Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Meeting of the Advisory Committee On Reactor Safeguards

Joint Digital Instrumentation and Control Systems and Reliability and PRA Subcommittees

Docket Number: N/A

Location: Rockville, Maryland

Date: November 19, 2014

Work Order No.: NRC-1229 Pages 1-234

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1323 Rhode Island Avenue, N.W.

Washington, D.C. 20005
(202) 234-4433

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

JOINT DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

AND RELIABILITY AND PROBABILISTIC RISK ASSESSMENT

SUBCOMMITTEES MEETING

+ + + + +

WEDNESDAY

NOVEMBER 19, 2014

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

COMMITTEE MEMBERS:

JOHN W. STETKAR, Chairman

RONALD G. BALLINGER, Member

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR. Member

JOY REMPE, Member

STEPHEN P. SCHULTZ, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

T-A-B-L-E O-F C-O-N-T-E-N-T-S

Presentation on Digital Failure Modes by EPRI 5

Presentation from Staff on Failure Modes Research 93

Public Comment 24

Closing Comments by Members 126

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

(1:03 p.m.)

CHAIRMAN STETKAR: We are in session. Good morning. This is the second day of the Joint Meeting of the Digital I&C and Reliability PRA Subcommittee meetings to discuss modeling of digital instrumentation control systems in PRA.

I'm John Stetkar, Chairman of the Subcommittee meeting. Members in attendance today are Steve Schultz, Dennis Bley, Ron Ballinger, Charlie Brown, and Joy Rempe. We're joined again with our consultant, Myron Hecht, and Christina Antonescu is our designated federal official.

I'll remind everybody please check all of your little communications devices and turn them off. People with large communication devices, please turn them off also.

Joy still has an organizational conflict of interest that you announced yesterday. That's still in effect. I think we've settled all the administrative things. We are being recorded. So, we will have a transcript. With that, we'll turn over the session to Ray Torok.

MR. TOROK: Thank you and good morning.

I'm Ray Torok from EPRI. We've got our team up here, Bruce Geddes and Dave Blanchard, and we'll continue where we left off. The first topic today for us is techniques for failure prevention and mitigation.

That's supposed to be sort of a subliminal message of discussion past what is a failure mode and what's a failure mechanism to what can you do about it. So, we're being a little bit sneaky there.

As I said, they're the main points as we're pushing the conversation ahead here to prevention and mitigation. What this is really about is an ongoing EPRI project, where we're developing guidance for utilities related to this, and we'll go into some detail as to where we're headed with that.

Keep in mind that this is an ongoing work here, an ongoing project, and in fact the three of us don't even agree on everything that we're going to talk about here today.

So, some of this is in a state of flux and whatnot, but we wanted to talk with you about the direction we're headed in anyway. So, you can see here a list of buzz words that have come up several times yesterday. I don't think I need to go over all that, but the things like diversity, defects and

triggers and so on, common cause failure. Lots of good buzz words in digital.

So, we will hit each one of those and explain where we're headed with the project; we'll give you a status and give you some conclusions. Now, the main purpose here is just to inform. We want you to know where we're headed.

Of course, we always welcome your feedback on these things. So, we'll look forward to that as well. As I keep saying, let's extend the discussion of failure modes to what can we do about it.

First, we have a list of what, for us, are key concepts here. They're going to be -- they're rolled into the work we're doing.

First one is protection against failures or common cause failures or whatever you want. It's about prevention and mitigation. We talk about how we see that role in this.

Software failure means whatever failures. You'll notice we were careful and put "failure" in quotes here. Think of that as a reference to all the discussion we had yesterday about what's a software failure.

But still, we agree with the discussion

yesterday. You need a defect and a trigger, and that's important. It helps. It helps, and we'll talk about why.

This notion that protection against failures and CCF can be done at various levels. That goes back to the diagram we showed yesterday, levels of interest that we've been applying in PRA and in hazard analysis. Common cause failure --

MEMBER BROWN: You left out the words in-plant architecture.

MR. TOROK: Architecture?

MEMBER BROWN: You said different levels of interest that you just -- and I've been waiting for this, in particular techniques in prevention when you talk about architecture. So, I'm going to repeat myself. It'll be on the record for two days that in reality when you look at software based systems, as well as analog systems, the protection really -- you're highest level of protection is based on that architecture and the fundamentals, which are redundancy, independence, deterministic behavior, diversity of defense in depth, control of access and simplicity.

Okay, so, we talked about all these little

software defects and triggers. If you don't mix software from division to division, that's one very major level of prevention because now you can deal with one channel having a failure, not necessarily that defect is going to occur. It depends on the type of defect; you want to assume in every other one of the divisions.

I only say that because after 22 years and 100 plus reactor plants worth of digital computer based I&C, I won't say it will never happen, but I never had a processing type failure occur in any dual -- set of dual -- the fact is, I never really had any that weren't design oriented, and even when we had a design one, it didn't occur simultaneously in the other channels with the same data coming in.

Software that's being processed in each of the other channels is not the same channel to channel to channel based on the independent data that you have coming in from the plant as long as your sensors and inputs are independent.

So, I really wish all your techniques for failure mitigation and prevention had a heavy emphasis on independence, and I don't mean just the old electrical isolation independence that we lived and

depended on in the analog systems, but the independence of communication between divisions in the software world as well as monitors to ensure that when you got the voting logic that you didn't lock up all because of the corruption of the data going from one division to all four loading units.

I just -- we've been emphasizing that now for five or six years, and it is very important, and experience-based, as well as what I would call intellectually based. So, I will -- Steve would've been disappointed if I hadn't interjected myself at this point, and I wanted to just make sure that was on the record.

I really think it would benefit your whole approach to doing stuff by emphasizing that architecture protection as well as trying to deal with little piece parts down the side, which is really hard.

MR. TOROK: Right. I appreciate the input. We've certainly captured that, and hopefully we'll come back and tell you how it turns out. I get the impression you've done this speech before though.

MEMBER BROWN: If you can poll the members, they can probably do it for me by now.

MR. TOROK: I think the protection that comes from the architecture is a big deal, and we have to give that --

MEMBER BROWN: Biggest deal. Okay, I'm done. Thank you.

MR. TOROK: Okay, so we've got that plant architecture in there. Common cause failures, CCF: There are a lot of different flavors of common cause failures and we're trying to cover them all, and we'll talk more about what we mean when we say that.

Overall, the goal is something like that: reasonable assurance of adequate protection against effects of failures. Okay, now, this is -- there are a couple of mushy words there. What's reasonable and what's adequate?

If I'm an engineer, I have feelings about reasonable and adequate. If I'm a regulator, I have feelings. They might be different. We're focused more on the engineering part of it because that's our role here.

So, as you know, we've been working on digital issues for quite a while now, and there's a list of things, most of which you guys heard about in the last couple of days as a matter of fact: Hazard

analysis, PRA, estimated failure rates.

Evaluating critical digital equipment is really a reference to work we did many years ago now in regards to commercial grade digital equipment because there are a lot of reasons why that's probably the best way to go in updating old analog equipment.

But the question then becomes, "How can you assess the commercial grade requirement to convince yourself it's of adequate quality for your intended application?"

If it's safety or even if it's critical non-safety, you don't want your feedwater system to go bump in the night. So, we did -- we spent a fair amount of time on that. Operating experience we talked to this group about, and of course defense and depth of diversity you've heard a lot about in the last day as well.

We've been working on these things for a long time. Now, during those years, a lot of other things have changed. The commercial products and products from vendors have continued to evolve and get more -- I think more robust as the designers learned more about what they can do to make their equipment more reliable and that sort of thing.

At the same time, standards have been evolving: IEEE standards, standards particular to the nuclear industry. The whole gamut, and of course guidance. Guidance that we produced and guidance that NRC produced, and so on.

So, a lot has been done. What we're trying to do now is take lessons and important information from all this previous work and put it together, and extend it to aggress the issues of the day here.

Now, bottom line here is I think we know a lot more about how to deal with the digital equipment than we did 20 years ago, and there's my note about SECY 93-087, which of course is a key document here in the SRM to it in regard to what you can do about digital.

I guess I keep thinking about that as sort of a block box approach. We don't know exactly what's going on inside that box, but we know it can do some strange things, and we need to worry about that. That's what the SECY is really about.

Like I said, a lot has been learned since then, and I think we can do better. We'll see.

So, the project; what I call it is

assessing and managing digital failure susceptibilities, and failure here means -- failure means misbehaviors, unintended functions and so on.

We want to get -- we really want to produce guidance for utility engineers so that they can do a better job with assessing their susceptibilities and figuring out what to do about it, using both prevention and mitigation, and then there's this notion of adequate protection.

Part of that is -- well, we'll get to it at coping analysis, which is a demonstration of adequate mitigation. Now, here we say EPRI is developing technical guidance. That's our role in this.

We expect that this work will also support an ongoing NEI effort, where they are addressing issues with CFR 5059, and there's an NEI guideline, NEI 101, which is guidance on licensing digital upgrades and addressing 5059 issues for digital.

The key technical issues that come into play there are this notion of malfunctions with a new result is one of them. It does the digital introduce that, and couples with that is the notion of the likelihood of a failure, a common cause failure. How

do you deal with that for the purpose of the licensing discussion?

There's really a heavy common cause failure emphasis in this whole issue. I don't want to put too many words in NEI's mouth. This is part of really producing technical guidance that we think will be of use here.

The two NEI leads on this are Gordon Clefton and Kati Austgen. Now, Gordon is sitting somewhere here, I believe. Can I give Gordon the opportunity to give his two cents for NEI here?

CHAIRMAN STETKAR: Absolutely, if he wants to. And he does.

MR. CLEFTON: Good morning. This is Gordon Clefton from NEI. Thanks. I appreciate the opportunity. The organization NEI has pulled together a large distribution list of people very interested in improving the situation here.

We've established with the NRC a good working group, and a good working relationship with clarification of some of the major problems the NRC had. The industry has answered those, and had a number of public meetings and drop-ins.

Our path forward is to address the

guidance documents out there. What we're seeing isn't so much that the process is incorrect in the documents that exist; it's they're just being executed improperly.

So, our intent is to improve the guidance documents significantly, and that's on both sides. The NRC has recognized some of the guidance documents that need to be enhanced, and we on the industry side have as well.

Our plans are to probably pull NEI 0101 and take its contents, and put it into appendix of our NEI 9607 to provide better examples. Currently, our focus group is setting up a pilot project for a 5059 non-safety system digital modification to a plant.

So, it will have examples of how to use the 5059 process properly. That has been one of the major issues identified. Next meetings are in December, and then we'll have another NRC public meeting in January. It is work in progress as we identified, and I say that we want to continue the good cooperation between the NRC staff and industry as it is working right now.

I'll answer any questions if you have them. And yes, we are looking at all the buttons on

Charlie's list. Thank you.

MEMBER BROWN: You can take action instead of saying it.

MR. TOROK: Okay. I want to point out this -- this ongoing EPRI project is often referred to as the EPRI CCF Project because of the heavy CCF emphasis here. If we start saying that, you'll know it's really the same project.

Again, from every point of view, we're trying to provide useful guidance for utility engineers. We have a Utility Technical Advisory Group that's helping to make sure that we do come up with something that is actually useful. But it's also expected to be useful for the licensing effort that we were talking about.

Okay. Now, with that, here are some key terms. Remember, I said we don't even agree among ourselves on all these things, but by the time we get done I think we'll have to have a set of terms that are going to function well enough for all of us.

Failure is pretty general. When a thing can't do what it's supposed to do within its acceptance criteria and common cause failure, two things misbehave for some reason. That's a very broad

definition of common cause failure.

