Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Joint Digital Instrumentation and Control
Materials Structures Subcommittee
Open Session

Docket Number: (n/a)

Location: teleconference

Date: Thursday, June 22, 2023

Work Order No.: NRC-2447 Pages 1-162

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

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

JOINT DIGITAL I&C AND FUELS, MATERIALS AND STRUCTURES SUBCOMMITTEE MEETING ON EPRI DIGITAL I&C PERSPECTIVES

+ + + + +

THURSDAY

JUNE 22, 2023

+ + + + +

The Subcommittee met via Teleconference, at 8:30 a.m. EDT, Charles H. Brown, Jr., Chair, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Chair

RONALD G. BALLINGER, Member

VICKI M. BIER, Member

VESNA B. DIMITRIJEVIC, Member

GREGORY H. HALNON, Member

JOSE A. MARCH-LEUBA, Member

WALTER L. KIRCHNER, Member

JOY L. REMPE, Member

THOMAS ROBERTS, Member
MATTHEW W. SUNSERI, Member

ACRS CONSULTANTS:

STEPHEN SCHULTZ
DENNIS BLEY

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

A G E N D A

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

8:37 a.m.

CHAIR BROWN: Good morning, everyone. This is a hybrid meeting of the joint Digital Instrumentation and Control Materials Structures Subcommittee. We will now come to order. I'm Charles Brown, the chairman of the subcommittee. Can I be heard, by the way? And, recorder, are you there?

Okay, thank you.

MEMBER BIER: And I hear you, Charlie.

CHAIR BROWN: Oh, okay, thank you. ACRS members in attendance are Ron Ballinger, Jose March-Leuba, Matt Sunseri, Consultant -- Steve, where is your name on here? I didn't put you on here. I know your last name is Schultz, but your name is not on your list. Walt Kirchner, Joy Rempe, and online we have Vicki Bier, Greg Halnon, and Vesna Dimitrijevic, and, I think, Christina Antonescu of the ACRS staff is the designated federal official for this meeting.

The purpose of this meeting is for the electric power researchers to EPRI to brief the subcommittee --

(Audio interruption.)

CHAIR BROWN: -- systems engineering framework. The framework is Board synthesized from systems engineering methods. It provides a fast way to risk inform digital instrumentation, digital I&C implementation to the nuclear industry worldwide.

EPRI will also discuss the current utilization status of the framework in near term revision. The ACRS was established by statute as governed by the Federal Advisory Committee Act, FACA. That means the committee can only speak through its published letter reports.

We hold meetings to gather information to support our deliberations. Interested parties who wish to provide comments can contact our office requesting time. That said, we set aside 15 minutes for comments from members of the public who are listening to our meetings. Written comments are also welcomed.

The meeting agenda for today's meeting was published on the NRC's public meeting notice website as well as the ACRS meeting website. On the agenda for this meeting, and on the ACRS meeting website, are instructions as to how the public may participate. No request for making statements to the subcommittee has been received from the public.

We are conducting today's meeting as a hybrid meeting. A transcript of the meeting is being kept and will be made available to all on the website. Therefore we request that participants in this meeting should first identify themselves and speak with sufficient clarity and volume so that they can be readily heard.

All presenters, please pause from time to time to allow members to ask questions. Please indicate the slide number you are on when moving to next slide. We have the MS Teams phone line, audio only, established for the public to listen to the meeting.

Based on our experience from previous virtual and hybrid meetings, I would like to remind the speakers and presenters to speak slowly. We will take a short break after each presentation at my discretion to allow time for screen sharing as well as the Chairman's discretion during the longer presentations.

Lastly, please do not use any virtual meeting feature to conduct sidebar technical discussion, rather contact the DFO if you have any technical questions so we can bring those to the floor.

One other thing I would like to emphasize is that this is a subcommittee meeting. And comments that EPRI receives, or anybody else hears from the subcommittee meetings, anything they bring up is their opinion, their thoughts, and what they are thinking relative to whatever the presentation is.

The committee only speaks as a joint committee thorough our full committee meetings when we rewrite reports which summarize and then provide recommendations and conclusions. So things we may say, which may be a lot, those are individuals' thoughts on the particular subject at hand. So keep that in mind, please.

We will now proceed with the meeting. Mr. Matt Gibson, the technical executive in the Electric Power Research Institute Nuclear I&C program will make some introductory remarks. Matt, you're on.

MR. GIBSON: Thank you, Charlie. And I just want to thank the joint subcommittee for inviting us to share our perspectives on digital I&C. EPRI does a fairly high volume of research in this area, and we create products for stakeholders that they can use.

Today we're going to concentrate on our digital systems engineering framework. Now we do other research on, you know, our digital I&C in general. We do research on alternate architecture using different kinds of technology. We do detailed research on wireless technologies, maintenance, techniques that are effective for maintaining your I&C systems. But predominately today we're going to talk about the framework and the products that are related to it.

So here we go. Don, Mary, you have anything you want to add to that? No?

MR. WEGLIAN: No.

MR. GIBSON: All right. And let's see if our technology is going to work today. Here we go, a little bit of a delay. But, you know, we're all familiar with the story of the elephant and the blind men where someone -- the blind men touch the elephant, you know. And they see the elephant through their touch and only see part of the elephant.

You know, the man that touches the trunk thinks he may be looking at one kind of animal. And then when the leg is touched, maybe it's kind of a plant or a tree. And the tail, you know, maybe it's yet another kind of animal, but not an elephant.

So that's pretty analogous to what we have faced with the emerging of technologies in the nuclear industry. And if I can figure out how to do this, there we go, I have the right button now.

What you'll see as we go through this is each one of these topics are the elephant, right, you know, your cybersecurity, your hardware reliability, you functional reliability, automation, human interactions, and systematic failures. We need a way to put all that together in a single process, because each one of them has a relationship with the other, you know, whack-a-mole, maybe you can visualize that.

Systems engineering allows us to do that. And every framework works on that principle. We're going to go through that. And you'll see a lot of things that, you know, maybe each of you know a lot about individually, or maybe you know a lot about a lot of this. But we want to give you a really good situational awareness of where EPRI is with this, with this idea and how it's being used

First off the history, so we didn't kind of this overnight or about ten years ago. You'll see this progression of the early products that we created as we looked into these things. And you'll see that progression in the light blue stuff. We start working on hazards analysis.

The 509 report you see in the top left, because I'll just refer to these as their last three or four digits number-wise. It's a little easier, because I think you can see that okay. The 509 report, we did a blind study of different kinds of hazard analysis methodology to see how well they work.

The way we did that was to take real events that happened that we had root cause analysis for, and ask a group of folks who had no knowledge of that to use this methodologies to find those same problems that had occurred in real life.

It's a very good product. We looked at several different hazard analysis methods. All of them had strength and weaknesses. When we post that, and we pretty much asked, you know, gave that to the industry as a tool, you know, use these. Use your own judgement about what kind of thing you're trying to achieve. Use the right method, right, the appropriate method.

We also worked on hazards for cybersecurity. You know, maybe that's a little special. We created a cybersecurity procurement methodology, digital instrumentation for the design guy. You know, I think over the years, and kind of in the last ten years, at least the I&C Committee has probably seen something about the DDG as it was called back then.

Well, as we progressed through

and continued to research this, we got several, you know, pretty good epiphanies. You'll see about 2018, 2017, up in the top, middle, you'll see a report in the HAZCADS, Revision 0.

Well, we had previously been working on a hazard analysis methodology for cybersecurity. It was clear to us, at about that time, you couldn't do hazard analysis for cybersecurity, because it's the same thing as the rest of the digital systems, all right. Because the hazards that a digital system can produce, or can cause, or be part of, are related to its function.

Cybersecurity is a cause of that malfunction. But it doesn't really produce different hazards from an equipment and, you know, a plant functional point of view. Certainly there are different hazards in cyberspace about someone stealing your information, or embarrassing you in public, and things like that. But we're going to -- the context here is in a plant functional area.

At that point we realized what we had was a universal method to do hazard analysis that could be applied to any cause, you know, your hazard, you identify the hazard, you identify the risk sensitivity of it. Now you could apply it. And that's where

HAZCADS, Revision 1 came from, roughly 2020.

Now the couple of takeaways for HAZCADS is we continue to use the blind study method where we took, or take, and continue to take real world events. We present those to a team of people who are blind to the event. They don't know really the outcome. They get all the same technical data that, you know, they would normally have, whoever made the original change to a plan or the original new design, and then they evaluate that and see if they can find a problem with it.

And the success rate for HAZCADS really is pretty close so 100 percent. And we said well, wow how could that be that much of a difference? And it really is not so much that HAZCADS is a perfect process, as it's that the way we were going about it before really didn't look at hazards systematically. You know, it was kind of a person's knowledge.

We accessed a presentation from an organization that said well, you know, we try to deal with these problems by putting our best people in a room for three weeks and have them think about it. And they still miss the problems.

And I asked him, well, what method did they use while they were in the room together for three weeks?

Oh, they were just brainstorming, right.

So the takeaway there is the structured methods pay off. They actually make a difference.

And we'll talk about HAZCADS in detail today, just one of the more unique things about the framework which is an overall systems engineering framework. We also did some work on bringing systems engineering to the forefront.

And usually when we -- you'll see at the 2016 column with the medium blue down at the bottom, you'll see an 8018 report. We went out and looked at other industries about, well, how do you do engineering, and how do you achieve good results? And what's your matrix, what's your performance matrix for that good result?

That's some good input that's in that report. Everybody uses that. The aerospace industry, the critical process industries, transportation, you know, Elon Musk, everybody uses systems engineering, right.

And so we said, it has a high efficacy. This is something that could really change the game. If you look at how engineering is currently done by licensees, and to some extent by vendors, not entirely, because it at the day they have to get stuff to work, so do licensees. But what you'll see is that maybe they're trying to do something that's more of a check list process.

They're trying to make sure all the lists of things they have to do have been addressed. And they do good work, I'm not saying they don't. And they produce, some, you know, good and safe designs. But they don't necessarily use the, excuse me, the iterative approach and the diagnostic approach that systems engineering does.

And it actually tends to be multiple processes. In other words, if you've got HFE is in its own process, cybersecurity is off doing its thing, you know, the safety people are hunkered down doing their thing, you know, plan integration, big thing. You know, what are the mechanical, what are the seismic people doing? What are the electrical EMC people doing, you know?

So we pulled all that together, all those topics together into one process, that's the digital engineering guide, and that's down at the bottom center in dark blue under 1816.

While we were doing that --

MEMBER SUNSERI: Can I just ask a

question?

MR. GIBSON: Sure.

MEMBER SUNSERI: I hear what you're saying, and actually you're making me really nervous now, because I think that before, if I was running my plant I was buying parts for my plant, I was relying on that vendor to, you know, send me a part, or certified, say, for however you want to that.

But now you're saying that inherently, by the way they develop them, there might be defects that aren't detected through the systematic approach, that they're sending me to my plant, and I'm installing them? I don't know, that's kind of what I'm hearing you say.

MR. GIBSON: Well, you think about the history. There is a non-zero possibility that that happens, right. I mean, we know that, and we have events that show that.

CHAIR BROWN: We're talking about -- are you talking about each part or are you talking about a system that the vendor is sending you to operate?

(Simultaneous speaking.)

CHAIR BROWN: -- parts that's why I'm -- I wanted to make sure.

MR. GIBSON: I mean, a part of the system or whatever, I mean, you know, part of the strategy at the plants is making sure the vendor's got the right controls to send us stuff that is error-free, right. And we do a lot of factory acceptance tests, and site acceptance tests to validate that.

So you're saying -- what I heard you say is that there may be a hole inside those vendor processes, because they're not using this systematic approach to design and development.

MR. GIBSON: Sure. That is what I'm saying.

MEMBER SUNSERI: Well, that's unnerving.

MR. GIBSON: Well, remember that, in order to do better, you have to recognize you have room to get better. That means you have to be a little critical about what you're currently doing. That's what we're doing here. I'm not trying to say that everybody is, you know, just some huge , you know, ice berg sitting here that's the ruination of everything. What we're saying is this can be better. And more importantly, it can be more efficient.

But there's more to your point. If you look at the industry OE, the NRC's OE, the industries' OE, I mean, those events happen all the time. You know, the factory acceptance tests do not detect all the errors, right. You know, they don't catch all the problems, or they get to a factory acceptance test and they have problems, which they should have not had by the time they got to that spot in the process.

Well, anyway that's the kind of -- it's just a thing you see in other industry. They get to a good answer, the best answer maybe, but certainly a good answer, fast and reliably. And that's kind of what the industry is trying to head toward, is being able to do better and do it quicker. Time is money.

All right. So we look back at this, we also have cybersecurity in here. We have an assessment methodology that's integrated into the framework. One of our -- I think more of our watershed researches is our investigation of off the shelf certified equipment that's certified to non-nuclear safety related standards in other industries, other process industries.

And you'll see that, a little off to the right, in the bottom in dark blue, safety integrity level efficacy for nuclear power, 300-201-1817. We did that research a little ahead of integrating the DEG.

And what we did with that is our hypothesis was if other industries are using self-certified equipment, which are mass produced to a high standard, high reliability standard, and they're successful at it, and they have safe -- they can boil gasoline and not kill anybody, or at least not unless they violate some other rules, well, how does that work for us maybe for nuclear?

So we looked at that. And we pulled a really close to two billion hours of operational data on high end logic solvers that had been certified by the SIL process. And if you're not familiar with that, that's standards IEC 61508 and IEC 61511 is used by most of the process industries for safety, and life critical platforms, and for applications, 61508 for platforms, and 61511 for applications.

So we looked at that. And the data was pretty striking, you know, it told us that this would be a pretty good thing. I mean, you could buy safety related, in our terminology, platforms ready to go.

Now you still have to put an application on them. You still have to integrate them. Remember, this is a stack, so to speak, of things you have to do. It's the basic platforms. The inner-workings of something like that can be proven to be highly reliable.

We will mention here, because we'll talk about it in some detail as we go through further parts of this, we do use STPA, system-theoretic process analysis, as part of HAZCADS (audio interference) four. And we add some risk informed features through HAZCADS. We'll touch that, you know, in more detail as we go.

MEMBER MARCH-LEUBA: Will you go in more detail on the risk informed cybersecurity?

MR. GIBSON: Yeah.

MEMBER MARCH-LEUBA: Because -- let me just put it now. A few years ago, you will remember the risk on cybersecurity was a teenager living in their mother's basement trying to impress his girlfriend. And in 2023 it's active warfare by state activists. It has grown, like, ten orders of magnitude. And I cannot tell you what it will be in 2024. So it is changing by the minute.

MR. GIBSON: Well, I'll give you an analogy so you can chew on it a little bit as we approach actually talking about this in detail.

From EPRI's research, safety and security are the same thing, right. They're identical, there's no difference between them. They the same word in other languages, all right. You just have to use the context to figure out which thing you're talking about, the nuance of it.

That's an important thing to understand, because if we, in the industry, think we have a mature review of safety, then we would never hook up your re-application system and allow children to have access to it, would we? No.

We would have a series of safety design and other access control protocols that are safety protocols, really. I mean, you just don't want unintended actuations of the system. You don't want unintended configuration changes to the system that would cause it not to work. All that stuff are safety things that people will be safety fitted out all the time.

So as you think about safety and security being the same thing, clearly we can use those same effective protocols that help us with security or safety things like, I mean, it's going to work for us. We'll see it a little later.

MEMBER MARCH-LEUBA: Vicki, we're seeing your hand, but let me --

MEMBER BIER: Yes.

MEMBER MARCH-LEUBA: Let me continue, because I'm online.

MEMBER BIER: That's fine.

MEMBER MARCH-LEUBA: I disagree that safety and security are the same thing. Security is there to prevent safety problems. You place a gate so that somebody doesn't come inside and cause a safety issue. So that's one thing. And then I always give an example in this microphone of the famous casino break-in where they broke in through the aquarium.

And obviously we are not going to connect a protection system to the Internet. Nobody would be crazy enough to do that. But what EPRI and the industry need to be looking for is where they are the aquariums at the plant. You are never -- the bad guy is never going to come in through the front door. They're going to come in through the aquarium.

And you have to be remain ever vigilant, and fund your departments, and continue to support them, and do the best you can knowing that you're going to be penetrated. Eventually, the bad guys will get in.

MR. GIBSON: Okay.

MEMBER MARCH-LEUBA: You want to say something about it?

MR. GIBSON: No. I have a lot to say about other things.

MEMBER MARCH-LEUBA: Vicki has a question.

MEMBER BIER: Yeah. I just want to chime in on, again, the same issue of are safety and security the same thing. And I think one big difference is that --

(Audio interruption.)

MEMBER BIER: -- So one of the examples I usually use, you know, like if San Francisco decides they need a strict building code because they have earthquakes, the earthquakes don't pick up and move to Houston because the buildings in San Francisco are now well protected.

But in security you definitely can have people outwitting your defenses, circumventing your defenses. It's kind of more of a, you know, a race. So, you know, I'm happy to hear the rest of the presentation obviously and, you know, may chime in later. But I just wanted to put that comment out there. Thanks.

MR. GIBSON: Thank you. So this is conversational, so this is all good. When we get to the other, where there's more detail and some other stuff, we can dig a little deeper into that. The framework elements though are, there's four of them. I've touched on them. First of them is there used to be industry standards.

And this is another controversial statement, but our research bears it out. The standards that you see, the current IEC, and some of these are IEEEI, so IEC standards, I abbreviate them here a little bit, are very effective. And they have (audio interference). I mean, they used hundreds of thousands, if not millions of things, and they achieve a high level of net functional reliability.

So, you know, our framework is really a synthesis of those. You know, any standard, you know, you have to have a process that you make on that standard so you can use it. And that's what we've done here. It allowed some leverages of economy to the scale.

If you're looking for new advanced reactors, which is supplied to them too, where are we going to get the people? You know, where are we going to get the equipment? How are we going to scale it? Who's going to make 200 or 300 of these, you know, if you believed in these reports, but, I mean, in power plants that are going to be built over time?

Well, that's with economy of the scale, these standards, and equipment, and personnel with qualifications to go with them, are literally, the order of magnitude, better than nuclear from just a mass. You know, just how much stuff, how many people, how much training available, that kind of thing.

The second part of that is used for systems engineering, you know, again it's a single process. It covers a complete life cycle, you know, from inception to retirement, including O&M phase. It's well used. Again, we were able to find good examples of how that works.

If you look at the standards that go with that, the IEC 15288 and 289, which was seven of those standards are the up and coming nexus for most engineering work. When you add STPA to that as a diagnostic tool, you get a pretty compelling case for using systems engineering on a regular, you know, as a core value, core process.

Another, just I'll touch on it here, and we'll talk about it some more later probably, is the whole world is going away from software to systems. For instance, if you look at the IEEE standard 1012, for instance, the 2004 edition, it only covers software. You look at the 2012 edition, it covered everything, software, hardware, people.

So the movement to look at the world through systematic means, through functional reliability, is probably now almost a decade old. And it's reaching fruition. If you look at the front matter of some of your traditional standards like IEEE 730 or 820 it'll say it's harmonizing 15288 or being harmonized.

You know, not lastly, but the third part of that is risk informed engineers. So, you know, engineers can do anything, but they can't do everything, right. That's kind of something to think about. So at some point you have to make tradeoffs, you have to understand resources. You have to actually understand what the real problems are too.

So risk informing the digital I&C practitioners' tool kit so that they can make good decisions, integrating risk informed elements of that are critical. We do that for other things, or the industries do that. You know, they don't waste a lot of time on things that are low consequence or low likelihoods. And so getting some feel of that and letting that factor into your graded approaches, or even your solutions, how it's structured, is another important part of our framework.

The fourth and last part is a capable workforce.

MEMBER MARCH-LEUBA: Other thing is risk informed theory. What's your ideas, your thoughts on chasing the last hard to find software error that may be latent in there, and you've never seen it? Is that something we can do with risk inform. I mean, because if you know --

MR. GIBSON: Well, it's a -- all right, so it's part of it. All right, today in your PRAs, and so I'm surrounded by PRA people, and you know who you are, right, so if you want to weigh in you can certainly do that. But to be risk informed, one of the key, or if not the core things is likelihood, right. Everybody talks about, hey, you've got to have consequences and likelihood. Only way to get to likelihood is to know how reliable your stuff is, right.

So what this does, what risk informing digital does is move the emphasis from deterministic, you know, duties, lists of things, and we'll be fine, to what do I need to do to increase my reliability.

I thought it was fascinating, you know, you brought it up, if I look at the Standards Committee, most of the reliability is over with the risk people. You know, I&C like it is, IEEE Committee for nuclear I&C, there's no Reliability Committee. All that's over in the risk people.

We collectively are going to the ANS

conference here in a few weeks. John is presenting on stuff in the risk section on I&C reliability. There are no I&C reliability presentations. I looked through the entire thing, there are none.

That's really a big takeaway for everybody. As you go to risk informed, reliability analysis shoots to the top of the list. You know why, it's because what risk people do. You know, you have to know what your reliability of your components are to predict the future. Because that's what risk does, right, you predict the future.

So if you have all this data, all these pumps, and valves, and ten to the minus this and that, you know, what their statistical reliabilities are. And unless you take that and plug it into a PRA and say, okay, I can predict the future now, because I'm holding -- this condition's the same, right, I'm making sure I do my maintenance and all of that, but it's all predicated on maintaining the reliability of those pieces of equipment at the same level that was used to collect the data in.

Would anybody want to brief me on that?

MR. WEGLIAN: I'll weigh in. We're going to get, oh, this is John Wedlian with EPRI. We're going to get to this in a little bit. But most of the software errors that we encounter are actually errors in requirements, not typos in the source code. And our process is designed to find those. And one approach is to change the design so that they can't happen.

And then the other approach, if you can't do that, is to have control methods to prevent them. But if you know ahead of time that it's a potential, then you can design your testing to look for them. But you can't do that if you don't recognize that it's a potential in the first place.

So to your point, the latent error that goes undiscovered until it happens is most likely an error in requirements, because you didn't recognize that that could have gone wrong. And therefore you didn't test for it to make sure that it does the right thing in that condition.

And that's what our process is designed to do, to identify those things that can go wrong and add it, either change the design so that it can't happen, or apply control methods like testing to verify that it does the right thing.

MEMBER MARCH-LEUBA: But to my previous question, I like what you're doing, because it is deterministic. How does risk informed feed into that process?

MR. WEGLIAN: So if the function that you're doing can't lead to a significant problem, you know, for nuclear safety, if there's 20 systems that can back it up, then why would you spend a million dollars to protect from that? So that's what risk does. It identifies these are the important functions, and you need to spend a lot of effort to make sure those don't happen. And these are your functions that are not important, and you can do the minimum on those. Because even if they fail it's not a catastrophic effect on your plant.

MEMBER MARCH-LEUBA: Historically we change the likelihood by having redundancy and diversity.

MR. WEGLIAN: Or this defense in depth, you get FLEX now. And the PRA, which is what we use for the risk assessment for the nuclear safety part, at any rate, it accounts for all of that, right. It looks for what's proceduralized, right, what are the operators actually going to do in an event, what systems are available to them if a particular system fails? And the PRA accounts for hardware common cause failures as well, not just software, of course.

And we can show with the PRA models that any one system can fail completely, and we still have success paths, right. And so our design basis approach creates very reliable systems that we have, you know, defense in depth to account for combinations of failures. We have very good designed plants. And we specifically look at what alternatives are there for the function that may be lost to see which failures are extremely important and which ones are not.

And redundancy is not always the best approach. Sometimes adding additional equipment, hardware, integration of additional systems that do something else, can add more complexity, can actually increase the risk rather than reduce it. It depends on the situation in the plant and what you're trying to do. So just relying solely on redundancy is not always the best approach.

MEMBER MARCH-LEUBA: Redundancy and diversity.

MR. WEGLIAN: Right. Right, diversity is another approach. But again, failures that we see can also be caused by unanticipated interactions between systems. So there isn't one answer that always works 100 percent. And an approach is designed to find for the particular system that you are trying to install, or modify, or build, or whatever it is, what is the best approach for that situation.

And looking at two different plants, you may come up with different answers. One may say we want a diverse system that can do these functions, and another plant may say we do not want that. We want that, we want an operator action that can manually start but not a completely redundant system that gets added in. And our approach is designed to identify what the best approach is.

MEMBER SUNSERI: I know I'm kind of slow on all this stuff, but I'm starting to get really lost. Because what I hear you talking about, when I think about redundancy, diversity, defense, and FLEX, all that stuff, that's about mitigation, right.

If we're depending on FLEX for this stuff, then we're way -- I mean, that's like the last line of defense in my mind. I thought we were looking at going for prevention, not mitigation, avoiding the mistakes, avoiding the errors, avoiding the malfunctions.

MR. GIBSON: We are but your FLEX, as a good example, is a low probability, high confidence event. I would say you look at your risk profile, there are things that happen often. And it graduates from things that happen much less often.

All risk -- no risk says you won't have any event. There's always some non-zero possibility we'll have something bad happen. And so what people do, for instance, with FLEX, is they say, well, this says something that probably won't happen very often. And when it does happen we just want to have this extra capability out here to mitigate this, again, high consequence and low probability.

So this is about risk, now. There's nothing ever zero and nothing's ever perfect. It's always about how perfect something is or how reliable it is, and what the consequences are.

So this, what we're talking about fits into that risk framework. And the things that you'll see happen through this process drive the likelihood of a problem that's consequential to a low state and a low rate, right. It doesn't absolutely prevent it, but nothing will. You know, when your duty is reliability, there's always you have to recognize that there's even a ten to the minus ten probability. That's still a probability that it could happen.

CHAIR BROWN: Let me comment here for just a second. We're now on Slide 5, and we're now at

9:17. So we had a little delay on the start, but this is part of the lead-in overall topic before we move into each of the other groupings.

I think the conversation and discussion is valid, and both Jose's point and Matt's point are correct. But in my mind we've got to separate stuff a little bit. I mean, you can't deal with -- if you look at your design engineering guide there's 369 pages worth of things to look at and things to consider.

And then you throw in the HAZCADS document and the TAMs document, then there is tons of information and things to do to make that right. By the time you finish that, you've spent about three years and $5 million, and you don't have hardware yet.

So I'm being a little facetious when I say that. There's got to be some balance between this risk total domination of looking at things and what are characteristics of the ways you can design things based on what they do?

For instance, some systems, like a protection system, you put in redundancy. And you use an architecture, but you start with an architecture. And then you work downwards to see if plant architecture, then individual systems, how do they fit into the plant architecture now having protection systems, safeguards, reactivity controls, pump controls for the pumps. For the plants that are out there and want to replace stuff, you look at those individually.

You want to start a pump with software, you know, have a controller that does that? Fine, go do that. It's a single point control. If you have 250,000 lines of code to do that, that's a problem, okay. You ought to have something simple doing that.

So there's a way to look at these things as you go through it intellectually, you know, engineering judgement-wise, but some things you just can't do. You can't test even -- I tried testing 250,000 lines of -- I tried testing 50,000 lines of code with a super computer back in the mid-'80s and early '90s.

It took forever, and we never finished. So we decided we have to look at are architectures going to protect us from a redundancy, diversity independence, deterministic processing all that stuff with watchdog timers, et cetera, for the protection system part. This is a very broad class of equipment. One size fits all, in my mind, just doesn't do it.

But that's my input to the discussion.

That's all. I think we need to move on to the next slide so we can get -- and look at these things individually --

MR. GIBSON: We're there.

CHAIR BROWN: -- as we go.

MR. GIBSON: The next slide, if I can get it to work. Come on, there we go. All right. So this framework that we had a good discussion about so far, it fits in the implementation level. So, you know, a model that you would use, let's say -- and remember that these products are designed to be used worldwide, both for this and then new reactors, not just in the U.S.

And so the way these products are designed, and they're deployed, they would be used to actually do stuff at the implementation level. Now there's going to be policy, there's going to be regulation, company policies, whatever, whatever authorities can decide what policies are, you know, the domains these products are used.

There should be objective criteria that are synthesized from policy. These are the performance based objectives that you want to achieve, and you want people to do it without necessarily telling them in detail how to do it right. They've got to come back to you at some point with some metrics, and some arguments, and such.

So this framework is aligned to fit in the implementation level. And it does support safety case style arguments, you know, claims arguments and evidence in sort of a hierarchy-like way. You know, you're down here doing stuff, you know, you say I did these things, what are my objective criteria that meet these policy objectives?

We've tested these in those scenarios, we think they work well in making an argument that what you've decided at the implementation level matches the objectives of the authorities' policies that are in place in your particular domain.

So you asked us how these are, so they're constantly being updated. You know, we get a review from people using them. They get improved. We would think that the implementation level products would change often. They would evolve. Your performance objectives less often, but they can change based on feedback and experience. And your policy level would be the thing that would change the least often, just sort of a decomposition stack, if you can see that in here.

The other thing to take away from this

particular view is that the objective criteria, the policy, the objective criteria, and all that sort of thing comes to the implementation level as a requirement. So if you have objective criteria, published objective criteria that you should be using, you're going to have to synthesize it into a requirement so that these processes can use that requirement to decide what to do. And that's the way this process gets policy and other exterior regulatory guidance.

I've touched on this slide. You know, we did this research, you know, on SIL. We looked at about 12 different logic solvers that cover this two billion hours. These platform visitors (phonetic) do, in fact, achieve the level of reliability you would expect. To be a SIL 3 it has to be redundant. So you're talking about the reliability of a redundant system to achieve its safety objective. That's published. I mean, you know, I think the NRC owns a copy of that. And if you're interested in looking at it, if you want you can.

Now NEI, they leverage that in NEI 17-06. And that's been endorsed in Reg Guide 1.250. They use SIL certifications for the dependability characteristics and for safety related digital things.

So we have that. And if you've seen NEI 20-07, another NEI effort, they also are using constructs based on that research. So that's just kind of, you know, where it's being used and where it's headed.

We used the idea of SIL certification, a graduated reliability based on systematic controls, and the premise that systematic controls drive reliability for things that are systematic errors, like software errors, design errors, manufacturing errors. Those are systematic errors. And so those systematic controls drive error level. And this research demonstrated that certainly is achievable on a mass scale.

It correlates well with our data from our other OE, worldwide for Korea, France, and China, because we mined their data. You know, they're members of EPRI so, you know, we take some time to get data from them that's not available anywhere else. And you see that CCFs in general are very low. And then any that's, like good digital related CCF, that would be just digital related CCF, is also even more rare. Most of the CCFs are at the application level. Who would have thought?

I'll give you a demonstration of that in just a few minutes of one of the scenarios that we used to test our STPA, HAZCADS methodology. And you'll see how that might be relevant.

What else, that's about what wanted to say with that.

It shows you that same sort of idea. You know, our research tells us that we really have to look at these domains of reliability independently. You know, they're done by different people, at different times, and different places.

Your platforms tend to be, especially if you use industry standard SIL certified platforms, there's a lot of them in the field. There's a lot of data, which is the risk person's bread and butter, there's a lot of data on their performance, right. So you can have some confidence about how reliable they are.

And if you're familiar with the concept of reliability growth where, over time, something becomes more reliable systematically, because you work the bugs out, you know, you've tested it more, you can have reliability growth in both the development phase as well as the operational phase. So the platforms, they benefit from that.

As you go up this pyramid though, at the very top applications could be a one-off. It might be three people in the world that know what that application does and may have been the only three people that ever looked at how it was made. You know, it used to in a little screen there. But that's where the real payoff is. It uses systematic methods to figure out where your application is. And this diagram --

CHAIR BROWN: May I interrupt you for a second?

MR. GIBSON: Sure.

CHAIR BROWN: When I calibrate my SIL platform I look -- what you mean is, like, I'll use an example of a Common Q platform. It's got an operating system that's been employed in safety systems.

MR. GIBSON: Yeah.

CHAIR BROWN: It's got application code that has to be integrated into it.

MR. GIBSON: That's right.

CHAIR BROWN: I'm just trying to put a perspective on these fancy words to make sure everybody understands what you're talking about. I mean, there are some common platforms across the board that get incorporated, just like when you by a PC, there's an operating system within it. You know, the Windows, and then there's all the application stuff you pour in that could completely destroy all its operational capability. I say that with tongue in check, because obviously there's always difficulties that occur.

So that integration effort, when you're just piling stuff in, is very important when you start putting the application codes in.

MR. GIBSON: Yeah.

CHAIR BROWN: I just wanted to, I mean, we can go on from here. I was just trying to put a cap so we could move on to the next slide, just to make sure what we're talking about.

MR. GIBSON: That's true, that's what a platform is. That's the thing that's post your application, you know, that's certainly not one of a kind. There's multiple ones of that. It's not custom made for your application, that sort of thing.

CHAIR BROWN: Yes, okay.

MR. GIBSON: All right. This kind of wraps it up. You know, you really have a reliability that starts with your components. And you have system, and you can have facility level reliability. You know, random failures and systematic errors contribute to that reliability.

And as we look at common cause failures

some of the driving things we're looking at is that we can -- we first have to have a failure or systematic error to have a common cause failure, you know. And generally, when we talk about common cause we're talking about common cause across redundancy expectations of some sort.

There are other definitions, but this includes emergent behavior, things that the system does that nobody knew it would do. So systematic error could be -- the equivalent of that for a human action would be an error of commission. It could do new things that you didn't know it did that aren't appropriate.

So if you want to achieve this systematic random reliability, yeah, so apply systematic controls. And if you drive your reliability to a high level, you drive your reliability to a high level, and it includes your CCF probability. Because, you know, even your hardware today, you don't hear people talk about a systematic reliability or a hardware re-application system. Because when you see all our data in a little while you see a lot of the problems are in the hardware. They're not in the software, all right.

So what we see is, well, you know, you do these things and there's this assumption of its reliability and of its design quality. Well, have you ever been -- ask yourself this question, have you ever been actually tested, if you ever went actually looking for those systematic errors in the design in a formal way?

So these things -- what I'm trying to do is -- this ain't about software, this is about functional reliability, the hardware, and the software, and the people together in one place, and the intersection that you have with those.

Anyway, that's the kind of idea. Your functional reliability, you have to worry about that at the equipment level but also at the life cycle. Because after you make it, and it starts running, then after a time goes by, I mean, you have to kind of get a sense of its current state.

And we understand that pretty good. I mean, we do surveillance tests and all that sort of thing, you know, check on stuff to see if it's broken down. And it also has relevance to a modern approach too.

CHAIR BROWN: Somebody's got a question right now. Vicki?

MEMBER BIER: I just wanted to, again, chime in on the concept of reliability growth. I think reliability growth has obviously served the industry very well in numerous ways. You know, a lot of things you identify a problem, you weed it out. And so our hardware and our systems have gotten better and better over time.

I'm not so sure that that concept applies as well to cyber reliability. Because while we are trying to improve our systems we can also have zero day exploits where something that looked perfectly safe yesterday all of a sudden we realize there is a huge vulnerability that somebody just figured out how to explore it. So I think in cyber it's not necessarily just growth. You can have both ups and downs in the process.

MR. GIBSON: Good comment.

CHAIR BROWN: Is that it, Vicki?

MEMBER BIER: Yeah, that's it. We can move on. Yeah.

CHAIR BROWN: Okay. Thank you.

MR. GIBSON: All right. We're going to get to a quick problem of the system of, you know, systems engineering and how it plays into here.

First off, this is your basic layout of systems engineering, requirements engineering, systems analysis and control, functional analysis, design synthesis.

You will notice that I think the big thing I want you to see here is the iterative nature of this. This is not a waterfall type of thing. You might go through a systems engineering iteration where you will go through it. It's not a might, you will go through it several times during the development of a change or a new system that you're designing, or a new plant you're designing. It requires systems thinking.

And that's really something that we are trying to develop some training for. And it's a new skill, because you have to start thinking in the whole, you have to be looking at the elephant in the whole. You can't be just thinking of a silo, because there is always going to be white space between your silo and somebody else's silo. And that white space could be very damaging.

So systems thinking helps you, even if you're not a super-duper expert in every one of these, if you're a super-duper expert in how things relate to each other, which is what this is about, then you can achieve high levels of system thinking.

