever you want to call them, commercial parts, there's got to be a better way to do this.

I think there's some ways that I mention later in my questions, but I just wanted to put it in perspective so that everybody would understand how you build stuff in the electronics world and how the piece parts do get tested, because they don't get 100 percent tested.

I'm going to save my other question for everybody else's. I'm going to save mine until after NEI. I don't want to -- I want to keep the whole thing moving and get both parts in and then I'll have my other questions. It relates more to my letter, the letter that I generated.

MEMBER BIER: So --

MEMBER BROWN: Yes, Vicki, go ahead.

MEMBER BIER: Okay, this is not my

area, but just from things I've read in the press and other areas like voting machines or military equipment, whatever, there's a lot of concern about parts that might come already compromised from Chinese manufacturers or other external sources. And has that been addressed? How big of a concern is that in this context, et cetera?

MR. TANEJA: Right. So, in our regulatory framework in general, we have what we call an SDOE, secure development and operational environment.

And in that effort, not only we require it, but also our Appendix B program and the commercial grade dedication program, one of the requirements is to assure that each part that you are using, right, are coming from reliable sources.

And there is a large awareness in the industry of these so-called compromised parts that are getting into their products. They have a person who is building these so-called digital devices, they have as much at risk as a user does. So there's a very high awareness, very concerned.

MEMBER BIER: Okay. Thank you.

MEMBER BROWN: Any other questions at this point? Yes?

MEMBER KIRCHNER: Dinesh, in practice, let's pick on some critical components, like the reactor protection system.

How does this all work out? In my mind, if it's under Appendix B the umbrella, so how do you feed the parts of a larger system or component?

MEMBER BROWN: Well, can we answer that question after NEI? That is a very pertinent question. I wanted to deal with that in a unified discussion.

MEMBER KIRCHNER: That's my only question.

MEMBER BROWN: No, that's good. That's very good.

MEMBER MARCH-LEUBA: For the staff, they prove that their microphones are there.

MEMBER BROWN: So if there's no more questions for the staff, NEI can come on up and –

MR. BENNER: Yes, the staff is going to stay here. Whatever questions come up, we're still available to take them.

MEMBER BROWN: Does he need the center seat or is the right hand or left-hand seat okay?

CHAIRMAN REMPE: Do you have someone

online that can share the slides? Wonderful.

MR. CAMPBELL: It's actually going to be the primary presenter today. I'd' just like to make a couple of introductory marks and then we'll --

MEMBER BROWN: Turn on the mic.

CHAIRMAN REMPE: Go ahead and ask them to share their slides, too.

MEMBER BROWN: When it's green it's on.

MR. CAMPBELL: I'm red-green colorblind so --

MEMBER BROWN: Touch it again.

MR. CAMPBELL: There we go.

MEMBER BROWN: Pull the mic forward.

MEMBER MARCH-LEUBA: Say your name, please.

MEMBER BROWN: Pull the mic -- pull the mic toward you. That's it. Thank you.

MR. CAMPBELL: Okay, can everybody hear me? And it looks like Andy Nack will be our primary presenter today.

My name is Alan Campbell. I'm the technical advisor with NEI. I lead our digital I&C working group and multiple task forces that we have underneath that digital I&C working group.

So I wanted to start by thanking the ACRS Committee today for inviting NEI to speak regarding our work on digital I&C commercial grade dedication.

The approach that will be presented today supports the replacement of aging analog systems in the operating fleet with digital systems that enhance the safety and reliability of our nuclear power plants.

This process provides a pathway for the use of commercial digital I&C technology that has been developed specifically for functional safety applications.

By using this approach, we will provide a consistent oversight process of commercial off the shelf components and are able to draw from the operating experience of other safety critical -- I want to thank the NRC staff for their review and comments of NEI 1706 and their participation in multiple accreditation audit observations that demonstrated the adequacy of both SIL certification and NEI 1706 oversight processes.

But at this time, I'll turn over the presentation to our primary author of NEI 1706, Mr. Andy Nack, and he'll go over the processes.

Thank you very much.

MR. NACK: All right. Thank you, Alan. As Alan said, my name is Andy Nack. I'm part of the NEI team.

So, what we've got today is a presentation that is a little bit abbreviate version of what we presented previously to the Subcommittee.

This slide here is just kind of a placeholder showing you where the document is available on the NRC's website with a quick summary of the scope that reflects what Alan just shared in terms of the overall goal of this document, the purpose of the document.

So one of the things we wanted to do today is to get a little bit more into what this safety integrity level ecosystem is and how it already exists and how we're just trying to leverage something that is already being utilized in other high risk industries.

So this safety integrity level concept, it was already mentioned that there's four levels.

So it's level one, or SIL one, would be for the least risky application going all the

way up to SIL four, which is the highest risk.

And so typically within a system that is certified or developed to a SIL level, there's three main types of components that are going to be involved.

And that's what we're showing here with the sensor, the logic solver, and some type of an on/off actuator.

And so there's manufacturers of these components that are using the IEC 61508 standard to ensure that there's systematic integrity and the appropriate level of reliability and hardware fault and tolerance based on what the particular skill is that their goal is to achieve.

And so, across the bottom I've got some example manufacturers that use IEC 61508 to design and manufacture products.

Once these manufacturers have the product ready for certification, they contract with Exida or TUV Rheinland or various other certifying bodies to come in to evaluate what they have done in their efforts to design and develop these products to be in compliance with 61508.

So, these manufacturers, as was discussed, are doing this because they know that

there's a market in high risk industries such as oil and gas or chemical processing or other industries that are going to, kind of like was discussed about the military, is going to buy a large quantity of the products that they design and develop and sell.

So these certified bodies are also then accredited by whichever accreditation body is appropriate for the country they're located in.

So for example, I just have DakkS at the top, because that's the German accreditation body, and that would be who accredits TUV Rheinland and the other two entities.

And ANAB would be the entity here in the US that accredits Exida.

And earlier, it was mentioned about the EPRI research. So these items here are summaries of what the conclusions were from that research that we were able to build upon when we were developing this guidance.

First one was that the SIL certification aligns well with EPRI TR 106439.

So this is where you can really get into the nuts and bolts of the types of activities, the design techniques, the features that were being

built into the products, align well with what was already in the existing process for nuclear in this TR 106439 document.

Then the certifying bodies are standard and rigorous, reliable evaluation process. The CBs, so that's the CBs.

The ABs, the accreditation bodies, ensures the CBs are consistent and trustworthy. The failure data indicates reliable operation and SIL certified equipment.

And SIL certifications are an accurate indicator of reliability. So to accomplish these conclusions, EPRI did an in-depth dive into what these certifying bodies and these accreditation bodies, what they do, what their processes are.

And the interesting aspects with the final two conclusions was that they actually did gather operating experience and compare it to what the certifying bodies had certified.

So they were able to see in the data that the actual failure rates of the certified equipment were -- the certifications were actually conservative in terms of the actual failure rates in the field.

So with one noted exception of a

situation where they were able to see that the failure rate was higher than predicted and certified, and it was actually a way that they were able to go in and find a systemic issue with the manufacturing process.

So part of the certifying bodies' evaluation process already included comparing actual operating experience against what the predicted failure rates were and when the actual failure rates are higher than what's predicted, they go in and figure out why.

And it is a very useful indicator of finding that systematic issue with the manufacturing.

They were able to in that instance correct it and see the reliability numbers fall back down into the range of being predicted.

DR. BLEY: Andy, this is Dennis Bley.

MR. NACK: Yes.

DR. BLEY: I'm glad to hear all this. We heard earlier part of the reason we've gone to this process is that manufacturers didn't want to dance through all the hopes that NRC applies for inspections and the like.

Do these accreditation bodies or the

certification bodies have agreements with the vendors that when they find something curious like you just talked about they can get in and rummage through the vendors' data?

MR. NACK: Yes. So the certifying bodies operate using ISO 17065. And that standard drives contractual agreements between the certifying body and the particular manufacturers where they make commitments like that, that they are – if – so if the manufacturer is wanting to carry a particular CB certification, they have to agree to provide that type of information to the CB.

DR. BLEY: Okay. Just thinking out loud now, which is a dangerous thing to do. This kind of implies that from a component vendor's point of view, the NRC process puts a lot of overhead on them whether or not they have problems, and here they're willing to allow outside involvement in their systems if there's indications of a problem. Is that a fair statement?

MR. NACK: Yes, I would say that's correct. And I think what was mentioned earlier about what the size of the potential market is for them to sell them to is a major differentiator.

DR. BLEY: Yes, okay, thank you. You have spoken to one of the questions I asked NRC earlier.

Are the reliability data that back up this process available to people in the various industries? Or is it proprietary to the vendors?

MR. NACK: It's available. So Exida is the CB I'm most familiar with. I know that they use various sources for their reliability data, some of which are probably the ones that you're aware of.

But they also collect data as they're doing their certification evaluations of manufacturers.

And Exida actually offers a platform that provides access to a lot of that data for use through someone creating a contract with them and gives access to all the data that they have in terms of operating experience.

DR. BLEY: Okay. Interesting. Thank you.

MR. NACK: Sure. All right. And so now, we'll jump into looking at the existing process for accepting or justifying equipment and then looking at how this new NEI 17-06 guidance enhances

that process.

So this right now is what the process would look like to go through qualifying and dedicating equipment for use in a nuclear application.

And so, the next slide, we overlay where the SIL certification provides some enhancement here. So the work that is being done is a qualification part of the process where you're determining suitability of the design for the application, looking at the systematic integrity aspect of that evaluation is covered by the fact that the manufacturer is adhering to IEC 62508.

Then getting into the commercial grade dedication phase, this is where you gain the ability to utilize the SIL certification in place of what would have needed to be covered using typically a commercial grade survey to address the dependability critical characteristics.

Then that gets you to where it says implementing the method one acceptance strategy, where you're still completing the commercial grade dedication using or completing the commercial grade dedication process for the critical characteristics that fall into those categories

of performance and physical critical characteristics that can be typically evaluated by some type of testing.

DR. BLEY: Andy, it's Dennis Bley again. We talked about availability of the data to the folks who are building components.