That allows for the case where, for example, a single hardware failure disables both, let's say, a system controller and maybe the display to the operator know what's going on. So, it's a very broad definition of common cause failure.

Diversity and defense in depth analysis has been referred to in many places in some of our work and branch technical position 19 and so on, and it has become kind of a confusing phrase for a lot of people.

For our purposes, we're talking about two aspects of it. The first one there is susceptibility analysis. It's trying to identify potential vulnerabilities to failures, including common cause failures, and also considering the measures in place to protect against them in defensive measures. That sort of thing.

Part of this gets into a qualitative assessment of likelihood of failure in common cause failure. On the other hand, there's coping analysis. Coping analysis for us means a demonstration that the mitigation that's in place is adequate to prevent the really bad thing from happening, regardless of how

good your preventive measures might happen to be.

So, we use those two terms: Susceptibility analysis, coping analysis.

CHAIRMAN STETKAR: Let me intercept you right here.

MR. TOROK: Okay.

CHAIRMAN STETKAR: Because when the appropriate time is, but I'll do it now; everything that I hear from you and to some extent from the staff focuses on this notion of failure in terms of not doing what we want it to do.

MR. TOROK: Yes.

CHAIRMAN STETKAR: With ignorance of the other things. The other things are I think some of us have more concern about those other things than the first because indeed there are many defenses built in the plants, diversity, to mitigate the first without people thinking necessarily very strongly about the second.

For the record, I'll just put a simple example. Two trains, two valves. Valve A can open or close. Valve B can open or close. I have four possible combinations. A and B can both open. A and

B can both close. I can get open close. I can get close open.

Those four combinations of things can have different effects on the plant depending on the conditions that they occur in, and even in the single openings, spurious opening if you want to call it that, could be a problem depending on what other systems in the plant are out of service.

The vulnerabilities to each of those -- and I like the term misbehaviors, the vulnerabilities to each of those misbehaviors, depends on how those open and close signals are developed through my entire logic. What input conditions do I need? What kind of failures - misbehaviors - can occur within the processing logic? And perhaps what kind of misbehaviors can occur in the final component interface modules that the output -- that talk to those pieces of equipment?

I don't see that kind of systematic thought process. That systematic thought process is fundamental to risk assessment. I only see the focus on something that I'll call common cause of both valves are supposed to open, and they both don't open. Only one of the four possible output states from that

system.

MR. GEDDES: That example is very much part of our discussions inside the project.

CHAIRMAN STETKAR: Good.

MR. GEDDES: We're time limited here, but we have -- we've prepared some presentations just to get that point across among our project team. Because we agree there is too much emphasis on failure. We believe that based on this definition of failure, and of course we're not published yet and this is subject to some adjustment, but we think various actuation is in that --

CHAIRMAN STETKAR: Bruce, I wanted to interject the discussion at this point because you may think it's in there, and indeed I could twist the words in the way I think to say, "Well, maybe it's covered by this." But in practice, I don't see that emphasis.

MEMBER BLEY: I think we have guys working on this, who know this stuff; you kind of assume everybody's thinking the same way you are. Unfortunately, we've got a lot of people out there who don't have the experience, and it's got to be explicit I think, or it gets lost.

It doesn't get lost everywhere, but here and there it gets lost, and the people who lose it say, "Well, it doesn't say I have to do that."

CHAIRMAN STETKAR: "And I don't have any examples to show me how I ought to do it either."

MEMBER BLEY: That's the other piece.

MR. GEDDES: That's a model sensor control or valve. We have cartoons that do just that. I believe there's room in this guideline to put those messages in there and make it very clear.

MR. TOROK: You're right. It's a good point, and what Bruce said is right. We talk about this among ourselves; we have to make it come out clearly when it's reproduced. I think part of this is why it is important to have a role for gained insights from PRA and also insights gained from hazard analysis because they support those things. So, that's why those are parts of this puzzle.

CHAIRMAN STETKAR: I think it goes if you -- if you were to develop guidance with a sensitivity to those combinatorics type process in terms of thinking, it might go a long way toward addressing this nebulous notion of common cause failure also, because a lot of folks think about, "Well, common

cause failure; something can make this system do stuff that it ought not to do."

Well, some people just think that it doing stuff that it ought not to do is not starting the --

MR. TOROK: Right.

CHAIRMAN STETKAR: But other people think about anecdotal experience of software and automobiles suddenly accelerating automobiles and those types of behaviors. They say, "Well, that's some sort of common cause effect." It isn't, necessarily.

I think mentally people start to lump too many things into this nebulous notion of common cause, and if we restrict the common cause just to things that prevent the system from doing what we wanted them to do, that doesn't really address the whole notion.

What I'm trying to get at is there might be a much narrower set of actual misbehaviors that prevent the system from doing what we wanted it to do that could better focus the attention on at least that class of stuff that we're calling CCF.

There might be other things that can happen that cause these combinations of open close, open open and that sort of thing. Think about it, because it's, as Dennis said, without the guidance and

some examples, you can read anything into the words that you want to read in and that's the problem.

MR. TOROK: Well, we got -- well, we'll get to this too, this notion of different flavors of common cause failures, one of which, an important one of which is multiple spurious actuations.

CHAIRMAN STETKAR: That's the analogy. I mean that's the analogy.

MR. TOROK: Well, but it's an important one as you point out though because the most common conception is the time to worry about CCF is when you have multiple redundant trains that are identical, and there's a lot more situations than that. There's several more that you need to think about.

So, we keep trying to point that out. We'll see.

CHAIRMAN STETKAR: Okay, I got my thing on the record so you won't have to hear it again.

MEMBER SCHULTZ: Well, I just want to expand it because -- and I think this is why John brought it up here. It is important to bring it up right up front that you indicated, Ray, that you want the definition of failure, common cause failure, to be

broad --

MR. TOROK: Yes.

MEMBER SCHULTZ: -- at the beginning of the discussion, and yet since you've used the word failure, and then you said failure of two or more structures.

MR. TOROK: Yes, yes.

MEMBER SCHULTZ: As you can see the mindset that one would normally have is it is not performing its intended function. It is failing to do so. That doesn't bring into play the four options that John has brought forward.

And so, it is really important to capture it here in your first two lines, and misbehavior versus failure is a very important distinction.

MR. TOROK: That's a really good point. You know, these two definitions, the first two, are lifted from an IAEA standard.

MEMBER SCHULTZ: Yes.

MR. TOROK: And we have to get beyond that is what you're telling me, and I think you're right.

MR. HECHT: But why is it necessary to distinguish between the misbehavior and a failure? What does a failure include -- I mean not include that

a misbehavior includes?

CHAIRMAN STETKAR: It's a conceptual trick. If I'm someone, and say, you tell me as an analyst that I must think of misbehaviors, I -- and this is the way my mind works or thinks, "Oh, misbehavior? Something could open when it's not supposed to be opened. That's a misbehavior."

If I have a mindset that says, "I am supposed to trip the plant," then the only failure is not trip the plant." So, it's a way people think.

MR. TOROK: If we're going to -- we, all the time, consider -- I think we treat misbehaviors as a subset of failures for our purposes, and that's all well and fine but I think what I'm hearing is we have to make that -- if we're going to do it that way, we have to make it painfully obvious that that's what we're doing so that people can't fall into this trap.

CHAIRMAN STETKAR: Failures are a subset of misbehaviors.

MR. TOROK: Okay.

CHAIRMAN STETKAR: Okay? Think of it that way. Failures -- failure to perform what I wanted it to do is a subset of all possible misbehaviors.

MR. TOROK: Okay, that's better.

MEMBER SCHULTZ: That's how I see it too.

MR. TOROK: Okay, thank you.

CHAIRMAN STETKAR: It's like safety related is a subset of important to safety.

MR. TOROK: I don't know if Dave would agree with you. We probably shouldn't wander off into that. Okay, moving right along. Okay, so what we're going to do in our approach is we're going to take the lessons from previous discussions and previous projects and so on, and apply those and expand to where we have to go.

Now, in some existing guidance at least for common cause failure, there's heavy focus on the issue of -- or on the notion that equipment diversity is going to solve the problem, or you can show that you're okay relative to common cause failure by doing 100 percent testability.

We think it's not just about that. There's more to it than that, and what you really care about is not how much diversity you have or how testable you are. What you really care about is whether or not you've got adequate protection against the bad effects that you're worried about.

For our purposes, what we're going after

here is what we consider to be a more holistic approach. You figure out what your susceptibilities are to these things, and then you evaluate your defenses against them, including design, design and defensive measures for example of which diversity can be one.

Consider both preventive and mitigative measures, and we'll talk a little more about that in a minute.

MEMBER BROWN: By the way, diversity does not always give you better reliability.

MR. TOROK: I'm with you on that. That's a good point.

MEMBER BROWN: I hate that thought process. I'm not against diversity, but it's the nature of the diversity in many circumstances. Since I designed software systems for two different software packages, half the protection system is one; half is -- and this was back in the early '80s when all this stuff -- there were no standards. There were no anything.

So, we -- in our program, we tried a lot of these different approaches, and you can add -- you add so much additional complexity by trying to

integrate diverse software into systems. Particularly, if you have a control system where you don't have -- you can't maintain strict independence between things as opposed to a shutdown safety safeguards of a trip system.

So, I just wanted to get that thrown in there. I love diversity. Love the -- but with those, you got to be careful.

MEMBER BLEY: Just to be clear, diversity protects you against common cause. It might not give you a --

MR. TOROK: It might protect you against common cause failure. You sure hope.

MEMBER BLEY: You would lean toward diversity to get something that avoids some particular cause that would affect --

MR. TOROK: I say it depends on the kind of common cause problem you're worried about.

MEMBER BLEY: Of course it does, and that's what I said. If you want to protect against a certain one, you can pick diversity to protect you against that one.

MR. TOROK: That's right.

MEMBER BLEY: It doesn't improve general

reliability. Getting the most reliable components, you know, lots of redundancy. It does that until you get a common cause.

MEMBER BROWN: I still have to admit that 35 years I never had common cause.

MR. TOROK: Okay, very good.

MEMBER BROWN: You got to protect against it.

MR. TOROK: Yes. I think we agree with everything you said. Hopefully, we still will at the end, or we will have something that fits. In doing this, and in protecting rather, against failure and against CCF, there are preventive measures and there are mitigative measures. We want to consider both of those.

Coping analysis for us means a demonstration that your mitigation is okay and is adequate. So, it's something you can do. Keep in mind that coping analysis by itself adds nothing in terms of defense against things you're worried about. It's just a demonstration of adequate protection.

In the end, we think that it'll come down to engineering judgment as to whether there's adequate protection. There's no yes or no. It's kind of gray,

and it'll come down to some engineering assessment.

Now, let's see. There we go. This notion of prevention and mitigation. On the left side here, we have causes of things that can happen. In the middle, there's the undesired event. That's the bad thing. Then on the far right, there are consequences. Consequences you don't like.

For the sources and the undesired event we have preventive measures, right? And on the other side of the event happens, and you want to contain the effects of it, that's what mitigation is about. So, we're trying to just explain the difference for our purpose what we mean when we say prevention and what we mean when we say mitigation.

Now, if you're talking about pipes, and for me this notion of prevention and mitigation applies to pretty much anything you can think of. If you're worried about falling off a bicycle, you can talk about prevention measures and mitigative measures, right? Mitigation is the helmet. Prevention? Maybe training wheels.

In this case, we're talking about piping. For pipes, how do you prevent pipe break, and the answer is use good pipes. You check on them, and you

do good welding and you inspect them and those kinds of things.

If the piping breaks anyway, there are other things to deal with the problem. There's isolation valves. There's ECCS and things like that.