Multiple disciplinary, the ability to see relationships, to communicate across disciplines, the ability to understand complexity, well, this is a question for you guys. I know you all have opinions, I'm not worried about you not having one. But what do you think though one of the biggest challenges is to risk informed approaches?

MEMBER SUNSERI: Well, you don't know what you don't know in this area.

MR. GIBSON: Huh?

MEMBER SUNSERI: You don't know what you don't know, you know, what happens on the inside these circuits.

MR. GIBSON: Well, that's fine. Anybody else want to -- what about risk people in here? What's the biggest barrier to risk informing I&C or anything else?

MEMBER REMPE: We're going to let Jose answer that.

MR. GIBSON: I believe you all were --

(Simultaneous speaking)

CHAIR BROWN: I could answer that, but you probably don't want to listen to me anymore.

MEMBER MARCH-LEUBA: I've been chastised before for using too much time and --

CHAIR BROWN: Have at it, if you want to say something.

MEMBER MARCH-LEUBA: So keep moving.

MR. GIBSON: Ha, ha, has. Well, I'll tell you the answer to that question.

CHAIR BROWN: My answer is no.

MR. GIBSON: It's Bullet 4, Bullet 4, ability to communicate across disciplines, all right. I mean, just stay at work. I mean, Mary, you know, of course, I've known Mary and John awhile, but I didn't really know them until we started this project, not like I do today.

In order to risk inform digital, we had to I&C-ify the risk people. And the risk people had to risk-ify the I&C people. And we did these blind studies we talked about. And this process required a risk person and an I&C person to work together as a team. And we --

(Simultaneous speaking.)

MR. GIBSON: And we find that they don't even talk to each other. Huh?

CHAIR BROWN: Communication is great, but let me just ask a question, because I asked you this question, and we said how do you risk inform? What does that mean relative to digital I&C systems?

Let me pick a system, and I think there's one coming up, a governor on a turbine generator set. We developed digital I&C systems for the controllers.

And that embodied both the speed control and the over-speed control. So there was a risk informed decision made in that, how we did it.

But it's a single channel. You get data in, you've got to go in, got to open a valve, close a valve, trip this trip valve, or not trip this trip throttle valve. It's the only decision you have to deal with. You don't put redundancy in, because you can't have two regulators both trying to -- or governors trying to run the speed of the TG set at the same time so you've got a single channel.

So how do you -- well, the first thing we looked at was you don't want to combine the over-speed with the speed control. So you have two separate -- you take the same data, independent sensors come in, independent sensors feeding two different processing units with independent power supplies to make sure you don't have redundant power supplies putting noise in that triggers both of them.

And then you have a single output for the speed control, and the other one's sitting on top of it waiting to do something. So, I mean, that's an architectural design approach for risk informing what you're doing.

MEMBER MARCH-LEUBA: In your process of

thinking, you were implementing a PI.

CHAIR BROWN: Yeah.

MEMBER MARCH-LEUBA: It was then during my service I used some redundancy and diversity.

CHAIR BROWN: Yeah.

MEMBER MARCH-LEUBA: That was my way of asking him to give me the floor. Ha, ha.

(Laughter.)

MR. GIBSON: All right. Well, go ahead.

CHAIR BROWN: Have at it.

MEMBER MARCH-LEUBA: The bullet that is missing in every risk informed or risk thinking is completeness. That's my favorite one. And it is missing always because it's impossible to do. So the reason it is the most important one is because you don't know what you don't know.

And if you didn't think of this failure mechanism, you didn't want it, you're telling me your core limit is in (audio interference) when there is something which is in the (audio interference) that I think of. If you don't consider the high tsunami, Fukushima was a very safe facility. But they didn't consider it.

And it's the issue with, in my opinion, you should assume your system is going to fail. I say, well, if it fails, I have another one that is not like it that will take over. And then assume it's going to fail. Don't try to convince me that you have looked through the 250,000 license holders and found only 50, because some of us have done (audio interference) and know how --

MR. WEGLIAN: That's a great lead in to a little bit later when we get into the actual risk assessment that we do. We assume everything fails. That's our bounding assessment, is that we say everything fails, and we start the risk assessment from there, and say is it safe enough if everything fails, and then at what level do we apply our control methods based on how bad that is if everything fails. So --

MEMBER MARCH-LEUBA: Let's talk about --

MR. WEGLIAN: -- we'll get to that.

(Simultaneous speaking)

MEMBER MARCH-LEUBA: -- example later. But keep in mind completeness. It's against the scientific method to gain the completeness.

MR. GIBSON: All right.

CHAIR BROWN: Also, Jose, interrupted me, which is just fine, okay. Because we looked at now what if those fail. There's are mechanical over-speed trip also, okay. So we looked all the way to a long plan.

There was one other major discussion in there. Everybody wanted the just redundant power supplies, auctioneer them, aid the basic voltage -- the governor in the over-speed trip units. You've got redundant power supplies, they're auctioneered.

(Simultaneous speaking.)

CHAIR BROWN: They're safe. Let me finish. I recommended in that design, you know, you ought not to do that. You ought to have four power supplies, two auctioneered for one, two auctioneered for the other independent thing. Everybody said no. We don't need it. It's too complex. So they put them together.

Three months later we had an operational experience on a submarine where, guess what, they had a -- they rode in parallel on the submarine. They had a hunting on that one machine trying to figure out what it was. One of the trouble shooting methods was to pull out one of the power supplies. They did that it immediately over-sped, and it over-sped past the electronic over-speed controller.

Fortunately there was an operator standing there to trip the trip throttles out. In other words, the noise, whatever, they pulled the wrong power supply, the noise was in there. It compromised both the governor and the over-speed trip device. So they went back and redesigned it an put four or five supplies in.

My point being is your methods for, to me, I don't know how -- but it was all software based. And we go through -- and this is not a critical comment, I looked at your HAZCADS in the other documents. People just programmed it, and we looked at the number of lines, and we did the best we could in terms of doing software checks. But then it ran, and it's been working beautifully now for ten years.

There's a lot of different factors in here. How much analysis do you do, and how much judgement do you do to get out? That's a risk decision right there. So I just think you have to throw in experience and understanding the systems you're dealing with.

When you have a safety system where you can run four different channels, that's another layer of architecture that reduces your risk to problems. And if you'd run it asynchronously, you have separate detectors feeding each channel, all that stuff falls into trying to minimize the risk of a common cause failure, even in the software which is, I mean, it -- no. I just wanted to give an example real world of some of this more esoteric --

MEMBER KIRCHNER: If I were Matt, I would have answered you, well, this is an iterative process. And you go through the loop once, and then you put experience in that way. And then you go through the loop in the (audio interference), and that's what I would have said.

CHAIR BROWN: Why don't we --

MEMBER KIRCHNER: -- so we could go on to the next --

MR. GIBSON: Thank you, that completes my slide.

CHAIR BROWN: Go on to the next slide.

MR. GIBSON: The DEG that we talked about earlier, the system engineering process, you know, what Walt was talking about, and that is part of the reliability growth concept that gets back to what you're talking about, as in you doing the iterative approach, you converge each time you look through here.

And this might sound like a lot of work. When we benchmarked, other people could actually do this faster than what we're doing in the nuclear industry, by a lot. Because when you first start this thing, you only get to deal with what you know. And each time you loop through it, you know more. And each time you know more, you use that information to gradually converge and become more complete.

And so, you know, this is sort of like the systems engineering loop based on I&C 15288. There's topical guidance in the DEG about different things. There's most topics like cyber, plan integration, hazard analysis, testing, V&V, are all in the DEG. And they're all used in each one of these loops.

You end up getting some architecture views once you do your function analysis, and allocation, and your relationship sets, or if you're getting V&V and you transition to the O&M phase, the RO&M phase of activity in the DEG as well. Somebody asked, and we mentioned earlier about the feedback, I think. You know, somebody made a comment about the cyber landscape changes. This process incorporates that.

There's periodic feedback that you can measure changes in the decisions you made. So you do a bunch of iterations, and then you do the bigger loop sitting out here where you iterate back. Right now, you know, no cyber professional out there would not do a periodic review of the threat landscape or the threat capability. That's built into these processes too.

To trigger this process again, if you see a delta -- but that'll go for reliability as well. Let's say you operate this thing for a while. And all of a sudden you start getting failures. That's going to trigger you to look back at this using these same tools and find out what's going on, right. Then you restore your reliability to the target reliability that you had when you started.

All right. So --

CHAIR BROWN: Before you go on, I meant to make an announcement earlier. Dennis Bley, one of our consultants, has also joined the meeting earlier.

MR. GIBSON: Very good.

CHAIR BROWN: I didn't get him earlier, so I apologize for that.

MR. GIBSON: Anyway, just to recap this, you know, there's seven phases in this idea, beginning with the neutral scope and all the way through to the O&M phase. There's nine topical areas. And again, I just, you know, I summarized those earlier. You can see a lot of them here. But this is comprehensive in that view.

This is an example, all right, because the

DEG is designed for you to use in day to day work. So it has to be scalable. And so what we do is, in your V model which really ends up being a process decomposition stat, we allow people -- let's say in this case you put it in a digital recorder.

And this recorder could be safety related. I mean, power plants have safety related recorders. You know, they're displaying something that's been adjudged to have a high safety significance, or a moderate safety significance.

So as you work yourself through this, you say, well, okay, everything above Level B in this decomposition I already know. I have bounding technical requirements that's, you know, this is not a new function, right, it's always been there.

And so the person doing the new design or the design changes is not going to have to deal with the things in Level B or in the context, I would say, in Level B and E.

And we used this systems engineering process to figure some stuff out. Your bounding technical requirements you already got. But now you've got to decide on your parameter values, you got to decide -- you got to go do some bench evaluations, you know, so that's your design synthesis. You get some hands on there and figure out what's going on. You refine our parameter values with a feedback loop on it.

So you converge in this recorder modification or change-out to the point where you can specify its configuration and any other things you might want to put on it. And then you're able to go to configure and install.

Now this is probably below the level that you guys might normally think about. But I'm just going to point out the DEG is for the least complex mod in the facility all the way to the most complex, including building (audio interference) design of it.

And this also demonstrates the system engineering concept where you can do this loop anywhere in the stack, at the top, in the middle, at the bottom. You can do it at the consensual level, you can do it at the detail design level. So these iterations are -- ideal iterations are very important.

We talked already some about this. And what you'll see is a heat map from one of our reports. This is probably going to be the 4997 report where we evaluated the different hazard analysis methodologies, strengths and weaknesses. STPA scored pretty good, but there are some things it didn't do.

But then we said what combination of hazard analysis methodology would be the most effective? And so it turns out systems theoretic process analysis and fault tree analysis would be highly effective when combined in being a hazard and risk analysis, a comprehensive one.

So, you know, our colleagues at Sandia Laboratories worked with us on this particular phase of the project. You know, you can find this stuff out in some of their labs there. And this was a good insight to combine it, so we did.

So HAZCADS, again, is our core hazard analysis process with the bedrock analysis and theoretic process analysis. I gave you some -- you know, we sent you some pre-material. Well, I won't try to teach you all the ins and outs of STPA, but if you want to ask questions, that's great. We can try to answer those. Here are the published handbooks. It's an open source process, there's nothing secret about it.

But in this architecture we do Steps 1 through 3 of HAZCADs, of STPA, I mean, in HAZCADS. We identify stakeholder losses. We identify hazards, we identify unsafe or undesired control legs. The fourth step, and plus some more stuff, we do what we call the downstream processes where we take the loss scenarios and we combine them with reliability insights. And then we use our liability, our cyber, our human factors, and EMC downstream processes.

Now if we move back to I&C 61508 it says you have to give -- consideration shall be given to the elimination or reduction of hazards which is fine if you go through a risk process. I mean, this is how 61508 and 61511, it's how OSHA works. If you have a risk reduction, that's what controls mean. When you say controls, you're talking about risk reduction. That's what always that means.

Well, at some point if you cannot reduce your risk with a, let's use 61508 and 61511 concepts, if you go through and say you have a highly risky process, you may be required to go back and redesign your process to make it less risky if you're going to say this can't be mitigated with a protection system.

This has to be, you know, you'll say you have to make it inherently less risky so that you can get that last mile with your protection or your control system. So that's why 61508 had you go and try to eliminate and reduce your hazards before you try to, you know, add a protection system to it.

Now for this, we created and made up one out of two RPS things, you know, we could use it for a prop to work with. And what you'll see is, you know, what would look like a conventional block diagram on the left and how an STP analysis would look on the right.

And what you'll see is a STPA is an investigatory or diagnostic process. It gets back to the concept about are you complete or not. Again, each iteration, you're going to go through, and you're going to go through the STPA process, we're going to ask questions about, you know, what if questions. How will this happen? What would be the drivers for that?

And the structured way you see on the right is called a control structure. And that's an output of STPA. Humans and equipment are all evaluated, all three at the same time with this. This is a control base, a control structure. It's a functional control structure.

And then when we add the causal factors which you use the output of these, you know, the first three steps, then you have a complete pathway between what causes the problem and what the consequences of the problem could be. And it gives you a real good insight on how to address it from a control structure point of view.

MEMBER KIRCHNER: I had just a quick question. In application, at least to the current fleet, almost all of the, I think everyone in the current fleet has some level of PRA. And that accounts for the details of how that plant was built out and modified over time. Or at least I hope they do.

How do you reconcile -- it would seem to me that the first thing you would use in your PRA, you look at vulnerabilities and then get into the weeds of, say, your digital I&C functions, piece of equipment, or platform, or something. Is that what actually happens or --

MR. GIBSON: Yes. Let's talk about that. Then John will really be down, so I'm not going to talk a lot, because I don't short circuit that.

But your PRA is a model, right. So it's one of the models, and we'll talk about it in another slide. It's one of seven models we use in this process. But like you saw in the previous slide when we evaluated the fitness of PRA to finding all the problems, not a probability of the problems but the actual problems that could happen, we see it has shortcomings. So by adding STPA to this, which we do, we combine the two together, we go out and look for hazards.

And HAZCADS stands for hazards and consequence analysis for digital systems. So we've positioned HAZCADS in the spot, or STPA, in that spot between the control systems and the equipment it controls, all right. So the equipment it controls is certainly going to most likely be in your PRA if there's risk in it.

But what you don't have is the contribution from a detailed hazard contribution of the control system because, you know, a lot of PRAs, I think, some of that's just truncated today. They just put a number in there, right, because it's a black box.

So to just improve that situation, then they've got new stuff that allows you to integrate hazards analysis insights into your, what I'll call traditionally doing risk. And John will go into that in some detail here in just a little while.

So we used, this is a test scenario. It's one of the test scenarios that we use to test the processes that we have, you go to STPA and HAZCADS. So the set up here is, the event is you have a turbine control system locks a cooling detection, right. So the old system, the one that's sitting there, has pressure transmitters going into different logic areas of your turbine control system.

And you can see on the diagram, if you have your low pressure, low flow, and high temp, many of those kinds of things that pass the set point, you're going to shut the plant down. You're going to have a turbine trip and probably a reactor trip.

That was a single point vulnerability, because any of those flow loop transmitters or any of those different process transmitters cause a turbine trip. And plus, the turbine system itself was non-redundant, right, so if it failed (audio interference).

MEMBER KIRCHNER: So this is for the main generator?

MR. GIBSON: Yes. Yeah, the turbine. Yes.

MEMBER KIRCHNER: The actual diagram you had was actually used? You mean you would take out 1,000 megawatts because you didn't put two sensors in?

MR. GIBSON: Absolutely. All of the plants are like that. And they're kind of reasonably reliable. You know, when I started working in the industry in 1982 the plant I worked at, you know, it would trip every quarter on some BS like this. I mean, you know, let's be real.

MEMBER KIRCHNER: That's within the whole INPO model that the liability and safety are --

MR. GIBSON: We're talking the same thing, you're going to push the reliability up. And that's a good segue, because this is really the reliability model.

MEMBER KIRCHNER: All right.

MR. GIBSON: That's what was the purpose of it, right, improve the reliability and remove simple vulnerability. And this is the proposed new system logic. So now you had three different transmitters for each of these parameters. And there's five redundant, you know, for pressure flow and temperature.

And then you had fault detecting voting for those three inputs. And all that's not on this diagram, that's actually on a tri-modular SIL certified PLC. So we could have internal failures to the PLC and would be extremely reliable, as we showed in the SIL certification, at a software and a hardware level, right. We're cooking with gas.

So we wanted, you know, to do your controller routine, automatically remove fault in instruments, okay. So there again, we're dealing with the single point vulnerability. But this logic that you see in here was intended to identify the fault in instrument by measuring the output. It was outside of calibrated range, et cetera, et cetera. There you go. We know when we have bad instruments, miscalibrated instruments, it gets bypassed. And so the voting logic can use the remaining instruments.

And the next to the last bullet tells you that even if two instruments are faulted that the logic uses the remaining valid instruments. If all three instruments are faulted, the logic is designed to send a shutdown signal. Hey, something sounds reasonable, on the surface of it, I suppose. You know, because if you've lost all your input you want to, okay, I don't know what's going on.

Well, guess what, this thing was calibrated, the flow transmitter, 0600 gallons a minute. The high out of range was 612 gallons per minute for your flow, the flow. The normal stat of cooling flow was approximately 550 gallons a minute. And one pump in service, which is what it usually is, is your redundant pumps. They're not running at the same time, or in theory they're not.

Two standard cooling water pumps exists, but there you go, only one, again, at the time.

They're routinely swapped though. Because you run one awhile then you run the other awhile. So you get even wear on the pumps.

But when you swap the pumps the in service pump remains on momentarily while the outer service pump is started. And when that happens the flow goes above 612 gallons per minute. And guess what, you've got a trip. So they did this VIG (phonetic) mod to reduce the single point vulnerability.

They put a lot of new stuff that was hideously reliable at that platform level. But they didn't catch this. They didn't catch, through reliability and hazard analysis, that there might be a possibility that, that being a flow case, that all the flow, the flow could be higher.

And then what they didn't ask themselves, why do I care if the flow is high. Well, high flow is not a bad thing. Why is there even a trip on high flow? So if it goes off scale high, why am I worried about that, especially if all three of them did it? Well, if you talk about it you say what's the likelihood of all three of the transmitters failing simultaneously? We just put in three, so I wouldn't have that problem, right.

So we used this as one of our diagnostic scenarios to test people to see if they could find a problem with this design. And they did using the HAZCADS and STPA methods. It was pretty compelling watching that happen. Because they started going through that iterative what if, what if.

And, Jose, your thing about completeness, and we'll talk about that a little more in a couple of minutes, this process does not achieve absolute completeness. But the likelihood that you miss something goes down dramatically. But your completer, you're more complete than you would have been otherwise, right, in a traditional methodology. That's the idea of it.

MEMBER MARCH-LEUBA: So it forces you to be a structure undedicated, and therefore you cover more. It's never bad.

MEMBER KIRCHNER: Yeah. When you designed this though, did you go back to get who was on your design team? Did they have the experience to know that we routinely start up one of these other pumps and --

MR. GIBSON: Well, you know, that's a good question. Because if you think back to the --

MEMBER KIRCHNER: This is one of the fundamental problems with PIRTS for PRAs, you put all the like-minded people together, and you don't necessarily get that -- I shouldn't say that but (audio interference) came out. The danger is that you put together a lot of experts in the same area. And you don't get that diversity of views so that you don't work completely --

(Simultaneous speaking.)

MR. GIBSON: -- right there. The STPA process and systems engineering in general is multidiscipline. And, you know, I don't have a slide to talk about this just for brevity, but it really requires -- this kind of stuff requires a big culture change. Because now it's team engineered.

When we did these tests you had operations people, I&C people, and risk people on the team doing the analysis of that to find that problem. And that's a good suggestion.

MEMBER MARCH-LEUBA: And was that before or after the bullet happened?

MR. GIBSON: That was after, that was for our tests.

MEMBER MARCH-LEUBA: I've never seen a benchmark that fails when you know all the answers.

MR. GIBSON: Right. Well, they didn't know what the answer was. But there were kept blind.

All these tests were blind tests.

MEMBER MARCH-LEUBA: This is an open meeting, right? I'm not meeting everybody that comes in. It is fully -- we cannot meet everybody, the public --

CHAIR BROWN: It's an open meeting.

MR. GIBSON: It's an open meeting. Yeah, there are no secrets here.

So I wanted to share with you some preliminary OE data that we've collected so far. We do annual OE reports. So this is getting ready to publish our 2023 OE report.

You're seeing in this, you know, just some anecdotal stuff. And this particular one, out of 1,200 OE records, and this particular data set is the NRC website, INPO's website, and some input from our Chinese members. Because they were able to give us a lot of data from their plants. They have a lot of digital plants, and so they gave us some of their, you know, basically their CR reports, their reviews.

We harvested those, this is what you see from the data. These are a fair indicators by category out of those 1,200 to give you a feel for, you know, where your big issues are. And this is for I&C now.

MEMBER KIRCHNER: And you say hardware, that's why I'm asking.

MR. GIBSON: This is I&C. This is I&C hardware.

MEMBER KIRCHNER: Hardware. How do you define the hardware, I mean, if a relay fails that's a piece of hardware.

MR. GIBSON: Yes. If it fails --

(Simultaneous speaking.)

MR. GIBSON: -- it fails in any of its physical attributes.

MEMBER KIRCHNER: Whatever, it doesn't open when you want it to, or it doesn't close when you want it too.

MR. GIBSON: Yeah.

MEMBER KIRCHNER: Et cetera, et cetera. Okay. That's fairly straight forward, it's a piece of hardware.

If a circuit card is pulled out and replaced with a new one, it now makes the system work, right? You've got 233 components on that card. They may just throw the card away in today's world. They may try to repair the card in the old days. And by the time you finish trouble shooting, you might replace three, four, or five individual parts. And then you don't know exactly --

MR. GIBSON: No, they're not inflated that way. This is at a functional replacement unit.

MEMBER KIRCHNER: The function --

(Simultaneous speaking.)

MEMBER KIRCHNER: Yeah, the circuit card level type or the relay brief. That's why I used that example. Okay.

MR. GIBSON: Yeah.

MEMBER KIRCHNER: That's good. So that's good --

(Simultaneous speaking.)

MEMBER KIRCHNER: -- reliable data.

MR. GIBSON: LRU, line replacement unit level --

MEMBER KIRCHNER: Yeah. That's good, thank you. You answered my question. We can go on to the next slide.

MR. GIBSON: So this is just some stuff, you know, this is the things, the software. We break it down by what we should, you know, this is both how it was written up and also our secondary investigation. Because we were able to talk to some of these people too, you know, with some of our members.

So 56 percent were application level problems in the software. And configuration parameters are also big here. You know, we parsed those differently, because we considered application level software being the design, you know, maybe it was a function block or some high level code in there. That would be the application.

Configuration parameters are also usually application level parameters. Well, not always, but they are just things, you know, parameters you set in the software to do what it does, firmware, 14 percent, operating system software, two percent. You see out there where the problems are.

And it really jives up with our other -- we try to double check all our OEs when we connected, because it just doesn't make sense. Because for the job, what kind of trend do we see. And it really matches with our reliability pyramid, or pretty good.

We also search for software, CCFs of all sorts, you know. Because that's a -- and we define the CCF as a loss of redundancy in our data. So if you have two redundant things that were supposed to, you know, keep a function going and they both fail, then that would be a CCF in the definition for this data. And so you see, you know, our hardware CCFs are running about twice the software CCFs.

And you see how it's broke down. Manufacturer software, they fit five. Broadcast storms, we consider that a -- I'm going to call it failure on the network. Over-range transmitters, which we just saw an example of that, that's a software CCF, if you want to call it that.

We are kind of, as we go forward, trying to advocate for functional, view that functionally. Because had that system been implemented in hardware, you still could have the same CCF, right. It wouldn't have mattered that it happened to be a software basis. It was a design. And then incorrect computer parameters are one of those are also redundant.

MR. GIBSON: We're good?

CHAIR BROWN: I would have determined whether anybody needs a break or are we satisfied with proceeding? Break? Did I hear you say that, Matt?

MEMBER MARCH-LEUBA: How are we doing on the presentation? It's already 10 o'clock.

CHAIR BROWN: We are 25 slides through 63. And we've got one hour. We're supposed to go to 12:30, is our cutoff. That's what the agenda says. So we do have to kind of keep things moving.

MEMBER MARCH-LEUBA: Let's have a break,

but let's ask our EPRI friends to talk a little faster.

CHAIR BROWN: Yeah. Ha, ha, ha.

MR. GIBSON: You know you can't win, you know, Charlie gives these instructions to practice. You have to speak slow.

(Simultaneous speaking.)

PARTICIPANT: Did he say this?

MR. GIBSON: He did.

MEMBER REMPE: You're correct, he said that. But we'd like to revise that.

(Laughter.)

(Simultaneous speaking.)

MR. GIBSON: I have my instructions.

MEMBER REMPE: We're learning, okay.

MR. GIBSON: I'm almost done talking.

CHAIR BROWN: I'm declaring a break, we will return here at 10:25.

(Whereupon, the above-entitled matter went off the record at 10:13 a.m. and resumed at 10:25 a.m.)

CHAIR BROWN: We're going to resume the meeting now. We are now unrecessed, and Matt, you're back on, or whoever.

MR. GIBSON: Thank you, Charlie. So,

we've had some good discussion. We're going to look at the digital systems engineering framework components. We're not going to do a deep dive on these. You have what we handed out earlier, and you have the materials, these are all week long courses if you want to really understand how they work. Look at that thing, I'm finding out --- go back.

I'm using a little wheel from now on. There we go. So, this is just an I chart, we're not going to talk about it much other than it's in your slide deck. And it is an enumeration of the pieces of the framework. And so, these are all --- the DEG is at the top, and there's all those things that make up the pieces of it that we can use in whole or in part.

This is a diagram that shows you the data flow, the flow between these. Your DEG is your anchor, you can see the HAZCADS is in green, that's where we do our hazard analysis, the DEG calls for a hazard analysis. Systems engineering calls for a hazard analysis, so HAZCADS is one of those. For simpler mods, or changes, or designs you can substitute FMEAs there for that instead, but it wouldn't come out into these other processes.

DRAM is your liability, basically what I would call your hardware and software liability, your

TAM, cyber security assessment methodology takes care of the cyber stuff. HFAM, human factors, Mary will cover that a little bit more in a minute, and EMCAM. Now, it should be noted, you'll see in this slide there's I&C standards scattered out through here.

And DEG, HAZCADS, and DRAM in particular implement a process hazard analysis frame work, or implementation I guess you would say, and a layer of protection analysis as it's described in IC61511. So, there we go, that's the framework itself. That's the pieces, how it's laid out, and you see the enumeration. Now, we're going to do a deep dive today on HAZCADS and HFAM, just because we don't have an unlimited amount of time.

But I do want to make a statement here about models. All right, so our research really has told us, not only in this research, but in the other research we do on alternate I&C architectures, which we're not covering today, but we have done modeling analysis in that too. You've heard the old saying that all models are wrong, but some are useless --- useful.

Thank you, John, I appreciate that, that does change the context of that statement a lot. The whole statement of that though, is what that person, Box I think the name of the guy was that said that, what he's really trying to say is all models are wrong, but they can be useful if they answer a question. They're not going to answer all questions, but to answer a question accurately, or reasonably accurately, then they can be useful.

And what you see here is a list of the seven models that we use in the frame work. Systems engineering, fault freeze, STPA, reliability analysis, exploit sequences, which is the modeling methodology for the TAM, and the reliability analysis, which we use in DRAM. And so, those models taken together try to answer the questions that need to be answered in order to get good designs done, and safe designs done.

And to deal with the questions we have in risk informing performance base. You'll see here how we connect the model to the product. And if you look at the questions you need to answer for what could go wrong, what are the consequences, how likely is something to go wrong, what performance is needed, those are the key elements of risk informed performance based.

And the framework elements attempt to answer those questions. And that's always a work in progress, but it's certainly well formed at this stage.

MEMBER REMPE: I may miss when you get to how you put it in the PRA, do you include uncertainty in the answers to those questions?

MR. GIBSON: Of course, of course.

MEMBER REMPE: That's good, just checking.

MR. GIBSON: Of course. Although exactly how to do that is a subject of some research we're doing.

MEMBER REMPE: I think it would make it more difficult, but I'll miss that part, so you can go by.

MR. GIBSON: Okay, that means you can get four or five minutes, Mary. But anyhow, one of the key models we use that you might not have seen before is relationship sets. And you can see the idea of them, there are four --- we modeled the whole system, we describe the system as system elements. You can view that construct throughout, because we do configuration management at the system element level.

We do different characteristics, and functional composition, decomposition at the system level. Hardware, software, human, and equipment under control are the four founding system elements. Everything should be able to be mapped to those, and included in those. And there are five relationship sets. Functional ones, connectivity ones, spatial ones, programmatic, and acquisition.

Again, we're not going to go into a super amount of detail other than to say you can see from this Venn diagram a little bit how the relationship sets work. Because each relationship set type, meaning your relationship sets in a design, but there will be one of these five types, and they'll have a bounding criteria developed for each one. That bounding criteria determines what system elements go in it.

What this lets you do is evaluate, and visualize dependencies, degrees of independence, and all these sorts of architectural characteristics. And you can evaluate with relationship sets, so it becomes an architectural view. Maybe not the only one, but a valuable one that allows you to understand when things are connected in some way, either through their functional connection, a data and control flow interconnection.

The fact that they're in the same cabin, or under the same roof, or they're spatially in the same spot, they are in the same calibration program, they're in the same cyber security password change program, whatever they're in that they share that, and you can see that relationship here. And acquisition where you can tell whether these system elements have common acquisition characteristics coming from the same vendor, or using the same products.

They have these different kinds of things in common relationship through the acquisition process. That's relationship sets.

MEMBER KIRCHNER: Just, could you elaborate on equipment under control, that could be safety related components, why put a fourth category there?

MR. GIBSON: Well, because a control system, remember the context of HAZCADS in the digital engineering framework are control and monitoring systems. So, those things in and of themselves don't do anything, they're a paperweight. So, they have to control something. Fluid, mechanical, electrical, they have to do something. That phrase equipment under control is what the I%C standards use in that context to describe the things you're controlling.

Now, one concept there is that your control system inherits the risk importance of the things you're controlling. Because obviously if you're opening and closing a valve, you're starting a pump, whatever that is, whatever the risk importance of that component under control is, your control and monitoring system inherits that risk, it has to be commensurate with that risk of that component.

MEMBER KIRCHNER: I get that part, I'm just trying to understand your universe that you're creating, and whether it adds a degree of complexity. Why wouldn't you --- equipment under control would be a special subset of hardware, or perhaps software.

MR. GIBSON: Well, I guess the best way to describe that is because the context is different. So, what this lets me do, is because equipment under control is a different context in the plan, it's the thing that makes something happen. So, I can look at these relationship sets, and see all the digital human things that are associated with that equipment under control.

And that helps me --- like say equipment under control will typically appear in your PRAs under basic events. Sometimes that's aggregated, but let's say you have a pump or a valve, and you have that in your PRA. Well, now I can tell if that equipment under control is here, if it's populated in any of these relationship sets, maybe even with another piece of equipment under control, now I can see a dependency that would have escaped me earlier.

The second reason we do that is because the SCPA process is modeled that way. You always talk about the process that you're controlling, and then you draw up control structures. And this lets us allocate the process under control to equipment.

MEMBER KIRCHNER: How do we fit that in the world of NRC regulations where you have safety related, you have things that are under tech spec, and so on. So, it ---

MR. GIBSON: Well, remember this is a technical process. So, if there's, let's say you have something that's safety related. Well, remember, even today when you have 50.69, there are things that are more risk significant, and some things are less risk significant.

MEMBER KIRCHNER: Yeah --

(Simultaneous speaking)

MR. GIBSON: Right. So, this kind of all works with that. But you don't really care at this point. What this is, is how are these things related to each other? So, let's say you have a piece of equipment that happens to be of some categorization, and it would show up here as equipment under control. And that would help you understand the criticality of the I&C that's actually attached to that thing, and trying to do something with it.

MEMBER KIRCHNER: What about the equipment that isn't under control. Is that caught up in the hardware, or for example we've seen debates over --- especially with the newer designs coming in, what makes the DRAM list, and what doesn't. So, what is under control, maybe not in the same way you use this definition, but what requires special attention, etcetera, etcetera, and what doesn't.

I'm just trying to understand (simultaneous speaking) has been identified in the I&C universe that has special controls that ---

MR. GIBSON: This is anything that the scope of this evaluation, relationship says based on what you're trying to do, right, and what's the system, the subsystem of your design, or the plant if you use at the whole plant level. You have multiple relationship sets, really powerful tool. So, let's say you're doing an advanced reactor, and it's using alien technology, nobody's ever seen this before.

You use this same process, right? Because at some point the control and monitoring function has to control and monitor something. And the thing it controls and monitors are these equipment under control, and that's what actually makes the world turn. They're the things that pump the water, the steam, make the temperature go up and down, do whatever. The actuator, the prime mover if you want to use that word for it.

MEMBER KIRCHNER: I'm just struggling with what's in the universe of equipment under control.

CHAIR BROWN: Yeah, Dennis, speak up, I see you were queued, so go ahead.

DR. BLEY: Yeah, I just wanted to sneak in. I'm trying to -- maybe I can pull Walt and Matt a little bit together. If we go to your forces through elements map, do you intend those to be orthogonal or, and I don't know, for function under control I think it would make it clearer. But if it's a pump that's under control, that's also hardware.

Does it fit in both categories? That's sort of what Walt's getting at I think in part ---

MR. GIBSON: It does not fit in both categories. The hardware is the control monitoring hardware, not the equipment it is controlling. And we reduce it to this --- this might look like a little bit of an abstraction, these elements, when you do these are the actual tag, and make, model, number ID that are being affected.

This is not an abstraction. That's one of our problems that we're curing with this, is if you do a lot of high level stuff, even PRAs for that matter, and you truncate, and you combine functions, all of a sudden you've got a basic event that might have a lot of stuff underneath it, right? What we have to do is connect that to the real equipment plant, the real hardware elements, software elements, the human actions that go into it.

Because otherwise it's hard to make our hazard analysis turn outward, right? We don't know what we actually have to do.

DR. BLEY: You throw a little bit of jargon around, I think I heard you say that in your four elements, the hardware that's listed there is hardware that controls other things.

MR. GIBSON: Yes, it's part of the control system, in this case the digital control system.

DR. BLEY: Okay. Well, it's probably clear in the documents, it's not clear in the view graph, I think is where some of these questions are coming from. If we go over to your diagram that I suppose is helping to give us clarity, I have to admit it doesn't give me clarity. And this is a cartoon, or this is something that you think is a real representation?

And then how do you garner useful information out of such a, as you called it, a Venn diagram?

MR. GIBSON: Well, the Venn diagram is mainly just one way you can view this. And what happens is, is when you do your relationship set analysis, there's a worksheet in these processes where you create a relationship set. You give it names, you give it a taxonomy, you develop the bounding criteria, which are a structured narrative about what things go in it, what things don't.

It then has to be populated with real component IDs about what you're dealing with. And so, that's what it really looks like. And if you visualize it, it's going to look a lot like this. Let's say you had a complete design, and you had relationship sets, you could create a visualization that had all that detail on it, which would be more detailed than this. This is just trying to demonstrate the concept of it more than anything else.

DR. BLEY: I think it would help --- well, it would help me, and it might help members of the committee who are with you here, to explain --- can you keep that other slide up? To explain the value of these five relationship types. Functional I kind of get, they're providing the safety, or other functions in the plant. Spatial, I'm guessing you're talking about where the equipment is actually located.

Which would (simultaneous speaking) me if I were doing some kind of event analysis that depends on spatial proximity. Programmatic, I suppose would help me if I'm looking at ways to change the program to improve things, or do you have other things in mind there?

MR. GIBSON: I'll try to hit those quickly. Functional, again, is what it does. So, if you have a function, this would allow you to associate system elements to a function, enumerate them in there, and if you have another function, let's say it was a diverse function.

DR. BLEY: I'm sorry, stay on that first one. So, you kind of have an arbitrary number, 15 functional relationship sets, and each one of those would tie together the things that are associated with that one function, true?