What about the people who are users of those components, either a utility company who's going to buy a new plant or a US reactor vendor who's looking to buy components to put into their plant?

Do they have access? And let's include the NRC as well. Do they have access to the data?

MR. NACK: They would be able to achieve the same access by engaging with Exida that a manufacturer would.

And so the way the SIL ecosystem works is that the end user is actually, or some integrator, is actually responsible for putting the different components together in a manner that still achieves the particular reliability targets required for the application.

So the failure rates are still applicable to the end user, maybe even more so than the manufacturer, because the end user is

responsible for making sure that the reliability targets are still achieved when they put all the different pieces together.

DR. BLEY: So that makes sense.

MR. NACK: So they're looking at the system reliability instead of just the individual component reliabilities.

DR. BLEY: If I'm an end user, do I have a contractual or other obligation to provide failure data I collect after I'm using the components back to this process?

MR. NACK: I wouldn't say contractually. I think in that type of a scenario, it makes a lot of sense for the end user to feedback failure data back to the manufacturer.

Because it's definitely in the interest of the end user to have the most accurate failure data as possible, so they would want to provide that information back to the manufacturer that would then get integrated into the larger data set.

DR. BLEY: Okay, thanks.

MR. NACK: Okay. And so now moving into a more detailed step through of what this NEI 17-06 guidance really is and the nuts and bolts here.

And I've included an example manufacturer, Yokogawa, and an example certifying body of Exida, just as a reference.

And then over on the left side of the screen, I've just noted that that's the Appendix B QA program that the dedicating entity would be operating under.

So starting out, step one, you're definitely going to need to identify what your requirements are for your application.

And then you're going to confirm that the equipment that you're evaluating is certified in a manner that encompasses what your requirements are.

Then you move into identifying what the critical characteristics are for the equipment as well as identifying critical characteristics of the service that the CB is providing when they're providing their certification.

Because I guess it's important to note here, there's actually two separate commercial grade dedication activities happening.

One is for the actual item that the manufacturer's providing and one is a dedication of the service that the CB is providing.

Then you're going to confirm that the certifications that the CB are providing are within the scope of what their accreditation covers.

And then you're able to complete the dedication of the CB service using that accreditation.

Then we'll talk more detail later about how an accreditation body or how an accreditation body and CB together get their initial approval.

And so that approval process happens before this to where that approval is part of what is necessary to complete this dedication of the service.

Then Step 7, we get into being able to use the certification. So the reason for the dedication of the CB service is so that the certification that's been provided by that CB now has the necessary pedigree to be used to – be used to determine the acceptability of the dependability critical characteristics.

Then the final step, Step 8, you're using traditional commercial grade dedication methodologies such as Method 1 Testing to determine the acceptability of the physical and critical performance characteristics.

And so that walks you through what the actual process is that this guidance is utilizing.

And then the NEI 17-06 does also include some indications of how to select SIL certified equipment.

And just at a high-level summary, you've got the equipment, must be able to prove -- to perform the required functions for the application.

The equipment must be certified for the appropriate SIL level. So for an example, if it's, if the application requires SIL two, the equipment must be certified to two or higher.

And the required safety functions must be within the scope of the safety functions identified on the certificate.

And just as an example of this, there's several actuators that are certified that it's important to look at what details of their actuation are actually covered by the safety function that's listed on the certificate.

So if the actuator does provide some variable in all type control, often the certificate will list the safety function as only including

the on/off range of that actuator's functionality.

So here's what I was referring to a minute ago about the different pathways to approving the CBs.

So before walking through the process of utilizing this NEI 17-06 methodology, the CBs need to have been evaluated by the industry using one of these two pathways.

One is this accreditation only pathway, where the accreditation body, it's been observed that they utilized sufficient rigor to look at the CB's processes but also their scheme.

And the scheme is what's specifically tying into the IEC 61508 requirements that are more the technical type of requirements in nature.

And the second pathway is a situation where a little bit more rigor does need to be applied to the assessment of the certification scheme.

And this is an example of what we encountered with ANAB during our observations was that during the initial observations, ANAB needed a little bit more rigor in terms of how they were evaluating the scheme that the certifying body was using.

And so, NEI 17-06 includes a

supplemental checklist that the nuclear industry can directly use interacting with the CB directly to supplement what the accreditation body has done in terms of looking at the processes.

So one of these two paths are available to gain the initial approval of the CBs for use within this process.

MEMBER HALNON: Andy, this is Greg Halnon. How often is the accreditation process?

MR. NACK: The accreditation or the AB at least in what we interacted with, with ANAB and Exida has some type of an activity every year.

I think the actual accreditation cycle is every two years but even on the off years, the accreditation body does at least a supplemental observation process that looks similar to a full accreditation activity but I guess is a little bit abbreviated.

So they're doing something every year.

MEMBER HALNON: Great. Do you know how long the certification process takes from – I hate to say the site visit but from the actual accreditation? A week? Two weeks?

MR. NACK: Yes, so, these interactions typically involve the CB providing the AB a lot

of information remotely ahead of time.

So a lot of the work is done up front of reading the procedures and figuring out what they want to look at.

So then the actual on-site activities are something more like the one-week range.

What we saw was the accreditation body utilized separate teams and so it was more like each team spent one or two days looking at their particular area.

And they might be operating in parallel. So like one team would be more focused on the procedures and the administrative aspects of 17065 while the other team was more the technical aspects, looking at how the manufacturer was qualified to do the work and how they're applying their scheme.

MEMBER HALNON: Okay. Who is on the accreditation visit? Are they consultants? Are they industry folks? What is the makeup of the team that does the accreditation?

MR. NACK: So, ANAB has a process that they use to qualify people. So they're representatives of ANAB. I don't know how they necessarily structure them in terms of, are they

direct employees of ANAB? I don't know. They may be operating as contractors of ANAB. But they have been evaluated by ANAB as qualified to perform the particular accreditation activity.

MEMBER HALNON: Okay, so they train their own folks.

MR. NACK: Yes.

MEMBER HALNON: The accreditation processes.

MR. NACK: Yes.

MEMBER HALNON: Thank you.

MEMBER BIER: Another question. Are the accrediting bodies currently all governmental organizations or no?

MR. NACK: No, they're not.

MEMBER BIER: Okay. So they're commercial or non-profit or do you know what the status is?

MR. NACK: I don't know. Alan, do you know? I don't know.

MEMBER BIER: It's not super important. I'm just curious.

MR. NACK: I'm not sure organizational wise the structure.

MEMBER BIER: Thanks.

MEMBER HALNON: This is Greg again.

MR. CAMPBELL: ANAB is associated with the answer.

MEMBER HALNON: So if you make the analogy to like ABET, the accreditation board for engineering technology programs, there are industry and academics and other folks who are involved in that field that give their time to the accrediting board itself.

And that's what I was trying to find a word. They draw their people from. That might be just good to look up if you would just to let us know. Because it speaks to, one, how independent they are and how consistent the process is year after year. Because if you get different people every single time, there are plusses and minuses. There's a fresh look but you also get less experience.

MR. NACK: Yes, and the other umbrella that all the accreditation bodies are under is the international accreditation forum where different accreditation bodies evaluate each other.

So you've got that dynamic going on as well that tries to maintain a standard application of what the accreditation bodies are doing.

All right. Then NEI 17-06 also provides some guidance on how the dedicating entities would need to adjust their QA program to be able to make sure it's set up in an appropriate manner to utilize this process.

And this is just a summary of the areas that it provides direction for it to be adjustments made in these procurement documents, what the tasks are associated with the digital dependability evidence and the QA evidence for digital dependability and their correction action program.

So details are provided in the NEI guidance for those areas. And then this is what's already been touched on a little bit, but this is where the nuclear industry will continually provide oversight of the accreditation bodies and the certification bodies on an ongoing basis, kind of trying to be able to look at what was just being asked in terms of are they maintain their level of rigor and are there people that are out in the field doing the evaluations maintaining the proper level of training and evaluations and such?

And so, we're currently in discussions engaging with NUPIC as a possibility for being the entity that would take on this task. But we're

kind of in a situation right now where NUPIC is interested in waiting on seeing the NRC endorse the process and then it looks like they probably would be interested in getting more involved. So --

MEMBER BROWN: Excuse me, I keep forgetting what NUPIC alphabet soup means.

MR. NACK: Yes, it's, I believe it's nuclear –

MEMBER BROWN: I'm not the only one.

MR. NACK: Yes, Nuclear Utility Procurement Issues Committee.

MR. GALLETTI: Andy, I'll just chime in. This is Greg Galletti from the NRC group. It just stands for Nuclear Utility Procurement Initiative Corporation.

MEMBER BROWN: That's not an NRC operation.

MR. GALLETTI: No, it's a consortium of licensees. So they would –

MEMBER BROWN: Go ahead.

MR. GALLETTI: I was just going to say, it's an organization based up of nuclear, commercial nuclear licensees and their representatives sit on the committee.

MEMBER BROWN: Okay, so the oversight by U.S. NRC really follows. It says NRC licensees or designees, not NRC body going out and doing this oversight. Is that the way you read this?

MR. NACK: Well, it can be. So the NUPIC, the utilities are ultimately responsible for the oversight but the NRC has the option to participate as they see fit.

MEMBER BROWN: Has that process been defined yet or is that still in play based on NUPIC's hesitancy on jumping in?

MR. NACK: Well, the fundamentals are as I described in the two pathways for getting the approval of the CBs and the Abs using the accreditation or the accreditation plus the scheme evaluation.

And the NEI 17-06 has the additional checklist included in it. That would be the process that the oversight would use to do the evaluations.

So the only open issue right now is are specific licensees performing that or will they jointly perform it under the NUPIC entity?

MR. ODESS-GILLETT: Andy, can I supplement your response by saying that the NEI

17-06 says that the licensee or its designee is responsible for this oversight.

MEMBER BROWN: Who spoke just now?

MR. ODESS-GILLETT: That was Warren. I'm sorry, Charlie, Warren Odess-Gillett.

MEMBER BROWN: Oh, okay. Thank you.

MR. ODESS-GILLETT: Yes. So that really is, I think, US NRC licensee as you were asking, Charlie.