I&C is analogist to that. On the preventive side, we have things like watchdog timers, and data validation. These are defensive measures and we'll talk about them more.

On the mitigation side, we have a number of things like backup systems and so on. You notice watchdog timers appear on both lists? I could put diversity on both lists as a matter of fact. It depends on how you're using these things.

The point is that the -- you can think of these defensive measures on the prevention side and on the mitigation side.

MEMBER BLEY: But the truth is if you march down a scenario, at any point, prevention are things that would've kept you from getting to that point, and mitigation is what will keep you from going worse after that. But if you move further down, what was mitigation becomes prevention --

MR. TOROK: Yes.

MEMBER BLEY: -- in your thinking, and people lose that.

MR. GEDDES: Of course Mr. Brown's five key points would go on the left hand side of the slide.

MR. TOROK: Well, some are mitigation. But anyway, they certainly would factor in here. Okay, now, next one. We're okay on prevention and mitigation, right? That's at least the words we use. Now, come back to defects.

We talked a lot about this yesterday, and I don't know that we need to dwell on it too much. We agree with what we heard yesterday. You need a defect and a trigger both to create a failure. And to get into the common cause failure arena, you need multiple defects maybe and multiple triggers concurrently. Those kinds of things.

Although actually for CCF, it can get more complicated than that, and we'll talk about some of the other flavors of CCF's here.

Now, what is a defect for a digital system? It could be a hardware defect. Doesn't have to be software, right? Could be aging hardware. Could be a requirement specification error that

somehow got factored into the design of the system.

Could be an error in design. Could be an error in insulation or operation. Lots of flavors of defects that could come into play. Could be an error in the logic. What are the triggers for a digital system?

Could be a random hardware failure. We saw one in the operating experience where the software had a glitch in it, but it was fine until a sensor feeding the system failed and the software reacted incorrectly to that.

So, in that case, the hardware failure was the trigger. That's a really interesting one because it is hard to turn that one into a common cause failure because you need multiple hardware failures concurrently to make it happen, right?

Another type of trigger could be an unanticipated but real plant behavior, right? One that's not factored into the design and doesn't know how to handle it. Now in anticipated conditions, anticipated test conditions, digital systems are pretty bullet-proof. But when they get into trouble is when they get into unanticipated conditions.

That's what I like to call, "When the

going gets weird." And so, it could be an unanticipated condition. Could be a condition that's unanticipated but real, but the designers felt that it was so unlikely that they didn't need to worry about it. That's another thing that could become a trigger.

It could be an anticipated real behavior that triggers something like a maintenance error or miscalibration. The real transient happens. Something has been calibrated incorrectly or set point is wrong. So, the system behaves incorrectly. That could be a trigger.

Could be an environmental disturbance. Tsunami, fire, flooding, whatever. Lots of different types of triggers that could come into play here.

Now, it is important to know here that just because you've got defects and triggers doesn't mean you have something that really gets you into trouble. Not all failures are bad; not all failures can -- I should say misbehaviors. Not all misbehaviors can become CCFs for various reasons.

Not all of them are safety significant or risk significant. The point here is that for real digital systems, you don't necessarily expect software to be defect-free. In fact, I'm not even sure what

that means.

You don't need that. What you need is software that doesn't do bad stuff. That's different. That's different.

This notion that there are defects and triggers is really important because -- and -- and -- because there are a lot of things we know about how to deal with, for example, how to reduce the likelihood of a defect by a good development process. V&V and all those kinds of things go after defects and reduce the likelihood that you're going to have a defect.

On the other side are defensive measures. You know, the watchdog timers and separation and so on. Those reduce the likelihood of triggers that can get you into trouble. It turns out those are really good knobs for us because we know how to influence both of those.

So, when you're doing a susceptibility evaluation, you're looking for evidence of those kinds of things: design measures and practices and what not that reduce the likelihood of defects or the likelihood of triggers, and therefore reduce the likelihood of the failure or the misbehavior or common cause failure, common cause misbehavior.

I'm going to get really tangled up in these words now, but I think you know what I mean. Right? So, we've got those two knobs: defects and triggers. And we can go after both of them in terms of protecting against common cause failure or a single misbehavior failure.

Okay, now, let's see. Okay, we talked about common cause failure context. Different types of common cause failures. This is what Bruce was talking about earlier. In this case, we've got a cartoon that shows the situation where we've upgraded all of the non-safety systems across the upper right there, and we're saying, "Okay, we're going to implement all those control functions on like platforms."

They're all going to be -- pick one you like. You know, the Fravowitz 101 system. And they're all going to communicate with each other on a communications bus. That's that blue bar. So, I guess I can do this. There's the communications bus.

So, these guys are all identical platforms. They're all programed differently for the individual applications that they're doing, but they are all communicating. They're controlling multiple

functions down here, and the question is, "Wow. What might happen now in terms of failures, in terms of misbehaviors, in terms of inadvertent actuations and those kinds of things?"

And this is maybe an extreme case, but if you're talking about a new plant or a --

MEMBER BROWN: That's not particularly extreme if you look at the way the new systems -- I'll just take the -- I mean I couldn't -- I don't have to throw stones. That is so non-bullet proof that every one of these networks that people are putting in these plants have a communication to some corporate network or whatever.

As soon as you do that, everything is on that bus. You've got not only the safety signals, the monitoring data going up to the control room, the control signals coming back to actuate whatever system you want to manually control, and if somebody takes control of that network bus, they can tell the operator, "Everything is just fine." While they're turning off the pump, or while they're opening a valve, or while they're driving a rod out. A group of rods, whatever the circumstance may be.

The control of access moves in all kinds.

That is just one of the principles that as soon as you combine all that stuff on a data network like that, you're just asking for a problem. And it is not recognized. Everybody says, "I got this software firewall, where I can change a bit here and a bit there, and boy I can make it do this. I have this great algorithm that can teach me."

No. You don't let anybody in. Ever. Sorry. I am kind of --

MR. TOROK: No, I don't disagree with you. Assessing susceptibilities is recognizing those kinds of things and then figuring out what kind of protection you have against them. That's kind of the game here.

MEMBER BROWN: You shouldn't have to assess anything there. It's obvious.

MR. TOROK: Okay, this one is obvious, but as I said earlier, there are different flavors of architectural context if I'm allowed to use that term.

MEMBER BROWN: Common network. One flavor.

MR. TOROK: Well --

MEMBER BROWN: How many times do I have to say that?

MR. TOROK: But you could have -- okay, let me try to go through. You could have redundant divisions that have identical equipment in them; identical pumps, motors and all that junk, but also identical controls system, identical software.

That's one architectural context that could get you into common cause failure conditions, all right? But another one is -- suppose I have multiple systems that use the identical equipment. I can postulate a failure there.

If I have multiple functions in one controller; now, in an old analog system and an old analog plant, you'd say for each function there's a separate controller because that's the way the plants are done to -- when you go to upgrade, it's really easy and really attractive to start combining functions in a single controller because these controllers can do that.

All right, that opens the door for certain kinds of problems.

MEMBER BROWN: Interesting you say that, because in 1979 before you were born probably.

MR. TOROK: I appreciate that.

MEMBER BROWN: The first microprocessor

that was military qualified was a radio -- it was a -- now I've forgotten.

MR. TOROK: A Z80?

MEMBER BROWN: Yes, a Z80. Thank you. It was a ceramic; it was military qualified, humidity, all that kind of stuff, hardened; 2.3 megahertz if you can believe that. You know, snail's pace ability to process.

When we went out to put the first design in, the vendors came -- and we had said, "Oh, no. You take one." We had like 29 instruments: pressure, temperature flow, level, all this other kind of stuff in these cabinets.

The vendor came back and said, "Gee, you don't need 29 different processors. All we need is four, and we can move the data around and minimize the number of parts and all this."

We looked at that, and it took us about five seconds to say, "No. We don't even know how to measure stuff right now and get it processed properly." So, we went and we had 29 different -- you know, a little computer in each channel. Just like we did in the old days. All we did was substitute a chip for all the parts that made up amplifiers and

bistables and all that other kind of stuff inside each of the little things.

Then we moved up as we learned, and at least thought we had a greater understanding of what we were dealing with.

And so, I mean your point is very well taken that this idea that now I've got this one system to control all is very pernicious. I mean it is everywhere.

MR. TOROK: I think nuclear plants have found themselves in the same situation you just described. Didn't you have a story about a plant where the vendor wanted to combine everything? Then somebody at the plant said, "No, I don't think so."

MR. GEDDES: Yes, I have a story.

MEMBER BROWN: We could trade stories and do this all day.

MR. TOROK: Okay, okay. The last thing on my list here for common cause failure context has to do with -- the one that's up here again is what I call sharing resources. The resource could be a data network. It could be power supplies. Could be timing signals.

There was an event at a plant a few years

ago where they had -- with a multi train control system, where they were -- the controllers were taking a timing signal using a timestamp data that went out to an archive.

Now, you say, "Why does the real time control system have to care what time the data is?" You know you can ask yourself that question. Anyway, what happened was the timing signal had a problem; went to like the digital -- the system went to all zeros. The controllers didn't know what to do with it, and in milliseconds they lost multiple trains.

I think -- I don't remember frankly what the control system was, but it tripped a plant. That's a shared resource thing that really happened.

MR. GEDDES: Charlie, one issue in this diagram -- this is just one example. You can slice this and dice this any way you want, but in this particular case, the objectives of some people from this architecture is to have an integrated control room.

So, should that -- are you suggesting that that's not a good design objective?

MEMBER BROWN: No, it's a perfectly good design objective. It's just a matter of how you do it

and what access. If you can maintain access within your control, within the plant where nobody else can get to it except if somebody says, "Here's the key to go get in this cabinet. Take the laptop down and go do whatever you need to modify some software or to change a set point, or whatever it is."

Once you start, you can over-integrate. Maybe the suggestion was, "Well, gee. You've got a vendor in Palo Alto, California. You've got a plant on the east coast, and he's got to make a software chain." I had this discussion, okay?

He was going to send the software change via the internet, download it into the shipyard, which would pass it in via the internet systems in the shipyard, down into the ship. You know, the submarine is the carrier in this particular circumstance. And modify the software in place.

MR. TOROK: Yikes.

MEMBER BROWN: Bad idea. Really a bad idea. I mean just the idea -- it's all a matter of how you integrate. That's all.

MR. GEDDES: We agree. One reason we prepared this cartoon was to prepare a key point that maybe it's not so clear in our discussion so far.

If you look at the two feedwater regulating valves A and B, and then the two feed pumps A and B, they might all be connected to that one individual feedwater controller, which might be a master-slave, but nonetheless, should there be four controllers or is one controller adequate?

MEMBER BROWN: No. Two.

MR. GEDDES: Why not four?

MEMBER BROWN: It's just a matter of how far you want to go. I mean you put everything into one basket.

MR. GEDDES: Well, the issue is can we tolerate, let's say --

MEMBER BROWN: Do you need both feedwater reg valves to operate in this case?

MR. GEDDES: We'll have to go to John's point of the four combinations: open open, close close, open close --

MEMBER BROWN: It depends on how you're going to operate that system. If one pump and one feedwater reg valve can operate the system, then you ought to have one controller, okay? And you're going to have to integrate -- if you have feedwater pumps that go up and down in speed in order to help control

it, or if you have the valve open and close or a combination, that changes the way the dictate of how you design that system.

MR. TOROK: That answer is it depends.

MEMBER BROWN: It depends. If you've got a constant speed pump, you just run the pump and control the valves.

MR. TOROK: In this case, let's say they're turbine-driven pumps. But what --

MEMBER BROWN: The turbine driven common speed.

MR. GEDDES: One of the issues we're trying to get to is what misbehaviors are we going to tolerate.