MR. GIBSON: Well, typically what we're trying to say is if you had a function (audio interference) so say you had two functions. Let's say you had a primary function, and a defense in depth function, or a diverse function. Then you would be able to see once you populate the system elements if there was any dependencies, or any lack of independence between those two.

You would see the sharedness of them, the connectivity of them. Or if they were in the same spot, like say if you had them both in the same cabinet, then you're going to share hazards. These allow our hazards to be correlated to our architecture is what they do at the end of the day. Because we use these same ones in cyber security too by the way.

Because when you evaluate a cyber threat, or a dependency, you use these same sort of relationship sets to know what control measures you have to put in place to protect, detect, or respond to that particular threat.

DR. BLEY: Okay, I'm sort of getting it. Now, let's jump to acquisition. And the only thing that comes to mind there would be if you're looking for maybe common cause effects because you're coming through the same acquisition source, or what are you really looking for with the acquisition sets?

MR. GIBSON: All right, so remember, this is used for everything, not just trying to proof a particular function. So, an acquisition relationship set will let you immediately understand let's say you had a certain brand of instrument transmitter in your plant, and you got them all from the same vendor. These relationship sets will immediately allow you to visualize the dependency that you have on that particular vendor, and that particular type of transmitter across multiple systems.

DR. BLEY: Okay, that's pretty much what I said but in different words. I'm done with this one, and thanks for your help.

MR. GIBSON: Thank you.

MR. WEGLIAN: If I could weigh in now, something that Walter asked about that I want to make sure is clear. So, we're designing a digital I&C system, so hardware and software are in that context. They're the hardware and software of the digital I&C system. The equipment under control is what it's affecting, pumps, valves, breakers, things like that.

You asked about other equipment, and I'm going to give an example, a new design reactor has liquid core, and has a freeze plug. And it's a passive system that if it loses power it's going to melt, and it's going to go somewhere else. That's not controlled by the digital I&C system, so that would not be equipment under control of the digital I&C

system because there's no feedback into that system.

So, that would not be part of this. Now, if it's part of the design it will be incorporated in the PRA for its function, and its probability of failure, maybe it plugs, or something like that. So, it'll be part of the risk assessment, but would not be any of the elements of this part because the digital I&C system does not have an effect on that component?

MEMBER KIRCHNER: Just one last thing then. On spatial what I was thinking was things that were cohabiting in the same cabinets, or I was thinking under the same zone of influence whether it be a fire, or a blow down or ---

MR. WEGLIAN: Equipment qualification, that kind of thing.

MR. GIBSON: It's also your HVAC, your support systems have a spatial --- air conditioning, environmental conditioning, it's all spatially oriented, right? So, you want to make sure that you can track dependencies. We've looked at this pretty hard, and we think this is bound (audio interference) hard to miss a dependence if you go through this relationship set process.

Anyway, this is a much bigger picture of it. Because you can see where we come down to DEG, we create relationship set as part of the architecture development. There's several steps in there, interface analysis, functional allocation, we do relationship set development in functional analysis. The key thing there is when we do hazard analysis, you will see where we put the dots.

When we do STPA we have to connect the results of the STPA analysis to some actual physical something, software, hardware, something, or person. So, that we understand what the cause of factors could be, and also what sort of control measures we have to apply to it, otherwise we'll lose our way here. And then John talked about this a little bit, but when we do HAZCADS it's possible that when we have, for instance, an unsafe control action, it looks independent when we look at it at the level we're doing it.

You could have a dependence in the background like spatial dependency, or acquisition dependency that not obviously comes out. So, in order to properly do the risk we use relationship sets to group the UCAs together where they have dependencies with each other. And then we can put it in a PRA, do bounding analysis on it, and that kind of thing without worrying what didn't we think of.

What dependency is working out there that could cause a problem that we didn't think could be there? You pull it down though, and this is really an important thing to take away here. We create loss scenarios. That's the complete thing that happens because an event that would occur. We apply control methods, or we identify the control methods we're going to use.

That gets allocated back to these system elements, because you've got the control, whatever it is has to apply to something real, software, hardware, person, equipment under control. And that gets pushed back to the requirements development phase. And this loop is iterative, and drives completeness of your design, something we don't do today very well.

This process drives your design to be complete after you've looped through this a bit. Let me see if I can --- there we go, it's on automatic pilot. This is a simplified version of this thing. This is the conceptual phase in the work flow. The DEG does the design, it does the whole design, the initial design, it just stays the conceptual phase, maybe the initial conceptual phase.

And then we push the output of that into the HAZCADS. And it does, it evaluates for hazards, and the criticality of those hazards, and downstream processes like DRAM and all these others. They work on some topic specific issues, and we bring those control methods in the requirements back to the DEG for another loop, because now the design gets updated.

Every time you go through this the design gets updated, that's the idea of it. So, you do this a few times, and then your design is arguably a high reliability design, statistically a highly, highly reliable design. The likelihood of you having a problem is going to be low. One of the things you asked about as far as the industry on this, I'm not sure how familiar you are with a lot of this.

The EB1706, if you search for it online you can download it, it's a bulletin document. That's the efficiency bulletin that implements the standard design process. Industry, that's a read, mandatory bulletin by the C&Os in the nuclear industry in the U.S. And so, we have the standard design process, and NISP-EN-04 is the digital system addendum to that. And then the DEG is called by the NISP as the way to do those activities in the NISP.

So, the industry has adopted the DEG, or is in the process of it, I mean it's a long term, multi-year thing. But they'll be doing that, they've already all got training. We've trained about 600 industry folk on that, and about 50 or so NRC folk on that.

DR. SCHULTZ: Matt, how are you defining the industry here? It sounded like when you mentioned the C&Os that you were talking about the existing nuclear, and I'm concerned about the emerging nuclear industry. The new plants in advanced design who use this.

MR. GIBSON: That's true. We define the industry in this as the extant plants. The people that own plants, license these today, your typical utilities that own plants. They're the ones who are the members of the insight community who made this proclamation everybody would do it, and that's essentially all of the utilities in the United States.

DR. SCHULTZ: But you see the need for this to be grasped and utilized by the advanced plant designers who are going to need this technology capability.

MR. GIBSON: We do. Those advanced plant designers, most of them are members of EPRI, they get to see this stuff too, and they're in various stages of trying to figure out how to get their hands around it. Part of it is the dilute between what they do to satisfy regulations, and what they have to do for a good design, which hopefully are the same, but not always.

For instance like Rolls Royce SMR, who will eventually sell reactors in the United States, or try to. They are in today (audio interference).

DR. SCHULTZ: So, EPRI can push on that, but the NRC can push on that as well.

MR. GIBSON: Yeah, that's really everybody at some point has to say this is the way forward or not. We produce these things, we research them, we think they're valuable, we think they're effective, we think they can solve a problem with it. It's really up to our other stakeholders that adopt it. We can't say hey, you must do this, because that doesn't work for us.

MEMBER KIRCHNER: Does this reconcile what the NSAG (phonetic) train of documents coming from IAEA ---

MR. GIBSON: Which ones?

MEMBER KIRCHNER: There's a lot of designs they're saying they're doing their safety to NSAG, don't hold me to this, 12 is the one that comes to mind.

MR. GIBSON: I think that's in the same

sort of arc. The IAEA has included the DEG as a recommended method to do systems engineering for I&C, so that's there. They've also had some recommendations on the TAM for cyber. You get the Canadian Nuclear Regulator has included the TAM in their regulation statement as being a valid way of doing what they require.

So, it's kind of growing out like weeds, it's not instantaneous that everybody's doing it. But IAEA is aware of this, we participated on technical committees, and all that stuff, shared this stuff with them. So, they're doing stuff. And they have the same, IAEA is a big bureaucracy too, and that's not meant to be derogatory, it's meant to just recognize how much it takes to change direction on something like that.

You've got to let a lot of people agree, there's a lot of talking, and it takes maybe sometimes years. All right, so that's what the industry is doing, you've seen that. (Simultaneous speaking). There we go, I think it's the last slide in this section. This is our users group. So, we have a users group that is created to further the digital systems engineering framework.

You can see the members, who are members of it down on the right. So, that gives you some idea of --- and they had to pay to be part of this, I'll just say that out loud because it's a measure of their interest, it's not something they get for their EPRI membership. So, that's going pretty good, we have our next meeting in September, it's been about a year and a half now since we introduced this.

So, we get a lot of feedback from all of those companies about these products, and as we do changes to them, they get a look at the drafts, and give feedback, and we ask them what they think, and do tests, and different sort of engagements to get real world feedbacks on these products as we change them. And we're doing that right now, there'll be a mass update in the first quarter of '24.

Because like I said, we've talked to 600 people now, we've got a big list of improvements we can make on usability. Remember, this something that people asked us to do, so it's a level of a process. So, when somebody says you ought to do this a little better, or that diagram doesn't work exactly right, it's not clear, we update all of that in these products. So, we're doing that.

CHAIR BROWN: Does this encompass all of the current nuclear power plant owners? I read through the list.

MR. GIBSON: It's pretty close in the U.S. Plus you've got Bruce Power in Canada, you've got a few ---

CHAIR BROWN: Does it have all the U.S. companies?

MR. GIBSON: Not entirely.

CHAIR BROWN: I don't know all ---

MR. GIBSON: I think the only company missing though, to be fair, is I think there has just been a merger between Vistra and somebody else.

CHAIR BROWN: Energy Harbor.

MR. GIBSON: Energy Harbor, yeah. Energy Harbor wasn't a member, but now they are, because now they're one company. So, I think NextEra is the only one missing off of this.

MEMBER REMPE: So, I'm curious about ---

MR. GIBSON: Progress is gone, it's part of Duke nowadays.

MEMBER REMPE: Before you move on, I'm curious why Curtiss-Wright, I mean most of them are plant owner operator organizations, and Curtiss-Wright has joined in because?

MR. GIBSON: They use these products, Westinghouse are members too.

MEMBER REMPE: Yeah, that makes sense too, but Curtiss-Wright I think of making components more than --- how are they using it, is it to help them make changes to future components that they're going to sell to the plants, or is there anything ---

MR. GIBSON: I'm not 100 percent versed on everything Curtiss-Wright does, but I think they do make systems. I mean Curtiss-Wright ---

MEMBER REMPE: So, they're selling systems, and getting an edge ---

CHAIR BROWN: They made a lot of I&C systems in the nuclear program.

MEMBER REMPE: So, they're improving their product to hopefully sell it to the plants is their angle. I'm surprised then that they don't have any competition trying to join in, it's just them.

MR. GIBSON: Well, I mean people ask us about it all the time. I expect this list over time, I expect it to get more international members over time. I guess just (audio interference) point in time. All right, he's pointing at you, John, so it's your turn now.

MR. WEGLIAN: Okay, so I'm going to talk about HAZCADS in detail. This is a flow chart, you kind of start out in the upper right corner with the

DEG provides information, and HAZCADS over in the left. We perform STPA, system theoretic process analysis, that's the last time I'm going to say all those words, I'm going to say STPA from now on.

And what we're looking for is unsafe control actions. He showed earlier the control system. And what STPA focuses on is not internal errors that can happen within your control system, but errors that can happen at the level of implementing something in the plant. I happen to work on developing software within EPRI, I'm here to tell you ever software has bugs in it, every single one.

But does it matter? There's a lot of bugs that just don't matter. So, what we're focusing on is when it's time to start a pump, open a valve, flip a breaker, something like that, can that be unsafe? That's what the unsafe control actions are. Looks at the effect on the plant, when can those be unsafe? And then we have a question, does that affect anything in the PRA?

We have other consequences that we consider beyond just nuclear safety, because this is a process, the plant wants to know is there going to be an economic impact? Is there going to be environmental impact, reputation harm, something along those lines? So, there are some consequences that we assess that have nothing to do with the PRA.

And so, we have a separate process where the plant makes a heat map essentially, risk matrices to define their risk reduction targets, RRTs, which is the output of HAZCADS for these consequences that are not assessed by the PRA. So, we have this other process for that, we call that pathway one. If it is in the PRA, then we ask well, how many systems are affected?

And that takes us to pathway two, three, or four, that's not important for us. I'm just going to block all of those, and say we use the existing PRA model to assess the impact of a complete failure of the digital I&C on the equipment under control to give a bounding risk reduction target. Again, what works well with this process is that STPA looks at the equipment under control, and that happens to be the equipment that's already in the PRA.

We already have basic events for the breaker didn't open or close, the valve didn't open, the diesel failed to continue running because of the over speed trip, or whatever it is. Those kinds of things are already in our PRA, so we can use the existing PRA to do our risk assessment for the systems that happen to be modeled in the PRA. So, our ---

MEMBER DIMITRIJEVIC: Hi, this is Vesna Dimitrijevic, I am the PRA expert in residence. So, the question for me here is that you assess the impact of complete failure by looking at the reduction target, which that doesn't match, because risk reduction is assuming complete success of that equipment.

(Simultaneous speaking.)

MR. WEGLIAN: I'll get in a slide or two to how we define the risk reduction target. So, if you could just hold that until I get to where we actually define those levels, if you still have a question feel free to ask it then.

MEMBER DIMITRIJEVIC: All right.

MR. WEGLIAN: I'm just trying to show you the overall process at this point.

CHAIR BROWN: Is that okay, Vesna?

MEMBER DIMITRIJEVIC: Excuse me?

CHAIR BROWN: Is that okay?

MEMBER DIMITRIJEVIC: Yeah, no, that's fine.

CHAIR BROWN: Okay, I didn't hear you say okay.

MR. WEGLIAN: Okay. So, we get from

either pathway one, or two, three, or four, we get a bounding risk reduction target, and we feed that into our downstream processes, DRAM, TAM, HFAM, EMCAM. And what they do with that, they may decide to change the design, and put new requirements on the design, and that gets fed back into the DEG, that's the up branch.

For things where they're not going to change the design, they're going to control that risk defined by the RRT by defining control methods. And if they're unable to meet that risk reduction target for some reason, maybe it's too costly, after these downstream processes have gone, they identify through loss scenarios, and they feed that into the relationship sets, we come up with combinations of UCAs that can fail at the same time.

I need the downstream processes to do this first before I can refine risk assessment, because before I got to that point I can't tell you which UCAs can fail together for the same reason, or same inherent cause. So, I need those downstream processes to do that. Once they do, then I can refine the risk reduction target for the areas where they weren't able to meet the bounding risk assessment.

I can now, what we call pathway five, I can redo my risk assessment, again, we'll see that in a slide or two for these combinations of UCAs based on the relationship sets to say is there a more refined risk reduction target that they can use for that? So, here's where we're getting to the risk ranking. We do this bounding risk assessment. Our first approach is we assume everything fails.

Not just software common cause, but any failure that it can do. And then we look at the change in risk if those failures occur. So, we're looking at a change, so this is a delta risk, delta CDF, delta LERF assessment. And if we say that failure of everything associated with the I&C system, the equipment that it controls, if that's less than a 1E minus 6 per year delta CDF, and less than 1E minus 7 in LERF, I give that a risk reduction target of delta.

That's the lowest that it can get. And each order of magnitude higher delta CDF that I get, I increase my risk reduction target up to a maximum of risk reduction target of alpha is delta CDF between 10 to the minus 4, and 10 to the minus 3 per year.

MR. GIBSON: I want to interject right there while you guys are absorbing this. The risk reduction target translates to a reliability target. So, ultimately if you want to reduce the risk, you want to increase the reliability to ensure the risk reduction range.

MR. WEGLIAN: Yeah, so your seal equipment would be expected to provide, for example, three orders of magnitude of reliability if you had an alpha RRT.

CHAIR BROWN: What does that mean, orders of magnitude, it's a thousand times better than something else?

MR. WEGLIAN: Yes.

MEMBER DIMITRIJEVIC: Okay, so let's discuss the risk reduction here. So, basically the intervals, you know, If you go to the Reg Guide 1174, right?

MR. WEGLIAN: Yes.

MEMBER DIMITRIJEVIC: So, let's discuss this. So, this is only applicable for specific control action, right? Not in the general for the equipment.

MR. WEGLIAN: It is for the entire design that is being evaluated. The digital I&C design ---

MEMBER DIMITRIJEVIC: I mean that is absolutely --- I mean everything in the plant depends on the control and stuff. So, I assume you're analyzing specific control actions, because there is not any --- you know, if you don't have a control in the plant how can you have that specific amount 10 to magnitude 6, so I'm not sure about this. The second thing when it comes to this digital I&C, but what I wanted to discuss is this reduction factor.

So, if you fail all control, and your difference that you're only increasing CDF let's say to less than 10 to minus 6, how is this risk reduction? It measures risk increase, so it's more (audio interference) risk achievement factors instead of risk reduction factors. So, this is actually showing you the total increase in that CDF is smaller than 10 to minus 6.

How is this connected to risk reduction? So, this is actually I have two questions. One is that, and the second one is what are you measuring, impact of what?

MR. WEGLIAN: So, let me tackle the if the risk reduction target is a delta. When I was at a utility I worked on a boiling water reactor, and our RHR system had three trains. Train charlie only provided water into the core, and there were nine other ways to get water into the core, so that one train was very low risk if it were to fail, because it had so much redundancy.

So, if I was doing a mod that only affected that train I would expect if it failed completely, my delta risk would be less than 10 to the minus 6, and this process would then say for that mod the risk reduction target is so low that the minimum level of activities that we would do on any mod at all is sufficient. You don't have to do anything additional to that.

If I'm replacing the RPS system at the plant that I came from, I'm going to guess that would be a risk reduction target of a bravo. And so, you would have more controls on that based on that mod. And so what we're doing is we're saying if anything under control can fail, then we fail it in the PRA model. And we look at what is that change in risk based on that failure and what ---

MEMBER DIMITRIJEVIC: Okay, all right, now I understand actually what you are doing. But I just want to tell you that you are using the wrong name based on the PRA principles. Okay, so what you are doing, you are not looking at total digital control of RHR, or God forbid, the plant, you're just looking at one specific control. If that specific control fails, you're increasing that CDF less than 10 to minus 6.

But see if you want to analyze risk

reduction you have to analyze if you make this totally reliable, what would be improvement in this? So, therefore maybe you should call this risk reduction factor, because that is something like a risk reduction factor.

MR. WEGLIAN: Yeah. It is not the risk reduction factor, it's the risk reduction target. So, this is the target that the downstream processes have to meet with their reliability. That's what we're --- that's how we defined it.

MEMBER DIMITRIJEVIC: Yeah, but you're not reducing risk if you're not going to pay attention to this control of that bravo, or whatever charlie train. So, you're not reducing any risk, so that's why RR is wrong, because you are not reducing. You're just going to say risk impact is small. So, that's a different thing. And also you're only analyzing one control action on that single train. So, it's not total.

MR. WEGLIAN: If the mod was only for that train, that's what we would assess. If the mod affected all of RHR, all three trains, then I would expect the risk reduction target to be bravo, or alpha, and they would spend a lot more on that.

MEMBER DIMITRIJEVIC: Yes, that is, yeah

MR. WEGLIAN: So, it depends on the scope of the mod.

MEMBER DIMITRIJEVIC: All right, okay. I just made my comment just to tell you that your name is confusing, and --

(Simultaneous speaking.)

MR. WEGLIAN: Okay, that's why it's a target. Because the downstream processes get that as an input and say your control methods have to meet that level of risk reduction. So, where it actually gets implemented ---

MEMBER DIMITRIJEVIC: That's not reducing risk. You're not paying attention. You're saying I don't need to spend the money on control of charlie, that's not reducing any risk. So --

(Simultaneous speaking.)

MR. WEGLIAN: They would do more on charlie than they would on delta.

MEMBER DIMITRIJEVIC: Okay, all right. I made my comment for the record.

MR. WEGLIAN: And if the risk --- if the delta CDF, or delta LERF exceed 10 to the minus 3 for delta CDF, or 10 to the minus 4 for delta LERF, we say that design is too risky. With this process you can't come up with enough control methods to get that level of risk reduction, and therefore you have to change the design in some way. That might be diversity and redundancy, right?

You might have to put in a new system that compensates for that. You may have to add human actions that can compensate for that. But whatever it is, if you get to that high level, it's unacceptable at the bounding risk assessment. And this is before we've done any refinement. This is the first time through.

If the delta CDF and delta LERF are too high, they have to change the design within our process to get it so that we believe that the equipment that's available for purchase is of high enough reliability to be able to achieve these kinds of reductions. So, here's an anticipated concern of yours. If I look at the risk reduction target of alpha, a change in CDF between 10 to the minus 4 and 10 to the minus 3, that's really high.

And we would not allow a risk informed application that had something in that range, that's true. But we're not saying that that is the increase in risk when we install this system. What we're saying is that would be the change in CDF or LERF if the entire system were to fail. That's also the current risk of your current system, what you have installed right now.

That is the change in risk, the change in CDF, the change in LERF if that existing system were to fail, that's what you're living with today. And what we believe is that digital I&C upgrades will reduce the risk compared to the existing analog systems as demonstrated by every other safety related industry that's gone digital, and they have improved safety with that change.

We believe that soon will be true in the nuclear industry. So, don't look at this and say that this is the change in risk of the system, that is not the case. This is we're defining a target level based on delta CDF and delta LERF that we set the bar for how our control methods, how strong they need to be to get us back to where we think it's very small, in reality an improvement in risk over the existing system.

So, after HAZCADs it gets fed down to DRAM, TAM, HFAM, EMCAM, and they're going to assign control methods to protect against these various types of failures. DRAM looks at random failure and systematic failures. HFAM is going to look at human factors, Mary is going to be talking about that shortly.

The TAM looks at cyber security. EMCAM is based on electromagnetic compatibility. This is where those relationship sets also become important. Because if the relationship set tells them that these are important because of spatial relationship, then their control methods will focus on equipment qualification, right? The temperature, humidity, those kinds of things.

Is it protected against a fire that can happen in the same location? Is it seismically mounted in the same location, same orientation? Those kinds of things would address a relationship set on spatial, but may not address a functional. Functional is will all my aux feed water pumps fail to start, even motor driven and turbine driven, because of the control system doesn't think it needs it, right?

That's a functional, and you would do different control methods for that kind of failure than the spatial. So, they get to tailor their methods for what relationship sets are defined. Is there a question?

DR. BLEY: Yeah, Dennis Bley. This is very systematic, it makes a fair amount of sense to me, it's also a lot of overhead, especially if you go back in some of the earlier stuff you didn't talk about in detail of using the Levinson methodology. If one uses this process to look at a proposed change, is there any relief on the traditional V&V kind of process that has to go on, or is this an add on on top of it?

MR. WEGLIAN: We anticipate that this new approach will replace what they're doing today. So, we're not just saying do everything you're doing today, and do more. We're saying what you're doing today is an inefficient process, replace that process with this new design approach.

DR. BLEY: I think I'd probably agree with you, but how do you get there from here? EPRI can't do it, NRC could do it, but IEEE, and all the other folks have to get on board as well.

MR. WEGLIAN: Yeah.

MR. GIBSON: I'm going to take that question. One of the challenges is that people won't turn loose what they currently do even when they get permission to do it. The industry is trying to adopt DEG, and are in the process of doing it. The biggest complaint we hear from folks is well we just added it to what we were doing, we didn't replace it. Even though that's the premise of it, that's what the C&Os wanted to have happen.

Because the internal auditors in the plants don't know how to evaluate risk informed stuff, this kind of thing, they don't know what good looks like. Your QA inspectors want to see a checklist, they want to say let me see your RFA, we're all done, you're good, move on. This requires more of an understanding of what kind of performance output you might get from this system.

And they're in the process of figuring that out. That's a thing that we all have to get aligned if we want to see a different way of doing this ultimately. That's the best answer I can give you there. Everybody has a part to play --

(Simultaneous speaking.)

DR. BLEY: You essentially repeated my question. I don't know how we're going to get there.

MR. GIBSON: I'm sorry, I spoke over you. What was that?

CHAIR BROWN: Say that again, Dennis?

DR. BLEY: I said Matt essentially reiterated my question, and didn't answer how we're going to get there.

MR. GIBSON: I'm glad I could be of help.

But the last part I wanted to say is everybody has a part. NRC has a part, the industry has a part, the vendors have a part. If everybody looks at the other person and says I can't do anything until the other person does something, then you aren't going to move anywhere, right?

MR. WEGLIAN: We do have some companies out there that are looking at this, trying to use it, and comparing it to the existing process, and we hope to leverage lessons learned there to one, improve our process, and demonstrate to the industry that it works, and gives you a good --- really what we need is a success story.

When somebody does this process, and says look at this, I saved 10 million dollars by doing this, everybody else is going to flock to it, right? We're already doing training, as he's mentioned, over 500 people have gone through DEG training. And so they're getting trained up on the process, we need to start actually implementing it, get some success stories.

And then if we build it, they will come. Once they see that they have a benefit, that they will get a better product at a cheaper price, I think that we will see a bow wave of people heading our way to try to get up to speed on this process.

DR. BLEY: Well, we thought that would happen with PRA 25, 30 years ago, it's been a very slow process. Charlie, this is an information brief for us, are we expecting at any time to hear any thoughts from the staff at a later date?

CHAIR BROWN: No, not right now.

DR. BLEY: Okay, it'd be real interesting to see how well they're following this, and what they're up to.

CHAIR BROWN: Well, the reg guides as they're presently configured, they drive you with different --- well it's not, I don't want to call it a standard.

DR. BLEY: It's just different.

CHAIR BROWN: Yeah. And I'd like to introduce one other thought process in there in terms of making sure the stuff works right, and all that kind of stuff there, is in some configurations the commercial plants have a different configuration than the world I came out of. Nobody wanted to shut down a reactor plant while a submarine was (audio interference) just don't want inadvertent shutdowns.

Those are potentially non-fun events, so you look very heavily at making sure you have systems in place that when something fails you don't compromise, or shut down the plant. The commercial plants have a little bit more flexibility in terms of they don't want to shutdown, but they can err in the direction of failures that drives you towards a shutdown as a mode of protection.

So, there's a little bit of difference in thought process. You're still going for the same thing, equipment that's very, very reliable, does what it's supposed to do whenever you ask it to do it, but I just want to throw in there's a balance in here. I think the commercial world is compatible with where you're all going, and what you're trying to do.

It's just a matter of overcoming the inertia in the manufacturers who build this stuff for the applicants, that they want to accept the process in order to deliver their product, and it should be better than what they were delivering before. Chris? Yeah.

MR. COOK: So, this is Chris Cook, branch chief Office of Research --

(Simultaneous speaking.)

CHAIR BROWN: Get closer to your mic please.

MR. COOK: Thanks. Member Bley, I just

wanted to respond to your question about what the staff was doing, or was partially doing. In the Office of Research we've been watching the DEG quite closely. About two years ago I think it is, Matt, we had training that we offered for the staff that was going through.

So, they went through a multi-day class to try to understand all the pieces, parts, and components that were in there. We've also been looking at individual components. Just last month we had some intensive training for inspectors, as well as NRC staff on the TAM, the technical assistance methodology that you saw that's a part of this going through. So, trying to understand those components.

Because we understand that we've been seeing it. I think we mentioned at the ACRS meeting just recently on the cyber that the TAM was applied at Global Three and Four as well as Columbia Generating Station. So, trying to get people ready for that, and understand it. So, definitely in the Office of Research we're trying to --- and those are just our past activities.

We have current activities right now dealing with both STPA, they're going on. We also have activities where we're looking at trying to assemble what we're calling some operating experience. We really get to that HAZCADS as well trying to understand the self certifications. Dr. Alverson (phonetic) here has been leading some of that effort.

So, anyway, we have a lot of, I think cross connections, connection points. We're seeing this, we're definitely trying in the Office of Research to be ready, that's what we see our job as being so that when NRR, or when our inspectors come across it, that it isn't the first time, that they've already had it available to them. So, that's really --- we're doing a lot, but I'm not able to say we're looking at changing this specific reg guide to put this in here.

That's one thing that we have been thinking about, is how should our guidance --- Member Kirchner was talking about how does this relate to RITNIS (phonetic) and how does this relate to all these other categories, outstanding question. So, anyway, that's been very much on my mind set. Another one of my staff, Mauricio Gutierrez is really working at trying to look at some of that, how we get into the guidance, and how do we do it in trying to do it.

We're also leveraging the MOU that we have with EPRI to look at it as well as the MOU that we have with LWRS. DOE as part of their modernization strategy, they're doing it, that's a lot of what this has been tied into. And I'm going to conferences as well to talk about it. So, anyway, that's just sort of a snapshot, sorry to advertise about the branch. But that's really where I felt like we're doing --

(Simultaneous speaking.)

CHAIR BROWN: No, no, that's fine.

DR. BLEY: Thank you, I wanted to push in one more area. Have they given you, or have you had the opportunity to sit in on any of the trial applications EPRI has been organizing?

MR. GIBSON: You were on the proof test.

MR. COOK: Thank you for that, it's helped. So, what we had a couple summers ago was a multi month long program called the proof test that EPRI organized to actually go through and do some of that testing. So, I had a couple of my staff participate in that activity to learn how this would go through by using a specific case. So, having that case, and doing it.

We've done this under the MOU so that it's really we can bring our technical insights, EPRI is sort of bringing in the information that's in there. So, Matt, I don't know if you had anything else you wanted to add about the proof test, or anything else on that.

MR. GIBSON: No. Generally the proof test was again, another test to gather information on usability, performance characteristics. We had eight people over three months do this process on lock changing to see how they did it, what performance they had.

MR. COOK: And that was really critical for us, because that showed us okay, that began our understanding. When you guys were looking at some of the functional sets, how do these pieces and parts come together, that was a start. Then we went to training, now we're trying the more we understand it, but we're still waiting to see how do we walk through or review, that's different.

I think the only one that's there in that part is perhaps the cyber security, because they're actually now to the point of inspecting results, products that have come out after the TAM has been implemented. So, that part is right there, but we haven't necessarily walked through a design. I think we're starting on one, that's right now with NRR, so I'm going to talk about it in the review.

I think that has some components that were in there, that was funded by a DOE study, or DOE had a large part to do with that from my understanding of the DEG.

MEMBER REMPE: It just sounds like this would be a great thing to try and get through LWRS as a pilot project that would help with the conversation of what is needed in the regulatory environment to make something like this happen. It doesn't sound like the research folks should have to be struggling on this alone. I mean, have you guys had those discussions, or?

MR. GIBSON: We do a collaboration with LWRS. To date I don't think that collaboration has coalesced around a regulatory thing. So, that's something, light water reactor sustainability program.

MEMBER REMPE: DOE is what he was talking about.

CHAIR BROWN: A DOE program.

MR. GIBSON: Well, INL runs that, but there are other DOE outfits that are attached to it too. But it hasn't really concentrated on the regulatory elements of it very much so far. Although I think that's an area of improvement.

MEMBER REMPE: Well, if you had a pilot, it seems like that would come up in the discussion, or something. But anyway, listening to the discussion here it sounds like something that's needed.

MR. WEGLIAN: Okay, I need to give Mary some time, so I need to finish up. I mentioned this already with the control methods. I didn't mention the word causal factors, but that's one of the things that these downstream processes look for. What can cause the unsafe control actions to occur? And then they tailor the control methods to address those causal factors.

And then there's a process for scoring the controlling methods against the risk reduction target that comes out of HAZCADS. So, the idea is given a risk reduction target of alpha, they have strong control methods that drive down the potential risk. Bravo does not require as strong of control methods, and charlie even less, and delta would be the minimum.

And we think those would equate to charlie would be about a SIL level one, and on the graphic here, SIL is safety integrity level, and SC is systematic capability. So, even if the letters are the same, they actually represent something different. But one gives it a target, and the other gives it the capability that it has to address that.

The acceptance criteria, as mentioned

earlier, is kind of tied to the Reg Guide 1.174 with the 10 to the minus 6 saying that was a very small change. If we're very high delta CDF, delta LERF, then we say we have to change the design before we go ---

DR. BLEY: Go back to the other --- I want to make sure I understand something on the previous slide real quick. I'm just trying to connect the dots between you're a, B, C, and D, and your triangle.

MR. WEGLIAN: The time delay is really --- and now I've got to do it again.

DR. BLEY: Okay, A is the lowest of the CDF ---

MR. WEGLIAN: A is the largest, delta ---

DR. BLEY: Largest risk?

MR. WEGLIAN: Yes, if it fails.

DR. BLEY: Okay, I'm just trying to connect the SIL, SC3 levels to your risk, which is what you were doing, and I just couldn't merge the two specifically.

MR. WEGLIAN: Yeah, SIL3 is the highest level of SIL that is widely commercially available. The process allows for a SIL4, but in practice nobody goes to that level.

DR. BLEY: Because it's not very reliable?

MR. WEGLIAN: It's not that it's not reliable, it's just if other industries need more than a SIL3, they change their design as well. And so, the SIL3 equipment is available for purchase right now, SIL4 would be hard to find. That doesn't mean that nobody could make it.

DR. BLEY: Is it better than SIL3, or ---

MR. WEGLIAN: SIL3 is higher than SIL2, which is higher than SIL1.

DR. BLEY: Hold it, that's not consistent with A, which is the highest risk.

MR. WEGLIAN: You are correct, we went with A, B, C, D to not conflate those two.

MEMBER KIRCHNER: SC stands for what?

MR. WEGLIAN: Systematic capability.

MEMBER KIRCHNER: So, nothing to do with seismic?

MR. WEGLIAN: No, not seismic.

CHAIR BROWN: Can I just ask a question? The lowest risk, the 10 to the minus 6 and whatever is a D?

MR. WEGLIAN: Correct, which is ---

PARTICIPANT: And the SIL level one is ---

CHAIR BROWN: SIL1 sounds like a D which is the highest ---

MR. GIBSON: Well, let's fix this, because this is a concept that we have to fix. The A, B, C, D are just sensitivities, they aren't risk. No real risk is involved here.

CHAIR BROWN: No, but the ranges ---

MR. GIBSON: But bear me out. So, when you have a low risk delta, meaning the risk change is the least, that's small, that's not saying the risk is small or big, it's just that the delta change is small, that gives you to a D. If you have a big change in risk, you can get a --

(Simultaneous speaking.)

CHAIR BROWN: I got it. So, SIL3 is the highest quality you can get, most reliable.

MR. GIBSON: Which brings that down to a high level ---

CHAIR BROWN: Takes you up into the change in risk is the smallest ---

MR. GIBSON: You bring it back to where it should be by applying that capability.

CHAIR BROWN: All right, sorry, I got it now.

MR. WEGLIAN: All right. So, if our delta CDF, delta LERF is too high we say you have to change the design. If you're at an alpha or bravo, we're saying if it were to fail that's a high change, so we need strong control methods to drive us down to back to where we say it's a very small change in risk, or improvement in risk is what we actually expect.

Charlie, now we're actually within the range of the Region Two in the Reg Guide 1.174, SIL1 is probably appropriate for that. And if you're in a delta, you're already a very low change in risk if it were to fail, and so the minimum requirements are required. You don't need to buy any SIL equipment at all. Whatever commercial off the shelf normal stuff should be efficient.

CHAIR BROWN: You can go to RadioShack.

MR. WEGLIAN: That would be fine. Norfolk Wire, that's where I would go. Coming back to here, I don't want to spend a lot of time on this, because again, I need to give Mary some time. But this process goes through the first time, and my downstream processes can identify things that can fail at the same time. That's at the relationship set level.

I now know combinations of UCAs that I identified through STPA that can fail for a common cause, a common reason, a common loss scenario is the terminology for STAP. And I can take those, and I can plug that back into the PRA model, and get a refined risk reduction target for control methods that are hard to meet at the bounding assessment where we assume everything failed.

Now that I have more information about how the system can fail, I can group those things, and do a more refined assessment, and say these ten UCAs can happen due to they're all in the same room, right? A fire can fail all of those together. What is the risk reduction if those all fail, I can give them a new number that maybe is easier for them to meet, but I need this process to go through the first time.

Because when I first get it as a PRA person, I have no knowledge of when UCAs can fail together, I have to assume they can all fail. Special note on software common cause, our operating experience both nuclear, and non-nuclear indicates that most of the systematic failures are a result of latent design defects due to inadequate requirements.