MEMBER BROWN: Okay, thank you for the more than clarifications, explicit statements.

MR. BENNER: Yes, and this is Eric Benner. I'll add some clarification, because there's a lot of layers here, right? I think everyone gets that.

So that was part of our challenge as the staff of, we needed to make our endorsement of this process sort of standalone.

So it's written right now, we understand that NUPIC may do some things and we're looking at -- there's current certifying and accreditation bodies and we wanted to make sure we didn't need to update the reg guide every time another party added to it.

So we set the standards for each of the

entities. And like Warren just said, right now it's constructed that since NUPIC hasn't stepped in to do this role, it's very clear that the licensee has this responsibility.

But we added our designee so that if NUPIC steps in to take on this role, then it's very clear what NUPIC needs to do.

Now, that layer is what it is. The NRC still has its independent oversight layer where just like for any Appendix B or commercial grade dedication activities we have, you heard Greg Galletti speak. He's a member of our Vendor Inspection and QA Branch. They have a rubric that they use to do different inspections each year.

I mean, they have a certain number of resources, so they pick and choose where they inspect. But just like for all commercial grade dedication stuff, they go out and we do our own independent look at each part of all these things to draw our own regulatory conclusions.

MEMBER BROWN: So you can step in when you want to?

MR. BENNER: Yes. I mean, if we see a problem, right, we always have the available to step in if there's a problem.

MEMBER BROWN: You're just not left out --

MR. BENNER: No. I mean, the bottom line is there's regulated activities so there are -- our process makes it clear whose responsibility it is to do those activities. And it continues to make it clear that we have an independent method. And those fundamentals don't change at all.

MEMBER BROWN: Okay. Thank you. Any more comments? Go ahead.

MR. NACK: Very good. And just to highlight some of the reasons why we want this process and think it will be helpful is that it does direct the nuclear industry to direct them towards these products that can be seen as better products in terms of engaging with manufacturers that are particularly interested in building in reliability and systematic integrity into their products.

Because that's the result of them complying with the IEC 61508 standards. And it does provide access to a broader collection of operating experiences to be used by the power plants.

Traditionally, you could use

commercial grade dedication on any product that you wanted to and it was hard from the outside to necessarily see what you were going to find before you really dug into it.

And so, SIL certification provides a helpful indicator from the outside so that you know what you're getting into from the start.

And then with improved efficiency, you are interacting with manufacturers that are able to sell these products that do have the necessary reliability and systematic integrity that are able to sell them to other high-risk industries as I mentioned earlier.

And it really is a benefit in terms of manufacturers are already familiar with interacting with people that want to dig into their process and see how they do things.

And the process also provides significant efficiencies in terms of the nuclear industry not having to perform their own commercial grade surveys, which are really seen as a redundant activity from what the CBs were already performing. And that brings us to any questions.

MEMBER BROWN: Walt, did you want to ask your question again or do you want me to ask

it for you?

MEMBER KIRCHNER: Why don't you go ahead and ask it for me? Because I can't quite remember how I phrased it. You made me hold it too long.

MEMBER BROWN: I'm going to -- I want to phrase this the right way because I think this is something that the NRC as a program needs, to provide about getting new stuff put into plants where it ought to be.

And there's a lot of resistance to doing this. It's a matter of some of the thought processes. As we've all talked about before, software-based systems introduces, relative to analog, introduces a whole new set of modes, possible modes of failure.

It can be anything from corrupt data to lockups to functions not being performed because you run out of time, et cetera. Silent stuff.

As we've emphasized in most of our discussions, this is my opinion in this case, not the Committee's opinion by any means. I hope it is, but not.

The protection against most of this stuff in the RTS and ESFAS world is multidivisional

protection system that meets a set of requirements, the redundancy and it's all the standard deterministic with none of our systems with permanency.

But they're all interrupt driven. At least I haven't found any. And then the control is physical as well as electronic access and still manage to interact with the staff on it.

Now, that's put in place. Watchdog timers are part of the primary, almost the only way that you can ensure those downstream, both the processing data, processors as well as the voting units if you're going to use digital components for voting units, other than analog logic service. Digital logic service, but not software.

TR whatever it is, it addresses watchdog timers in considerable detail throughout the supplier, particularly the concession 6.4.

It actually talks about an ESFAS application of single unit versus a double unit, which we talked about before.

There were a number of examples. With single units, we're talking about. And looking through the IEC, there was an interest relative to the single versus multi in part six, Appendix

B, EU.1.1, where it says, this standard incorporates a number of measures which deal with systematic failures.

However, no matter how well these measures are applied, there is a residual probability of systematic failures occurring.

Although this does not significantly affect the reliability calculation, there's a lot of those that goes through the IEC, for single channel systems.

If I want to start a pump or do this, the potential of failures which may affect more than one channel in a multi-channel system or several components in a redundant safety system, paren, i.e., common cause failures, results in substantial error in reliability calculations are applied to multichannel or redundant systems.

The International Standard recognizes taking a PLC with your logic and reliability and dependability calculations. It doesn't necessarily transform into a multidivisional system, which is what we really kind of rely on in our RTS and ESFAS systems.

Now, I'm going to segue back to the example, 6.4 in the TR, Topical Report, 10, whatever

the number is, 10636439, where you evaluate all the equity evaluated, excuse me, the application of the programmable logic control in an ESFAS system, a multichannel system.

And they go through an evaluation, two sets of evaluations. One, make sure I get these straight, oh, yes, they evaluated the need for an external watchdog timer challenge failures, and it concluded that the feature wasn't required because the internal diagnostics had such a high degree of coverage with internal failure, the implementation of watchdog onboard and watchdog timers, that's in software, watchdog timers, basically, is what you're talking about, is sufficiently robust to protect against failure.

Modes of interest with these features combined with the fact that the systems are functionally tested every month and there's a manual backup, and therefore no watchdog timer is required, hardware off guard.

The example then said, well, okay, hold it. We've also got to look at a failure analysis considering the possibility of a failure that could disable redundant PLCs into automatic actuation. In other words, silent, I guess, across whatever

that mode would be.

And then they go on to say the likelihood is considered very low based on a review of the software development process. Okay, the marble process. They're always good.

A successful operating history with the controller and similar application. This is a one-line controller. Knowledge of the device design. And wonderful failure management provisions.

Monthly surveillance checks and an extensive testing program performed by the vendor and utility integrator to support the dedication.

Okay. However, we did do a defensive in-depth evaluation of that, but determined that since we have operator backups, we don't need a watchdog timer, which was a terrible message to be sending.

There's some inconsistencies is all I'm saying, when you apply, just, other examples of PLC that you find that's been used in a lot of applications, those get software upgrades.

It happens inevitably, and software applications, you have to change the operating. You download the provisions however you want to

frame them.

They have to be compiled when they're done. And five years later, if you use a different compiler, then you use the initial design, you may get a different way that code is compiled.

I only make a statement like that because there was one circumstance I was involved in where we had a system that worked just fine but we had to get a new device and put our software in it.

We had a different compiler and now the system didn't work. Fortunately, it wasn't an operating system. It was a testing system.

So it's all these things point to the need for some emphasis in my thought process in what's lacking, and not just my opinion, not the Committee's opinion, that 1.250 is a clarifying position.

Is it the utilization of this process doesn't ever gain or put aside the need to evaluate our reactive protection and safeguard systems via the standard review plans, the DSRS, the Reg Guides, the ISGO 6, BTP 7-19, et cetera. And that the silent failure routine, I mean, if you go, all of those documents talk about watchdog timers

somewhere in the architecture.

I would just think it would be useful to have something that identifies this says this part's okay but it has to be used in an integrated system, particularly in multidivisional systems, that we utilized skill, need to be adhered to or appeal part of the process.

That doesn't come through as part of the guidance.

MR. BENNER: Yes, and I'll start, and this is Eric Benner now.

MEMBER BROWN: Did I pay for you all?

MR. BENNER: Yes, and this is Eric Benner again. I'd say we completely agree. The lens through we look at this is, the commercial grade dedication process in no way, shape, or form, that's what your design and licensing requirements are.

So while the references we talked about are when we actually design, an applicant designs something, the license that we set certain requirements and we apply all those guidance standards.

So this process says, hey, I already have a license. I already have a system. I

already have a design.

I already have components. And now I need to replace part of that with new systems or components.

So they still have an obligation to make sure that whatever they're doing fulfills the design and license requirements. But I see your point, particularly in this situation, that sometimes you believe, but this has been the case for commercial grade dedication, not just in SIL but across the board is, right, you want to buy one thing, because that is what the design says, and you buy something else and you think that something else works the same exact way but it doesn't.

That's part of what this process is all about is to say, okay, you're taking on this new responsibility to get this new thing and put it into your system, put it into your facility to do a certain function.

We put a bunch of tests in place that licensees and these other bodies do to convince ourselves that it's actually going to do what you say it's going to do.

But I respect this idea that a run-in

to the classic scenario, particularly as you move to digital, particularly because software component may be introducing failure mechanisms that you haven't really considered before.

So we'll certainly take that offline to see what reinforcement we'll need.

MEMBER BROWN: So hopefully I'm writing the report on this and I've tried to incorporate enough information in there to try to get this point across.

The fundamental is hardware watchdog timers come in a couple of different varieties. A PLC could have a built-in hardware watchdog timer in but just it's not, it's separate.

They've got to be separate. You can't depend on the operating system software. I mean, it's got to be separate. But it could have that component built in but just not used in some circumstances. Or it could be an off-board one that's incorporated based on your design approach.

So, I mean, the point being is that, and I don't want to be pedantic about this, it's just that we've worked hard over the last 12 years. Every new plant design we've worked on where we had software-based processing and voting units,

I'm not applying it to the equivalent.

We didn't do it in the HIPTS process because it's hardware, fundamentally, and log computer based by the time you program it.

So, I mean, we just can't lose that capability or that idea. You've agreed that we can use these and they're okay, but they don't have that.

Well, but this thing is not capable of incorporating -- we used this in the architecture, it can't incorporate it. That's my concern.

Now, Jose had a comment, I think. You raised your hand.