MEMBER BROWN: You have to look at it --

MR. TOROK: That's an application specifically question, really.

CHAIRMAN STETKAR: It's a plant specific question. It's not this cartoon specific.

MEMBER BROWN: Exactly.

MR. GEDDES: Well, we used the cartoon --

CHAIRMAN STETKAR: No, the cartoon is -- I know where you're going if you can get there.

MEMBER BROWN: There's nothing wrong with the network. I mean there are dual networks in there so if a network fails then they can still maintain. In this case -- and that helps you with the integrated control because it allows you to control the data in a manner that is consistent. However, you got to be careful how you do that.

MR. TOROK: Well, there is a misbehavior. One system overloaded the network and created a broadcast storm that disabled another control system and it was tripped, right? So, those things have to get considered along the way.

Now, we talk about what are the common cause failures. Well, I use the word CCF. We're going to be stuck with this CCF, common cause failure, where we really mean it more broadly than that. But you affect multiple things one way or another, either in terms of failure or in terms of actuation or some combination of those. Could mean all kinds of crazy combinations here.

Okay, now, what we wanted to talk about a little more was examples of defensive measures because Charlie likes this, right? Charlie likes defensive measures. And so, here's one where we talk about --

MEMBER BROWN: Go back.

MR. TOROK: Oh, no.

MEMBER BROWN: You're talking about defensive measures, okay? Because this applies to both analog as well as computer-based systems. You talk independence; you're controlling a steam turbine generator set, governor system.

It's an analog system. You have an overspeed trip device, and you have a controller to drive the turbine speed controller. This is a real event. I won't tell you where it happened, but the operators noticed that one of the machines seemed to be -- how do you call it? Lugging, or getting -- the speed was oscillating in a matter in which was not normal.

Okay, that was not normal. They took the machine offline and started troubleshooting. Well, what do you do? You start picking out things. You troubleshoot. Okay, change out a power supply. Auctioneered power supplies.

Take out a power supply machine; almost a guy tripped it before it hit. It's 150 percent over speed trip. Well, turns out that the other power supply -- the normal automatic trip did not operate,

and the key was they had auctioneered power supplies. Power supplies fed both the independent, supposedly independent overspeed trip, and the normal speed controller.

One of the power supplies not only was trying to get the machine to change speeds, but had also effectively overridden the automatic overspeed trip signal. Disabled it.

MR. TOROK: Right.

MEMBER BROWN: Independence means independence. It doesn't mean -- that's the point I'm trying to make. That is critical in both the control system, as well as the reactor trip and other types of multi division systems.

Independence is probably the most important mitigative, preventive feature you have. It could be lost easily. I made that argument, by the way, in the design of a new system where they were common. I said, "That's a bad idea." And they -- the government, the Navy; I was just a consultant here. This was about six years ago.

I said, "No, no, no. You've got to have a separate set of power supplies for the overspeed trip, as well as auctioneered." "Well, where have you ever

seen that problem?" Well, I've never seen that problem. Let me finish. I'm almost done.

Never seen that problem before. Well, they blew me off. Six months later, this occurred, and now they were back, redesigning all the systems to put in independent power supplies.

I'm just saying independence is critical. So, I'll stop.

CHAIRMAN STETKAR: I need to make sure that we allocate an hour for the staff, and we have a couple of administrative things to do at the end. And we need to end at noon. So, not your guys fault, but we'll try to --

MEMBER BROWN: I'm finished.

CHAIRMAN STETKAR: We'll try to be better behaved.

MEMBER BROWN: My lips are sealed.

CHAIRMAN STETKAR: Do you have some fundamental points that you need to make in the next 25 minutes or so?

MR. TOROK: I think we can get there. I think we can get there. So, I just wanted to talk about certain kinds of measures just to give you a flavor of the kinds of things we're talking about, and

also to make sure everybody understands that there's not just one or two of these things out there.

So, in this case, it's an example that sometimes we call the minefield metaphor. So, this boxes the operating regime of some system. The domain or every place if can go, and in -- and let's say this system is something that's monitoring some inputs and under some circumstances is going to take action. But mostly, it just monitors things and checks a couple inputs against set points, and just keep going.

So, it just keeps doing the same thing over and over again. In this case, it -- so, it stays on this one path, and what's important here of course is the path. We know the path works because it was tested and is used all the time, and it avoids these potential bugs, the little bombs there.

And so, there may be problems in the software. There may be defects, faults, bugs, whatever, but the system never sees them. Now, that's all well and fine during the case where the system doesn't have to take action.

There are times when it does. If it sees something and you see the set point has to initiate some other action, that's fine. You leave that green

path and you get on this other path. The idea is in that path it's not maybe the normal mode of operation, but it is one that's been heavily tested and whatnot. So, there's pretty good confidence.

It also does not hit any of these bombs that are out there. There's certain things you do, and we don't need to go through each of them in detail, but there's certain things you do to make sure the thing stays on the path; the path you know.

Now, what you really have to worry about is the case where it somehow can get off that path. And in a well-designed system, you can find the operation to a well-tested path and you force it to stay there.

Now, this is really important. It's a really important concept because what that means for example is if I have a -- if I'm worried about potential bugs in the operating system, and I'm using the system in such a way that the operating system does the same thing at every time step and never deviates from that, then even though there are bugs out there in the operating system, I'm pretty confident I can't hit them.

That's pretty huge, right? So, now, this

notion of -- this is about this notion of defective software. It doesn't need to be defect-free. I just have to be pretty good about avoiding defects and having confidence that I'm avoiding defects if they're there.

So, in a well-designed system, and real systems are all over the road in this regard, right? But in a well designed system, you can avoid problems. This is a real important concept here.

This has to do with things like cyclic behavior, and what some people say is a system is blind to plant transients. A plant transient won't put this thing in a path that it doesn't know.

So, that's a good defensive measure. Now, some other concepts that come along with the watchdog timer. What does that do for you? If it protects or it -- if it detects the process for lock up, it does whatever it is told to do, really. It could put the system in a safe state, for example.

Now, is that protection or mitigation? Both, yes. Okay, could notify the operator there's a problem.

MEMBER SCHULTZ: The watchdog would be to initiate something.

MR. TOROK: Okay.

MEMBER SCHULTZ: So, it either initiates a notification signal, or it initiates some kind of -- whatever it is, mitigation process.

MR. TOROK: Right. Now, in that process, the mitigation process would be where the watchdog is effectively saying, "Look, something is wrong. I don't know what it is, but I'm going to take action right now to put this system in a safe state."

MEMBER SCHULTZ: To initiate a problem?

MR. TOROK: To initiate, yes. Now, it is important though to -- there are good ways and bad ways to do this, and I think one of them that came out yesterday is if you're going to do a watchdog, you don't want it to be done in software that's running on the same processor that's doing the control function because if that locks up, you don't have a watchdog anymore.

MEMBER BROWN: I don't know that I don't have a watchdog running its own software.

MR. TOROK: The watchdog needs to be independent hardware based. Exactly. That's part of this. This notion of an infinite loop architecture; you don't want a lot -- branching can get you into

trouble because it makes it more difficult to understand all the potential unanticipated conditions you can get into; all the abnormal conditions.

So, you say, "Minimal branching is a good thing." Back in the olden days, if you had a lot of branching, they called it spaghetti code, right? The software guys? You just really didn't know what it might do under abnormal conditions.

Let's see. Oh, data validation; there are cases where when the system sees unexpected data, a value goes negative that never should've been negative. You know, a -- what do you call it? An autopilot for a plane that doesn't understand an attitude below sea level because there are places where you can fly below sea level, right? Those kinds of things.

Data validation, where you're checking for those things ahead of time, such as the system, can deal with any data value from negative infinity to positive infinity. That's a good thing. There again, you may be able to at least put -- prevent the system from doing something bad.

What's really interesting about this particular defensive measure, and some of the others,

is you don't care what caused the data to go bad here or what threw it out of range. Doesn't matter. The system can do the right thing as long as you know what you want the system to do if this happens.

MR. HECHT: By the way, that's not sufficient force because if you sensor data value, you better be able to do something about it.

MR. TOROK: Yes, you want to be careful. There are cases where -- and you want to be careful about how you do that. There is one where airplane autopilot was doing -- we hate to do these stories, right? But the idea was the autopilot was flying the airplane. It was gradually losing power to an outboard engine. This is a 747.

It got to the point where the autopilot couldn't keep the plane on the right track anymore. What did it do? It did exactly what it was programmed to do, by the way. It said, "Your airplane pilot? I'm out of here."

So, what happened is the underpowered wing dropped, and the plane didn't want to descend. Lost 15,000 feet of altitude. So, you can do it right, or do it not so right. The answer there was don't let go of the airplane. Scream at the pilot for help, right?

MR. HECHT: Use the last known good value, or --

MR. TOROK: Those kinds of things. That's right. So, you need to be a little judicious about how you do that. That's kind of the point. There are other kinds of defensive measures. In a real time control system, ideally, you don't use times and dates, right?

Now, some people say, "We need times and dates so we can archive data." Well, that's all well and fine but let's be careful about it. One way to be careful about it is don't let your controllers decode the timing signal. Just let them pass it along to the archive.

So, it doesn't matter what that timing signal is doing. It can't disrupt the controller. So, there are things you can -- games you can play like that.

We talked about power supplies and being careful about how you do that timing signal. Communication was there; ways to deal with potential problems coming from there.

Segmentation: don't put too many -- if you're going to have communications, make sure that

you're not tying too many things together that are critical to each other.

So, I go back to Dave, and he would say things like, "Look, for that particular plant, what really matters -- the only common cause issue that can get you into trouble is if it affects that system and that system." Don't let those systems have any legs, right?

Diversity: there are a lot of different flavors of diversity. These are two of my personal favorites. Functional diversity and signal diversity. The reason is because in the operating experience we looked at, we saw a number of cases where these things saved the day.

RPS, reactor protection, is full of functional -- or signal diversity, really. There are multiple signals that can trip the plant, right? Water level, pressure, temperature, neutron flux, whatever. That's a good thing. You don't want to lose that kind of thing.

On the other hand, if you compare it to platform diversity, for example; if I have redundant trains doing the same thing functionally and they have the same requirements and so on, platform diversity

doesn't buy me too much. But if, on the other hand, I can have a backup that's functionally diverse, now I'm -- now I'm in much better shape.

Okay, so, there's some thought that should go into that. Diversity: here we are dwelling on diversity again. From our standpoint, diversity is all well and fine in some cases, but it's not the know-all, end-all answer to everything.

As I said, we saw cases where functional signal diversity were really good in practice in nuclear plants, but you also get into this issue of added complexity, issues with training and maintenance and so on.

If I have two diverse channels that disagree with each other, how do I decide who is right? You know, all of those kinds of questions come up.

What does platform diversity do for me if there are requirements errors that are basically factored into both platforms? The answer is doesn't buy me a hill of beans, right? So, let's see what else.

Oh, diverse backups. Now, Dave did some analysis where he looked at potential for diverse

backups in terms of providing additional protection. In PRA space, you factor in spurious actuations, potential spurious actuations.

In the case Dave looked at, it turned out that diverse backup actually increased the core damage frequency because of the potential for spurious actuation.

So, you want to be a little careful about those things. In fact, in that case, it's -- for the diverse backup, it is more important that it not spuriously actuate when you don't need it than it actuate when you do need it. So, it is an interesting insight from the PRA perspective.

Now, there's a notion that in diversity, in some cases we can be pretty confident on health. In others, you don't know. I mean if I have two different digital platforms, how do I know they both don't have a Y2K problem embedded there? Maybe they do. Maybe they don't.