Usually his example of the flow pump over ranging, the requirements were wrong. The requirements should have been that the range on that pressure transmitter could have been high enough for two flow, right? Two pumps, and run at the same time. It's an inadequate requirement, or uncontrolled system interactions where they didn't realize that two systems working together could lead to something.

It's very rarely a typo in the software that would have something like that. Because that usually gets caught in testing. Misapplication of diversity as a means to address the potential for software common cause can actually contribute to additional system complexity, which can actually increase the potential for latent errors. I'm not saying don't use diversity.

What I'm saying is blindly applying diversity as the only means to address risk may actually make the risk worse. We have to be smart about it, and our approach is designed to make you smarter in how you address these kinds of things. Use diversity when it's appropriate, use something else when that's more appropriate.

So, HAZCADS identifies and risk ranks these potential systematic errors, all of them, not just software common cause, which would be a subset of those errors. And then the other tools in the framework establish the control methods to address those. Here's just a summary of everything I said. We use STPA to identify what could go wrong, what could be unsafe through interactions of the system?

That's what we focused on. We start with a bounding risk assessment. We revised our requirements, or we apply control methods to account for these errors, but we do that commensurate with the risk, right? If it's very low risk, we don't have to do a lot, if it's very high risk we do have to do a lot.

And if needed, we refine the risk assessment based on our identified loss scenarios if we couldn't meet the bounding risk reduction target for a particular control method. That's the end of my presentation.

MS. PRESLEY: Are you guys ready for the next phase of this?

CHAIR BROWN: Are you the human factors part here?

MS. PRESLEY: I am. So, we're going to talk ---

CHAIR BROWN: Before we do you, since you're now going into this amorphous area of human factors, and the other part has been kind of hardware, and designs, and software, and stuff like that. So, this is short, it's just something I observed in going through the DEG, and looking at the TAM thing, the cyber part, but let me talk about the DEG first.

If it's not obvious, and I think Chris may remember this, he may not since he's not in NRR as thoroughly, but when we've been focusing on the digital I&C systems, whether they be in new applicants, or otherwise, the focus has been to start with defining the architecture. Don't try to say you're going to meet all the positions in every Reg Guide, and every IEEE standard, and tell me you've got a safe system.

The architecture is the boundary conditions for defining whether that system is going to be safe or not, because it tells you where your soft spots are. And when I read the DEG, it mentioned architecture, but in a very generic manner in about 422 places. So, it's just a lot of listings in case you go through it. What I missed on the lead in to your whole thing, which is what we've been trying to get the staff to emphasize with applicants in the reg guides, there ought to be a preamble of some type.

That says look, you've got to define what does my plant look like. Which parts are safety related, which parts are safety critical, which parts etcetera, etcetera. And then you start layering out how complex what you need to do relative to all the stuff you have both been talking about in terms of the development process. I'm just making this as an observation.

To me the architecture is the fundamental stone you start with, and if you start talking about processes with individually the piece parts throughout it, you lose the focus. The first point or place you would ever talk about a system or plant architecture is in section 4.2.8 where you have a notional diagram, figure 4.4 which shows a giant plant with safety systems, and other plant systems, etcetera, and a network, and everything else.

Unfortunately all the data that comes from all the systems goes into a giant network which is all jumbled up in server software, which is not very reliable or safe. That's a different thing. The one redeeming value, it shows data diodes coming from the safety systems out to the outside world. The downside, it shows safety systems communicating back and forth, not out just to the systems they've got to shut down the plant with.

My point being that's pretty late in the point in the system, in your process rather, to start thinking about the overall plant architectural. I just think you all ought to emphasize how important knowing what your plant looks like, what the piece parts you're dealing with that you're going to have digital control systems control before you start talking about all the little nuances.

Which I don't disagree with, they're all there, but it's just a matter of how you structure it to get people thinking in my view properly. Now, that's my observation, that's my personal comment, and that ---

MR. GIBSON: That's good, all feedback is good.

CHAIR BROWN: And that's what we tried to do in PTP 719, Reg Guide 1.152, 1.62, etcetera, etcetera. Know what you're looking at overall so that you know where to pay attention. That's just a suggestion when you're going down the path for whatever revisions you're going with. And I would hope you would fix up that overall notional plant to be a little bit more ---

MR. GIBSON: It's top of my list, Charlie, to make that notional plant a little different.

CHAIR BROWN: You had safety A, and safety B, and you showed them communicating back and forth, and that's not a very good idea. Good way to shut everything --- or compromise its ability to shut everything down. Anyway, so that just was a good place before we get into the human factors, because I hope you're going to address in human factors, when you have to go to backup systems for human factors.

Shutting down the plant when your systems fail totally in compromise. Is the answer to that yes or no?

MS. PRESLEY: Maybe not at the level of detail you wish, just because of the time constraints.

CHAIR BROWN: There's a big controversy on whether using diverse software systems is a good compromise, and you can through your switches, and trips, and breakers, which is really ---

MR. GIBSON: So, really to answer that, this is process oriented. So, when you do a hazard analysis and HAZCADS, model the operator, you're going to create a loss scenario, and one of the loss scenarios is going to be you lose whatever. And now the operator has to take action, and you're going to evaluate that.

CHAIR BROWN: He's got a manual switch somewhere, what does it do, and how does it get it done? Because two wires going down to the contactor is a lot different than another computer with quote diverse software.

MR. GIBSON: That's right.

CHAIR BROWN: And I think that's the kind of thought process in the human factors area I think needs to be addressed. I didn't really see that when I --- I mean, I didn't read 369 pages in 10 hours, it just didn't work out very well for understanding. So, kind of a thoughtful --- I have no problem with the document system, in covering the other part of it.

MR. GIBSON: Good feedback.

CHAIR BROWN: So, I'm done with that part.

MR. GIBSON: Party on there, Mary.

MS. PRESLEY: Okay. So, we just got the ---

CHAIR BROWN: No, I'm not done. The TAM part, there's all kinds of stuff in your TAM cyber security which is all kinds of good stuff, and you finally got talking to data diodes part way through it somewhere. That's actually the highest level of protection you can have because it's an air gap. But that's not in the preamble area. What's the structure?

How do you structure protecting yourself cyber wise for critical components? And the air gap approach is being the best, and how do you deal with others where you don't need it? It should have been up in the front, and then lead in to how you address in other areas. It's just how you approach doing it, and define it, and make it clear that an air gap --- it doesn't help you on physical access.

People can come in and screw up your software when they make mods, that's always been the case whether it's hardware or software, but now we've got the electronic path that complicates everything. So, the emphasis on the highest quality down to the lowest, how do you deal with it. Where do you use software to protect your virus system, blah, blah, blah, whatever, those are for other ways. Anyway, now I'm done.

MS. PRESLEY: All right.

MR. GIBSON: Now you can start.

MS. PRESLEY: Okay. So, John just went through HAZCADS, and now we're going to look at one of the downstream processes, which is the HFAM, the human factors assessment methodology, and it's a risk informed approach for human factors engineering. And here on the left you can see very simply what John was talking about. We have these reliability targets that come from HAZCADS, and they go into the human factors engineering process.

And then the human factors engineering process feeds back HSI design, but also feeds back on function allocation, and task attributes as you go through the design loop. So, the risk informed approach has the benefits of being graded, and it allows us to really right size what's a human ability versus (audio interference). I'm going to try to power through some of this so you can get through all of it.

So, these are the key activities that are typical in a human factors engineering, an HFE process. I'm not going to go through those activities, and HFAM doesn't change the general process. But what we do is make it more usable, and accessible to the user, and we integrate it with the systems engineering process.

So, some of the key features is where are the touch points that the human factors process hits with the systems engineering process, particularly the EPRI DEG. How do you integrate the risk insights from HAZCADS into the process? And then we provide a two phased graded approach. The first phase looks at the scope of the design based on the DEG.

And that allows you to allocate your resources appropriately at the beginning of the project, and pick the right tools that you need to do the human factors engineering. Not every project requires a dedicated HFE expert, but we do want to make sure that the right skills are applied at the right time, the right level of detail for the design. So, that's the first phase.

And then the second phase, once we get more into the detail of the design, and have unsafe actions to look at, we use the risk reduction targets, or the reliability targets, that's more clear, from HAZCADS. And that will tell us how much level of effort we need to put into each UCA target in terms of HFE design to protect against unsafe human actions.

CHAIR BROWN: So, straight to graded approach, it's kind of a screening process in a way, before you do the more detailed phase two type stuff, is that the way I would read that?

MS. PRESLEY: You still have to go through the whole process, but so you're not screening out. What you're doing is trying to figure out what level of detail you need to go to, so yeah.

CHAIR BROWN: I call that screening, you're just screening what level of stuff needs to be done. That's fine, I got it.

MS. PRESLEY: Yeah. And then the other, I guess for me the holy grail, because I'm an HRA background, we've been able to bring the HRA tools, and the data, and the experience with HRA, and use it as a tool within the human factors process as part of the treatment of important human actions to help come up with to make sure --- to ensure that you're meeting the reliability targets.

And then this helps on the PRA side, because then there'll be consistency between the design process, and what your design says a human can do, and what your PRA credits. So, to do that --- so, that's the HFAM side, and those are all the slides we had on the actual HFAM piece. The next is the HRA research that we're going and doing on the PRA side.

And this is important because currently HFAM references the existing HRA methods, which are pretty good, but they're not optimized or developed for digital systems specifically. So, now we're going through the process to understand what's different for digital systems in the area of what data do you need to collect as an analyst, what human failure modes you might be susceptible to.

What new performance shaping factors you might be susceptible to, what the level of difficulties you might have, and we recognize that digital is all over the map. So, it can be from very focused modification of replicating an analog with just a digital all the way to new reactors maybe remotely controlled, totally different control room structure.

So, what we call digital from a human perspective can be across this very broad range. And so, we're taking a graded approach at our digital HRA research. So, that's why you see design A, mini mods. The humans will perform very similar to existing plants you may have. And then our existing methods and processes are totally applicable.

You may have plants that may have maybe computerized procedures, or maybe more automation than our traditional plants, and our existing methods are pretty good, but may need some augmentation in those areas. That's maybe design B. And then design C would be these totally new and different concepts of operation where our existing methods may not be so adequate.

CHAIR BROWN: Do you try to address in the digital systems the actual components that may be used that the operator or the human has to execute with? For instance, a lot of it is people use a push button to do something, or you have a mouse and click, or you have a touch screen that maybe doesn't respond when the operator hits close, and it doesn't close. Touch screens can be touchy.

MS. PRESLEY: Sure, those are ---

CHAIR BROWN: And some touch screens have a sensitivity of --- and this is the way they're designed, if your hand gets close you don't necessarily even have to --- it happened to my son in law in the car when he went to change his screen, he didn't touch it, it just changed as he moved his hand towards it. So, are you trying to take the new parts that he has to deal with, and how that affects his human actions?

MS. PRESLEY: Yes, we're looking at the physical systems ---

CHAIR BROWN: Okay, thank you, that answers my question.

MS. PRESLEY: And a really good example of that particular thing is that we have some OE that shows there was one design that they were looking at touch screens, and the second checker to verify would put their finger where they were looking, and that would inadvertently activate what they were trying to second check. So, those are definitely part of the HRA.

But equally part of the HRA is how does it change your concept of operations, or how you work together as a team? So, if you're on a physical display board, it's easy for the shift supervisor to see you are on this part of the board, so I know what you're looking at. So, you have some situational awareness of what people are doing.

You don't necessarily have that same situational awareness, or that second checking function maybe when people are just sitting behind their screens. So, we're looking across the board at how human performance changes when your interface changes. All right. So, there's three general data sets ---

DR. BLEY: We can't hear you out here, Charlie.

CHAIR BROWN: It got fixed, don't worry about it, something popped up on the screen, that's all.

MS. PRESLEY: All right, so I'm going to keep going. There's three major sources that we're looking at for our initial evaluation of the HRA stuff. And as you can imagine, because digital is a broad set, we have a broad set of data, so we have experimental data from places like INL and Halden. Those look at broad range of scenario types and design features, but they're small sample sets, so it's largely qualitative data.

We have literature review, and OE review from nuclear and non-nuclear sources, again, broad range of design types, but they're not large statistical data sets. And then we have training simulation data of which we've collected the first set from the Korean simulator studies. And 45000 data points, great statistical data set, excites the nerds like me, but it's on one specific design.

So, we have to question how generalizable that is. So, we're trying to take these three types of data sets, and synthesize them into lessons learned, and pull that into our HRA methods. And then the last slide on this particular piece is a special note on human errors of commission, and this is very similar to the systematic failures for software, software common cause failures.

When you have humans interacting with a system, and they have the ability to --- human cognitive errors of commission are when humans do something they shouldn't do, but they're probably doing it because they have a good reason to do it. So, maybe their procedures tell them to do it, or their instrumentation is misleading, but they're doing the wrong thing, or they're fighting against the automation because they don't understand the automation.

So, in the PRA traditionally we don't take an unbounded look for these types of errors. If we have a specific cause to suspect we will include it in the model, and one example are fire, we look for spurious operations, or multiple spurious operations where humans can be misled. But typically we don't just go and search for these in an unbounded fashion.

But with automation, and more automation, the conversation around errors of commission is definitely increasing. We see an uptick in this, and we see in the new standards, discussion of incorporating it more heavily. So, we have to question whether or not PRA process is the right place to consider this. And from our perspective, STPA is actually designed to look for these types of errors.

So, if we're looking for them appropriately through the design process, then we should be able to use that process as the right tool to address errors of commission, and then only include them in the PRA, again, when we have a very specific cause. For instance if we were unable to mitigate one that was, or design one out that we found through the STPA design process.

So, that's the end of my human factors

piece. I'm quicker than the boys. Any questions on that? I know I didn't answer your question on the backup.

CHAIR BROWN: No, you did fine. You said that no, you're looking at the combination of the things, and that's all you can do, appreciate that.

MS. PRESLEY: All right. Okay, so then the last bit is how we look at digital systems in the PRA. So, the life cycle of the design goes from design, implementation, all the way through operations, and configuration management. And I think I have an animation. So, we've checked the box for design and implementation in terms of consideration of risk through HAZCADS and the associated downstream processes.

And we did that through sensitivities, and through matching our control measures with our risk reduction targets, or our reliability targets. Now we need to make sure we have a coherent approach for the operations and configuration management. Basically what I call your assessment PRA, or your living PRA that you use after the fact.

And when I say coherent approach, I mean you can't go through this rigorous design process and say okay, I have a design that's acceptable, it's risk acceptable, we believe that this is a low risk design, and it goes through all of that, and then you put in maybe a conservative, or an arbitrary value in your PRA that says sorry, we have a problem. So, we need to make sure that the insights from the PRA on the back end match the qualitative, all the work that went into the design end so there's parity.

All right. So, what do we have on putting it into the PRA? Right now, as you can see, a lot of bubbles. We don't have a coherent process, or a systematic process for including these elements in the PRA. It's kind of all over the board, and especially if you look at it internationally, what people model in the PRA, and how it's modeled in the PRA, and what data, or assumptions are used is really quite all over the board.

So, what we're working on right now is a first cut at how do you include digital systems in the PRA model, and then what do you put in numerically as well. So, our research is going to capture the current state of knowledge, and we're really relying heavily on the foundational data, qualitative and quantitative, and that work that Matt's group has done.

And then we're going to make sure it also matches the use cases, because all models are useful, some models are useful.

MR. GIBSON: All models are wrong, some are useful.

MS. PRESLEY: All models are wrong, some are useful. But they need to match the use case, and what you're trying to make a decision using the PRA models. So, that's the piece we need to match up, is the data, and how are you using your models, and what kinds of decisions you're making with your models.

DR. BLEY: Mary?

MS. PRESLEY: Yes, sir.

DR. BLEY: It's Dennis Bley.

MS. PRESLEY: Hi Dennis.

DR. BLEY: Hi. I'm not sure it will help you, but you ought to take a look at the research NRC funded back 10 to 15 years ago on this area. None of it came to real fruition, but you might find some useful nuggets in that work.

MS. PRESLEY: Yeah, so part of this effort is looking at existing references, including the stuff that EPRI did I think around that same time frame you're talking about. If you have specific references, Dennis, I think I know what you're talking about, but if you have specific ones, maybe offline I can ask you.

DR. BLEY: Yeah, that's fine, do that. There was several projects at Brookhaven, one at another lab, and then there was one at an outside contractor that I'm aware of, and they all had some aspects that you might find useful.

MS. PRESLEY: Okay, thank you so much for that. All right, so our proposed approach, and again, this is in progress, and still pretty early in progress, is based on defining these use cases, and then relooking at the data and existing guidance and lessons learned from HAZCADS. And there's a couple of things before I go into some of the detail I want to make clear as ground rules for our research.

So, incorporation of the design into the PRA has to be consistent with the insights of the design process, we already talked about that one. It has to be consistent with the overall PRA modeling approach. Which means same sort of level of detail, same sort of types of assumptions. So, we cannot be --- we cannot have major mismatches, very large conservatisms, or screening out things that we shouldn't be screening out, or putting too much in.

Because the value of the PRA is that it lets us look across systems and compare. So, we need to have parity in the modeling approach between digital systems and how we deal with the rest of the equipment, and human actions in the PRA. And then the third is that you need to make sure you're continuing to reflect the as built, as operated plant.

Okay, so the first piece is digital systems should be modeled at a reasonable level of detail. There's sometimes modelers get very enthusiastic, and model in extreme levels of detail. Practically this has issues with model complexity, being able to verify the model, being able to run the model. Second, model level should be consistent with the boundary conditions of the data.

So, you can't go into the super, super subcomponent level if your data is not collected at that level. So, this has implications for when we think about software. For example, when we talk about reliability, we're going to talk about functional reliability, and software shouldn't be separated from the hardware, because software is implemented through the hardware. And typically when we collect data, we collect it at the functional level.

So, trying to take that functional level stuff, and then decompose it artificially causes issues, as you can imagine. The second piece of this proposed approach is based on the fundamental assumption that our control methods that we've used through HAZCADS and its downstream processes reduce the risk to acceptably low levels. So, this is important because we're making a qualitative statement when we do the design process.

We're saying that I have reduced my risk substantially, and now I'm in that low acceptable risk region. So, while we may not have specific numbers, we qualitatively are saying that we have made that much of an impact on our risk when we apply certain sets of control measures. And that's the piece that needs to be coherent with whatever data or information we put into the PRA.

And that's for both the functional reliability, and the common cause failures. And that's because what we've done on the design side, that reflects our best estimate idea of what the actual risk and importance of these actions are. Okay, so what does that --- yes.

MEMBER DIMITRIJEVIC: Hi, this is Vesna Dimitrijevic. So, you have here the chicken and egg problem, right? I mean you use the PRA to design and define your targets, and then you put in things in the PRA, which will change your input in design.

MS. PRESLEY: Well, this is assessment PRA, so this is after the design is done, and been implemented. So, this doesn't feedback then --- this might influence the next modification you might make, but this doesn't ---

MEMBER DIMITRIJEVIC: Are we talking here about existing plant, or the new designs?

MS. PRESLEY: Either way, this is after a design has been complete and implemented. Whether it's an existing reactor or a new reactor, at some point you'll have finished the design, you'll have implemented it into your plant, and now you'll have to have a PRA that you can use to make your operational decisions, or have on file for your safety case, or whatever. But this is at the end of the life cycle part of the operations.

MEMBER DIMITRIJEVIC: You guys are aware that your targets are not relative, but absolute, and so therefore they will work fine for today's industry. But if you apply your lowest requirement target to the increase of 10 to minus 6, that's not going to happen in --- most of the new designs are coming with such low numbers that increase of 10 to minus 6 will mean thousand times increase in existing core damage.

So, I mean, and I was going to bring this in then, the relativity of these risk measures are --- they have to be reexamined for the new designs, because that's one of the big discussions, that we're using absolute or the relative risk measures. But another thing here where you have to have this process of using these risk targets in design, and then trying to incorporate some of the important things like human actions back.

I mean, that can change totally the risk targets. So, I have a lot of concerns about your categories, and how that will work. And about this, as I said, egg and chicken problem, so just want to raise that.

MS. PRESLEY: Thank you.

MR. WEGLIAN: So, I just want to make it clear that what Mary is talking about right now is after the design is done, and it has been installed into the plant, what does the PRA look like to assess the system that is now installed in the plant? So, in the slide she's going over right now, there's no feedback into the system design anymore. Because not only is the system design done, it's been installed.

This is when the new digital I&C system is now part of the plant. And for a new reactor, this would be when the plant is built, this is what they're going to have with them.

MEMBER DIMITRIJEVIC: Okay, I just pointed out that this can change your targets, and I understand that you're saying that. But these are also maintenance, and ITAAC, the other things going there that this impacts the importance, and that importance can change totally.

MS. PRESLEY: So, I'm going to talk to your second point in the next slide. But for your first point on new reactors, and them having a different risk profile, that's part of the research that we're looking at in use cases, is how would that change in an advanced reactor, and does that change, and what does that look like? So, that's definitely on our radar.

CHAIR BROWN: We need to keep moving, I would like to get through your last slide.

MS. PRESLEY: All right. So, the consequences of --- so, risk is likelihood times consequence. So, the first piece is making sure the consequence is captured in the model. And long story short, you have a cause effect relationship for the potential unsafe action. And if that potential unsafe action survives to the final design, you need to make sure that the consequences associated with that are incorporated in the PRA somehow.

So either if it has a non-unique consequence, you can map it to an existing portion of the model, an existing basic event. But if it has unique consequences, for example a new common cause failure grouping that you didn't have in your model before, you need to make sure that that consequence is reflected in your model. And that failure can be hardware, software, or human error.

These potential unsafe actions need to be incorporated logically from a consequence perspective into the model. And this is the piece, Vesna, the logic has to be reassessed as the PRA evolves to reflect the as built, as operated plant. So, as you change your human actions, or change something in your PRA, you may see a difference in consequence.

And if you have impacted your risk reliability targets, then you have to go back and say --- well, if your targets have increased you have to go back and say well, are my control measures still adequate? So, you do definitely need to make sure you're looking at that consequence, and that those assumptions that you made remain valid. So, the second piece is the likelihood.

And of the two, consequence or likelihood, consequence is more important. Because likelihood, we have kind of two ways we can look at likelihood, and our current research is investigating both approaches. Likely one will be useful in some areas, and the other will be useful in others, and that's the use case piece.

But the first way is to create some generic failure rates based on the available data, and the qualitative insights that we have gained through the I&C research. And the second way is to actually not quantify this at all, but similar to the way HAZCADS approached it, keep the events in the model, and use sensitivity studies to understand if risk has changed.

And then when risk does change, to see if our control measures are still adequate. So, there's two ways we can look at likelihood, and that's the direction that our research is going right now. But I want to emphasize in the long term, industry needs to start gathering data, and we need to do that in a way that is consistent, and that the boundary conditions of the data match what we put into the model.

So, we have a way to collect data, transfer that data directly into the model. So, uncertainty, I'm sure this has come up, completeness uncertainty certainly has come up. Uncertainty is not new, PRA does not create uncertainty, PRA exposes uncertainty, and digital is not the only place where uncertainty exists. So, we want to just recognize that up front.

And we also want to recognize that conservative treatment is not the answer to uncertainty all the time. And in fact if inappropriately applied it can mask risk insights. So, in this particular place we recognize that we don't do risk based decision making, we do risk informed decision making, and that constitutes the other pertinent information.

And the two particularly important pieces here are performance monitoring, so that's the data collection piece. So, when we make certain assumptions if we put a number in the model, or when we say a control measure is adequate, but we need to monitor the data in the OE to make sure that those assumptions that we make hold, and that if they don't, we have a way to respond to them.

The second piece is defense in depth and safety margins. So, this is where I know, Matt, John said flex, and you reacted. So, we actually have many layers of defense in depth built not the process. From the DRAM we have first of all you design it out. If you can't, can you protect, can you detect, can you respond to a fault? And then if all of those fail you have multiple functions, you have diversity in your functions.

And then if that fails, you have FLEX. So, we're looking at accrediting defense in depth across the board, not just at the small level. So, those are the pieces that help flesh out the picture of how digital uncertainty is considered in the PRA process. Yeah, I can skip this one. So, the last slide is about looking at the whole elephant.

And just within EPRI getting our I&C guys, our human factor, our cyber, our PRA, our HRA all talk in the same language and with the same vision required a real cultural shift. And we ran into all these things where digital is different because, you know? And every time we did that, we're like well, no, it's not really different, we're coming up against the same issues we have in other areas.

But maybe it's more pronounced, and so we've refined our methods and tools. But it's still the same overall process, it's still the same types of uncertainties, and complexities that we already deal with in risk informed world in general. So, that's it.

MEMBER DIMITRIJEVIC: Mary.

MS. PRESLEY: Yes, ma'am.

MEMBER DIMITRIJEVIC: All right, so a couple things, I just want to make a couple wise guy remarks. So, one of the things because you brought up Mark bringing up the FLEX equipment, and he had a really good question, are you concentrating on mitigation, or just prevention? And he didn't say prevention, there is a better word for that. But it is important in this process if you're using the PRA, you are not using initiating events, the fault trees, which are already there, integrated in the PRA.

And the digital I&C will play a lot of function in the preventing actual events, not just mitigating them. And so, maybe that should be considered in one of those processes. The other thing, which is why I said the wise guy remark, you said that this is a risk informed, and not risk based process, so I mean you can tell to Charlie how does safety classification impact the total risk classification.

Because there is not any connection between those two. So, I just thought that Charlie would be thrilled to know that. Okay.

MS. PRESLEY: All right. Well, I will let John answer how initiating events are touched.

MR. WEGLIAN: So, I didn't go over it in this. There is another part of HAZCADS that looks explicitly at UCAs that can cause a plant trip. So, as an initiating event. It's a lot more complicated than what I've shown before. It's still tied to a delta CDF and a delta LERF, but we bias the initiating event frequency. You can't set it at a frequency to true in the same way that we do the probabilities, so it has to be a different approach.

So, we bump up the frequency based on the plant data, and in expectation of how many additional trips you would have from the UCA. I can go offline if you want some more information on that. But we do take that into account, that if it could be an initiating event, how that can be an impact on the model.

MEMBER DIMITRIJEVIC: You know a lot of the initiating events have fault trees associated with them, but they're already there, integrated in the PRA model. So, I mean that's why I just wanted to say something which you may have forgotten.

MR. WEGLIAN: So, most of what --- well,

yeah, if you had a failure of main feed water for example, that might have a developed fault tree. But if it's just a generic plant scram, if you're looking at the RPS system and it inserts a scram, most plants that's a single basic event based on plant history. And so we handle both approaches.

Actually it's easier if it's a developed fault tree, because there's usually a basic event you can set to true, and you don't have to attack the frequency directly.

MEMBER DIMITRIJEVIC: That's true.

CHAIR BROWN: We've got two minutes.

MR. GIBSON: We're done.

CHAIR BROWN: You're done, okay. At this time, before I go around and ask for comments from the participants here, I'm automatically connected already to the phone. Is there anybody on the phone line that has been listening that would like to make a comment in the public, or on Teams? Hearing none, I will call one last query to the members here. Anything else?

MEMBER SUNSERI: I thought it was a good presentation. I mean, I learned something, I wasn't trying to bash, or flex, I was just pointing out that that's way down in the chain of events. But I thought it was interesting.

CHAIR BROWN: Okay, good, thank you. Greg, and Vicki, you all have any comments? I think Dennis is gone.

MEMBER HALNON: Yeah, I'm good Charlie.

CHAIR BROWN: Okay. Vicki?

MEMBER BIER: I agree with Matt, it was a good presentation. I see a lot of pluses and some concerns, but not show stopping ones. So, it sounds good, I appreciate the opportunity to learn about it.

CHAIR BROWN: Thank you. I don't think I've missed anything administratively, I haven't done this in a while. Okay, one more just closing comment from me is I really do appreciate you all coming in, and taking your time to present this to us. I thought it was very comprehensive. And providing the other documents to give us a little bit of feel for how you're incorporating this, and what you're doing with it I thought was valuable.

And it's good for us to know this as we're working with the staff and everything, so I do want to thank you very much for that. And I forgot to ask Chris, did you want anything else? You're good, okay. You looked like you wanted to say something.

MR. GIBSON: No, I was going to say it was our pleasure, so thanks a lot for having us.

CHAIR BROWN: All right, with that, this meeting is adjourned exactly on time for once.

(Whereupon, the above-entitled matter went off the record at 12:30 p.m.)

EPRI Digital I&C Perspectives

EPRI Digital Systems Engineering Framework and Related R&D

Matt Gibson-EPRI
Technical Executive

Mary R. Presley-EPRI
Technical Executive

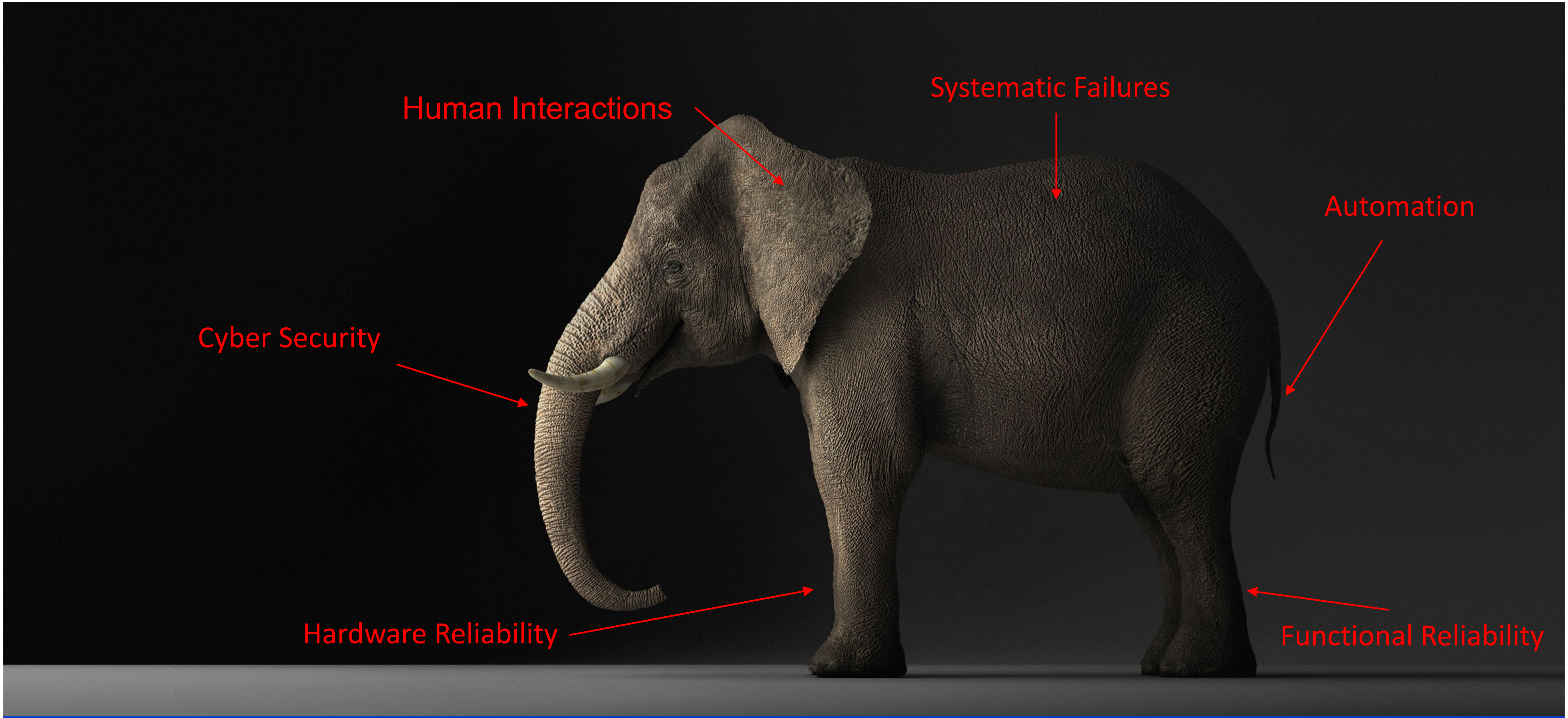
John Weglian-EPRI
Principal Technical Leader

Joint Digital I&C and Fuels, Materials and Structures ACRS Subcommittee Meeting on EPRI Digital I&C Perspectives

June 22, 2023

www.epri.com

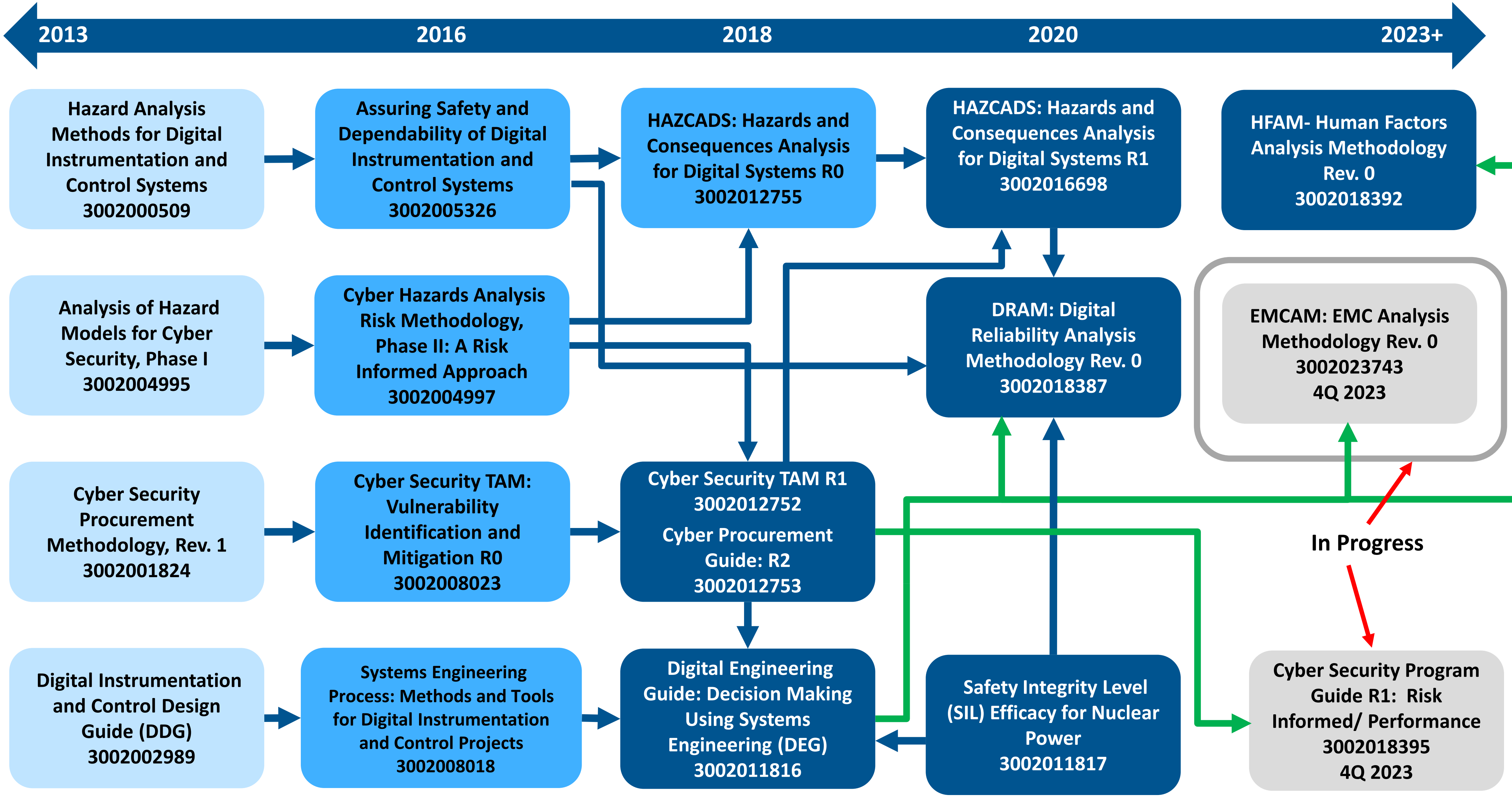
Looking at the Whole Elephant



How to address design requirements, risks, and hazards from various sources in one integrated process