MEMBER MARCH-LEUBA: Yes, this concept comes very often in software reliability. The issue is open identification of requirements. Before you start doing the testing, you have to identify whether a watchdog timer is needed or not. And it's easy to forget, especially if the watchdog timer is embedded into the PLC, that you need to test it.

So I don't know if we have enough emphasis. The best way to design the software is to have good requirements.

The best way to design or to certify

the parts is to know what the part needs to do. And that's crucial.

MEMBER BROWN: There's always, there's software timers throughout most that are interrupt-driven because it stops and goes off and does something.

So there's a timer in the software. There's one of them every five milliseconds. It was off doing something and it stopped everything that came back and every five milliseconds it was testing.

It would be insane to be doing it in my opinion, when I read the Topical Report, but that's what they were doing. The system worked so it's in use.

The point being that there's a lot of little ones in there, but if the timers are part of the software and the software stops, for whatever reason, you're toast. And this is the important part. I'm sorry, go ahead.

MR. BENNER: And this has played out significantly, not so much in these discussions, but in a different realm. Applicants have looked at the self-diagnostic capabilities of these systems to eliminate required text message

analysis.

And we've done some of that but we also basically have the same concern you've had, Member Brown, of, hey, what if the self-diagnostics aren't working?

What is your mechanism to know that these self-diagnostics are still working? And as we have allowed elimination of some certain balances, we've put in what we think are the right checks and balances that the operator does have touchpoints to ensure that those processes are indeed giving you what you think they're going to give you.

So conceptually, we've been working this issue and I think it's been not so much in this forum.

MEMBER HALNON: And this is Greg. Forgive me for being a novice. A component was supposed to be able to do a self-diagnostic, either watchdog timer or some other, wouldn't that be a critical characteristic that would have to be brought through the process and eventually tested in some way?

MR. TANEJA: You know, that's really where, if you're relying on that sort of diagnostic,

and that, and some of these safety critical devices, some of these SIL requirements are that there is a failure outcome, which it puts it into a safe state.

So if it does fail, the result, it's essentially doing what a watchdog timer would do. Essentially, put the output into a safe state and so those are then become the requirements for that product they are getting certified.

And I think one of the points that Andy alluded to was that you have to, if you are going to use this process, you have to see what does the SIL certification mean and what feature is it certifying, and for your application, are those features suit your requirements or not?

But that assessment has to be done very early in the process, before you even go and start to dedicate that item for use.

Does it have the level of certification that meets your requirements for your given application?

So I think, and Member Brown, to your point, yes, we worked on developing the SRPs and the DSRS and all of these ISGs, to really shift our focus toward meeting these fundamental design

principles for the INCs and looking at these dependability of performance and repeatability and dependability where we are talking about, what are these lockup situations and how do we protect against these things? But that is an effort that we pay a lot of attention to when we are doing the overall design application.

Now, here, if you are buying a part, you still have to meet your overall design requirements. What are your requirements for your system? And so that requirement match has to be done by the designer very early on in the process.

So, I don't think we are downplaying any of that effort. I think what we are trying to say, by using the SIL certified product, what you are getting is actually you are getting better products into your plant than you would otherwise.

If you were to dedicate any commercial off the shelf item that has not been proven in the industry, so what we are getting from a SIL certified product is a product that a manufacturer is marketing to a safety critical industry.

So they are saying that I have a market, I'm going to get this certified. They're spending their effort and money in developing a product and

getting it certified because they have a large user base.

But what does that give us? It gives us a larger data to rely on, the reliability data that we get, because we have a larger user base of their product.

So there are these benefits that we want to try to capture, and I think what we are getting from that, it will not be applied properly in our safety systems. We're getting our reliability and hopefully --

MEMBER BROWN: I understand that around the circle discussion, but when you lay out requirements, you've got to do that in the context of the overall system you're dealing with.

And you've got to address the potential weaknesses of what you're dealing with. For instance, when you talk about self-diagnostics, there are a couple of different ways to do that. If you have a deterministic process, which I used in my naval program, every function was performed on every sample period, and at the end, there was enough room where we implemented, we did a certain amount of self-testing.

And then you hit the end. There's a

watchdog timer there. If it didn't get to that point, okay, then it goes back to next cycle, and at that last stop, it knows where it stops and you go through the whole process again.

Every function is tested. No interruption, all the way to the end. Guess what's at the end again? Another watchdog timer waiting.

If you don't get here, I'm going to give you an alarm. Or in a submarine, you may not necessarily trip the reactor. It's not a good idea to do that when you're in certain locations and places.

But you make people aware of it, ever however you want to do it. That's fairly straightforward.

When you do that in the testing, self-testing, and it's an interrupt self-testing where you're 10 percent through and, oh, I'll self-test this little function. Oh, okay, that's working. Okay, come back and I keep going.

You may not ever finish. You may lock up in between. You can't. There's always the potential for that processor not to finish its process.

It never triggered whatever it should trigger at the end to restart again. And the problem with resetting most of these companies' products, like I won't mention the name, but the one platform we used, it took five to ten minutes to reboot. That's horrible.

MEMBER MARCH-LEUBA: Charlie, I wonder if you're confusing apples with oranges.

MEMBER BROWN: Oh, probably.

MEMBER MARCH-LEUBA: Yes. I mean, as the staff said before, there is a step in the design requirements and the range of system. Now you raised the problem of replacing this particular part in the presentation.

The system is really where we already reviewed this. And I want to make sure that this part is as good as the whole.

MEMBER BROWN: The analog one. In this case, they're going to be replacing analog stuff with digital stuff. That's what they're driving at, primarily. Primarily.

MEMBER MARCH-LEUBA: They have to make sure that the system works. And what I like about this approach of having a large user base is that databases will see the reliability of hundreds of

systems, not two.

So there is some feedback. Maybe you did your evaluation and you made a mistake. You put hundreds of these on the field and you find out you made a mistake, put some fix in there, get some feedback, and you fix it.

MEMBER BROWN: I'm not disagreeing with using the process. I'm only looking to make sure that in the process of doing this, we don't distract the overall end result.

The evaluations of the process we go through. The first process, you weren't here, the first one we looked at did not have watchdog timers in it.

We had to insist on it. It was like sucking blood out of rocks. It took us a year and a half to get the FSAR revised.

CHAIRMAN REMPE: So, colleagues, we have four minutes left and we do have to have public comments. And I know Walt has been wanting to make a comment.

MEMBER BROWN: Oh, I'm sorry.

CHAIRMAN REMPE: And so I just, if there's questions from staff --

MEMBER BROWN: No, I'm done.

CHAIRMAN REMPE: If there's time, and then let's make sure there's time for public comments.

MEMBER BROWN: Let's go ahead. Yes, go ahead, Walt. Sorry.

MEMBER KIRCHNER: So I can see that the main thrust here is for implementing digital systems, commercial grade dedicated equipment. I was just thinking ahead to advanced reactors and stuff. This is an observation, not a question.

It points back here to the Reg Guide Appendix B, design control, procurement control and such, and advanced reactor people are basically saying, Appendix A, Appendix B doesn't apply to us. We're not LWRs. But I'm just looking ahead to think of new advanced reactors.

Would the expectation, you think, Dinesh, be you would look for them to in a comparable manner go through a commercial dedication process for their I&C systems? It's a leading question.

MR. TANEJA: Again, the advanced reactors, if they have -- if they have a case where there is a safety function that has to be performed under certain given circumstances and conditions, so for our postulated condition, if the equipment

needs to perform that function, that component needs to be qualified and proven that it's reliable from that function.

Now, if you want to call it an Appendix B or you want to call it a dedicated item, or you want to call it whatever you want to call it, on that new FSAR 53 framework or MP framework, at the end of the day, I need to have a system or a device or a system that reliably performs that function repeatedly if it's required, right?

And I think that is a discussion that we had a couple of the new vendors was that it's really upon you to demonstrate that you are designing this system with high reliability and availability.

And that reliability, how do you demonstrate that? Now, some are saying that we are going to follow the IEC 61503 framework, which actually has done pretty good with the risk significant industries otherwise.

So we'll see what they come back with.

CHAIRMAN REMPE: Charlie, do you want to be the person to ask for public or you want me to?

MEMBER BROWN: No, you can do it.

CHAIRMAN REMPE: Oh, okay. So we're at that time where if someone, a member of the public is out there, if you are on MS Teams, just unmute yourself and make a comment.

If you're on the phone line, I believe you have to press star-six to unmute yourself. But, feel free to do so.

(No response.)

CHAIRMAN REMPE: Okay, there's been ten seconds so at this point -- yes, Charlie?

MEMBER BROWN: You answered the question.

CHAIRMAN REMPE: Okay. Go ahead.

MEMBER BROWN: I'm sorry. No, I just wanted to thank the staff at NEI for a very good summary download from the last Subcommittee meeting where there was a little more detail. But I think this was a substantial presentation. We got to get to the meat of the overall process and what you're trying to accomplish.

And I thought it was done very well and the discussion was animated, as I would have expected in our normal format with these I&C discussions. I just thought it was a good talk.

CHAIRMAN REMPE: I agree.

MEMBER BROWN: Thank you.

CHAIRMAN REMPE: I believe you have a draft letter that you plan to read in in the next hour and we can discuss it and continue the discussions that you and Jose and Walt were having.

Larry, if you're off, or Christina, if you're out there, we need to get hold of Sandra and whoever's going to be helping us with the letter and get it brought up. And so, why don't we take a break until 3:40? And that'll give us nine minutes to try and find the appropriate people.

MEMBER BROWN: What about 15 minutes?

CHAIRMAN REMPE: Okay, Charlie, just for you, how about 3:45? We're going to do 3:45. You get 14 minutes. Get a head start. And I hope that NEI and the staff will stay around and listen to the letter. And, as always, we want factual corrections and --

MEMBER BROWN: No, it's not going to happen.

CHAIRMAN REMPE: Charlie drafted the letter, so I'm sure it's factually true. But anyway, we'll see what happens.

MEMBER BROWN: No, I tried my best to describe the processes, and I'm not sure I got all

the --

CHAIRMAN REMPE: At this point, though we're going to give you your 14 minutes before they turn to 13.

(Whereupon, the above-entitled matter went off the record at 3:32 p.m.)