If I go looking for it, I can figure something out, but the point is that diversity, while it can help, doesn't really guarantee that you don't have CCF vulnerabilities.

So, our position on that is diversity is

all well and fine. Be a little careful. There's downsides to it. Use it where it makes sense. That kind of thing. But don't think of it as a panacea.

I put this quote in here. It turns out, 20 years ago, a bunch of smart guys wrote a letter to the Commission, and said basically what we just said. Diversity, maybe you should be a little careful about that.

What's interesting, what struck me anyway, is that data on this thing. When I saw that, I thought, "Wow. We are still struggling with the same question now 20 years later." So, okay, moving right along here.

So, the goal, the way we're looking at it is this notion of reasonable assurance of adequate protection. There again, there's some software in there, but there are a lot of things you can look at in digital systems as you're trying to develop assurance that you have adequate protection.

There's the traditional hardware practices. There's shake and bake testing and so on, the QA that supplies the nuclear safety systems and so on.

Software development: a lot of standards

now. A lot of work has happened in the last 20 years with software development standards. However, we need to keep in mind that process based standards don't necessarily ensure good design. They have a good process that'll be a well-documented design. It may not be good. May not even include any defensive measures.

Typically, the software standards talk about process. They don't talk about design attributes. So, we need to be a little careful about being a little too confident in development practices.

For us, the defensive design measures are probably more important in various areas in the software and the architecture and so on. Now, there's this note here. When we looked at the operating experience in the nuclear plans, it looked like whatever the designers were doing, it was working pretty well.

The software was not the primary cause of potential and actual common cause failures. It was other stuff. It was miscalibrations and set points wrong on redundant channels and those kinds of things. It was hardware failures, in fact.

So, at the time, when we published this

report, one of our observations or conclusions was it looks like what these guys are doing is really working. What we need to do is go figure out more about what they're doing, and make sure we keep doing it because it's working.

MEMBER SCHULTZ: The real concern about the common cause here isn't that it's something you're going to see in everyday operations. It's in a very unusual situation. It's going to hit you and it's going to be a very unlikely event. We don't have enough experience yet to have covered things that we care about. It's 1 in 10,000; 1 in 100,000 because that's why we care about these things.

MR. TOROK: Yes.

MEMBER SCHULTZ: So, you can't just go on what we see happening. Of course it's not a big problem. If it were, it would've gotten fixed in everyday operations.

CHAIRMAN STETKAR: And it's not the 1 in 10,000, just by counting up the fact that I have, you know, 200 reactors operating for 50 years each or something like that so that I have suddenly 10,000 operating years because essentially all of that time the system is operating within it's normal

environment. You don't have 10,000 yearly demands of these unexpected triggers.

MR. TOROK: Right.

CHAIRMAN STETKAR: We essentially have no experience with those.

MR. TOROK: Well, what we do have, and what we're trying to credit here, is the experience of the vendors and their platforms. Not necessarily nuclear experience, but now for example, the control systems all have watchdog timers.

Why is that? Because they learned 20 years ago that the watchdog timers were very helpful in making the systems more reliable. Same things with data validation and other defensive measures. We do want to take advantage of those.

MEMBER SCHULTZ: I'm not saying -- of course you've got to look at that. That's important. It does affect everyday operation and safety. But it doesn't assure you under the bad situation that we're covered just from looking at --

MR. TOROK: Rare events do happen, right?

MEMBER SCHULTZ: Sad to say.

MR. TOROK: Dave keeps telling me that.

MEMBER SCHULTZ: Go ahead.

MR. TOROK: Anyway --

MEMBER SCHULTZ: From everything else you've shown us over two days, you haven't fallen into that trap, but just those couple of bullets on the slides.

MR. TOROK: Well, what we are doing as part of this project now is we're going back to some of the designers of the equipment; the ones who are willing to talk to us about the types of -- based on their expertise and experience, the types of defensive measures and design practices and so on that they have found useful.

So, we'd like to capture the knowledge that they have based on their experience. So, we're trying to do that.

CHAIRMAN STETKAR: That's interesting you say the ones that are willing to talk to you.

MR. TOROK: Well, in some cases.

CHAIRMAN STETKAR: In some senses, that's troubling.

MR. GEDDES: Let me speak to this, because I'm the one that's going after that particular task. I come from -- I used to work for AREVA, and now I consult with different companies, but it all depends

on how you phrase the question.

If you say, "Would you agree that watchdog timers are a good thing." Everyone might say, "Well, yes." If you say, "Does your platform have a watchdog timer?" "I'm sorry, I'm not allowed into my proprietary sanctum." So, it goes to phrasing and consensus building, and that's what we're trying to get to.

MEMBER BROWN: Or, does the watchdog timer actually have some software that I can tell where it's -- I mean it can be hardware, but it can have a software interface. You don't want that either. So, it's a matter of when you ask that question -- they're not totally good if they're not --

MR. GEDDES: We're going deep. We're taking a real deep dive here. For example, single bit errors. Are error checking and correcting codes a good practice or not? Data communication issues; can they segment a system well enough so that a broadcast storm is limited to a particular segment, a functional segment of the architecture?

If we're going -- we're trying to get much deeper than these cartoons that show conceptual ideas. If we publish another report that says, "Here's some

great concepts. Go do that." I won't have any traction. You have to get this in consensus with people that actually design and build the systems

MEMBER BROWN: Data correction, data error correction is fraught with peril. You've got -- if you don't -- you've got to be very careful if you're going to change data that's coming through.

I know we opted not to use any of it at all, and just let each division operate independently and take the -- let it go the way it went.

MR. GEDDES: Can we interview you?

MEMBER BROWN: Yes. I'll talk to you any time you want, but I can't tell you anything because it's all process.

CHAIRMAN STETKAR: The only reason I made this comment is everybody says digital I&C is a huge concern for the international nuclear industry. This is not just within this room. Everybody is facing it everywhere. All of the vendors are facing it. To have a particular system vendor say, "I can't talk to you because mine is proprietary, as an industry group, I understand that I can't talk to me. I don't want them to talk to me."

That is somewhat troublesome because it

says that they don't want -- they think they are somehow outside of the scope of this problem.

MR. GEDDES: In some ways they are, because remember, there's a lot of non-safety upgrades that are well underway. We're talking to suppliers that don't do nuclear everyday.

So, we say, "We represent the nuclear industry. Would you agree?" And they kind of go into vapor lock. We have to be really careful how we pitch it to them.

MR. TOROK: We try to keep it on a functional level as opposed to -- it's like, "What are you doing? Are you doing data validation as opposed to the details of how they do it?" Because usually, they think of that as proprietary --

MR. GEDDES: Their response is, "Nobody's ever asked us that before."

MR. TOROK: Anyway, so we are trying to capture what we can get from them and factor that in. As I said, this is a work in progress. We don't know where that's going to land. Let's see where else.

Mitigation, how good is your mitigation? How good is the coping capability. That's part of building assurance that you got adequate protection.

Test coverage in some guidance says, "If you can do 100 percent testing, you're good." We say, "I don't know about that because it didn't do anything for me; for example, in regards to requirement specifications."

But extensive test coverage is a good thing. We don't disagree with that. Performance operating history, especially for commercial grade equipment and depends on as far as whether they have records and whether the experience is successful and adequate and relevant to what we're trying to do and those kinds of things.

The point is commercial grade suppliers have had decades to get the bugs out, and figure out how to make their systems very robust. So, that can be important. You know, if you're talking about designing from scratch a digital control system of some type, and, "I'm going to design from scratch and I'm going to do it under my Appendix B program. It's going to have wonderful QA and software development."

I still say what are the odds you're going to get it right on the first try? Compared to a commercial guy who has had 20 years to figure it out. You know, and so we want to take advantage of that

kind of experience to the extent that we can.

Let's see. Oh, risk and safety analysis. Dave keeps coming up with interesting insights in regard to what's important from a risk standpoint, and we want to be able to factor that in. You know, it also gets into this notion of hazard analysis. Where are the hazards and what -- identifying susceptibilities and whether or not the protection is good and those kinds of things.

Simplicity. Everybody believes -- I think there's great agreement that simplicity is a good thing, although no one knows exactly how to put a number on that. I think still we can apply that in a qualitative sense. So, we're trying to do that.

MR. GEDDES: It's 1 minus complexity.

MR. TOROK: There's a wise guy in every crowd. Okay, but what it comes down to is you look at all the sources of assurance that you've got to play with and -- and it comes down to engineering judgment is whether or not it is reasonable and adequate.

So, that's where we're headed. Now, one of the questions that keeps coming back at us is, "Okay, but safety and non-safety are different. In safety we've got all this guidance and standards, and

all this junk. In non-safety, we don't. What's going to happen there."

You're right; there are different aspects of safety and non-safety, and if I'm looking at an assurance argument, there's some differences that are going to come into play. Here's a swipe at trying to characterize some of the differences here for redundancy and independence. The safety systems have that by regulation. The non-safety typically use master-slave or architectures even when they have redundancy. That's a difference.

Qualification testing is automatic for safety. For non-safety, it could be wherever. Software quality assurance, again, safety systems are good. Non-safety is all over the road. Some of them are really, really good. Some of them just aren't.

Functional complexity: Typically simple for safety systems by design. Non-safety can be anywhere, and we saw that of course in the operating experience where the incidence of certain kinds of failures was much higher than non-safety. We attributed it to some extent to the complexity and the difficulty in anticipating abnormal conditions and so on.

System interactions: The safety systems are required to be separate and independent and those kinds of things. Non-safety? We've got potential for all kinds of connections. Operating experience typically to safety systems are weak there, and the commercial or the non-safety commercial systems are strong there.

MR. HECHT: Could you elaborate on that point?

MR. TOROK: On what, operating experience?

MR. HECHT: Not weak, that there's not much of it. Safety systems. I guess what does not much mean?

MR. GEDDES: Well, we see turbine control, feedwater control, rod control, plant computers. Every plant in the US seems to have both systems. There's one that has a true integrated digital protection system. That's Oconee. One.

MR. TOROK: That's on the nuclear side. We looked at another case of two different -- two systems sold by the same vendor. One is safety, and one is non-safety. The non-safety one was used in other industries, and at the time they had -- I wish I could remember. Roughly 30,000 of these things, these

platforms and applications in various industries.

On the safety side, the one that was developed under QA and all that? There were seven in the world.

MR. HECHT: Okay. I guess my question is that if they're being made up of components or modules or things like that, which are used elsewhere, do you consider operating experience only for the integrated system, or --

MR. TOROK: No.

MR. HECHT: -- would you consider each one of those modules if it is applied elsewhere to be --

MR. GEDDES: That's true, yes. I'm saying there's one protection system in the US. That's Oconee. But that's not the only instance in the world. Of course not. That platform has a legacy that goes back 30 years.

There is application level experience, and then there's sort of the platform level. We do distinguish that in the OE research report. But both matter. Application and in integrated environment, and then it's individual components. We agree with that.

CHAIRMAN STETKAR: If I program my

platform to reset trip set points as a function of where I am in power history and things like that, that doesn't make any difference from my plant. It doesn't make any difference how many years I have on that particular chip set. That's -- that's enough.

It is safety, and for that particular -- it's different application software for that particular application function.

MR. TOROK: Application serial code is often serial number 1, right? If that's what you're saying, yes. Of course, you like to avoid serial number 1 as much as you can.

MEMBER BROWN: Well, your housekeeping code may have some variability in it also when you -- when you move it over to another -- to another plant. I'm not saying across the Board, but there can be interface points where you have to touch it.

MR. TOROK: It turns out -- yes, we got to keep going. Defensive measures? I'd say safety and non-safety are all over the road. The safety has some things that are required, and non-safety they've got decades of evolution that are helping them.