II. Introduction to the Overall EPRI Digital Systems Engineering R&D Strategy

How we got Here- A Development History



EPRI

EPRI's Digital Framework Elements

EPRI's ***high-quality engineering process*** uses the same modern methods and international standards used in other safety related industries to reduce implementation cost

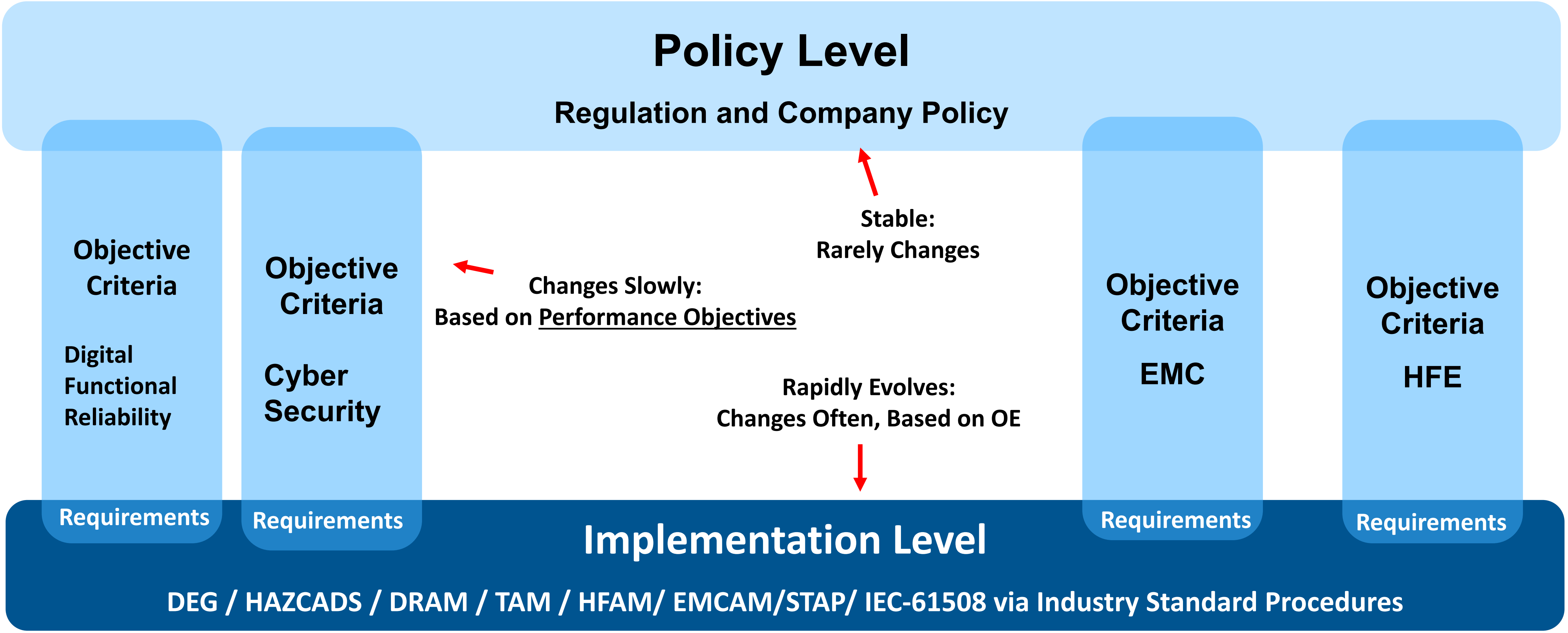
Utilize Industry Standards	Use the same proven design and supply chain structures that non-nuclear safety related industries use (IEC-61508/61511/62443). This leverages the economies-of-scale achieved in other industries.
Use of Systems Engineering	Use of a modern, high performance, single engineering process that leverages systems engineering in the transition to team-based engineering for conception, design, and implementation(IEC-15288,IEC-15289, IEC-12207,STPA).
Risk Informed Engineering	Making effective engineering decisions via hazards and risk analysis to integrate all digital engineering topics into a single engineering process (STPA,FTA)

Capable Workforce

Modern Methods to Support Nuclear Fleet Sustainability and Advanced Reactor Design

EPRI

Policy Level vs. Implementation Level Activities



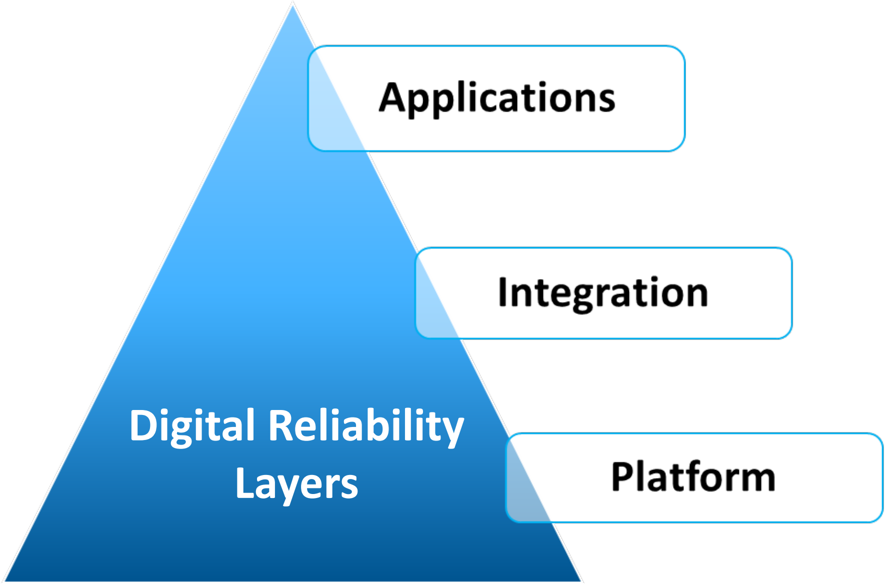
EPRI Products are Used at the Implementation Level (what you actually do)

Performance Objectives provide the Interface between Policy and Implementation. Supports a safety case argument.

Safety Integrity Level (SIL) efficacy for Nuclear Power

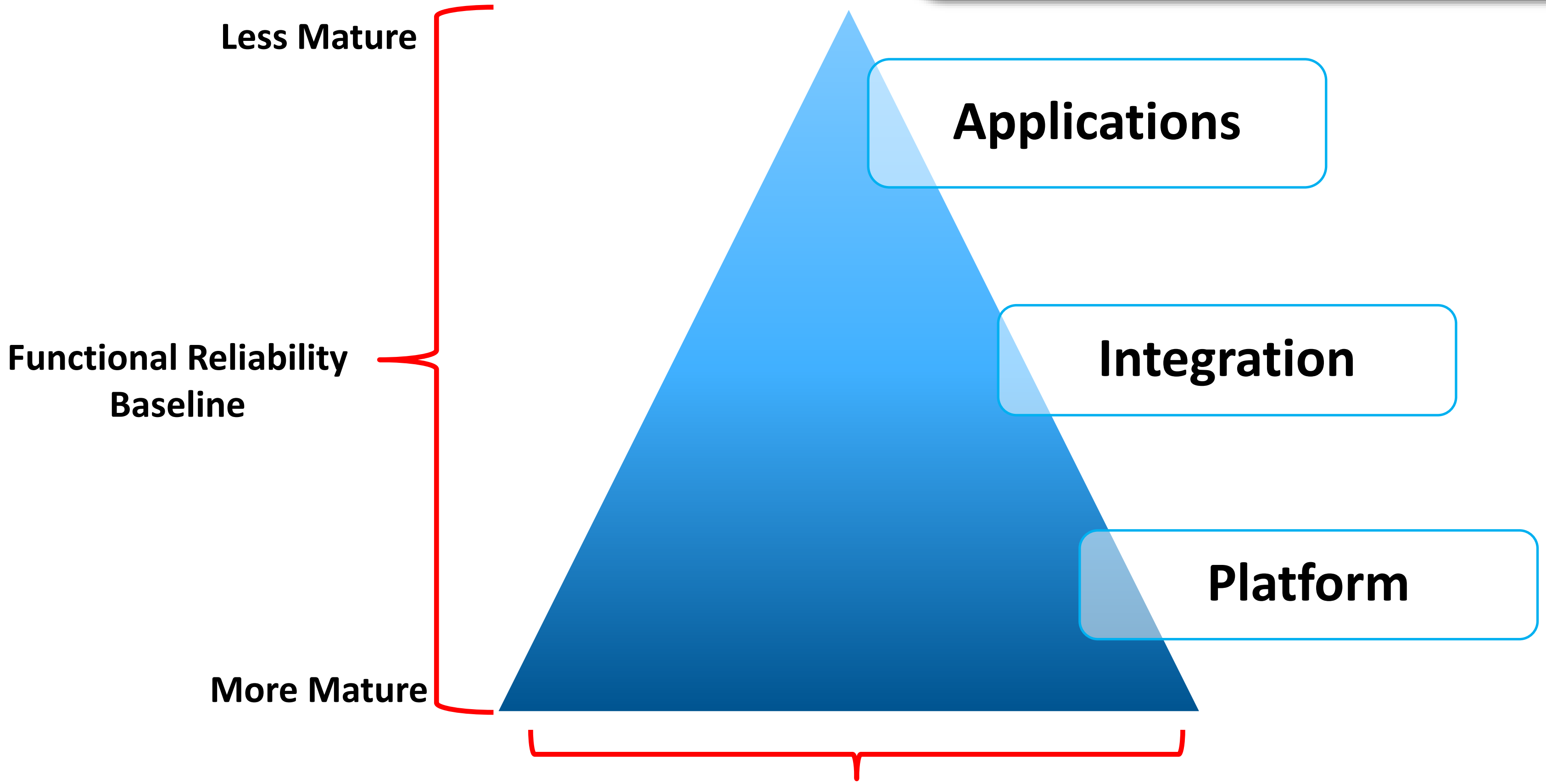
- EPRI research on field failure data from SIL certified logic solvers revealed no ***platform level*** Software Common Cause Failures (SCCF) after over 2 billion combined hours of operation for IEC-61508 SIL certified PLC's (3002011817)
- Indicates that using <u>existing</u> SIL certifications, at the ***platform level***, has a high efficacy for use as surrogates for some existing design and review processes.
- **Leveraged for NEI 17-06/RG-1.250 and NEI 20-07 in US**

- Correlates well with EPRI review of global OE (Korea, France, China, etc.) that indicates:
  - Safety related software is no more problematic than other CCF contributors when subjected to deliberate safety and reliability design processes.
  - There have been no events where diverse <u>platforms</u> would have been effective in protecting against SCCF



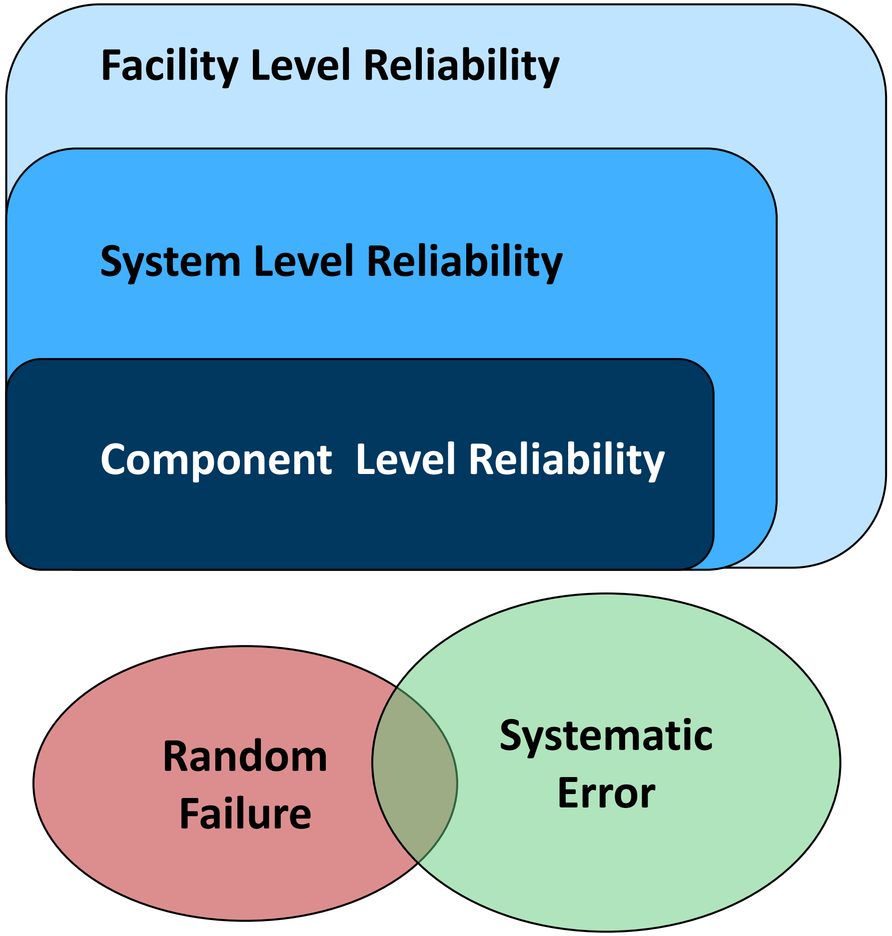
Reliability Layers

Functional Reliability, which includes software, hardware, and human elements should be segmented by layers: *platform, integration, and application*.
Then Considered Separately



Production Data and OE Quantity and Quality Dive Maturity and Reliability

Digital Reliability Model



Reliability Axioms

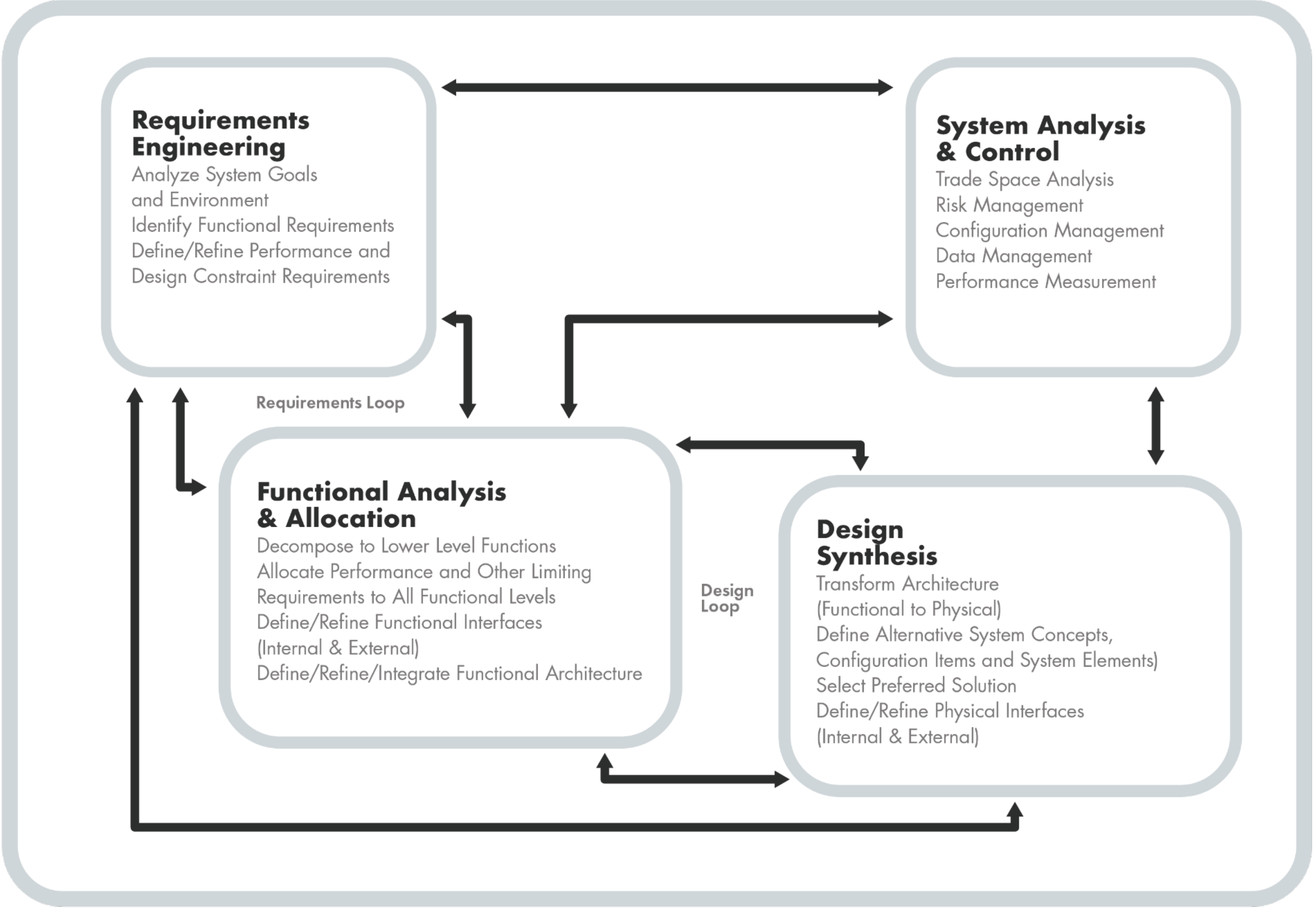
- Common Cause Failures must **first** have a failure or systematic error (including emergent behavior)
- Achieved Systematic and Random Reliability is inversely proportional to the likelihood of a CCF
- Reliability is best achieved via a cost, likelihood, and consequence equilibrium
- Net Functional Reliability is the prime objective (at the system/facility level)
- Focused Models can provide actionable reliability Insights (FTA, STPA, Relationship Sets)

- **Functional Reliability is an Equipment Level Challenge**
- **Functional Reliability is a Lifecycle Challenge**

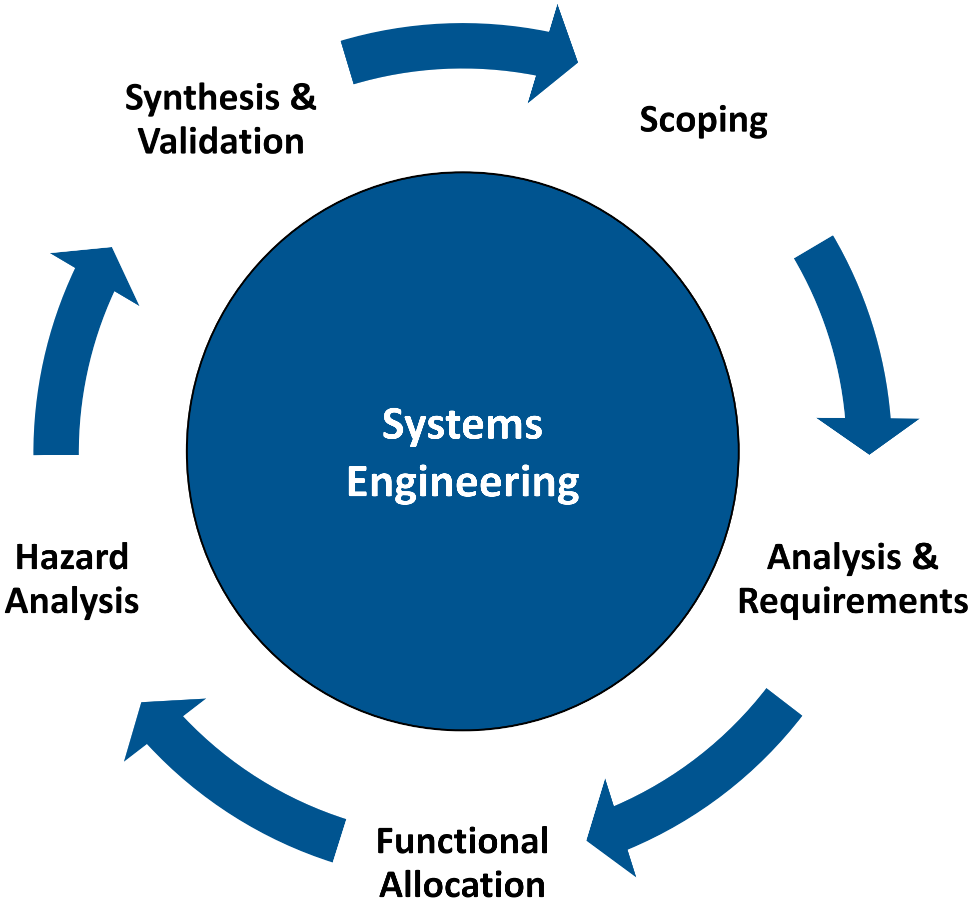
III. Systems Engineering- A Modern Approach to the Technology Life Cycle

Systems Engineering - Discovery, Iterations & Refinements

- Systems Thinking is the key skill required to use Systems Engineering
- It is multidisciplinary and requires teamwork
- Requires ability to see system relationships in a holistic manner
- Ability to communicate across disciplines
- Ability to understand complexity



Digital Engineering Guide (DEG) – Systems Engineering

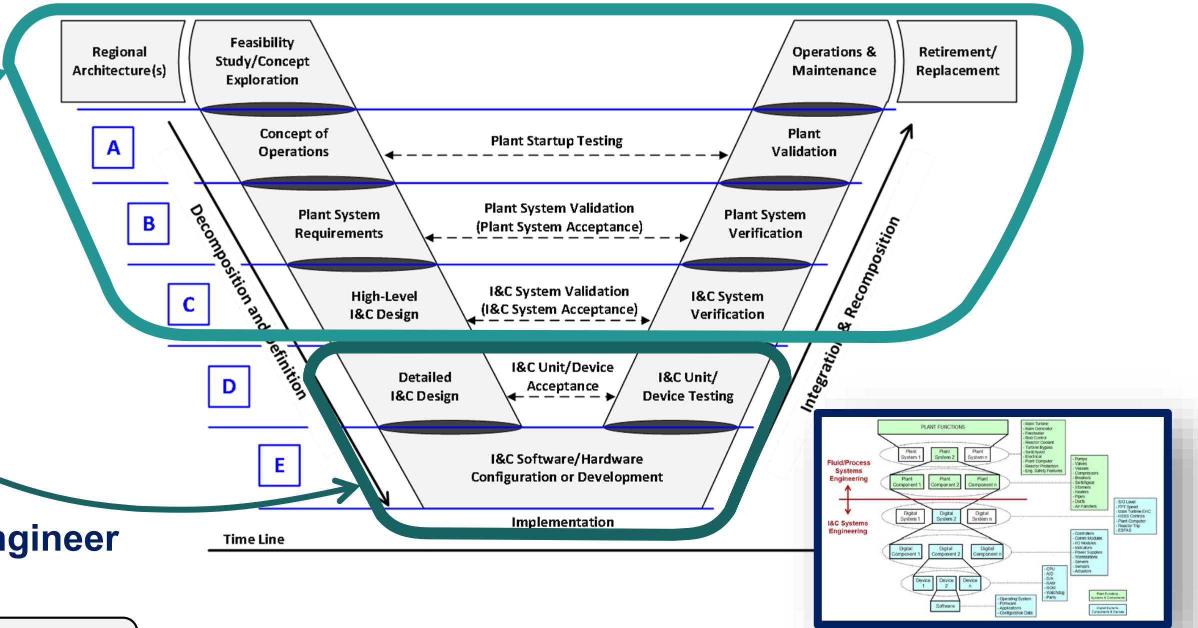


- **Lifecycle Phase Based using Perform/Confirm method**
- **Iterates through the SE process for each phase in a <u>non-linear fashion.</u> Synthesized from the IEC-15288 Framework**
- **Includes the topical guidance for each phase**
- **Iteratively converges on the final synthesized design**
- **The DEG Addresses:**
  - Division of Responsibility (DOR)
  - Requirements Development
  - Hazard Analysis , Reliability Analysis (including CCF) and Mitigations
  - Architecture Development including Relationship Sets
  - Functional Allocation (including Human/System Allocation)
  - Verification and Validation (V&V)
  - Testing
  - Transition to the O&M Phase

SE Process Example

1. Bounding Technical Req'ts.
2. Decide Parameter Values
3. Bench Evaluation
4. Refine Parameter Values
5. Specify Configuration

Predetermined by the plant and plant system designs

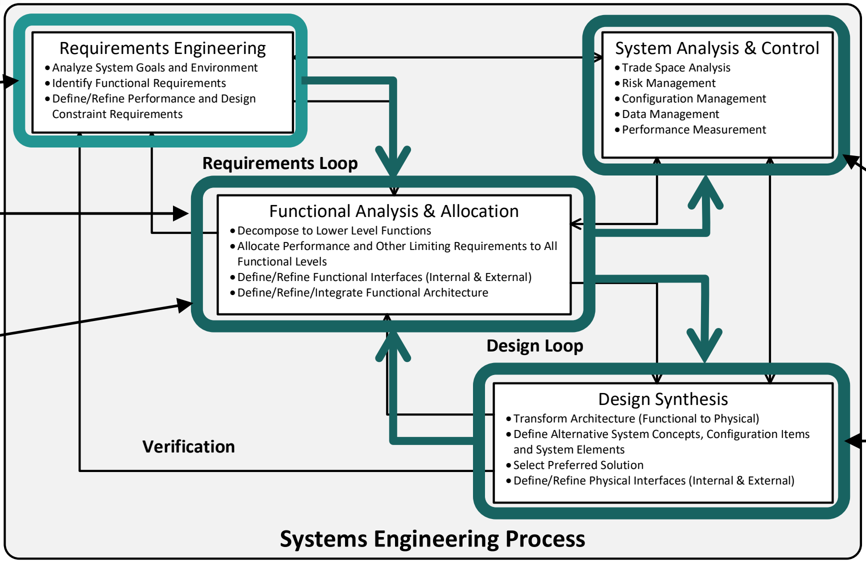


Determined by resp. engineer

1. Bounding Tech. Req'ts.

2. Decide Parameter Values

4. Refine Parameter Values



Configure, Install & Validate

5. Specify Configuration

3. Bench Evaluation

Also Consider:

1. Desktop Simulation
2. Reusable Style Guide
3. Model Number Optimization

Choosing a Hazard Analysis Method

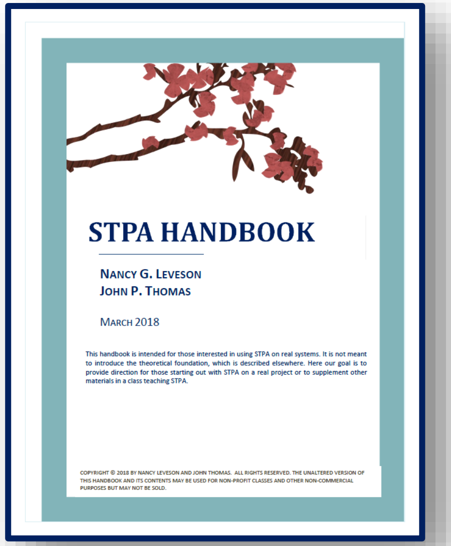
- **Hazards and Consequences Analysis for Digital Systems (HAZCADS) evolved from analysis, experimentation, and testing to find an effective methods or combination of methods that would provide usable hazard insights for the design process**
- Comparative analysis and testing concluded:
  - STPA showed the most promise in terms of a holistic approach to diagnosing the systematic errors of a nuclear plant and the related controls.
  - While STPA is strong in many areas it:
    - does not diagnose component level reliability failures
    - does not prioritize or rank the importance of the identified UCA’s
    - Is not a design synthesis tool but rather a design diagnostic tool
- EPRI has integrated STPA with a Systems Engineering based design process that achieves design synthesis that can then be analyzed by STPA via HAZCADS.
- HAZCADS combines the results of STPA and FTA to provide risk-informed prioritization of UCA’s and the associated loss scenarios.
- Loss scenarios are limited to topical areas of interest which reduces combinatorial growth. This insight is combined with reliability analysis and relationship analysis to fully develop control methods that address each loss scenario.

Criteria	Sub Criteria	FMEA	FTA	HAZOP	STPA	PGA
Traditional use for safety analysis	None	Green	Green	Yellow	Red	Red
Potential for Identification of Non-Traditional Equipment Failure Modes and System Behavior	New failure modes unique to cyber components are identified	Green	Red	Yellow	Green	Red
	New interactions enabled by cyber design features are identified and characterized	Red	Yellow	Yellow	Green	Red
	New system effects from cyber-related failure modes and interactions are characterized	Red	Red	Green	Green	Green
	The interrelationships between cyber and non-cyber system elements are identified	Red	Red	Yellow	Yellow	Green
Potential for System Characterization and Risk Prioritization	Potential for system characterization	Red	Green	Yellow	Green	Green
	Potential for risk prioritization	Red	Green	Red	Yellow	Green
Suitability for Software Implementation	None	Green	Green	Green	Yellow	Yellow

Criteria	Sub Criteria	FTA-FMEA	STPA-FMEA	STPA-FTA
Traditional use for safety analysis	None	Green	Green	Green
Potential for Identification of Non-Traditional Equipment Failure Modes and System Behavior	New failure modes unique to DI&C components are identified	Green	Green	Green
	New interactions enabled by DI&C-design features are identified and characterized	Yellow	Green	Green
	New system effects from DI&C-related failure modes and interactions are characterized	Red	Green	Green
	The interrelationships between DI&C and non-DI&C system elements are identified	Red	Yellow	Yellow
Potential for System Characterization and Risk Prioritization	Potential for system characterization	Green	Green	Green
	Potential for risk prioritization	Green	Yellow	Green
Suitability for Software Implementation	None	Green	Yellow	Green

HAZCADS Basis: Hazard Analysis via STPA

- IEC Std. 61508-1 (2010) requires a determination of hazards of the Equipment Under Control (EUC) and the EUC control system, and "***consideration shall be given to the elimination or reduction of the hazards***."



For the determination of hazards and their causes, HAZCADS and DRAM/TAM/etc. apply the four-part Systems Theoretic Process Analysis (STPA). Insights from this diagnostic process are pipeline back to the DEG for aggregation and requirements updates.

STPA Step One
Identify
Stakeholder Losses

→ **STPA Step Two**
Identify
System Hazards

→ **STPA Step Three**
Identify
Unsafe Control Actions

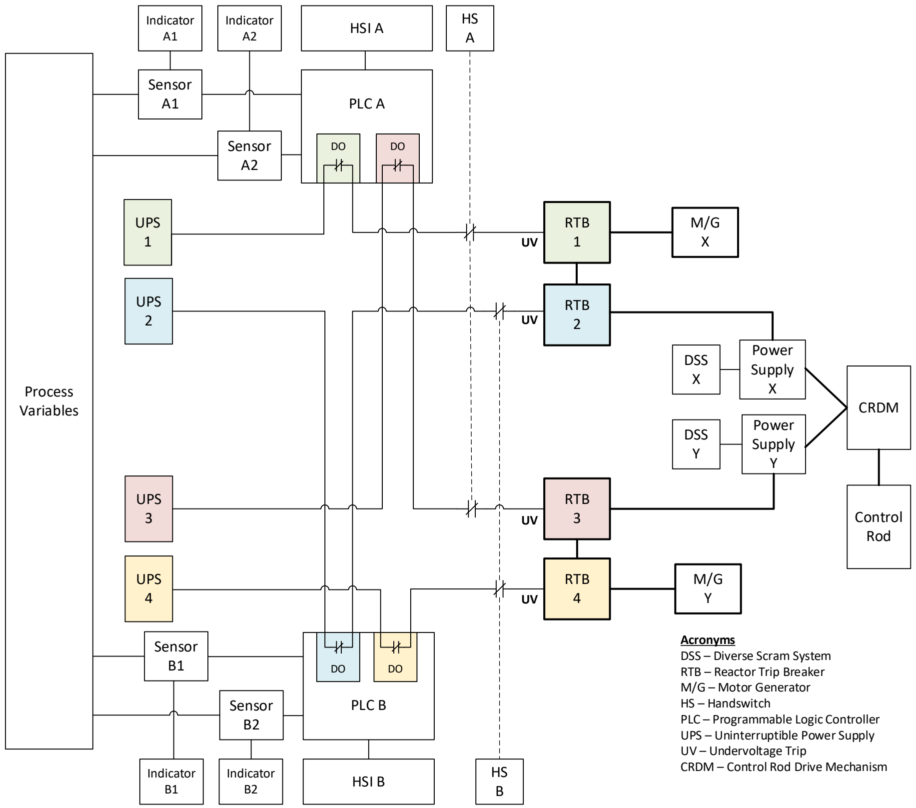
These steps are in HAZCADS

→ **STPA Step Four +**
Identify
Loss Scenarios + Reliability Insights

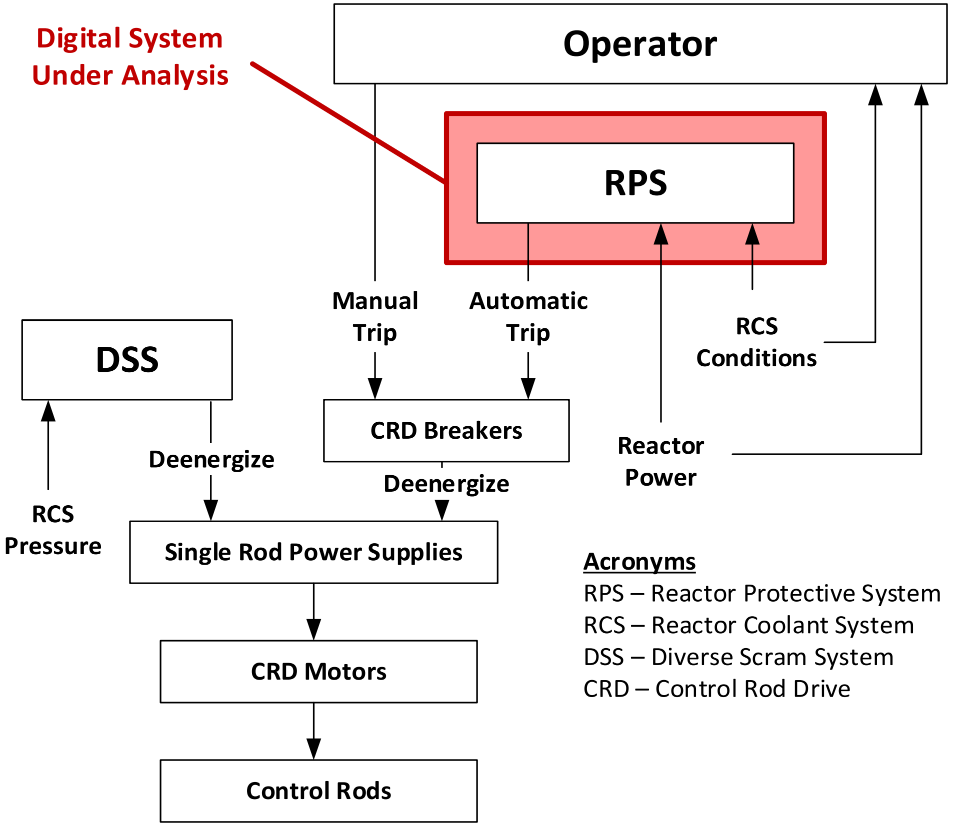
DRAM/TAM/HFAM/EMCAM

Systems and STPA

Notional 1oo2 RPS Concept



STPA Control Structure



The STPA Control Structure is a Diagnostic Model

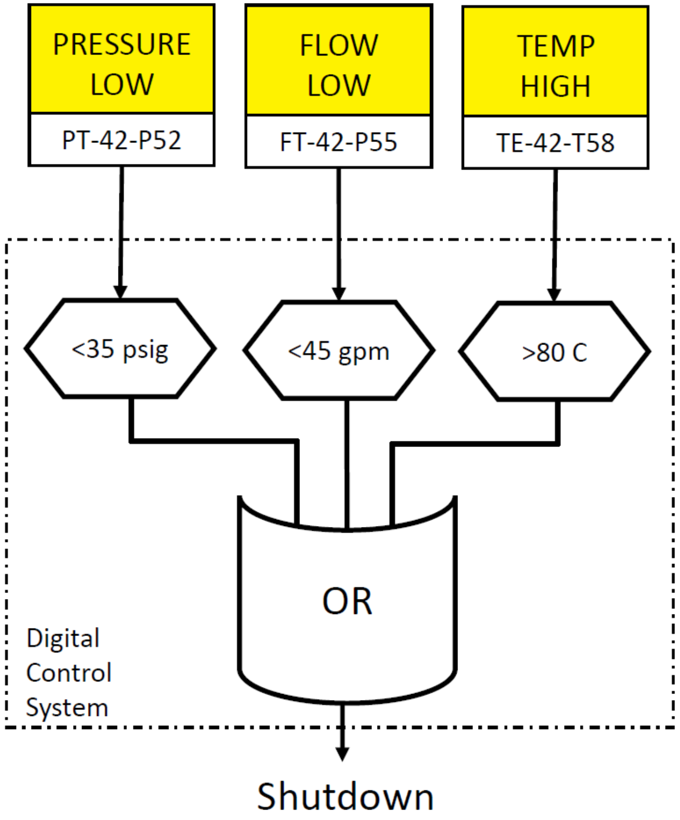
Example of Test Scenarios
Real Event

Turbine Control System Loss of Cooling Detection

Problem with Existing TCS Design:

- The existing TCS design contained a single point vulnerability
- Failure of a single cooling flow transmitter could cause a turbine trip

Old System Logic

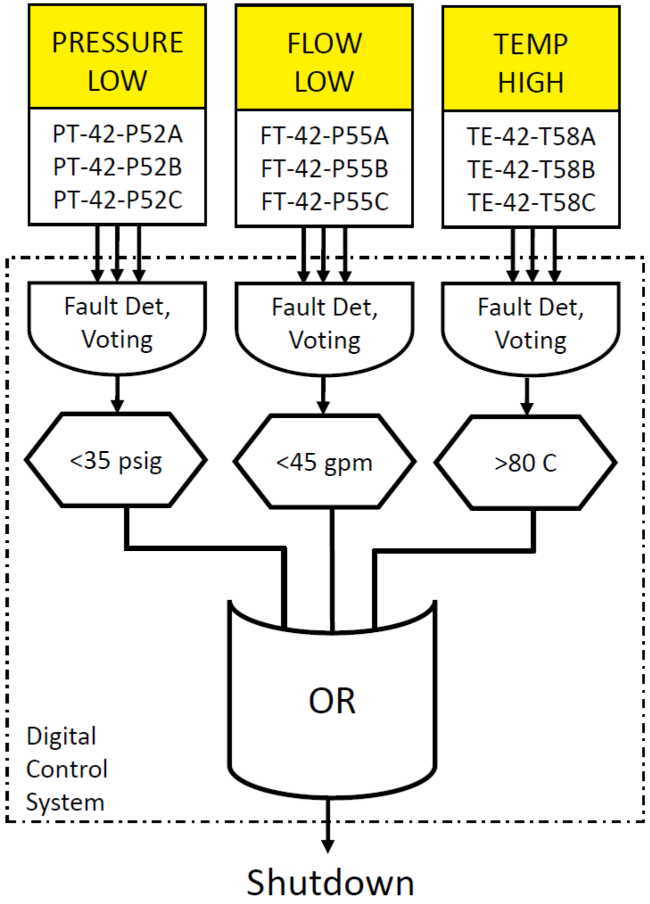


Turbine Control System Loss of Cooling Detection

Proposed Solution Based on System Requirements:

- Replace the single flow differential pressure transmitter with three differential pressure transmitters providing input to a 2oo3 coincidence trip logic
- The digital controller will detect and automatically remove a faulted instrument from the logic
- The logic is designed to identify a faulted instrument by measuring the output either high or low outside the calibrated range
- When one instrument is faulted, it is automatically bypassed, changing the voter logic to use the remaining two instruments
- If a second instrument is faulted, it is also automatically bypassed, and the voter logic uses the remaining valid instrument
- **Finally, if all three instruments are faulted (e.g., all sensors out of range), the logic is designed to send a shutdown signal (turbine trip)**

New System Logic

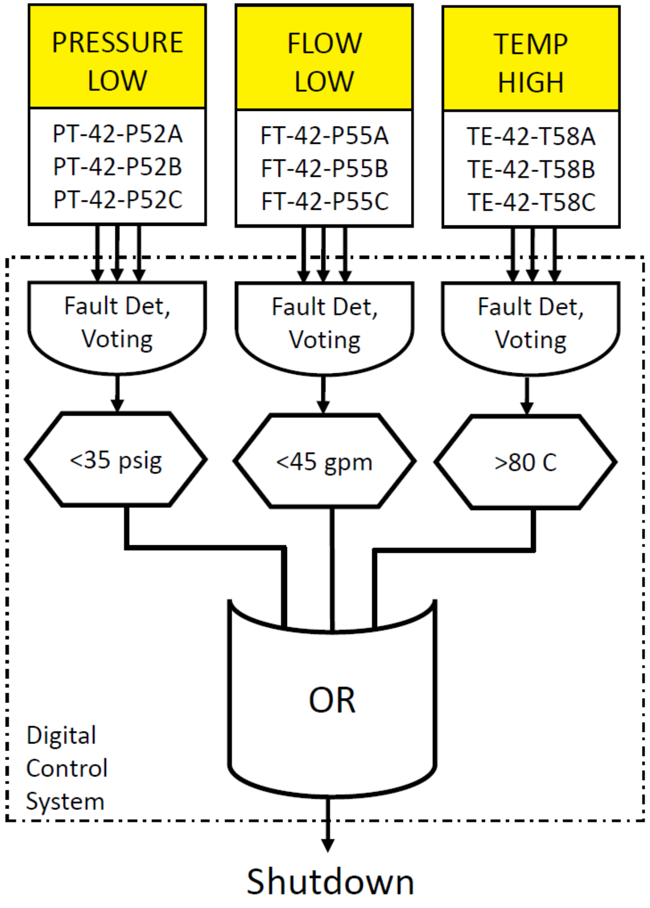


Turbine Control System Loss of Cooling Detection

The issue:

- The flow transmitters have a range of 0 - 600 GPM
- The high out-of-range instrument setpoint for the DP transmitters corresponds to 612 GPM.
- Normal stator cooling flow is approximately 550 GPM with one pump in service
- Two stator cooling water pumps exist, only one is running at a given time
- The stator cooling water pumps are routinely swapped during power operation such that wear on the pumps is even
- To swap the pumps, the in-service pump remains on momentarily while the out-of-service pump is started
- When both pumps are in service, the stator cooling flow routinely exceeds 612 GPM

New System Logic

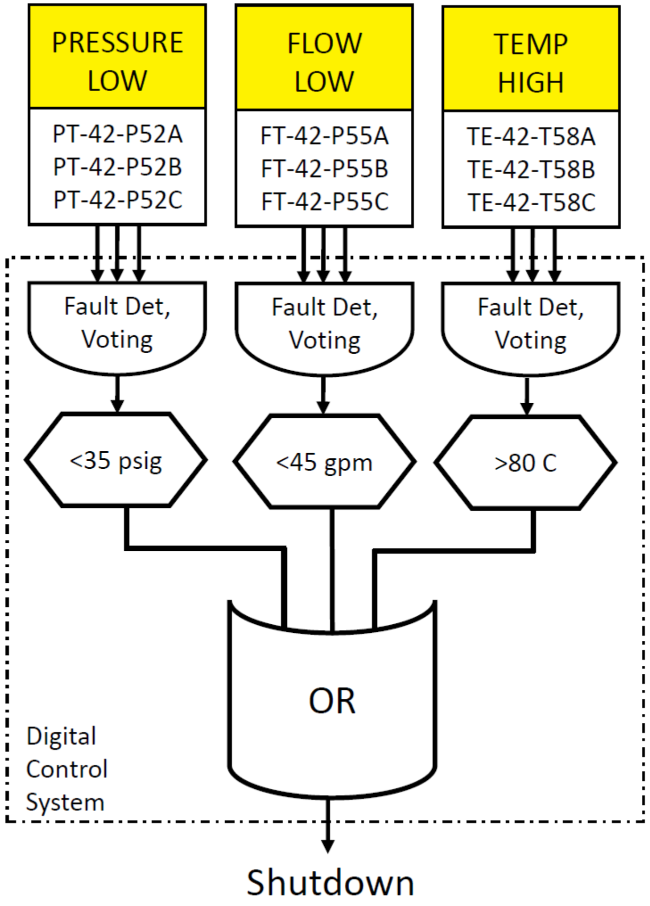


Turbine Control System Loss of Cooling Detection

The result:

- The design team did not consider both stator cooling water pumps running simultaneously when developing system requirements
- During the first stator cooling water pump swap, all three of the stator cooling water flow transmitters simultaneously over-ranged
- The design deficiency based on inadequate requirements resulted in an unanticipated turbine protection system behavior that caused a main turbine trip and subsequent automatic reactor trip.
- **The problem was found during HAZCADS blind study tests.**

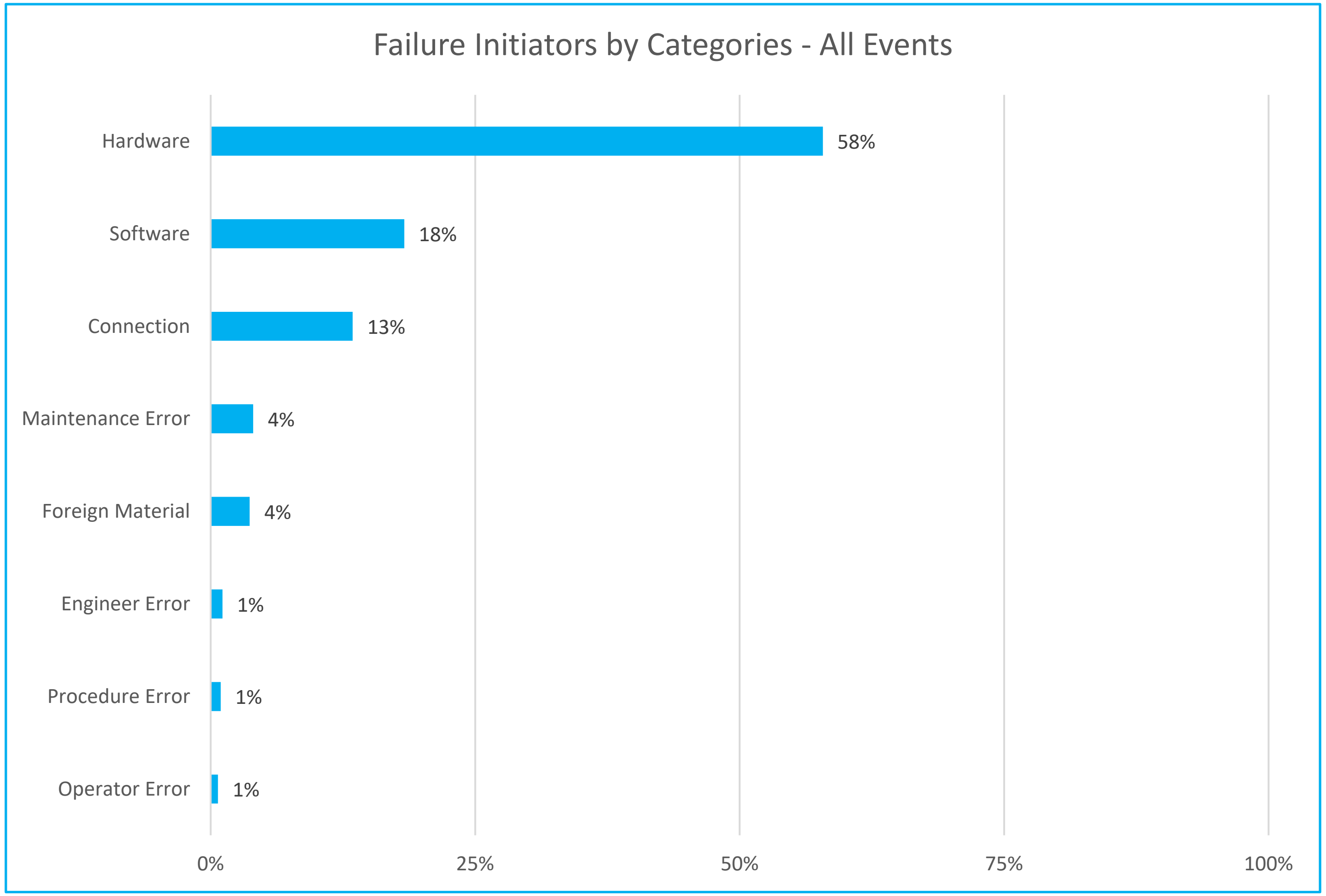
New System Logic



Preliminary I&C OE Research Data-2023

Preliminary 2023 results indicate failure initiator statistics (~1200 OE records reviewed):

- Hardware 58%
- Software 18%
- Bad/Loose Connections 13%
- Human Error 8%
- Foreign Material 4%

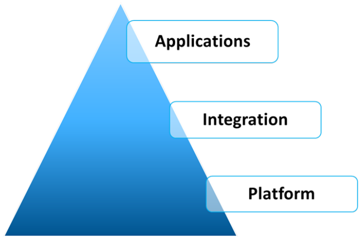


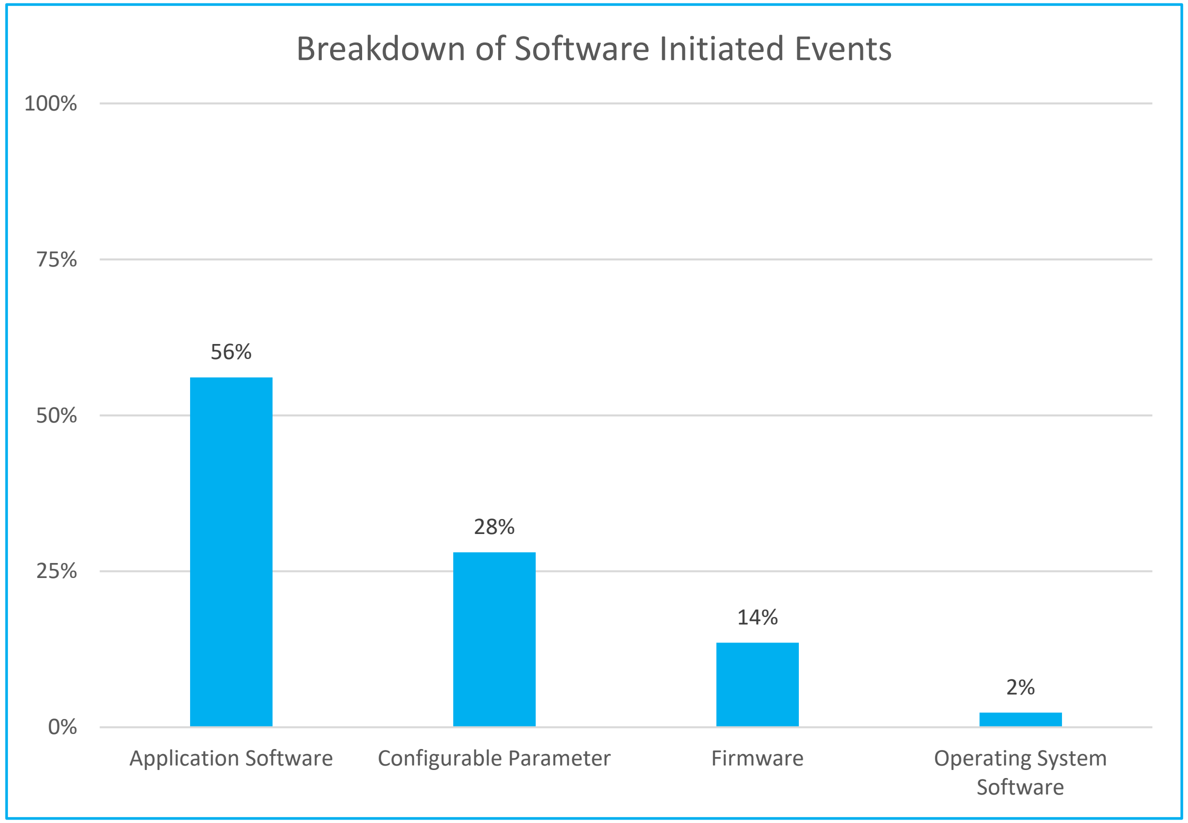
Preliminary I&C OE Research Data-2023

Approximately 18% of digital I&C events were initiated by software.

A breakdown of software-initiated failures by software classification is provided below and in the graph to the right:

- Application Software: 56%
- Configurable Parameter: 28%
- Firmware: 14%
- Operating System Software: 2%



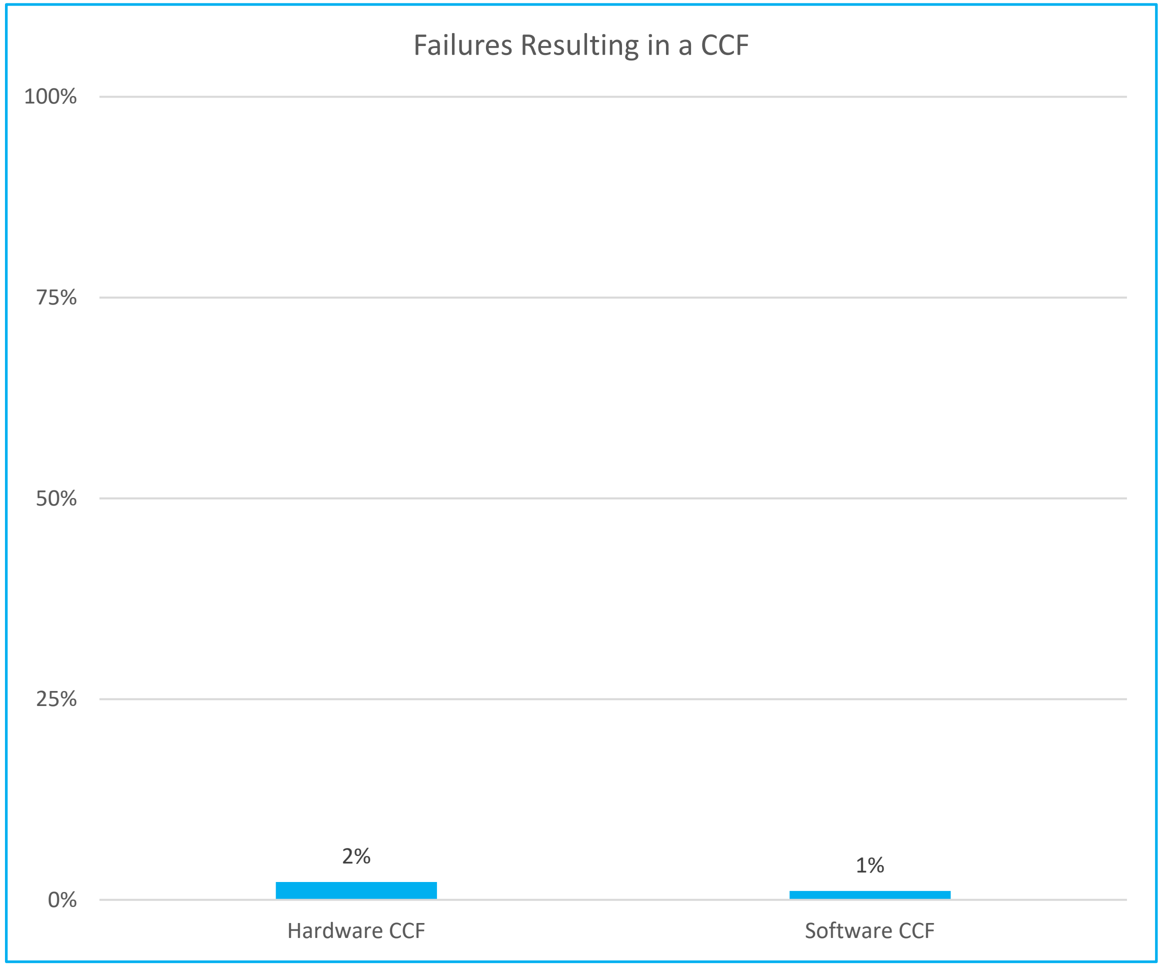


Preliminary I&C OE Research Data-2023

The table on the right provides a preliminary picture of I&C failures resulting in a hardware or software CCF **(loss of redundancy).**

A breakdown of software CCFs is provided below (out of ~1200 OE events):

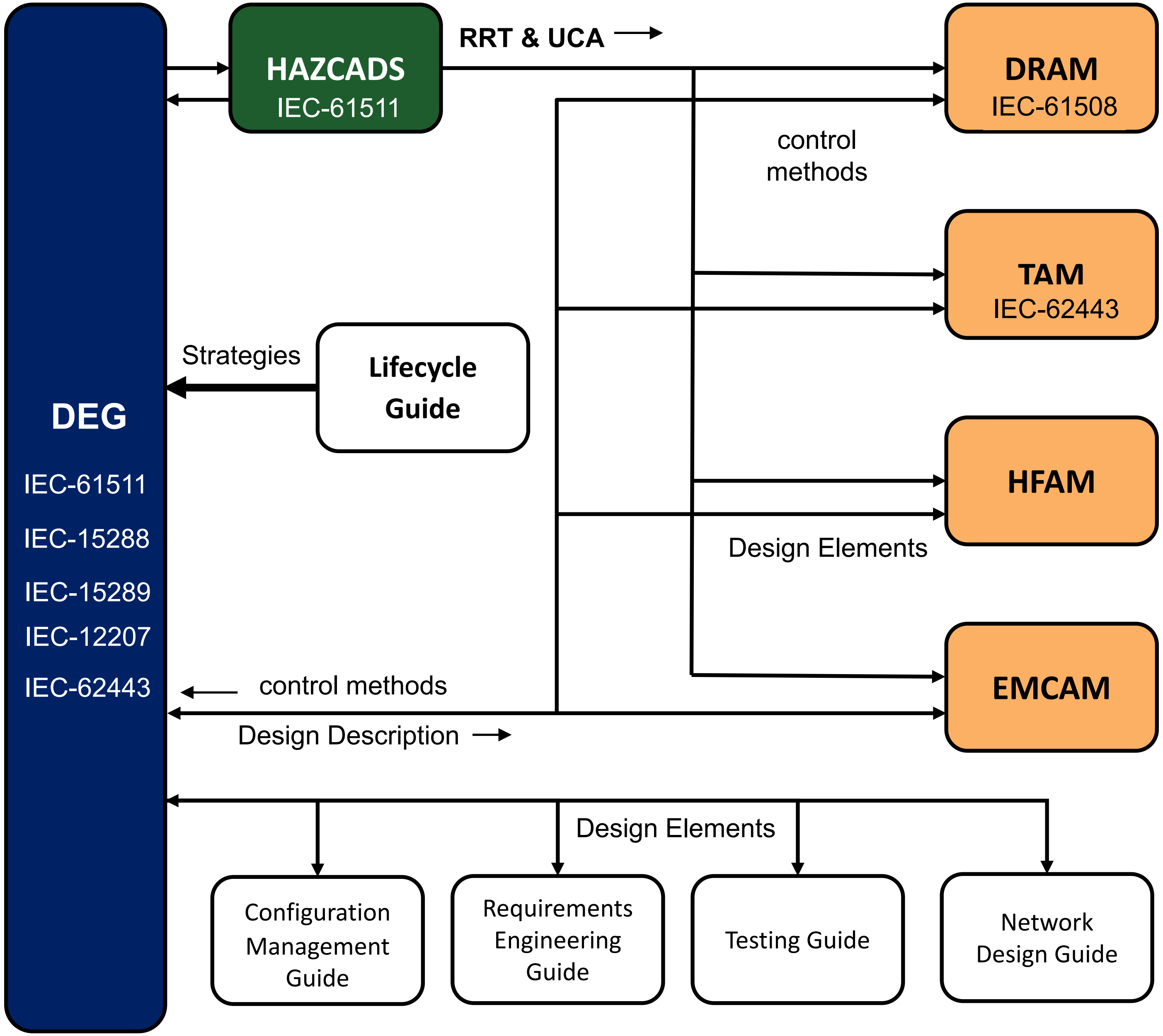
- Manufacturer Software Defect: 5
- Broadcast Storm: 3
- Over-ranged Transmitters: 3
- Incorrect Configurable Parameter: 1



IV. EPRI Digital Systems Engineering Framework

Digital Systems Engineering Framework Components

EPRI ID	Title	Description
3002011816	Digital Engineering Guide: Decision Making Using Systems Engineering **(DEG)**	Core Systems Engineering method Synthesized from IEC-15288, IEC-12207, and IEC 15298
3002016698	**HAZCADS:** Hazards and Consequences Analysis for Digital Systems - Revision 1	Risk Informed Digital Hazards Analysis using STPA and FTA. Implements Process Hazards Analysis (PHA)/Layers of Protection analysis (LOPA) for IEC-61511
3002018387	**DRAM:** Digital Reliability Analysis Methodology	Random and Systematic reliability analysis. Synthesized from IEC-61508 and identifies Loss Scenarios and control measures forms part of LOPA
3002012752	Cyber Security Technical Assessment Methodology: Risk Informed Exploit Sequence Identification and Mitigation, Revision 1**(TAM)**	Technical cyber assessment method. Identifies Exploit Sequences and develops the associated control measures
3002018392	**HFAM -** Human Factors Analysis Methodology for Digital Systems: A Risk-Informed Approach to Human Factors Engineering	Integration of HFE and HRA to risk-inform HFE. Evaluates and scores HFE designs on a task basis with HRA tool sets.
3002023438	Digital Systems Engineering: Digital I&C Lifecycle Strategy Guide	Provide guidance on the overall system lifecycle and provide detailed guidance on elements of IEC-15288 not covered by the DEG
3002015755	Digital Systems Engineering: Configuration Management Guideline	CM guidance for digital system. Develops the strategy and methods to identify and manage hardware and software configuration items.
3002015758	Digital Systems Engineering: Requirements Engineering Guideline	Provides guidance on engineering actionable, bounded, and testable requirements
3002028391	Digital Systems Engineering: Test Strategies and Methods	Provide guidance on testing digital components and systems
3002026367	Digital Systems Engineering: Network Design Guide (Fall 2023)	Provides Guidance on wired and wireless network design via detailed use cases
3002023743	**EMCAM:** Electromagnetic Compatibility Assessment Methodology (Fall 2023)	Provides a Risk informed and Graded approach to EMI/RFI
TBD (2024)	**DMG:** Digital Maintenance and Management Guide (Spring 2024)	O&M Phase Guide on maintenance of digital equipment



DEG –Synthesizes the Systems Engineering framework from IEC-15288. Includes all relevant Lifecycle topics. Takes strategic input from the Lifecycle guide

HAZCADS –Uses STPA/FTA to identify hazards and associated UCA . FTA and Risk Matrices develop a Risk Reduction Target (RRT) which informs the downstream processes. Implements a PHA/LOPA from IEC-61511.

DRAM – Identifies Hardware and Software reliability vulnerabilities and develops loss scenarios. Develops and Scores protect, detect , and respond/recover control methods using the RRT

TAM –Identifies cyber security vulnerability classes. Develops Exploit Sequences. Develops and Scores protect, detect , and respond/ recover control methods using the RRT

HFAM – Develops human actions and interfaces. Identifies and scores Human Reliability using the RRT

EMCAM – Identifies EMC vulnerability classes. Develops and scores protect, detect , and respond/ recover control methods using the RRT

RRT= Risk Reduction Target
UCA= Unsafe Control Action
STPA=System Theoretic Process Analysis
FTA= Fault Tree Analysis
LOPA= Layers of Protection Analysis
EMC= Electromagnetic Compatibility

Use of Models for Engineering within the Framework

The Digital Engineering Framework Currently leverages seven distinct models:

Model	Question to be Answered
Systems Engineering	What are the key systems elements, the functional allocation of those elements, and what is the reliability of those elements? (DEG)
Fault Trees	What are the Risk Sensitivities within a Dependency Scope? (HAZCADS,PRA)
STPA	What are the Systematic Hazards and Pathways? (HAZCADS, DRAM, TAM, HFAM,EMCAM)
Relationship sets	What are the system element dependencies and degree of independence across multiple relationships? (DEG)
HRA	What is the reliability of Human Actions? (HFAM)
Exploit Sequences	What are the exploit objectives, pathways to those objectives, and the method of exploit? (TAM)
Reliability Analysis	What are the failure frequencies that impact Probability of Failure on Demand-PFD? (DRAM)

- EPRI continues to leverage or develop additional models as the "questions" become better defined.
- Performance based design requires the design questions to be defined and bounded.

To be useful, a model must answer a key question

Relationship Sets

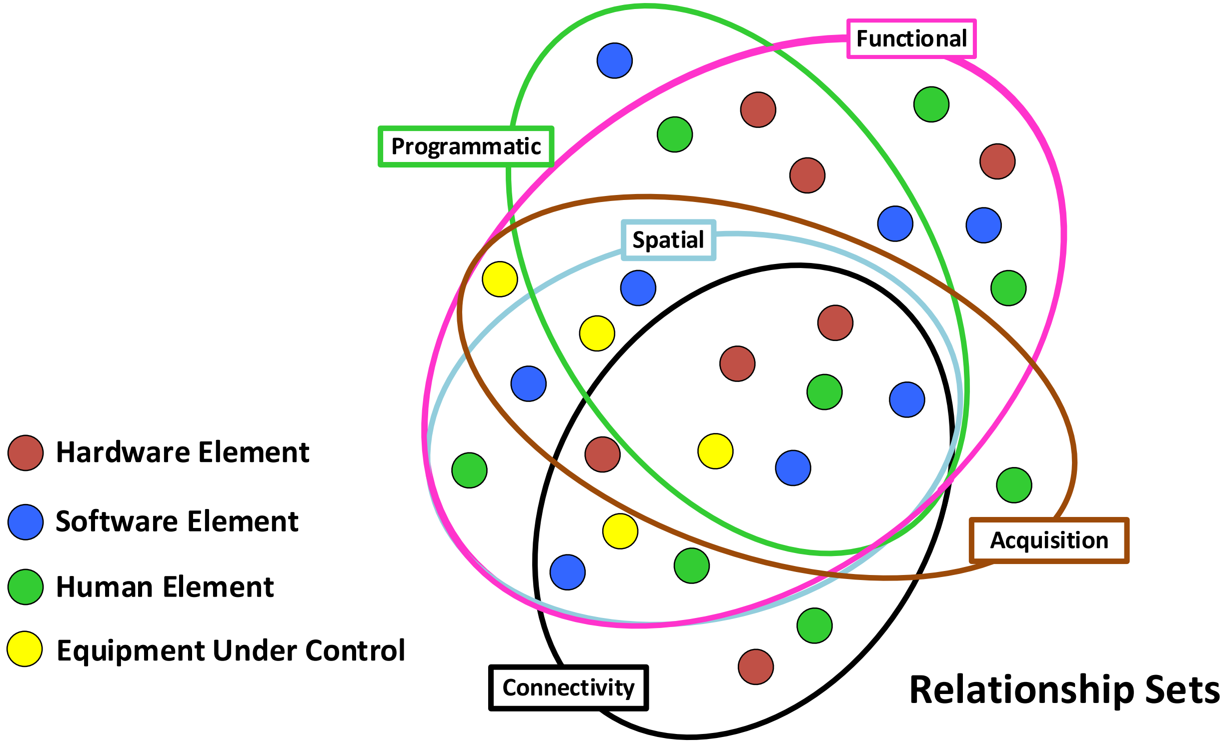
Relationship sets are an architecture view and contain all system elements scoped within the new design or design change.