NEI 17-06, Rev. 1 Overview

7 September 2022- ACRS Meeting

NUCLEAR ENERGY INSTITUTE

NEI 17-06 Rev. 1


NEI TECHNICAL REPORT NEI 17-06, Rev 1

Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications Revision 1

Prepared by the Nuclear Energy Institute
December 2021

https://www.nrc.gov/docs/ML2133/ML21337A380.pdf

- Issued 12/3/2021 (ML21337A380)
- The purpose of this document is to facilitate the commercial grade dedication process for digital equipment by crediting SIL certification by an accredited and NRC-approved certification body in lieu of a commercial grade survey and critical design review

Safety Integrity Level (SIL) Overview

- SIL Foundation
  - Systematic Integrity
  - Probabilistic Reliability
  - Hardware Fault Tolerance

LOGIC SOLVER

SENSOR

ON/OFF ACTUATION

SIL Certification Process

Accreditation Body

Accreditation

Certification Body
ISO 17065

Evaluation Service

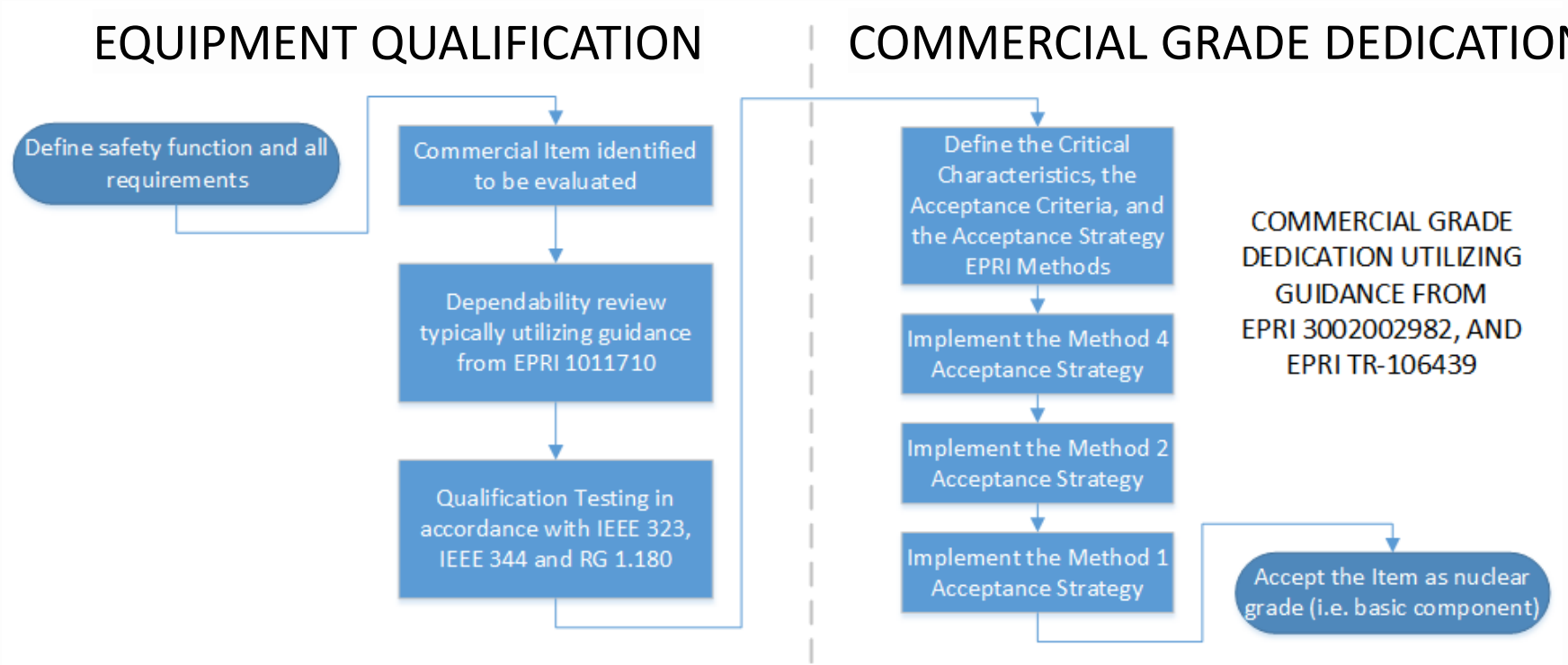
OEM
IEC 61508

Conclusion from EPRI Research

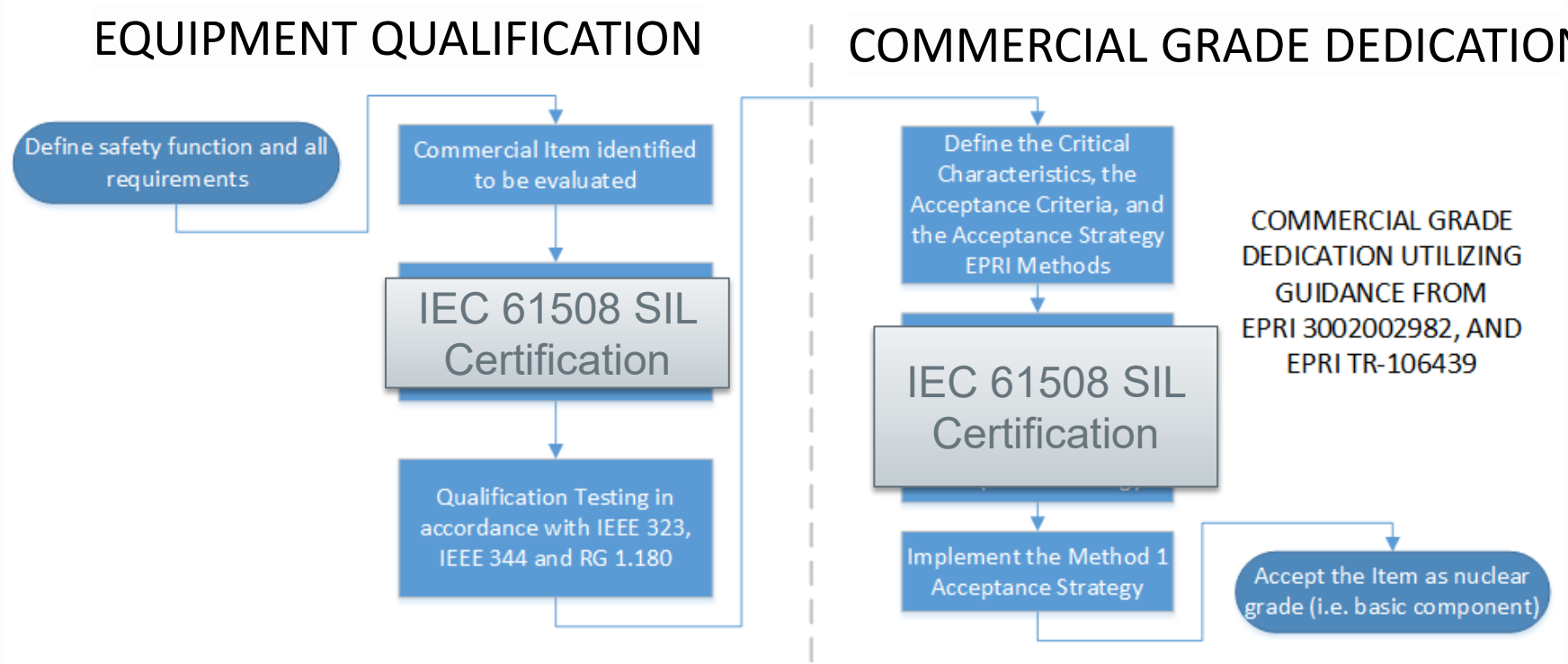
Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power. EPRI, Palo Alto, CA: 2019. 3002011817.

- SIL certification aligns well with EPRI TR-106439
- Certification Bodies (CBs) have a standardized, rigorous, and reliable evaluation process
- Accreditation Bodies (ABs) ensure CBs are consistent and trustworthy
- Failure data indicates reliable operation of SIL certified equipment
- SIL certifications are an accurate indicator of reliability

Justification Process- Current



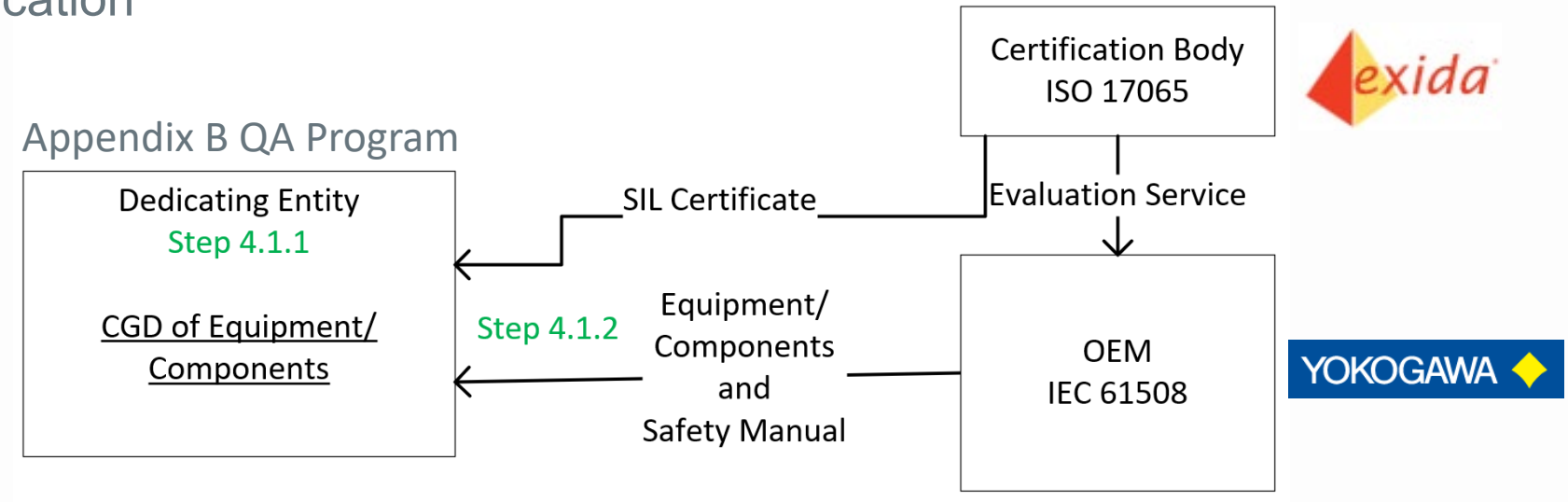
Justification Process- with NEI 17-06



Application of the SIL Certification Process

Step 1. Identify the requirements of the end user's application

Step 2. Confirm SIL certification encompasses the requirements of the application