Test coverage is high for -- I've said it here it's tied for safety because they're functionally

simple. And for non-safety, it can be much more difficult.

CHAIRMAN STETKAR: I'm sure it's high because they don't ever run through all of the particular -- all of the possible permutations and combinations of input signals in and out of the possible reactors. So, it's higher.

MR. TOROK: Okay. Now, in terms of risk significance they are -- I go to my PRA guy. Safety and non-safety both can be either highly significant or not so significant.

Anyway, the bottom line is you play the same game again. You're going to look at whatever it is you have and use your judgment to make some assessment, whether or not that is adequate.

Admittedly, that's qualitative, and it's a little bit mushy. So, where are we right now? Our EPRI target audience is various engineers who support digital implementations in the plants in one way or another.

What we're trying to do is produce guidance for them. We want to help them reduce the likelihood of defects and triggers, right? And therefore failures and misbehaviors. Let's see.

We want to help assess their susceptibilities to failures and common cause failures and so on. This issue of coping analysis for -- is kind of up in the air for safety systems. At least the guidance right now is when you do a coping analysis, you assume best estimate conditions because the likelihood of the common cause failure is low, and so it makes sense to use best estimate assumptions rather than design basis assumptions.

For non-safety, it's kind of up in the air. You might say, "Well, if have good defensive measures and so on, maybe there I'll reduce the likelihood to the point it makes sense to use best estimate analysis."

I don't know where that's going to land. We anticipate having examples that demonstrate how you apply these principles to real problems, and we'll see where that all lands.

We're looking at a final report for the middle of next year. We just published what we call a technical update, which is an informal EPRI report, and it documents where we are to date. To a large extent, it's just the words that go with this presentation, and it's a fairly brief document.

I don't know if you guys have that or not, but the plan is to make that publically available.

MEMBER BALLINGER: By the way, free is in the eye of the beholder. They want $25,000 to download that.

MR. TOROK: Yes, but that's old news. As of last week, a decision has been made to make this publically available.

MEMBER BALLINGER: As of this morning, you couldn't do it.

MR. TOROK: I'm sorry about that. But part of the reason for that is I am here instead of back there, where I could rattle some cages. That hasn't happened yet, apparently. I didn't know that.

MEMBER BALLINGER: I tried it last night, and I tried it this morning.

MR. TOROK: I didn't know that. I will follow up with that one and let you know when it's available, okay? I'm through. How did we do?

CHAIRMAN STETKAR: Okay, any other questions for EPRI on this topic? They're going to come back after the break and tie up on an example, I think. If not, let's take a break until 10:20.

(Whereupon, the above-entitled matter went

off the record at 10:06 a.m., and resumed at 10:22 a.m.)

CHAIRMAN STETKAR: We are back in session, and let's see if we can cover EPRI's final topic in their presentations. We'll turn it back to Ray.

MR. TOROK: Yes, I think we can be pretty quick on this one. It's about this hazard analysis demonstration. This is where we developed the guideline we talked about last September. Bruce has got it here.

The feedback we got back from our advisors was, "That's great. Now go do some demonstrations. I'm sure that this does what we say it does." So, the one utility stepped up and said, "Hey, let's try this on an upgrade we're working on. And so, we've been working with them on that."

This is a work in progress still. So, Bruce is going to explain what's going on and where we are.

MR. GEDDES: Okay, so, to be clear, there's two projects. One that the utility has embarked on that is underway, and then an EPRI project to observe how they apply this guidance and take lessons learned.

So, when we say project, we're talking about the EPRI project here. So, it's a trial application, and we've presented this to the subcommittee last year and we want to capture lessons learned, see how effective the methods are and what learning is actually occurring out in the field, and any pitfalls or measures that we need to take to improve the transfer mechanisms or the guidance itself.

We do have an EPRI project team: Dave, myself, John Thomas from MIT and Ray. We're providing a little bit of training, a little bit of training, a little bit of coaching. We're having some onsite workshops to sort of observe and participate on a limited level.

So, the Palo Verde project -- now, we're talking about the Palo Verde project. It's an exciter, a main generator exciter EPRI project. It's actually a very extensive project. They're replacing the exciters in all three units.

They are non-safety of course, but critical to generation as you would expect. The exciter system at its fundamental level consists of a controller, bridge rectifiers and certain peripherals,

and because of the nature of the Palo Verde machine, they're actually putting new transformers and new equipment out in a new building adjacent to the turbine building.

There's a long story behind that, but after we got there and saw why they were doing that, it makes a lot of sense. So, we want to elaborate that point. But when you put bridge rectifiers, they are shunting 200 ramps of DC current in a building outside of a desert.

HVAC becomes a very critical part of functional -- piece of the mod. So, in talking to the Palo Verde engineers, if they lose HVAC in this new building, then they lose the rectifiers on an overheat trip in about ten minutes, or less than ten minutes, okay?

Charlie, it's true inside the turbine building too.

MEMBER BROWN: I'm just not used to requiring air conditioning to warrant -- 22 degrees and 100 percent humidity.

MR. GEDDES: No matter where you put the rectifiers, overheat, loss of -- they need to be cool. That's just the point. Maybe not on a ship.

So, each new building is equipped with three redundant HVAC units, and each of those units is sized for 100 percent load. Now, the basic steps of this report, the hazard analysis guideline is there's nine basic steps for any particular method, scope and objectives, an upfront function analysis, the level of interest discussion that we presented yesterday.

Figure out which method or combinations of methods make the most sense, identify the resources, set up a schedule, do a preliminary hazard analysis and then do the detailed analysis. Then make sure you do something with it when you're done. Make sure it is acceptable, documented and well-maintained.

So, the Palo Verde exciter hazard analysis or scope is the main generator exciter system; the exciter building HVAC system, and the objectives are to identify and resolve potential hazards that can lead to a loss of HVAC that ultimately leads to a main generator trip.

So, there's a few moving parts in this analysis. The function analysis is pretty simple. The basic functions for the exciter, exciter controls, HVAC and HVAC controls are defined in a function process map which is part of the functional FMEA

method that we talked about yesterday has been developed. Dave has been observing that particular piece.

The levels of interest are the exciter, the controls on the operator interface, the digital control system on all three redundant HVAC units. In any given building, there's one building per unit. There's three units. The interfaces between the redundancies and the human system interfaces are what the Palo Verde engineers decided to focus on, as well as the electrical power supplies to the HVAC units.

Palo Verde decided to apply the functional FMEA method for the exciter system and controls on the operator interface. We got there. We saw some spreadsheets. We saw a conference room with laptops and engineers working away on that. It was very interesting.

Then they decided to apply the STPA method that the MIT systems theoretic process analysis method for the exciter HVAC controls system. Dave is working with a couple other guys on fault tree analysis for the electrical and mechanical portion to power supplies and the compressor evaporator portions of the exciter HVAC system.

So, step 5: Consider a blended approach. Palo Verde chose the functional FMEA to help identify hazards to be assessed, and then to do a further review using the STPA method.

Now, we do note that the functional FMEA fault tree analysis in STPA view the control system in the context of the integrated plant design. The Palo Verde engineers did specify a design FMEA from the supplier bottom up. You know, hundreds of pages of tables, single point failure FMEA. That had not -- either that hadn't been done yet, or it wasn't available for us to see.

So, we do know that that's happening, but our participation on this project as observers or coaches is -- we've seen and coached a little bit on this functional FMEA and STPA.

CHAIRMAN STETKAR: Is the use of the STPA an overlay to try to say, "Well, gee, is the functional FMEA really -- does it really -- is it good enough?" Or, do they have more confidence in one, or do you --

MR. GEDDES: It's too soon to tell yet because we don't really have the results. We've just seen them making some progress. I would say that so

far they're probably seeing certain hazards come out of STPA that they didn't see in the functional FMEA.

MEMBER BROWN: Okay, well, that's why I was asking the question was to try to validate one versus the other and see which is the more powerful method. Is that part of this effort?

MR. TOROK: It's supposed to be for the functional FMEA identify sort of the high level -- you want to look at harder with STPA. So, we don't know where that's going to go.

CHAIRMAN STETKAR: The functional FMEA does have a -- I forgot how many questions there are.

MR. TOROK: Guide words?

CHAIRMAN STETKAR: Guide words. Even with kind of a rigorous application of those guide words, you're still --

MEMBER BLEY: Well, did the same people do them both?

MR. BLANCHARD: The Palo Verde people did functional FMEA, and they are moving onto do STPA on the controller itself.

MEMBER BROWN: Same guys?

MR. TOROK: Same people, right.

CHAIRMAN STETKAR: That'd be interesting.

MR. BLANCHARD: I think they moved from the FMEA when they got to the controller to the STPA approach, as opposed to having the big overlap to compare results.

MR. GEDDES: What got them interested in this demonstration was a presentation about STPA that we made last year at an industry conference, and one of their senior managers said, "I want that on my exciter project." The engineer said, "Well, let's do a functional FMEA too just to see what it tells us."

It's too soon to say, because this is all preliminary. We saw spreadsheets that were not independently reviewed yet. This is just an engineer working on his laptop.

CHAIRMAN STETKAR: I think at one level, that would be really interesting if one method actually does identify some - whatever you want to call it - hazards or vulnerabilities, and not. Especially if it's applied by the same people with nominally the same level of rigor.

MR. GEDDES: I would say that they are applying the same level of rigor and interest. They're not favoring one method over the other per se.

MEMBER BROWN: It would be interesting to see if each one of them identified the same vulnerabilities that the other one did, plus some more, or whether one identified one and the other one identified some totally different ones, which means almost sending a different message in terms of is there a uniform --

CHAIRMAN STETKAR: It goes back to this blended approach.

MEMBER BROWN: Exactly.

CHAIRMAN STETKAR: Might be the way you need to go.

MEMBER SCHULTZ: I guess it's not real surprising. It's be interesting to see how it turns out. Forty years ago, when we first started doing fault tree analysis -- you can also do success tree analysis. They're mathematically the same thing. But what was found back then was the same kind of people doing a success tree analysis ended up incomplete and didn't find everything that somebody coming at it from the failure point of view did.

Just something about the mindset. So, there could be some of that going on here too. It'd be real interesting to hear. We'd like to hear back

when you can tell us what you know.

CHAIRMAN STETKAR: That's going to be part of your report on this process?

MR. TOROK: Yes. Let -- our lesson is learned. You know, in regard to use of method, yes. What we won't talk about is proprietary details of the systems they're installing. That doesn't matter to us for this purpose. The effectiveness of the methods does.

CHAIRMAN STETKAR: You ought to be able to sanitize it enough to identify elements of what was discovered by each of the methodologies.

MR. TOROK: Sure.

CHAIRMAN STETKAR: Okay.

MR. GEDDES: I would note that one of our early worries about this project is that the staff, Palo Verde staff, might punt it to us to do it for them, and we said no. "We're interested in watching you do it. If you get stuck, just call, email or whatever."

So, they took it and they're running with it, which is really great. To that end, of course they have access to proprietary information, but they are not allowed to share it until we get to an NDA.

So, that stuff hasn't occurred yet.

So, the preliminary hazard analysis, the functional FMEA was performed to identify the must-do and must not do functions of the functions of the exciter control system. Like I said, Dave has been looking at that. He is observing the activities that are going into that.

Now they're doing the detailed hazard analysis, which is the STPA method.

Since last year, there's been another workshop at MIT, sponsored by Nancy Leveson, and to everyone's surprise, there are people out in the field developing tools spontaneously. They're not commissioned.

Nancy was pleased. We had a poster session one evening during the workshop, and some guys from the University of Stuttgart said, "Look at our new STPA software tool." They projected on the screen, and we said, "Hey, that looks pretty good."