There four of system elements

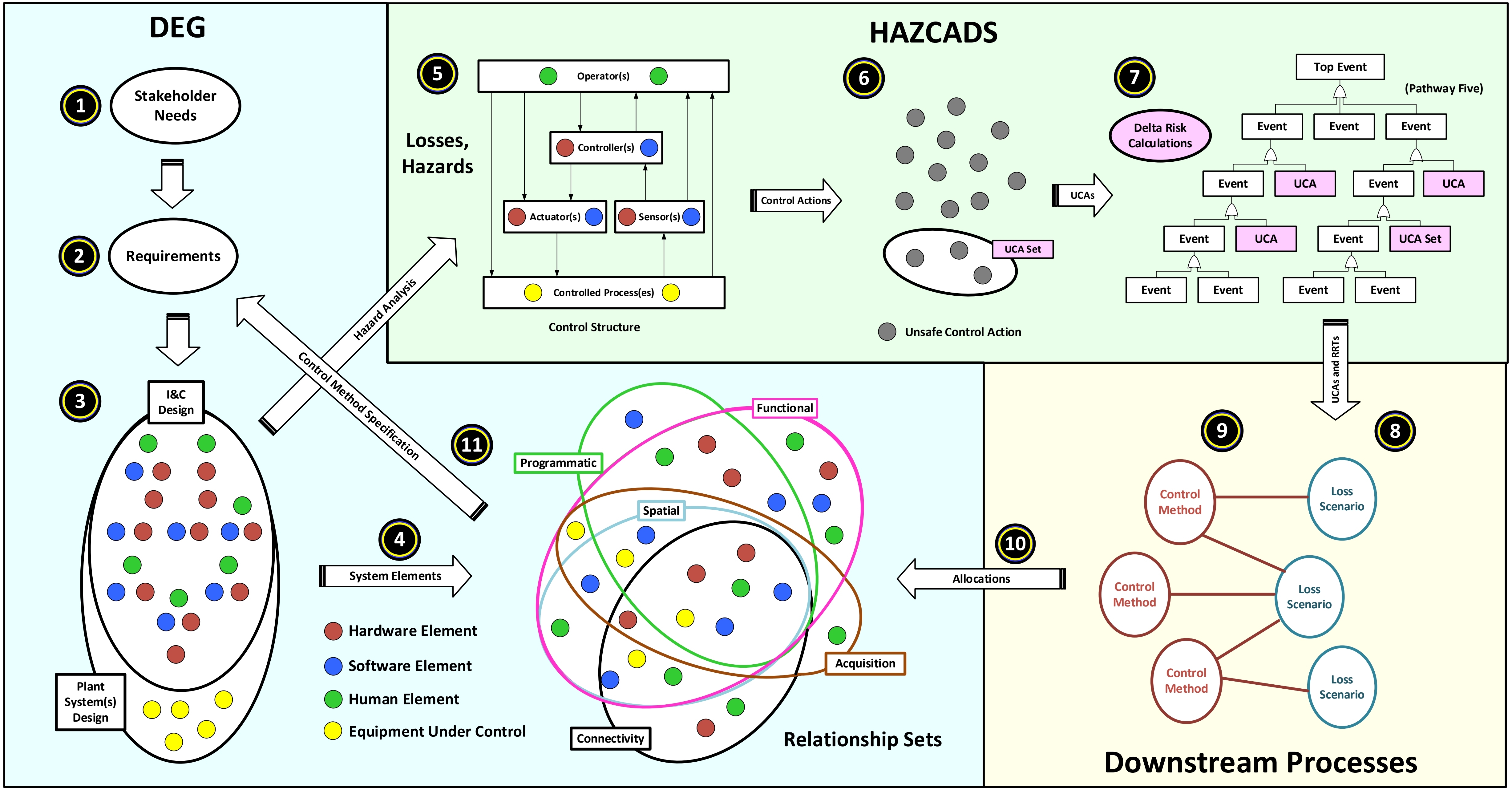
- Hardware
- Software
- Human
- Equipment Under Control

There are five relationship set types:

- Functional
- Connectivity
- Spatial
- Programmatic
- Acquisition



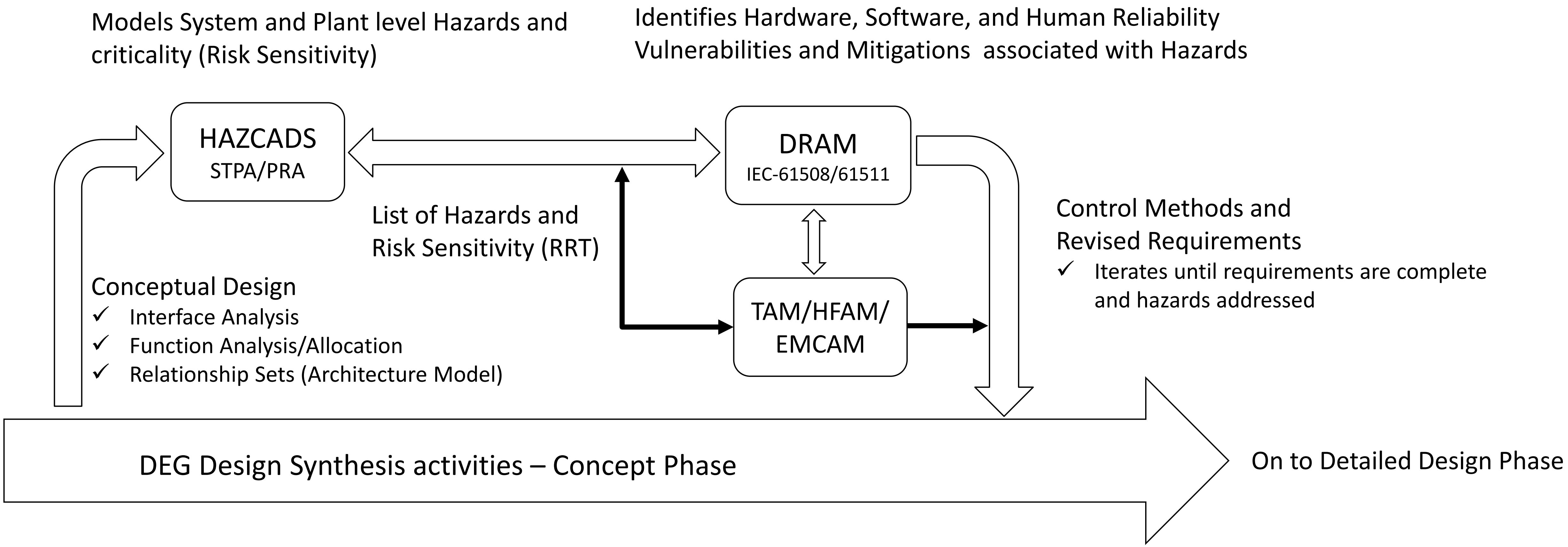
Models the Relationship Between System Elements



DEG
HAZCADS
1
Stakeholder Needs
2
Requirements
3
I&C Design
Plant System(s) Design
4
System Elements
Hardware Element
Software Element
Human Element
Equipment Under Control
5
Losses, Hazards
Operator(s)
Controller(s)
Actuator(s)
Sensor(s)
Controlled Process(es)
Control Structure
Hazard Analysis
Control Method Specification
Control Actions
6
UCA Set
Unsafe Control Action
UCAs
7
Top Event
(Pathway Five)
Delta Risk Calculations
Event
UCA
UCA Set
UCAs and RRTs
8
9
Control Method
Loss Scenario
10
Allocations
11
Programmatic
Functional
Spatial
Acquisition
Connectivity
Relationship Sets
Downstream Processes

Workflow- Conceptual Phase

Diagnostic Process to Identify Digital Hazards & Risk Sensitivities and Refine Requirements

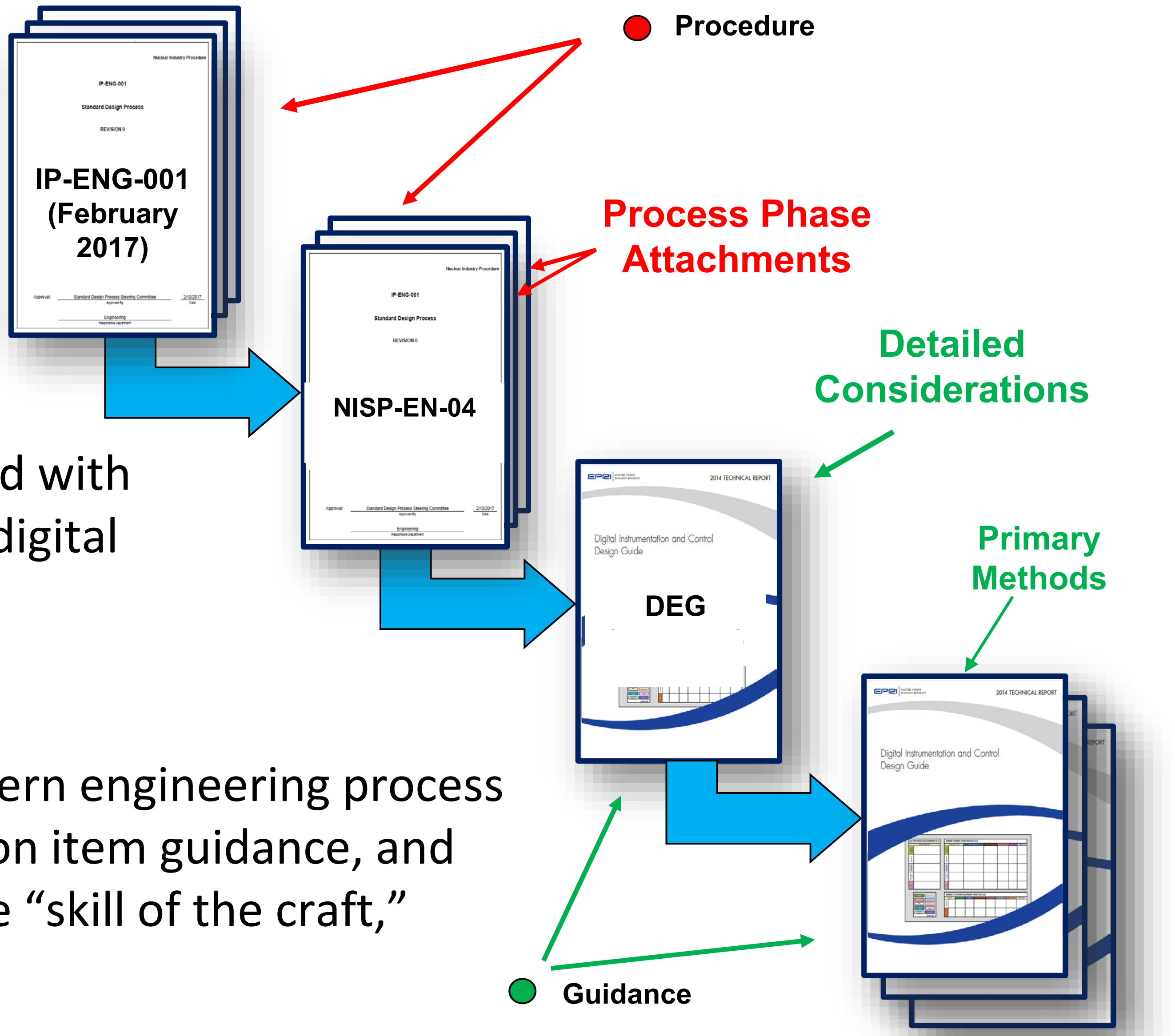


US DEG Implementation

- IP-ENG-001 (Standard Design Process)- Main Procedure
- NISP-EN-04 is the Digital Specific Addendum to the SDP under the same mandatory Efficiency Bulletin (EB 17-06)

- Same process phases as IP-ENG-001, tailored with DEG-specific supplemental information for digital implementations. **Including Cyber Security**.
- Provides the user with **"what to do"**

- DEG provides detailed guidance using a modern engineering process with digital design considerations, information item guidance, and division of responsibility methods to improve "skill of the craft,"
- Provides the user with **"How to Do"**
- **Digital Training/Tech Transfer completes the framework**



Supplemental Funded:
Digital Systems Engineering User Group - 3002022140

A forum for information sharing of digital specific material

Fall Meeting 2023
September 19th & 20th

- ✓ Operational Experience
- ✓ Lessons Learned
- ✓ Interactive community
- ✓ Common Design Packages
- ✓ Cyber Security Evaluations
- ✓ Member Feedback

Current Members to Date

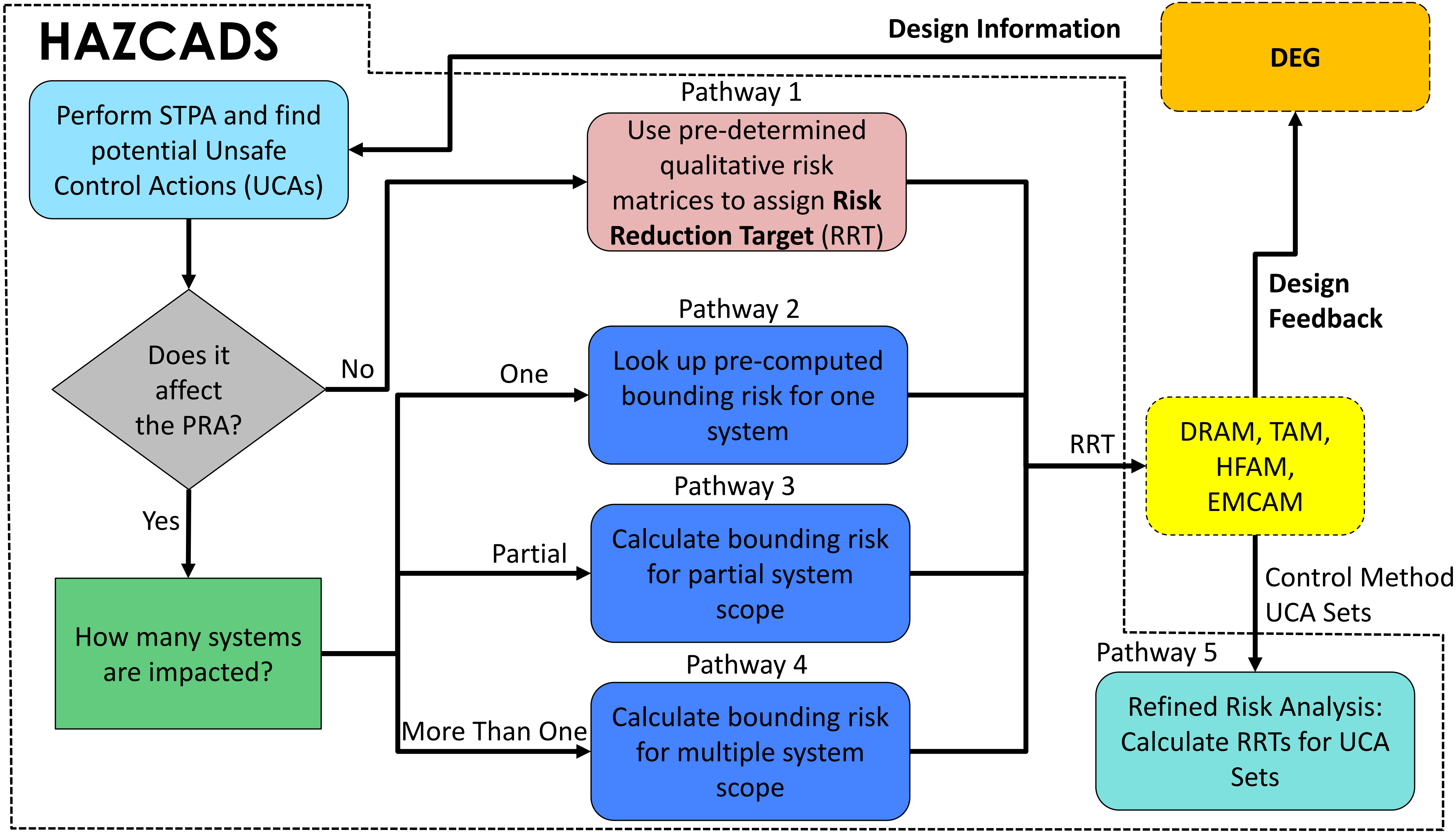
Framatome
Constellation Energy
Dominion Energy South Carolina, Inc.
Dominion Energy, Inc.
Duke Energy Corp.
Entergy Services, Inc.
Evergy Services (Wolf Creek)
Callaway (Ameren)
Palo Verde
Sargent & Lundy Engineers
Southern Company
Tennessee Valley Authority (TVA)
Vistra Corp. (Comanche Peak)
Westinghouse Electric Company, LLC
Xcel Energy
PSEG (Salem/Hope Creek)
South Texas Project (STP)
NPPD (Cooper)
Enercon Services
Curtiss Wright
Bruce Power

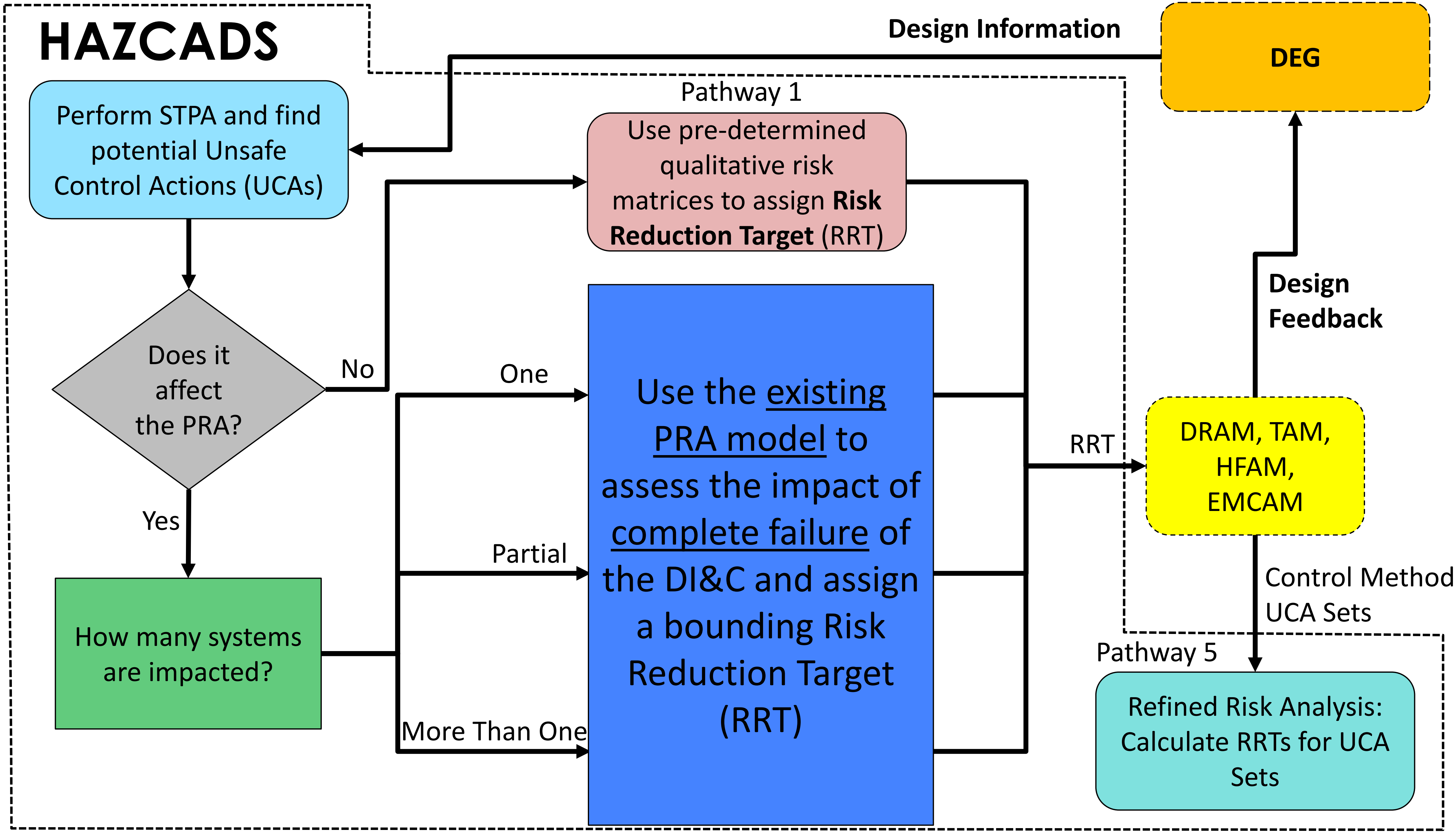
Current Activities:

- ✓ Harmonization of the DEG,HAZCADS,DRAM,TAM,EMCAM,HFAM, and Digital Lifecycle Strategy Guide. Improves coordination between products and updates with current OE.
- ✓ Roll out of the member sharing website.
- ✓ Nuclear Digital Project Experience Baseline 2022 published. Updated annually, members of this supplemental can download EPRI Technical Report 3002023748. This report provides a baseline of installed digital equipment across members.

V. Risk Informing the Design and Operation of Digital Systems including PRA integration

HAZCADS: Hazards and Consequences Analysis for Digital Systems - Revision 1
3002016698


HAZCADS
Design Information
DEG
Perform STPA and find potential Unsafe Control Actions (UCAs)
Pathway 1
Use pre-determined qualitative risk matrices to assign **Risk Reduction Target** (RRT)
Does it affect the PRA?
No
Yes
Pathway 2
One
Look up pre-computed bounding risk for one system
Pathway 3
Partial
Calculate bounding risk for partial system scope
Pathway 4
More Than One
Calculate bounding risk for multiple system scope
How many systems are impacted?
RRT
DRAM, TAM, HFAM, EMCAM
Design Feedback
Control Methods UCA Sets
Pathway 5
Refined Risk Analysis: Calculate RRTs for UCA Sets


HAZCADS
Design Information
DEG
Pathway 1
Perform STPA and find potential Unsafe Control Actions (UCAs)
Use pre-determined qualitative risk matrices to assign Risk Reduction Target (RRT)
Does it affect the PRA?
No
Yes
One
Partial
More Than One
How many systems are impacted?
Use the existing PRA model to assess the impact of complete failure of the DI&C and assign a bounding Risk Reduction Target (RRT)
RRT
Design Feedback
DRAM, TAM, HFAM, EMCAM
Control Methods UCA Sets
Pathway 5
Refined Risk Analysis: Calculate RRTs for UCA Sets

Risk Ranking

- HAZCADS uses a bounding risk assessment process, when the risk is calculated quantitatively through a PRA model
  - This approach evaluates all failures including any common cause (not just software common cause failures)
- The risk sensitivity assessment is based on the change in risk if the UCAs occurred

RRT	Change in Core Damage Frequency – CDF (per year)	Change in Large Early Release Frequency – LERF (per year)
D	ΔCDF ≤ 1E-6	ΔLERF ≤ 1E-7
C	1E-6 < ΔCDF ≤ 1E-5	1E-7 < ΔLERF ≤ 1E-6
B	1E-5 < ΔCDF ≤ 1E-4	1E-6 < ΔLERF ≤ 1E-5
A	1E-4 < ΔCDF ≤ 1E-3	1E-5 < ΔLERF ≤ 1E-4
Change the Design	ΔCDF > 1E-3	ΔLERF > 1E-4

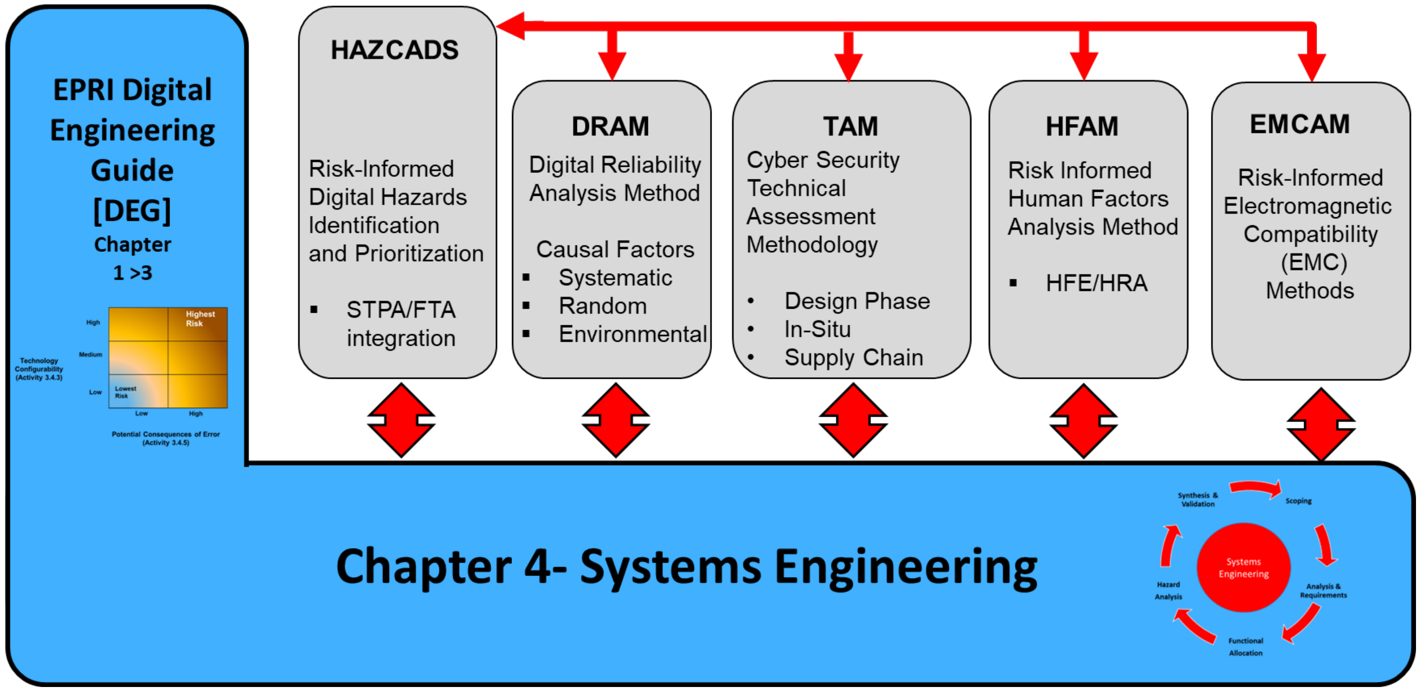
Anticipated Concern: An RRT of "A" Is Really High!

- Delta risks of 10^{-4}/yr to 10^{-3}/yr are really high and normally would not be allowed for risk-informed applications
- True, but this is not the increase in risk of the system – this is the risk if the entire system fails
- This is also the risk of the current system were it to completely fail
- In reality, we expect digital I&C upgrades to reduce risk compared to the existing, analog systems as demonstrated in other safety-related industries

RRT	Change in Core Damage Frequency – CDF (per year)	Change in Large Early Release Frequency – LERF (per year)
D	ΔCDF ≤ 1E-6	ΔLERF ≤ 1E-7
C	1E-6 < ΔCDF ≤ 1E-5	1E-7 < ΔLERF ≤ 1E-6
B	1E-5 < ΔCDF ≤ 1E-4	1E-6 < ΔLERF ≤ 1E-5
A	1E-4 < ΔCDF ≤ 1E-3	1E-5 < ΔLERF ≤ 1E-4
Change the Design	ΔCDF > 1E-3	ΔLERF > 1E-4

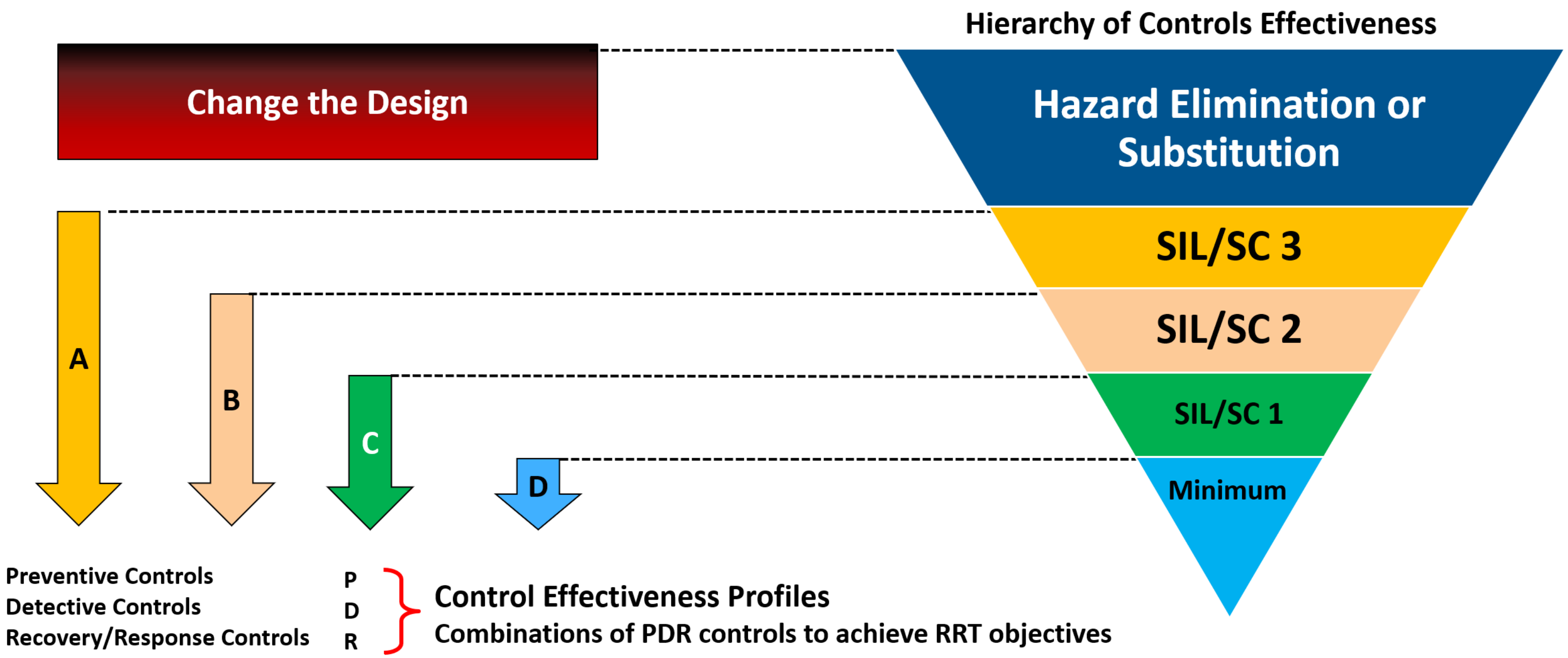
Downstream Processes (after HAZCADS)

- The RRT from HAZCADS is used by the "downstream processes" in the EPRI digital framework
- Each downstream process assigns control methods to protect against a type of failure
  - DRAM: Assigns control methods to account for random and systematic errors
  - HFAM: Assigns control methods based on human factors
  - TAM: Assigns control methods based on cyber security
  - EMCAM: Assigns control methods based on electromagnetic compatibility

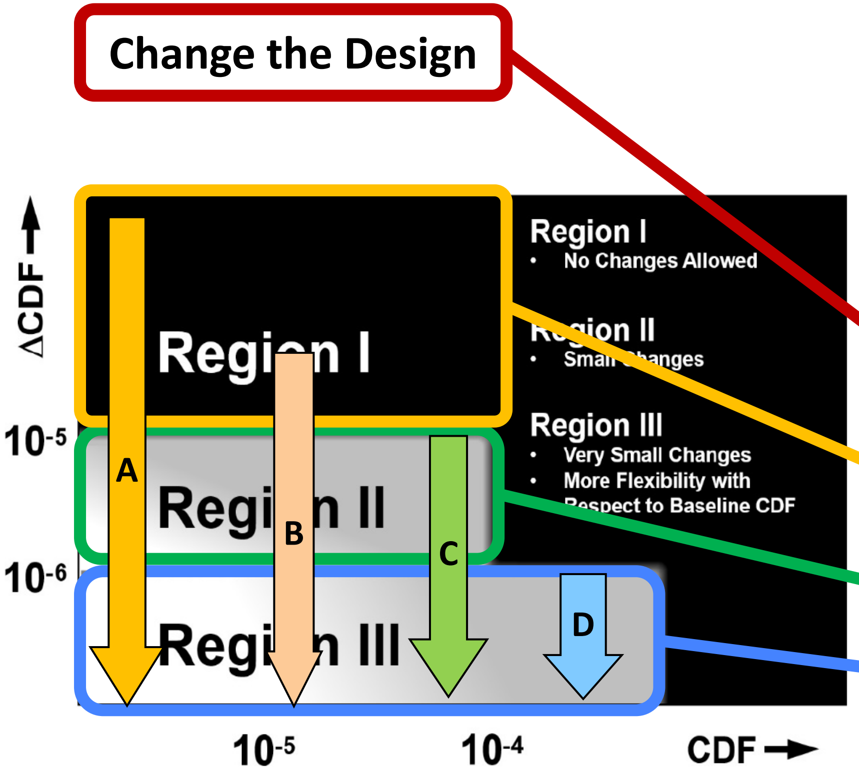


Control Methods

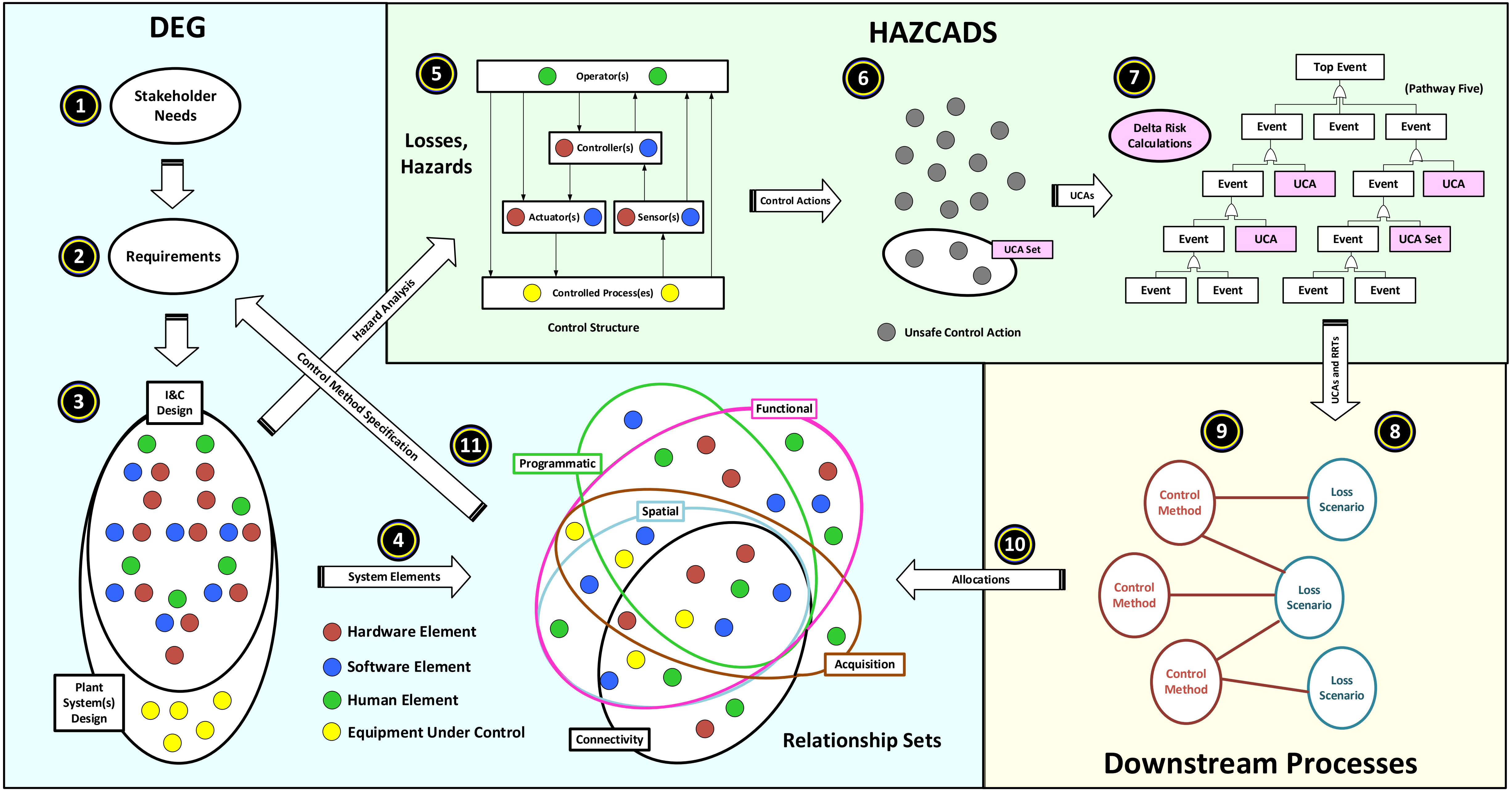
- DRAM, TAM, HFAM, and EMCAM:
  - Determine causal factors for the UCAs
  - Establish control methods that are aimed at addressing those causal factors
  - Score the control methods against the RRT from HAZCADS
- This process may impose new design requirements or add implementation requirements on the system



RRT Acceptance Criteria



RRT	Change in Core Damage Frequency – CDF (per year)	Change in Large Early Release Frequency – LERF (per year)
Change the Design	ΔCDF > 1E-3	ΔLERF > 1E-4
A	1E-4 < ΔCDF ≤ 1E-3	1E-5 < ΔLERF ≤ 1E-4
B	1E-5 < ΔCDF ≤ 1E-4	1E-6 < ΔLERF ≤ 1E-5
C	1E-6 < ΔCDF ≤ 1E-5	1E-7 < ΔLERF ≤ 1E-6
D	ΔCDF ≤ 1E-6	ΔLERF ≤ 1E-7

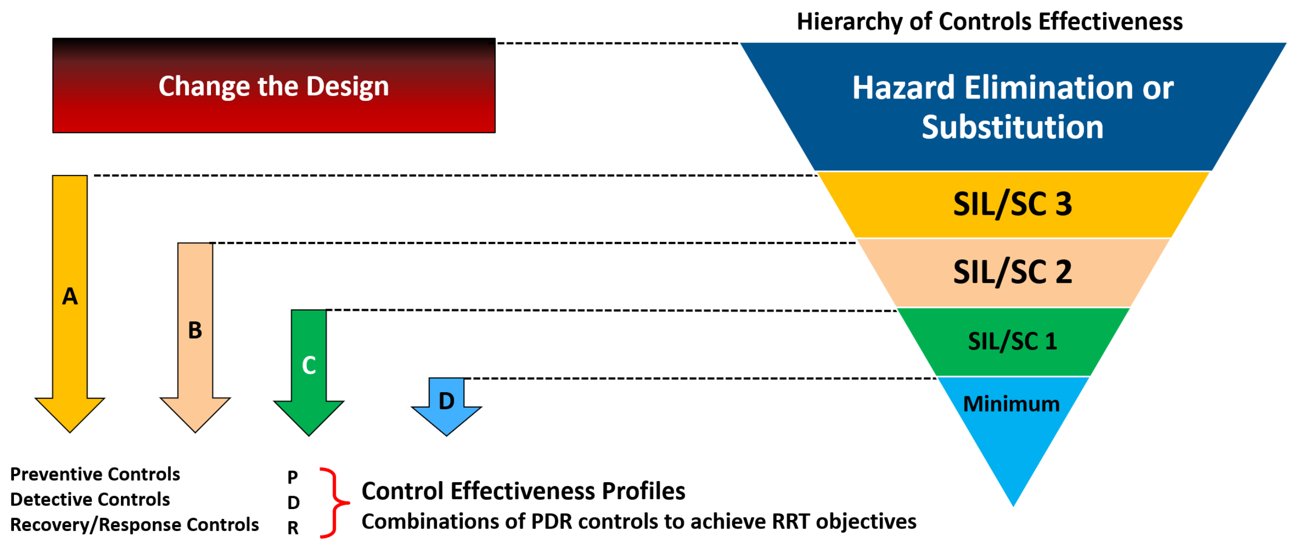

DEG
HAZCADS
1
Stakeholder Needs
2
Requirements
3
I&C Design
Plant System(s) Design
4
System Elements
Hardware Element
Software Element
Human Element
Equipment Under Control
5
Losses, Hazards
Operator(s)
Controller(s)
Actuator(s)
Sensor(s)
Controlled Process(es)
Control Structure
Hazard Analysis
Control Method Specification
Control Actions
6
UCA Set
Unsafe Control Action
UCAs
7
Top Event
(Pathway Five)
Delta Risk Calculations
Event
UCA
UCA Set
UCAs and RRTs
8
9
Control Method
Loss Scenario
10
Allocations
11
Programmatic
Functional
Spatial
Acquisition
Connectivity
Relationship Sets
Downstream Processes