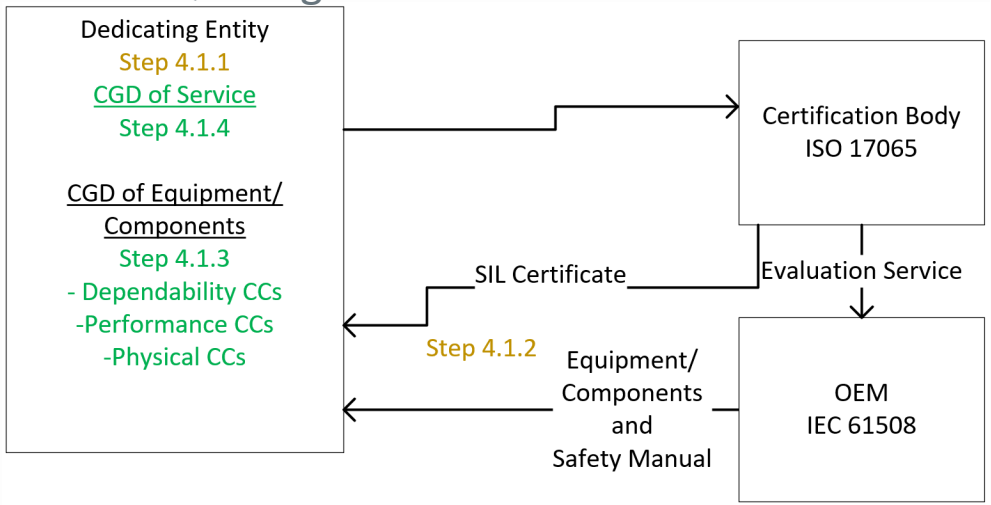


Application of the SIL Certification Process

Step 3. Perform a technical evaluation of the equipment to identify critical characteristics

Step 4. Perform a technical evaluation of the CB's service to identify the critical characteristics of the service

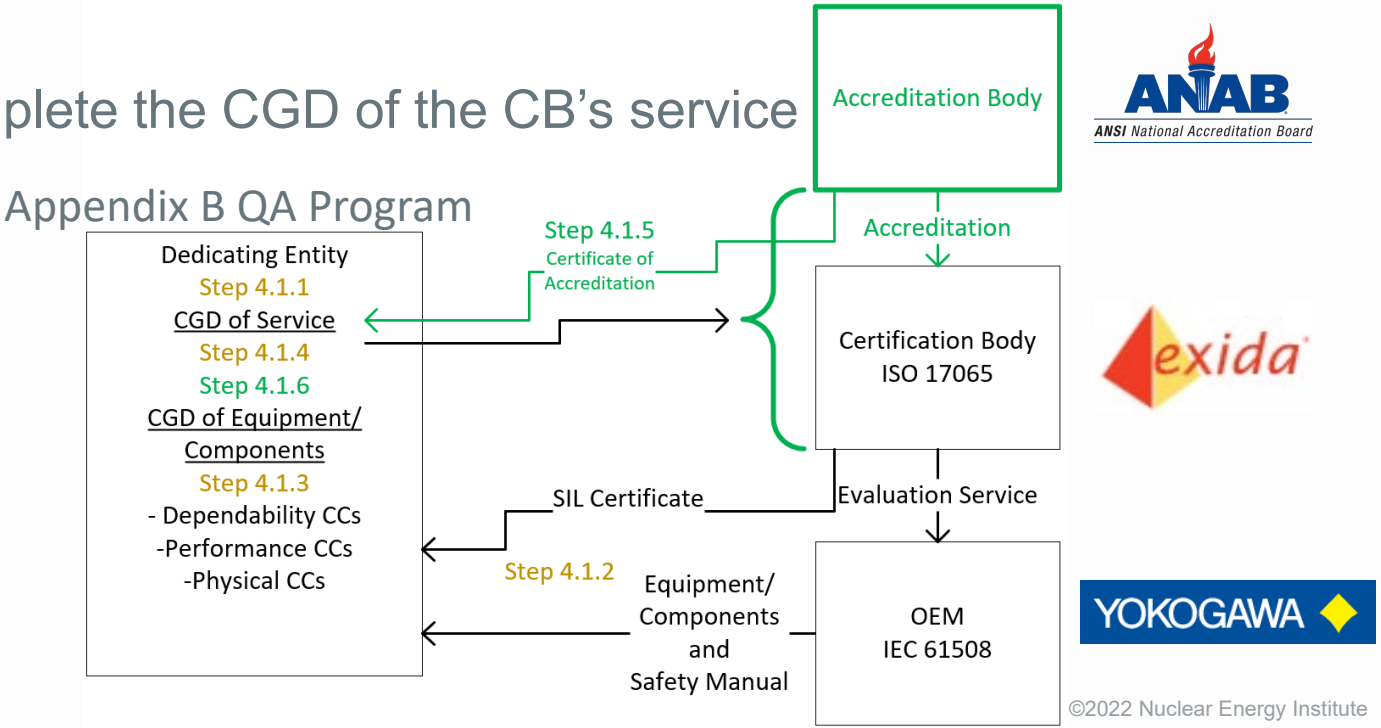
Appendix B QA Program



Application of the SIL Certification Process

Step 5. Confirm that IEC 61508 certifications are within the CB's accreditation scope

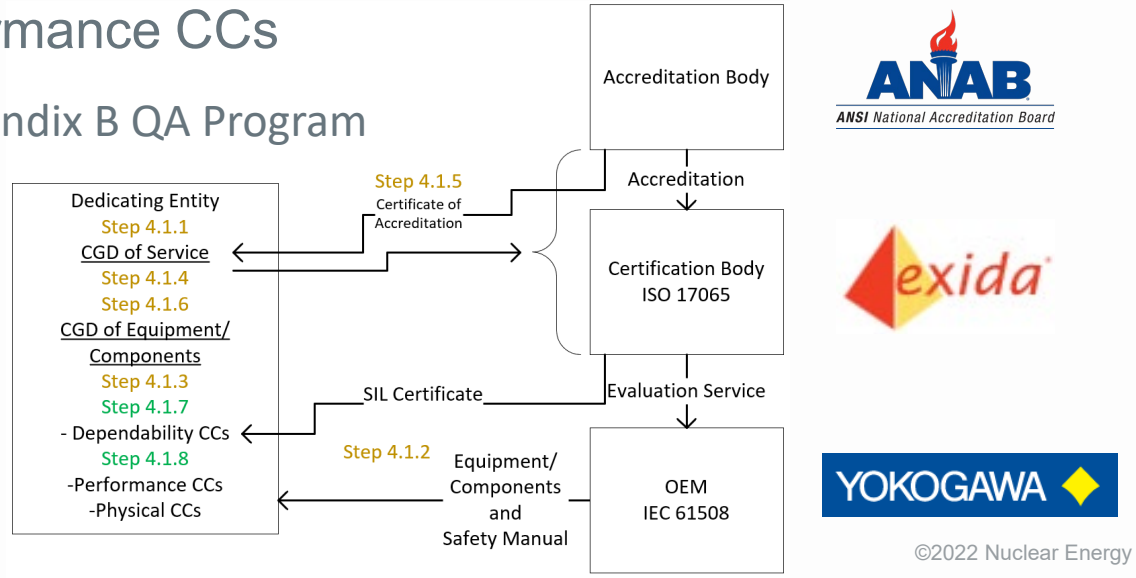
Step 6. Complete the CGD of the CB's service



Application of the SIL Certification Process

Step 7. Use the SIL certification to complete the determination of acceptability of the dependability CCs of the item CGD

Step 8. Use traditional methods to determine acceptability of the physical and performance CCs



Selection of SIL Certified Equipment

- The equipment must be able to perform the required functions for the application
- Equipment must be certified to IEC 61508 at the required level
- The required safety function must be within the scope of the safety function identified in the certification

Paths to Accepting Certification Body (CB) Services

- Accreditation Only
  - Accreditation Body observed conducting a satisfactory ISO 17065 assessment of the Certification Body

- Accreditation Plus Scheme Evaluation
  - Accreditation Body observed conducting a mostly satisfactory ISO 17065 assessment of the Certification Body
  - Additional assessment performed of the Certification Body's certification scheme

Dedicating Entity's Quality Assurance Program

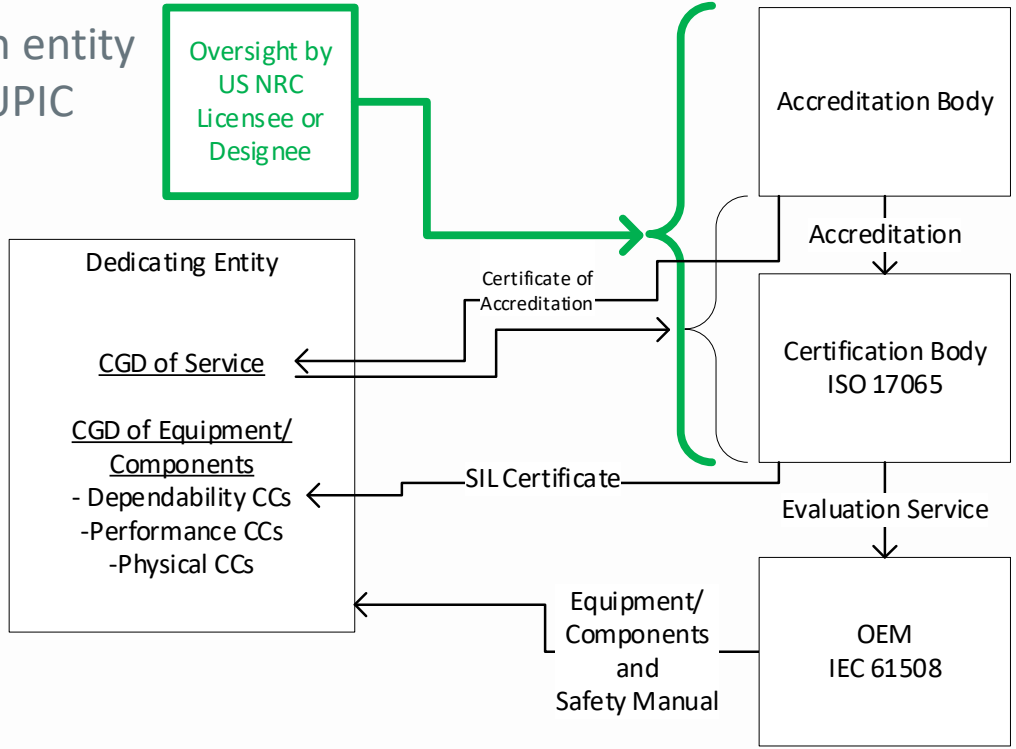
Adjustments will be needed to Appendix B QA programs concerning:

- Procurement Document Control
- Tasks Associated with Digital Dependability Evidence
- QA Evidence for Digital Dependability
- Corrective Action

US NRC Licensee Oversight of the SIL Certification Process

Possibly an entity such as NUPIC

Appendix B QA Program

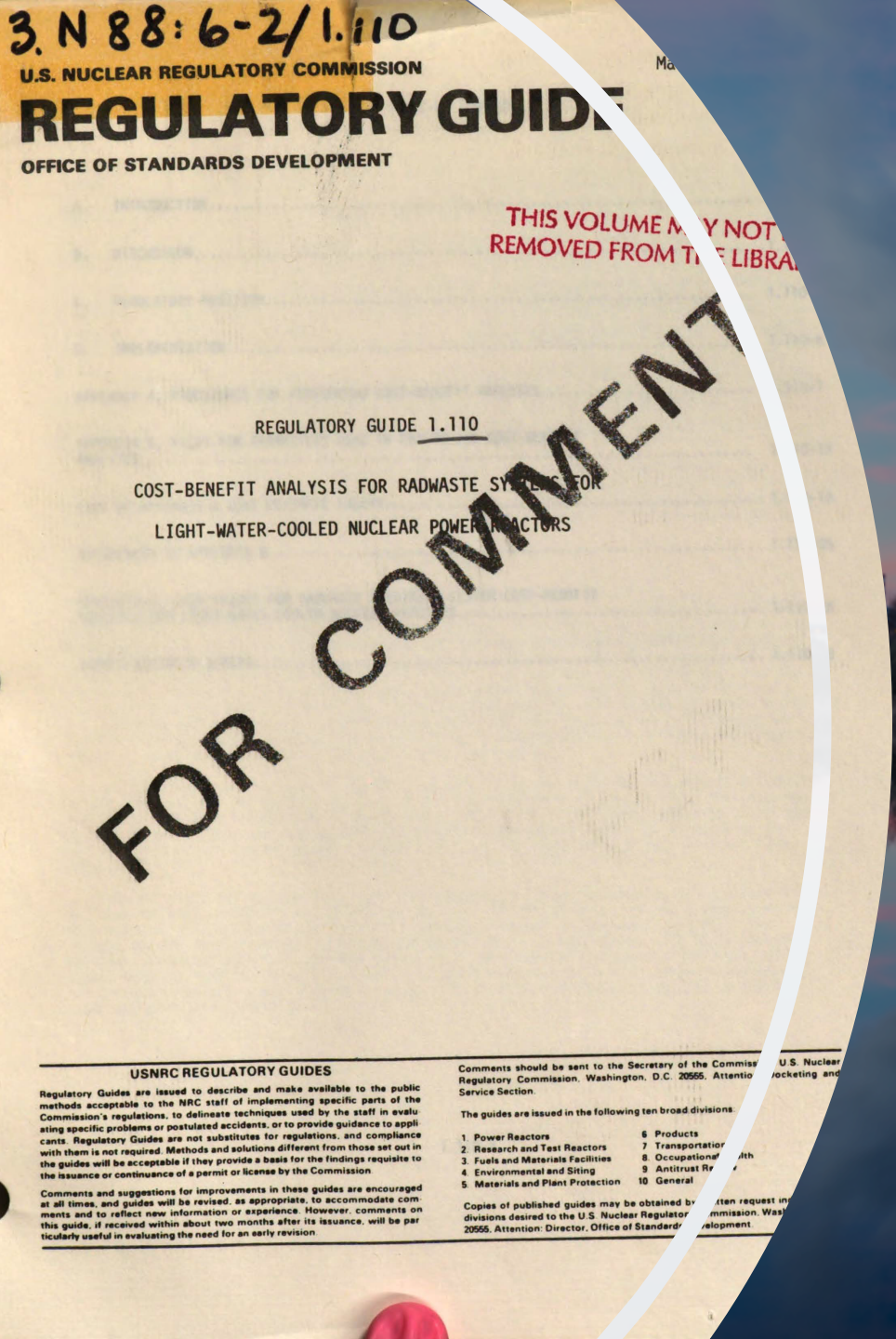


Benefits

- Better Products
  - Manufacturers are building in reliability and systematic integrity
  - Broader collection of operating experience

- Improved Efficiency
  - Economy of scale- joining other high-risk industries to give manufacturers a larger market to sell into
  - Products are pre-approved by CBs, not requiring commercial grade surveys

Questions



Draft Regulatory Guide DG-1402

Proposed new RG 1.250

"Dedication of Commercial-Grade Digital I&C Items for Use in Nuclear Power Plants"

September 7, 2022

ACRS Committee Meeting

Opening Remarks

Eric Benner, Director
Division of Engineering & External Hazards

Office of Nuclear Reactor Regulation

DG-1402 Working Group

Dinesh Taneja, Technical Lead
Sr Electronics Engineer, NRR/DEX/ELTB

- **Michael Eudy –** Project Manager, RES/DE/RGPMB
- **Bernard Dittman** – Sr I&C Engineer (Retired), RES/DE/ICEEB
- **David Rahn –** Sr Electronics Engineer, NRR/DEX/ELTB
- **Greg Galletti –** Sr Rx Ops Engineer, NRR/DRO/IQVB
- **Odunayo Ayegbusi –** Rx Ops Engineer, NRR/DRO/IQVB
- **Jack Zhao** – Sr Electronics Engineer, NRR/DEX/ELTB
- **Jonathan Ortega-Luciano -** (Former) Rx Ops Engineer, NRR/DRO/IQVB

Meeting Topics

- DG-1402 Scope & Purpose
- Background:
  - *CGD of digital equipment*
  - *DI&C Modernization Project (MP) #3*
  - *Development of NEI 17-06*
- DG-1402 Regulatory Basis
- DG-1402 NRC Staff Regulatory Guidance
- Resolution of Public Comments on DG-1402
- Historical Perspectives of CGD

DG-1402 Scope & Purpose

- Endorse NEI 17-06, Revision 1
- Endorse applicable parts of the industry consensus Std. IEC 61508, 2.0 Edition
- Endorse applicable parts of the industry consensus Std. ISO/IEC 17065:2012
- Describe relationships with existing endorsed CGD guidance documents RG 1.164 and EPRI TR-106439

DG-1402 Background

- EPRI TR-106439 describes an approach for the evaluation and acceptance of commercial-grade digital equipment
- RG 1.164 describes acceptable methods for the dedication of commercial-grade items and services.
- In April 2016 NEI proposed a task under DI&C Integrated Action Plan (IAP) to leverage SIL certification to IEC 61508 in commercial-grade dedication of digital equipment
- Proposed guidance to follow the NRC approved NEI 14-05 process for procuring commercial-grade laboratory calibration and test services

DG-1402 Background (continued)

- In parallel, EPRI initiated a research on SIL certification of digital equipment used in non-nuclear process industry and produced report EPRI 3002011817, “Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power”
- As a part of MP #3 task, NEI initiated developing NEI 17-06 guidance informed by the EPRI research
- The NRC staff provided continual feedback during NEI 17-06 development
- On multiple occasions, the staff observed audits of certifying body (exida, LLC) by the accrediting body (ANAB)
- After resolution of NRC staff comments, NEI 17-06, Rev. 1 was submitted in Dec-2021 for NRC endorsement

DG-1402
Regulatory Basis

- 10 CFR 21.3 defines basic component as, among other things, “commercial grade items which have successfully completed the dedication process” and provides definitions for “commercial grade item” and “dedication”

- 10 CFR Part 50, Appendix B, Criterion III, “Design Control” and Criterion VII, “Control of Purchased Material, Equipment, and Services,” includes provisions for QA and quality control that are applicable to the acceptance and dedication process for commercial-grade digital I&C items

DG-1402 Staff Regulatory Guidance

Position 1

1. DG-1402 endorses, with clarifications, NEI 17-06, Revision 1, on using IEC 61508 SIL certification to support the acceptance of commercial-grade digital equipment that is dedicated as a basic component in accordance with EPRI TR-106439

DG-1402 Staff Regulatory Guidance

Position 1 clarifications

a. The NRC staff considers SIL certification to be a commercial grade survey for the purposes of Part 21. Thus, considers dedication of the certifying body's services and verification of SIL certification to be adequate for verifying dependability critical characteristics

b. Each dedicating entity should dedicate the services of each certifying body and should not rely on dedication by, e.g., another NRC licensee

DG-1402 Staff Regulatory Guidance

Position 1 clarifications (continued)

c. In keeping with NRC staff-accepted practices, the certifying bodies' SIL certification process should be observed every 3 years

d. In accordance with 10 CFR 21.3, the NRC use of the term "basic component" includes dedicated commercial grade items

e. Dedicating entities should take measures to avoid the acceptance of expired, counterfeit or fraudulent SIL certificates

DG-1402 Staff Regulatory Guidance

Position 2 with clarifications

2. DG-1402 endorses, with clarifications, use of IEC 61508, Edition 2.0 as described in NEI 17-06
   a. Dedicating entities should verify the certifying body's accreditation consistent with the guidance in section 6.3 of NEI 17-06
   b. Dedicating entities should verify that the substantive requirements of the later editions related to the dependability characteristics remain unchanged from the IEC 61508, Edition 2.0

DG-1402 Staff Regulatory Guidance
Position 3

3. DG-1402 endorses the use of ISO/IEC 17065:2012 by certifying bodies to perform commercial grade surveys as described in NEI 17-06

Resolution of Public Comments

The NRC received 5 public comments on DG-1402 that have been adequately resolved

1. In response to comment 1, clarification has been added to Staff Position 1.b. that partly states, "…each of the licensees or dedicating entities relying on the results of a commercial grade dedication performed on behalf of licensees or dedicating entities remains individually responsible for the adequacy of the commercial grade dedication."