So, we provided a copy or showed the download link to the Palo Verde engineers, and they said great. They're using it.

MEMBER SCHULTZ: Did you have a chance to go through it to the extent you're convinced that it

forces you through all the thought processes the method wants?

MR. GEDDES: Yes. Now, there are -- there are a couple different approaches you can take with STPA. You can take a higher level abstract point of view, and you go through sort of a group exercise to identify the hazards, and then the provide/not provide, the behaviors.

You can fill out some spreadsheets at a very high level, or you can take a deep combinatorial view using the process model variables. If you recall the presentation we made last year, that approach, the second approach, can lead to some large combinatorial data sets.

There are others for developing algorithms and tools for reducing those combinatorial sets to something that is much more understandable. Those are not ready yet.

So, the Stuttgart tool is more of a procedural tool. It marches you through the basic steps of STPA and provides of course a report at the end. But we think it is useful.

We wrote a procedure in the guide, but using this particular tool forces you to step-by-step

document the results as you go.

The next workshop is in December, next month. We understand that the detailed hazard analysis results, even if they're maybe not independently reviewed yet, will be available for us to come in, take a look, provide additional coaching that they might want, and then we should be on our way to -- or they should be on their way to finishing this particular piece of that project.

Then we should be able to publish a lessons learned report in 2015.

MR. TOROK: To some extent, we're -- we have to go with their schedules. They have other priorities. They have a plant to run, don't you know? We have to respect that. So, we're trying to be flexible schedule-wise.

CHAIRMAN STETKAR: One other thing in terms of lessons learned; I'm assuming you're going to monitor the amount of resources of effort that were required for methodologies because you already mentioned hundreds of pages of FMEA.

I don't have any experience on STPA, but reading about it - the little I've done - sounds like it could potentially be much more resource-intensive.

So, I'm interested if they're applying it on a fairly well-constrained system.

MR. GEDDES: I think they are, and this is just my own personal experience having done very large design bottom-up FMEAs; hundreds or thousands of pages. I've been involved, and I believe STPA is much less resource intensive.

CHAIRMAN STETKAR: You think it is? Okay, okay.

MR. GEDDES: Absolutely. In a couple of days, you can get a lot of insight using STPA, and it might take you a couple of months or a couple of years with the bottom-up FMEA. The bottom-up FMEA depends a lot on design information.

Often, the design FMEA you might have a conceptual design FMEA at the front end of a project, but then you get through the detail design, the software's design, the hardware's design, integrations occurring. Then there's some guy in a cubicle somewhere, pounding our line after line on a spreadsheet. You know, it's very painful in some cases.

CHAIRMAN STETKAR: I wasn't trying to say that the FMEA's are not resource intensive. It's just

my impression was that the STPA could be even more.

MR. GEDDES: It takes a different way of thinking. It takes some exposure, some training, some coaching. But once you get it, when the light bulb goes off, John Thomas did it for me at the workshop - the first workshop - three years ago.

I sat through three days of presentations, and then John spoke, and it just -- I had this ah-ha moment, and I realized, "I can get at the conceptual design phase or any phase of the project if I apply this systematic approach. You know, systems thinking. I can get a lot of insights very, very quickly." But I had to rethink the problem.

MR. TOROK: And for a complex system, it depends on the system you're looking at, right? But we saw cases where you end up generating these very large tables that you have to deal with.

For me, it seems analogist to where fault tree was 30 years ago when it was unmanageable, and then various tools were developed. Now, it's a lot more of a convenience. Everybody is doing it.

MR. GEDDES: That's if you take the combinatorial approach. You can abstract a problem up

a little bit and still gain a lot of insights.

MR. TOROK: But the good news is these tools to do that are being worked on now. So, it looks like the future is going to be okay.

MEMBER SCHULTZ: You didn't, along the way anywhere, take a modest system of some sort and maybe have Dave take the previous approaches, and you try the MIT approach?

MR. GEDDES: That's exactly what we did in this report. We took --

MEMBER SCHULTZ: Okay, so that is what went on.

MR. GEDDES: We took that HPCI/RCIC turbine control system.

MEMBER SCHULTZ: But that's the way you did it?

MR. GEDDES: Dave did a fault tree. We had John Thomas and Glenn Dean and another researcher --

MEMBER SCHULTZ: Okay, so they did it. Okay.

MR. GEDDES: If you recall, we gave them just the block diagram, and they came back three days later with --

MEMBER SCHULTZ: I remember their results. I didn't know that you had played that kind of game. That's interesting.

MR. TOROK: It's amazing how quickly they were able to come up with some of this.

CHAIRMAN STETKAR: Great. Anything else for EPRI? If not, thank you very much. Again, thanks a lot for not only this morning, but over the last -- yesterday afternoon and this morning. A lot of really good information.

MR. TOROK: Thanks for --

CHAIRMAN STETKAR: We really appreciate it.

MR. TOROK: -- letting us come talk to you. It's really useful for us too.

CHAIRMAN STETKAR: I hope the staff is ready, because surprisingly enough, we're a little bit ahead of time. Let's go -- I guess they're ready.

(Whereupon, the above-entitled matter went off the record at 10: 41 p.m., and resumed at 10:46 p.m.)

CHAIRMAN STETKAR: We're back on the record now, and we'll hear from the staff on failure modes research. I guess you're up.

MR. GUTIERREZ: Hi. How are you? Thank you. My name is Mauricio Gutierrez. I'm from the Division of Engineering. You already met Ming Li, who spoke yesterday, from the Division of Risk Analysis.

We're here to present to you an update that responds to comments and feedback that you gave to us during the September 2013 DI&C subcommittee meeting on RIL-1002, which was titled, "Identification and analysis of failures modes and digital I&C safety systems."

So, we hope to make the case that DRA and DE have a common understanding of how digital systems fail, and that our research efforts are complimentary and aligned. During this presentation, we will review some background information. We'll recap some digital system failure mode related research that the staff has worked on, or is working on, and we'll recap the feedback that you gave to us at the September 2013 meeting.

Then, we will summarize the staff actions that results from your feedback. This will include a description of a perspectives of our two respective divisions in terms of technical objectives and how we approach them.

We'll also include a discussion to show that we share a common understanding of how digital systems fail. We will discuss terminology that we use, and show that there's a lot of agreement. We will also show that the failure modes we have identified are aligned. We will then provide some conclusions and present our next steps.

So, background here: The ACRS has had concerns about digital failure modes for a long time. The roots go back to the Commission direction to risk inform the licensing process. Those concerns were brought to the Commission attention in 2008, when the staff requirements memorandum M080605B was issued.

That SRM directed the staff to report the progress made with respect to identifying and analyzing digital I&C failure modes, and to discuss the feasibility of applying failure mode analysis, the quantification of risk associated with digital I&C.

Okay, so, from the DRA side, we have these bulleted points. Ming, would you like to say --

MR. LI: Yesterday, I briefed the committee -- yes, the number 1 and number 3, BNL work. Today, I'll focus on the second bullet, "Failure mode taxonomy."

This failure mode taxonomy research is one of the two initiatives from research on digital I&C. The other two approach this research under the working group at WGRisk were formed.

The group members are from international -- most of them are from Europe and the US, and Asia, Japan in this effort.

The objective of this research is to develop failure mode taxonomy for digital and safe system failures with a complete set of failure modes. But due to the major disagreement among -- among the group members, the outputs the classifications scheme for the failure mode taxonomy.

So, the complete set of failure modes, that part, is a major part of this research. So, the classification scheme classified the failure modes. I will call it the existing digital and safe failure modes; in terms of the location of the failures and the effects of the failures, and the current situation of the failures. That means how the failures will be detected offline or online.

Personally, I believe the technical contribution from this work, number one, in addition to that classification scheme. Number one, the level

of detail. They define the level of details by using so-called example systems.

So, in the example systems, they came up with system architecture and also hardware architecture and software architecture in generic formats.

So, in part of the EPRI study, I saw some similarities. That's all I have to say.

MR. GUTIERREZ: Okay, from the DE side here, our response to SRM has consisted of several work projects here. The first one was research information letter 1001, and NUREG/IA-0254.

Those two reports dealt with software related uncertainties, and software fault modes and effects analysis. You were briefed on those reports on May 4, 2011. I'm sorry, they were completed in May 4, 2011, and the ACRS was briefed on June 22, 2011.

We received some comments from you on that, and they impacted what we did with RIL 1002, which is the second report, which is on identification of digital safety system failure modes. We briefed you on that on September 19, 2013.

That was a draft report. We got your feedback. We completed this earlier this year on

September 3, and it is now publically available. The third part of our response to that is RIL 1003. That's scheduled for completion next year. That's on the feasibility of applying failure mode analysis to quantification of risk association with digital I&C systems.

So, the last feedback we got from you on September 19th, regarding RIL 1002: Overall, you gave us positive comments. However, you did raise some concerns that there are two respective divisions, DRA and DE; had divergent understandings of how hardware and software fail.

Some of you requested harmonization of failure modes identified in RIL 1002 with work that has been presented by EPRI. You suggested altering the negative conclusions of our draft report, and the staff here agree to supply a joint briefing with both DE and DRA staff present, which is this briefing right here.

So, a summary of the staff actions that we took. DE and DRA staff have been meeting regularly since that meeting to consider your feedback. We've discussed our technical objectives and perspectives. We've discussed the terminology we've used to describe

digital system failures, and the failure modes that each of us have identified in how we use them.

We've found a lot of common ground. The following changes were made to RIL 1002. The executive summary was re-written. We added a set of failure modes identified by our review of some of EPRI's research. The conclusions of RIL 1002 were also rewritten.

We also removed language that implied that the synthesized failure modes in RIL 1002 not applicable to PRA applications.

So, the purpose of this slide, slide 8, is to show where we began our discussions. We were trying to see if we really did have gaps or disagreement.

So, we started with the basics and we reviewed the fundamental objectives of our research goals. We began by reviewing our technical objectives and perspectives. Now, this slide shows that there are perhaps nuanced differences, but we found that we have a lot more in common than what we don't have in common.

Both of us have safety as the ultimate objective, and how we get to that ultimate objective

of safety takes slightly different approaches. This does not impact our technical understanding of how digital safety systems fail. Is there anything --

MEMBER BROWN: I'm taking a deep breath.

MR. GUTIERREZ: I mean I can let you read the slide here. I don't know if there's anything specific here that you'd like either one of us to go over.

MEMBER BROWN: I just have one question relative. You don't have to go back to the last slide, but you commented that we had suggested altering negative conclusions to provide positive uses. You said you had taken action to rewrite. I presume you did that not because we told you do, but because you evaluated what was there and you either agreed or disagreed, modified what have you to make them consistent with the real world as opposed to some theoretically abstract thought process that we tried to impose on you.

MR. GUTIERREZ: That's correct.

MEMBER BROWN: Okay.

MR. GUTIERREZ: We sat down, and looked at your comments. We said, "Hey, this makes sense."

MEMBER BROWN: I would've been dismayed if

you had just -- they said that's what it is, and that's what we're going to do. Sometimes it's appropriate. When I make certain comments, it's very, very appropriate.

MEMBER BALLINGER: You act in Oracle mode, do you?

MEMBER BROWN: Command voice in Oracle mode, yes. Okay, sorry.

MR. HECHT: Can I ask a question?

MR. GUTIERREZ: Yes.

MR. HECHT: One of the things about RIL 1002 and there's a fundamental --

CHAIRMAN STETKAR: Speak up a little because we're recording here.