Special Note on Software Common Cause Failures

- I&C Operating Experience (OE) (nuclear and non-nuclear) indicates that most systematic failures are a result of:
  - Latent design defects due to inadequate requirements
  - Uncontrolled system interactions
- Misapplication of diversity as a means to address the potential for software CCF can contribute to additional system complexity, which could increase the potential for latent errors
- HAZCADS identifies and risk ranks the potential systematic errors (not just software CCFs) and the other tools in the EPRI digital framework establish control methods to address them

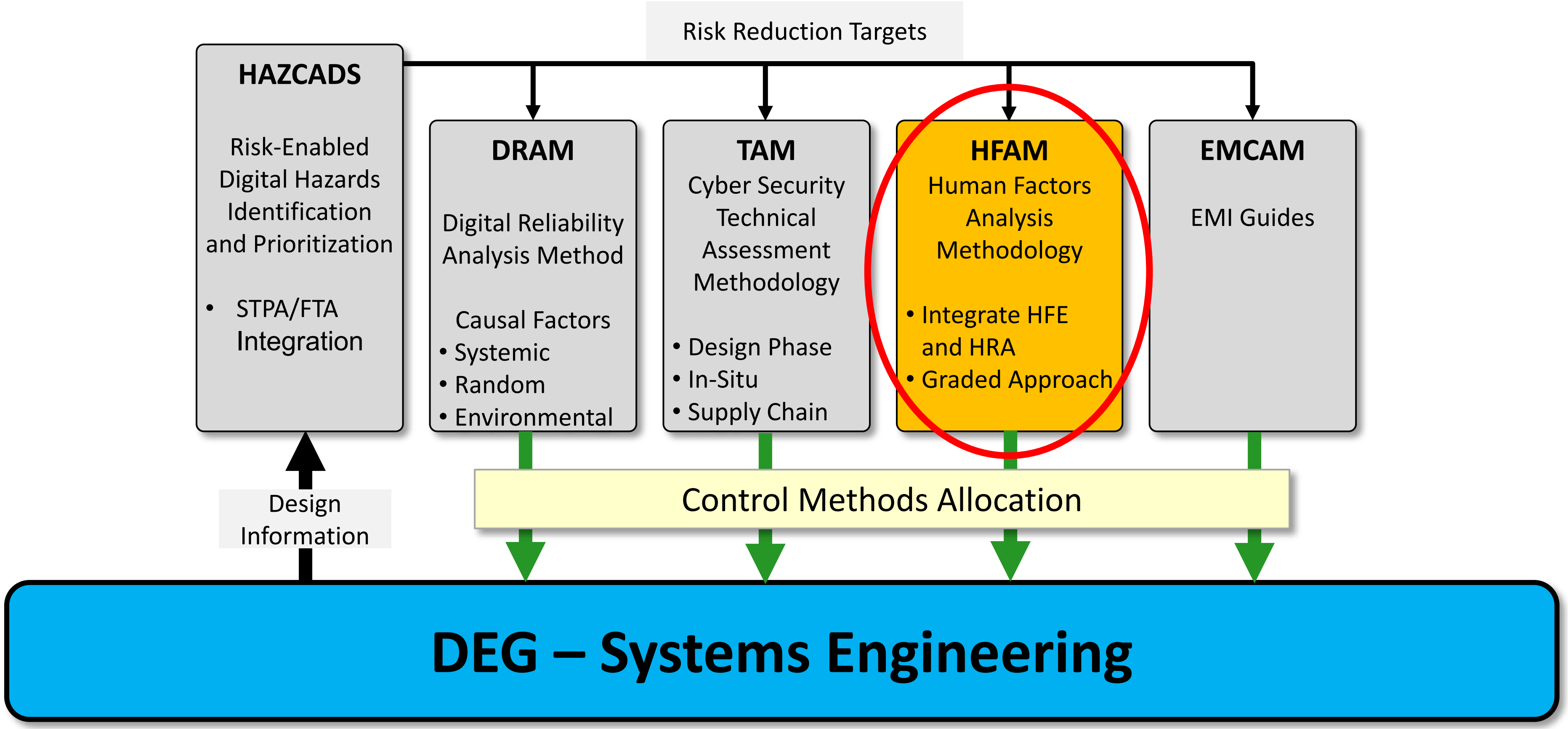
Summary of EPRI's DI&C Risk-Informed Approach

1. Identify what can go wrong (what could be unsafe) in the system
2. Establish a <u>bounding risk assessment</u> of the identified potential errors
3. Revise system requirements and/or assign control methods to the system commensurate with the risk
4. If needed, refine the risk assessment based on identified loss scenarios that cannot meet the RRT

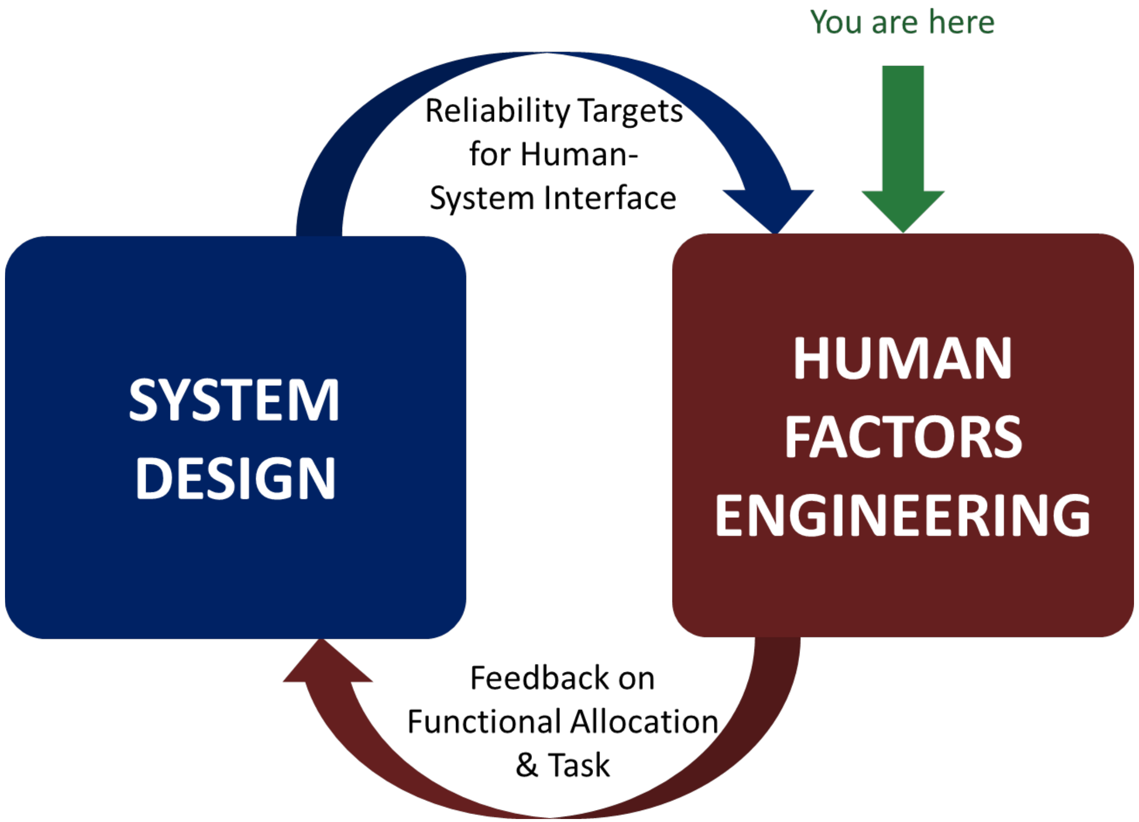


HFAM - Human Factors Analysis Methodology for Digital Systems: A Risk-Informed Approach to Human Factors Engineering 3002018392

HFAM = Part of the DEG Framework



What is a Risk-Informed HFE Approach?

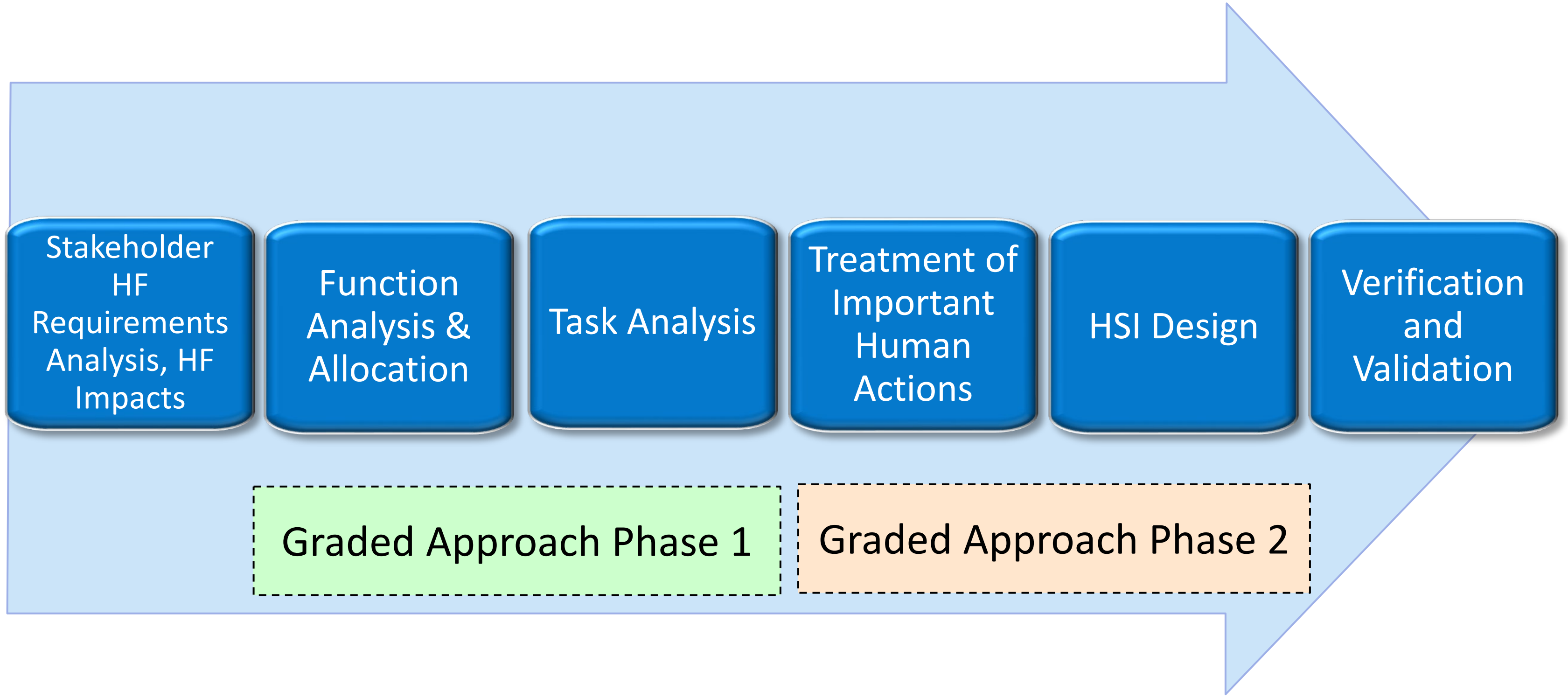


How HFAM applies information about risks to analysis and design activities to:

1. Apply a graded approach to determine required HFE activities
2. Design the system to fit human abilities and limitations
3. Give adequate prominence to human error in system design - prevent or mitigate unsafe control actions.
4. "Design Out" potential system errors to avoid:
   - unnecessary interactions
   - instructions that are hard to understand
   - poor use of visual design
   - bad or no error trapping
   - subjecting the human to extreme physical or mental stress or workload
5. Develop evidence to demonstrate that the system will be safe and will not be or cause a hazard to people or environment.

Key Features of HFAM*

1. Integrated with a comprehensive systems engineering process (EPRI DEG)
2. Integrated with risk insights from HAZCADS
3. Provides a graded approach with 2 levels of gradation
   – Phase 1 based on the scope of the design within the DEG
   – Phase 2 based on the RRTs from HAZCADS
4. Integrates the use of HRA methods to assess the reliability of human tasks

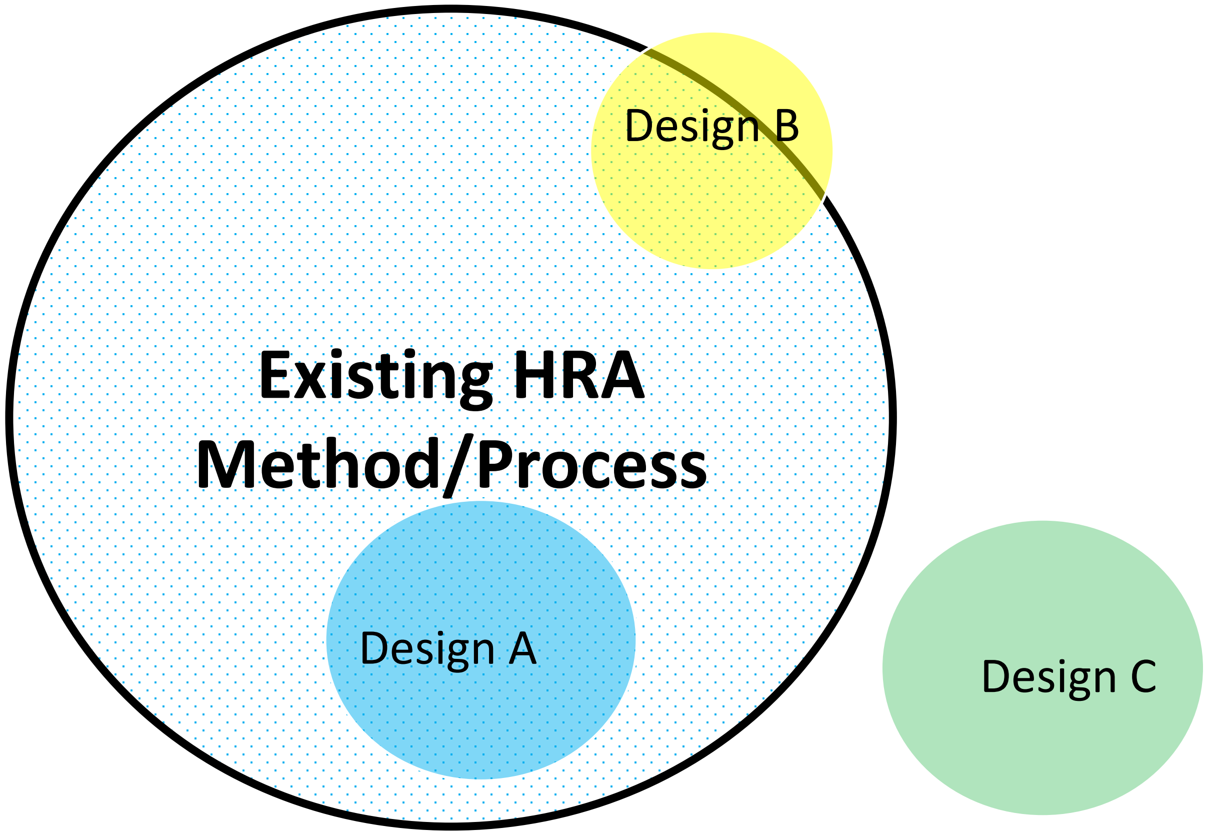


****Human Factors Analysis Methodology for Digital Systems:*** *A Risk-Informed Approach to Human Factors Engineering*
[EPRI 3002018392; 2021]

EPRI

Digital HRA Research

- What's Different?
- Plant Orientation & Data Collection
- Identification of Human Failure Events
- Definition & Task Analysis
- Quantification



Graded approach to method development, starting with current methods

Data Sources in Use Today

Three major sources for initial evaluation

1. Halden & Idaho National Lab experimental data (broad range of design features, but qualitative or small samples)
2. Literature and operational experience review (broad range of design features, but qualitative or small samples)
3. Training simulation data* (large quantitative data set, but based on one design / concept of operations)

How can we combine data to understand the reliability of human interactions in a digital environment?

- To be useful in human factor engineering?
- To be useful in validating or updating HRA methods?
- With data in a useful format, what else could we inform?

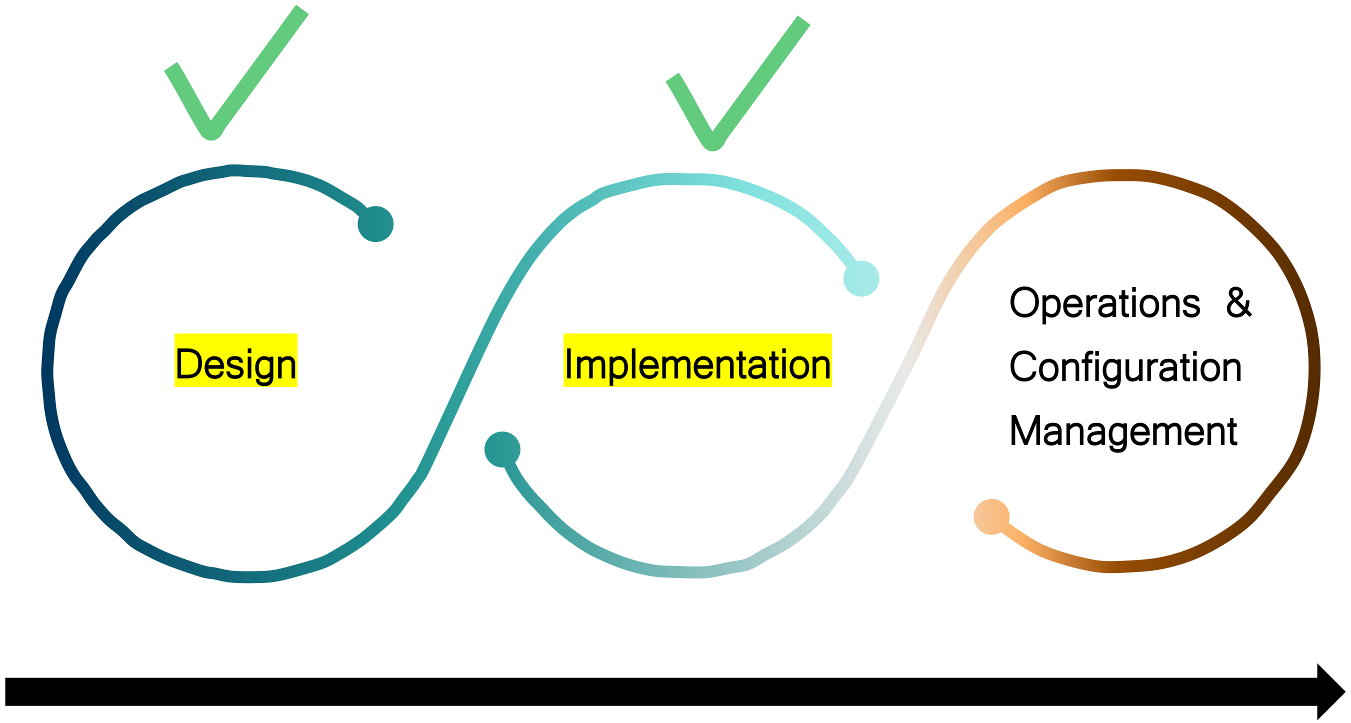
***Data to Support Human Reliability Analysis (HRA) for Digital Environments:**
Data and Analysis from Korean Simulator Studies; EPRI 3002020751; 2021

A Special Note on Human Errors of Commission – Using the Right Analysis Tools for the Right Tasks

- In the PRA, human cognitive errors of commission (EOC) are typically "ground-ruled out" unless a specific cause is identified
  - Other processes are used to minimize the likelihood and protect against EOCs
  - When modeled, limited treatment of consequences are considered
- Consideration of expanded treatment of EOCs in new standards for plants with large amounts of automation
- But…STPA is designed to find these types of systematic errors
  - Use HRA experience with EOCs to build loss scenarios
  - Design out high-consequence errors and provide adequate control methods for other potential unsafe actions
- Not necessarily something we need to "quantify" in the PRA, but is a candidate to be integrated in other ways

PRA Enhancements for Digital Technology for the O&M Phase

A PRA Look at Digital Systems

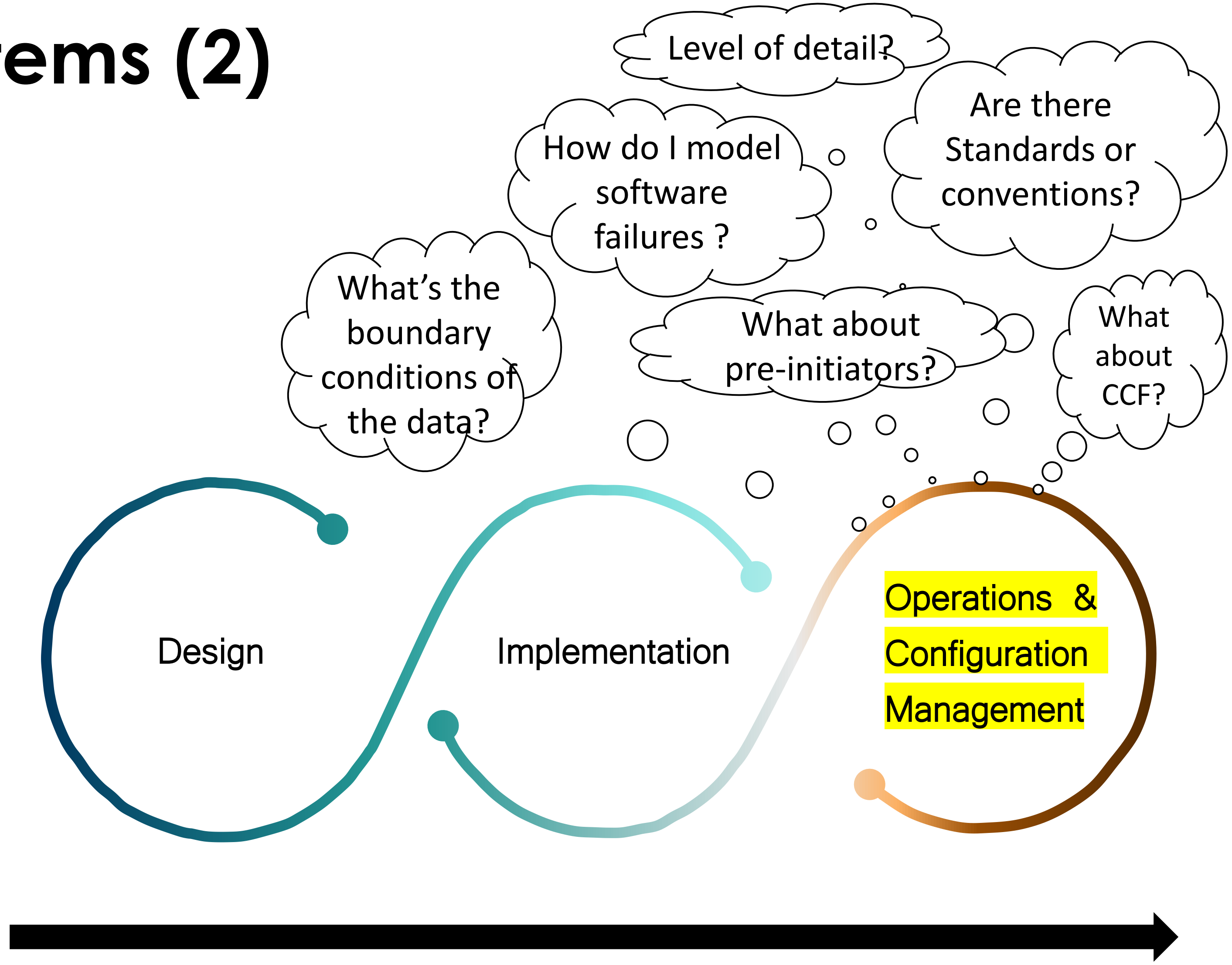


Coherent approach to assess and address risk across lifecycle

- We have an effective tool for risk informing the design and implementation phases – HAZCADS [EPRI 3002016698] and associated processes

A PRA Look at Digital Systems (2)

- We need something equally useful for "day-to-day" use once the digital I&C mods are installed
  - Simple to build, simple to understand, and "roughly right" modelling and data – that can be implemented and used now and refined over time
- Research: Capture current state of knowledge, data and use cases
- Consensus: Socialize with international technical community
- Continuous improvement: Reflect additional operating experience as it becomes available
- Consistency: Iterate as HAZCADS and related processes are refined



Coherent approach to assess and address risk across lifecycle

Proposed Approach (In Progress)

- Research in progress
  - Collecting/developing examples and use cases to test proposed approach
  - Re-look at the data, existing guidance and lessons from HAZCADS
  - Ensure consistency with RIDM framework
  - Ensure plant reflects "as built, as operated", including change management

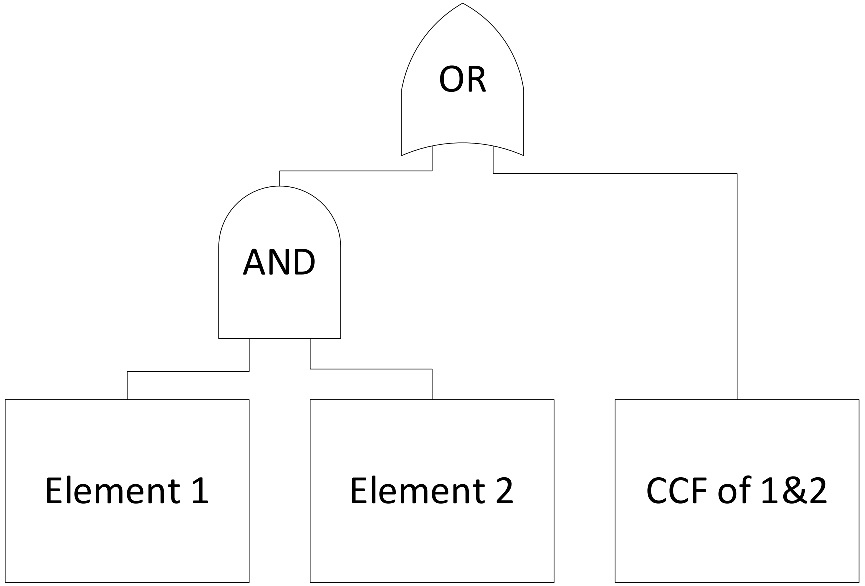
- Incorporation of the design into the PRA should
  - Be consistent in insights from the design process
  - Be consistent with overall PRA modelling approach
  - Continue to reflect the "as-built, as-operated" plant

Proposed Approach (In Progress) (2)

- Digital systems should be modeled at a reasonable level of detail adequate to support decision making
  - Over decomposition introduces unnecessary modeling complexity
  - Modeling level should match boundary conditions of collected data
  - Software should not be separated from hardware (all software is implemented through a hardware system) → *Functional Reliability*

- Fundamental Assumption: **Control Methods** implemented through the design process reduces the risk to *acceptably low levels of risk*
  - Both for functional reliability and common cause failures
  - Qualitative analysis reflects the best state of knowledge (best-estimate); this is key for consistency between design and assessment phases

Capturing Consequence of Digital Failures* in the PRA



Cause and Effect Relationship

- The cause-effect relationship of potential unsafe control actions (UCAs) that survived to final design should be retained in the PRA or documentation:
  - UCAs with non-unique consequences should be mapped to existing basic events for documentation
  - UCAs with unique consequences can be included explicitly in the model
- Logic reassessed as the PRA evolves to reflect the as-built, as-operated plant

*Can be hardware, software or human error; systematic or random.

Considering Likelihood

Two potential approaches for capturing likelihood of a functional failure (research currently investigating both approaches):

1. Create "generic" failure rates based on available data + qualitative insights and include that probability in the model.
   - Data from existing EPRI and industry research and databases
   - Qualitative insights based on strength of the implemented control methods, per the downstream processes

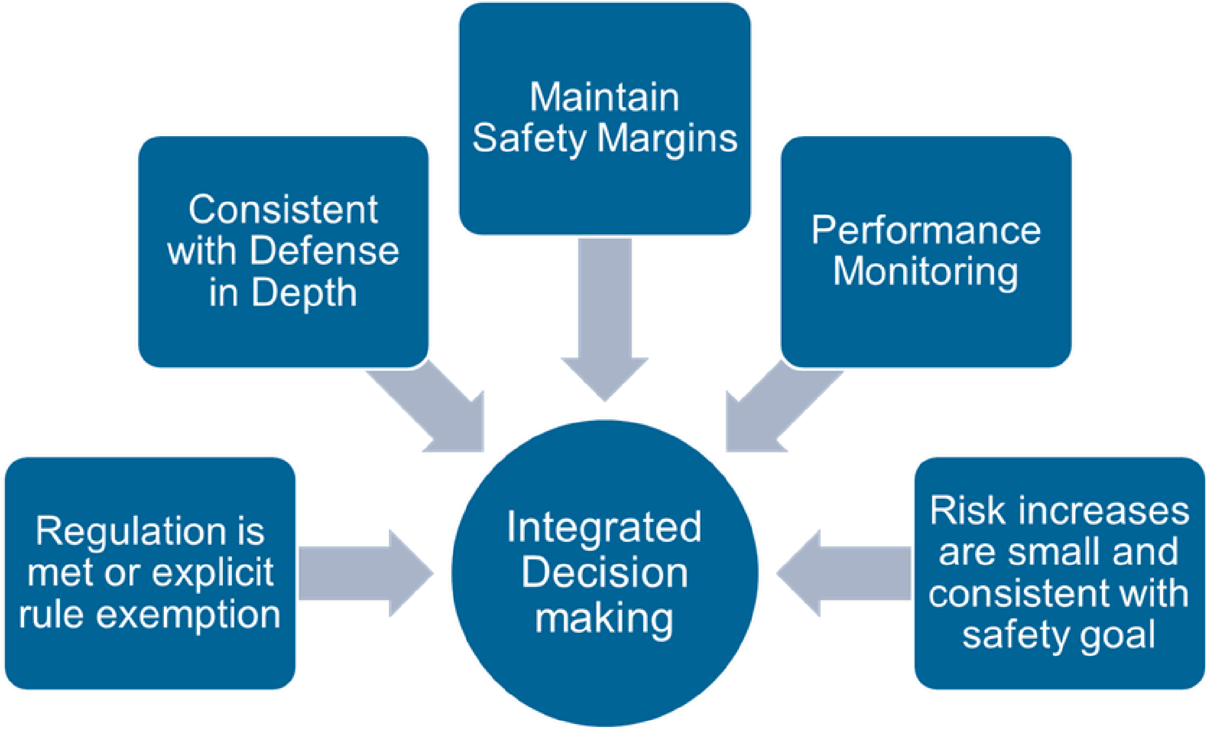
2. Do not quantify in base model, but use sensitivity studies to understand if risk has changed
   - Control methods were determined to be adequate at the design stage to mitigate against base RRT level
   - Sensitivity studies can be used to understand if the control methods continue to be adequate due to other changes in the model/plant

- Long term industry data gathering needs to be put into place and match the boundary conditions of data application
  - Normal data updates at the equipment or function level will indicate if there is a performance issue and the control methods need to be re-evaluated.

Consistency with Processes for Treatment of Uncertainty

- Risk-Informed Decision Making (RIDM) is the process of using risk information with other pertinent information to make decisions

- NUREG-1855 and EPRI companion document (1026511) provides guidance on how to deal with uncertainties in risk informed decision making
  - Recognizes that conservative treatment does not lead to best decision making; can mask insights or be overly burdensome
  - Provides guidance for dealing with large uncertainties through the RIDM process
    - In this case, performance monitoring through data updates is key to ensuring the system behaves as expected
    - Defense-in-depth is key to understanding the reliability at the plant facility level

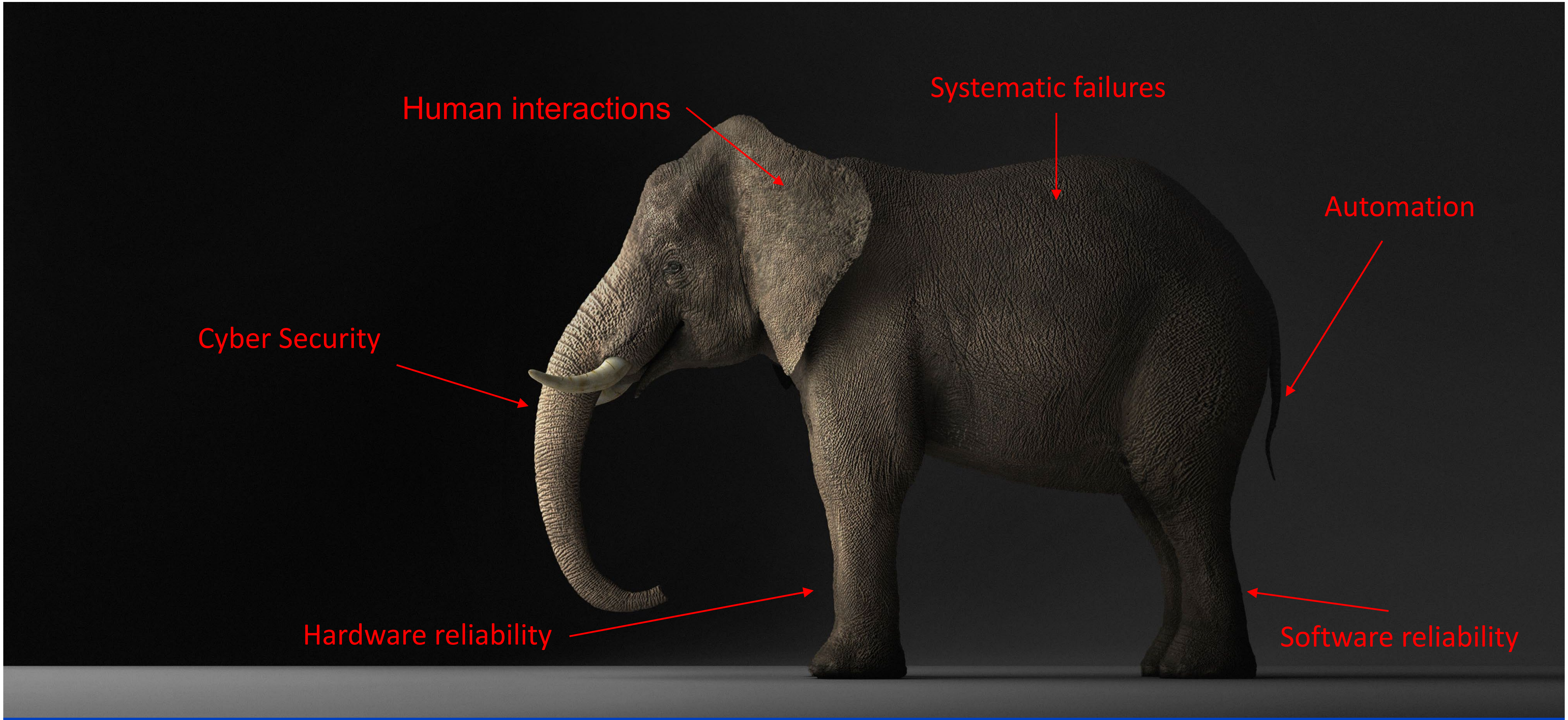


Modelling DI&C in the PRA – Summary

- Software reliability is directly proportional to the systematic controls and the design/implementation constraints.
- By adding the risk-ranking (RRTs) to what could go wrong (UCAs), HAZCADS provides the designers the information they need to assign the appropriate level of control methods to obtain an adequate baseline risk
- If the design is adequately reliable, PRA should be used to ensure the as-built, as-operated plant continues to remain adequately reliable
- Performance monitoring through data gathering should match the PRA modelling through appropriate boundary conditions
  - Do we have the right data collection frameworks in place?
- *Research is still in progress*

Data, cause-effect relationship is important; explicit quantitative modelling is not

Looking at the Whole Elephant



…digital is new, but not really…


Together...Shaping the Future of Energy®