2. In response to comment 2, Section B of DG-1402 has been revised to state, "NEI 17-06 leverages an internationally recognized safety integrity level (SIL) certification process that relies on International Electrotechnical Commission (IEC) 61508,"

Resolution of Public Comments (continued)

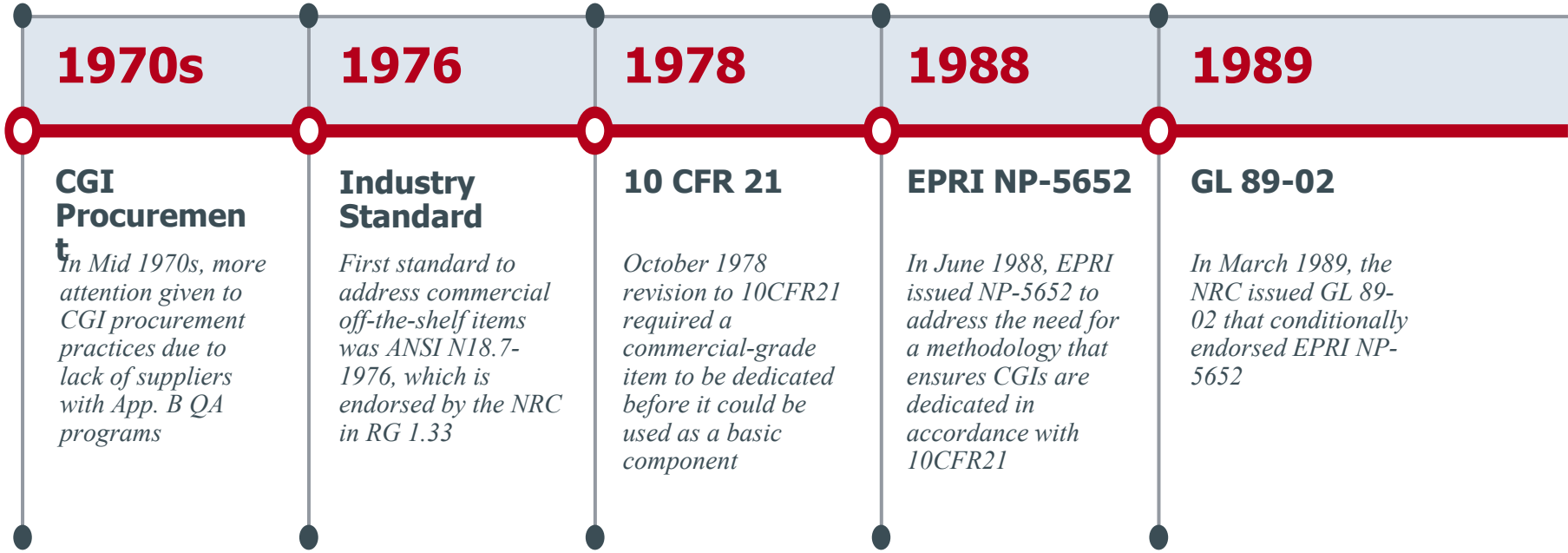
3. NRC staff agrees with comment 3 and the recommended edit has been made to Section B of DG-1402, “The NRC staff considers SIL certification to be a commercial grade survey for the purposes of Part 21.”

4. NRC staff agrees with comment 4, but not entirely with the recommended edits. Staff Position 2.a. has been edited to clearly indicate that NEI 17-06 is leveraging an existing certifying bodies’ accrediting process.

5. NRC staff disagrees with the comment 5 recommendation of a reduced frequency for observing certifying bodies certification process. Therefore, no changes were made to DG-1402 as a result of this comment.

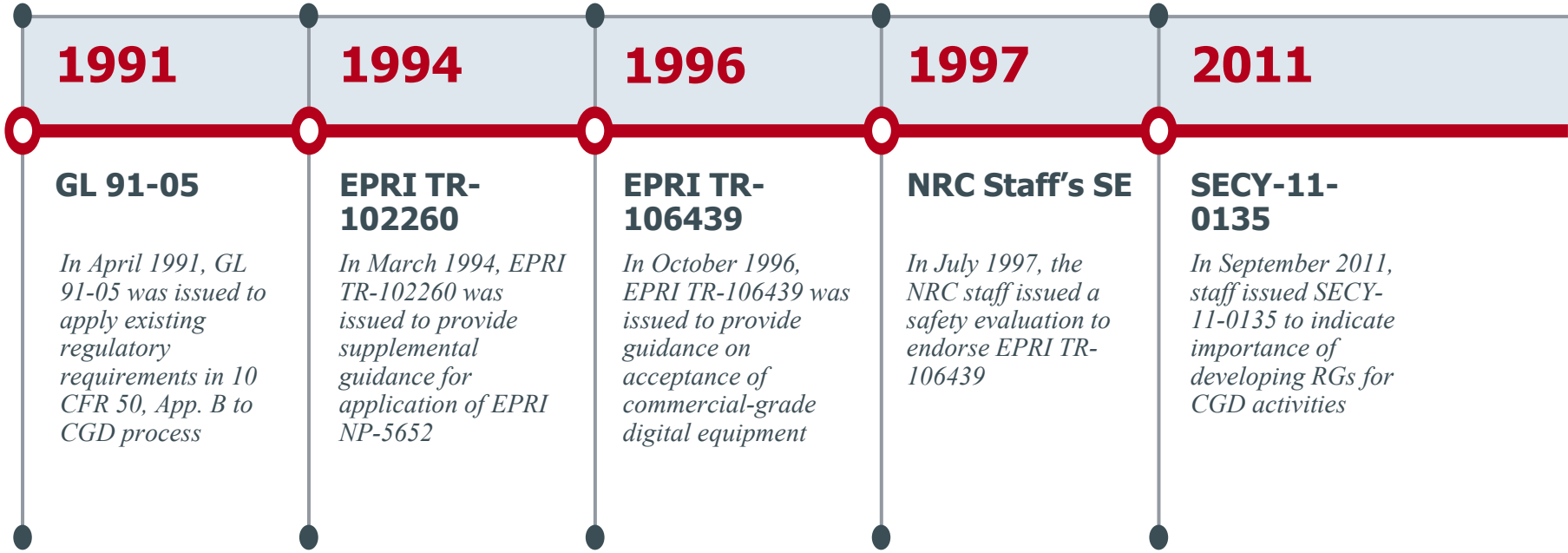
CGD of Items & Services

Historical Perspectives



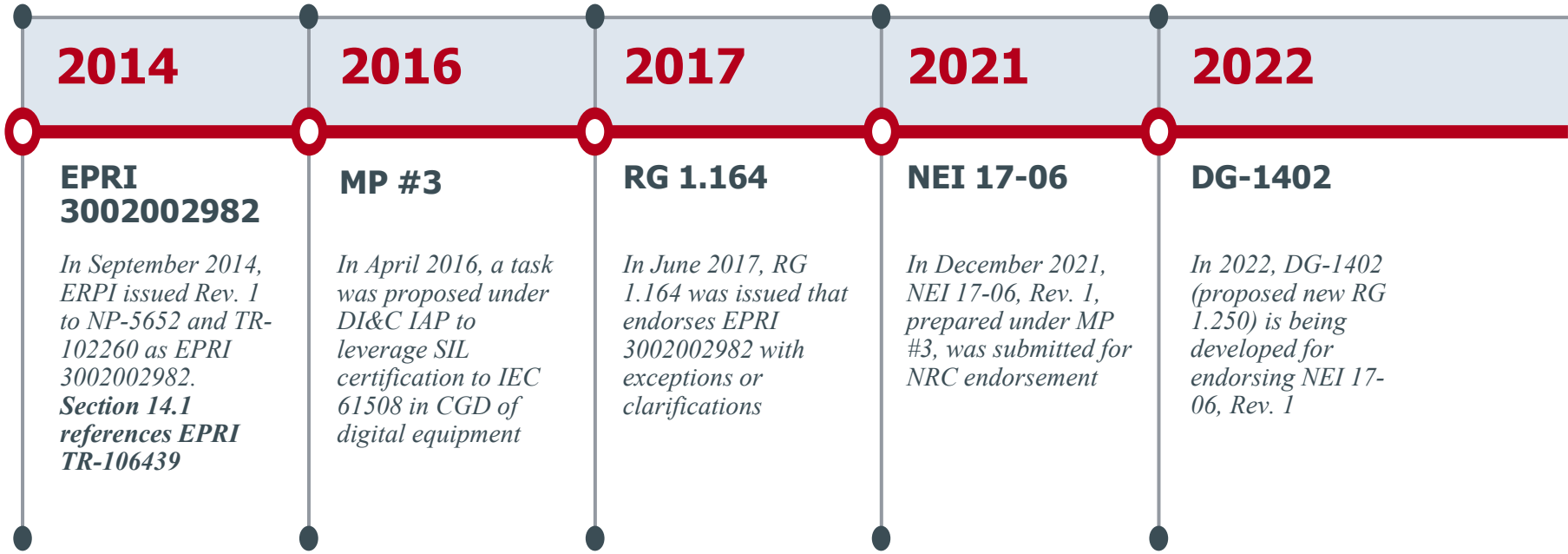
CGD of Items & Services

Historical Perspectives



CGD of Items & Services

Historical Perspectives



Questions