MR. HECHT: Fundamental conceptual dichotomy between the discussions that we've heard over the last two days, and with RIL 002, they have a concept of something called the fault mode, which implied that they were looking at defects in the software as opposed to the defects plus the trigger, and I would say plus the platform, although that hasn't yet been recognized, which is I think what has been established over the past few days by I think most of the industry and EPRI and everybody else.

The last version of RIL 1002, at least that I saw, still had that concept of the fault mode.

MR. GUTIERREZ: Yes.

MR. HECHT: Why?

MR. GUTIERREZ: Well, look, I mean I think the next couple of slides will get into this a little bit. So, I guess I'll just jump right into them.

We took a look at our definitions. This is once again going back to the fundamentals of what we're trying to do. Both of our respective groups have used definitions from standard organizations.

You can see here I've highlighted in red; we're using some definitions from the same organization, IEC. They have different standards, and they have different definitions for some of the terms that we're using here, such as fault, failure and failure mode.

Fault mode is another one that we found in IEC 60050. We chose that term because, for RIL 1002 and also for NUREG/IA 0254, because our group here at DE felt that it best communicated the points that we were trying to get across.

We understand that there are disagreements, and because of that, because of what we

found in the literature, because of the way people were communicated, we tried to define them and use them consistently throughout these reports.

CHAIRMAN STETKAR: Is there -- let me just shake the tree a little bit. Is there some chance that all of these wise people who sit in rooms and put together these standards really aren't thinking about the problem correctly, and that perhaps others are thinking about it differently, and that maybe just trying to pare at the notions and perpetuate their way of thinking might not be the way to solve the issue?

MR. GUTIERREZ: Well, I mean I don't want to -- there's a lot of expertise out there. I'm not the expertise on the world or this entire field, but --

CHAIRMAN STETKAR: But what I hear from you is you're saying, "Well, because all these standard organizations use this vocabulary and think this way, that's why the staff must think that way."

MR. GUTIERREZ: No, no. I mean we don't. We didn't blanket accept everything here, right? I mean we chose the terms to use in our reports because we thought that this is the best way to communicate the issues that we're trying to talk about.

So, we did consider different definitions. I spent a lot of time talking about the word failure and software failure, and you guys got into that discussion yesterday. It's a tough subject. Do you want to say something?

CHAIRMAN STETKAR: Identify yourself.

MR. BIRLA: Sushil Birla, NRC research technical advisor. I think what is presenting is very consistent with the issues you folks have been bringing up. The connotations with the word failure, and the -- if you look at the morning presentation by EPRI and notice the distinction between a defect somewhere in the system, for example in the software, and the end result at the output of the system, which would be a failure, how do you make these distinctions clear to the reader?

Do you create your own terms? Do you use the overload? The same term in a different context but a different meaning? Do you trace back your use of a certain term to some standard?

This has been a very difficult journey. In different standards you see actually different definitions, and some of them are sloppy as you alluded to.

So, we are not endorsing the -- that the people who created these standards were absolutely right, but we are using the standards, or certain selections from certain standards, as a means of communication and basing as far as we could our usage of the term to be consistent with some definition we found somewhere in some authoritative reference.

Now, if you give him a chance to go through a couple more slides, he will describe to you how we are trying to address that problem, which is the one you alluded to; that maybe the way these terms have been defined isn't the right way of thinking about them.

CHAIRMAN STETKAR: Okay, thanks Sushil.

MR. GUTIERREZ: So, going onto the next slide here, when looking at these three terms that we highlight here: fault, failure and failure mode. When we compared the definitions that we selected and we found a lot of commonality in what we're talking about. So, when we really get down to it and start talking, we really do think that there is not a gap in how we understand how digital safety systems I guess fail, or other terms that have been used are behave or misbehave.

There isn't a gap between our two groups in those terms.

Okay, this next slide, slide 11 here: The information I'm presenting here is not in RIL 1002 as it is organized on this slide. The information, though, is not new. Once again, it is just to stress the point that we have a common understanding of how digital systems behave and misbehave.

So, here on my left here, I guess RIL 1002 set L. So, that set would synthesize from failure modes that we identified and all the references we reviewed, and the experts we consulted for producing RIL 1002.

The middle set, set J, came from WGRisk effort, and this was done before any reports had been issued. I don't think the final had been issued yet, right?

MR. LI: This came from the survey. So, the test score will come from a survey listing FMEA work. So, this came from a summary of the survey. Not the proposed failure mode taxonomy.

MEMBER BROWN: Is set L what we saw? Is that your revised issued in September?

MR. GUTIERREZ: Yes. So, set L was

formerly called set K. We added one more, which is the last one here, the EPRI guide words. You saw these in an earlier presentation by EPRI. I think yesterday.

These EPRI guide words are now set K in our report, and we've put everything through the process that we used to get our synthesized set, and we find that they met.

I think that's all I had for this slide here.

For slide 12 are our conclusions and next steps. I think we believe that DE, DRA and EPRI all have a common understanding of how digital system behave and misbehave. We think that the set L in RIL 1002 is a set of failure modes that could be useful for both DE and DRA.

We agreed that failure mode set L is incomplete, and we are uncertain how many other failure modes remain to be identified. Both of our respective divisions are considering potential uses for set L.

We've been talking about vocabulary. We're considering inclusion for the I&C research plan fiscal years 2015 to 2019; Vocabulary Harmonization

Project. We still have RIL 1003, which will address that second part of the SRM to address the feasibility of traditional quantification methods for use in digital system assessments.

We've captured some information and some comments that you've had on earlier presentations, which we will also consider for inclusion in that report. That concludes my part of the presentation here.

MR. HECHT: I guess the reason for my --

CHAIRMAN STETKAR: Sit close to the mic, please.

MR. HECHT: The reason for my concern is that once again, I'm looking at what I believe is the last version of this report, and it has statements in there like software is an abstraction. Appendix A2 has the reasons for avoiding the term failure for software. It says, "Because software does not wear out or degrade." That's still in the report, isn't it?

MR. GUTIERREZ: Yes.

MR. HECHT: Well, yet you have software failure modes that you showed earlier.

MR. GUTIERREZ: No, I do not have -- I

have not used the term software failure modes for this report. I'm talking about digital system failure modes. The definitions are important, and we're using the definitions consistently in this report.

That's why you're finding some of this discussion that you have in Appendix A over there. That's consistent with the definitions we have used. This, I think, is common practice in technical papers as long as you define your terms and use them consistently.

Well, that's been done before, and we feel we've done that here.

MR. HECHT: Okay, so I guess the point is that if you want to call it a digital system failure mode rather than a software failure mode, and you want to -- because that's fine. You use that consistently, although I think the sense of the term software failure mode is not only the source code on the storage medium or on the page when it's used in common terminology.

The basic concern about software in I&C and particular safety systems has always been because of the common mode or common cause failure issue. So, on this, we have the notion that this digital system

has got something, or software, embedded in it, and that that digital system with the combination of the platform and the constructions running on it, and the triggering mechanisms there, I guess that there's no -- no issue. So, that's good even though it's --

MR. GUTIERREZ: It's been tough. It's been very challenging to communicate these issues. We did the best we could.

MEMBER BROWN: You done?

MR. GUTIERREZ: We're done.

MEMBER BROWN: You commented on software and then you said, "No, no, no. Digital system failure." When you -- all the words and nuances there; when somebody talks a digital system to me, as opposed to -- it had two or three different meanings. Because I throw in software based digital systems; I can view that as combinational logic based systems.

Those have two different generic subset -- I won't say they have kind of two subsets. I might miss one. But if you go back and look at the old discreet component combinational logic, that's one version. Now you have that PGA type combinational logic that has developed based on software telling it what to do as opposed to hard-wired. It's a different

concept.

So, that has -- there's no software in those common combinational logic, but you program them externally to respond to logic, to respond a certain way. Once you've wired it, there. Theoretically what you want to do. So, are you including all of that range in your term digital, so that's why you exclude software? You're trying to address the whole plethora of digital system?

MR. GUTIERREZ: Yes, the --

MEMBER BROWN: Platform type characterizations?

MR. GUTIERREZ: You're right in that there's a broad spectrum of what's called digital system. You're very much correct. I think NUREG/IA used complex logic rather than software. But yes, I mean we were trying to be as broad as we could be in terms of being inclusive with the words, "Digital system."

MEMBER BROWN: If not -- again, I'm a designer, but I view the combinational logic, combinational design digital systems. They have a different mode of failure than you're going to -- well, I'm not calling it because it's not software.

They have different modes of failure than does software-driven.

MR. GUTIERREZ: You're right.

MEMBER BROWN: Which has a whole wider range. So, that's why I wanted to ask the question. So, you're intending for this to cover the whole spectrum?

MR. GUTIERREZ: Yes. We tried to.

MR. BIRLA: This is Sushil Birla again, NRC Research. So, just a clarification on that answer. There can be very complex digital systems, and there can be very simple digital systems. So, our set K -- set L, I should say, which defines 10 of them, covers the whole spectrum, meaning the most complex that we see. We don't know whether there will be more complex ones. That's why he says technically we don't acclaim completeness.

Now, if you had very simple systems, you don't need all 10 of them. Take the 10th one, for example, time behavior. Even if you have a software-based system that doesn't have any redundant elements we will not have real time behavior. Only non.

So, consider the answer in that context. So, you could reduce this to a smaller set if you had

a very simple system, of the kind you were thinking about: electro-mechanical relays.

MEMBER BROWN: You said 10. I only count nine on this page. Did I miss something.

MR. BIRLA: There might have been two packages.

MEMBER BROWN: Two short or two long? Is that two? All right, I'm just trying to make sure I understood the distinction that he was making relative to Myron's initial comment. How do you intend to use this?

MR. GUTIERREZ: I mean we're exploring different ways of using it, using it now.

MEMBER BROWN: I forgot what RIL is.

MR. GUTIERREZ: Research Information Letter.

MEMBER BROWN: Okay. So, I guess it's nice, but does it go get filed somewhere? Where does it get -- where does the ability to use a common set between various organizations in NRC get -- I don't know, triggered is the wrong word.

MEMBER SCHULTZ: Maybe that means tell us more about your second last bullet.

MEMBER BROWN: Well, I guess that's a good

point. Are you trying to coalesce these three columns into one? Is that what you're -- is that what you mean by harmonization? I mean I didn't have any big problem with the three columns because it kind of describes --

MR. LI: My understanding of the vocabulary is terminology where we tried to unify the terminology. Correct me if I'm wrong.

MEMBER BROWN: That's internal? That's within NRC? I mean --

MEMBER SCHULTZ: What's your intention of this harmonization.

MR. LI: The first step is within NRC.

MR. GUTIERREZ: Yes, that's the first step. I don't know that we can harmonize the world with vocabulary.

CHAIRMAN STETKAR: But what a minute. Don't be so glib with that answer. "We don't know if we can harmonize the world." This is something that both the regulator and the industry, throughout the world, are struggling with. And you taking an arrogant approach that we will develop our own internal vocabulary, regardless of what anybody else is doing, to me is irresponsible.

MR. GUTIERREZ: I don't think that's what we're doing.

CHAIRMAN STETKAR: So don't do that.

MR. GUTIERREZ: Absolutely not, no. I wouldn't -- I think when I talk to people about any of these definitions, I've always treated it with respect, and I try to consider everything that they point out.

CHAIRMAN STETKAR: So, why don't we try to reach a consistent understanding without saying, "We're going to develop our own and we can't try to harmonize with everybody else?"

MR. GUTIERREZ: No, I'm sorry. I think my intent was taken the wrong way here. I'm not throwing out anything. I'm not trying to be glib.

I think what we've found when we had our own discussions here between DE and DRA is that as we talk about things, we slowly move into a better understanding of what you mean. That's what we're trying to do.

CHAIRMAN STETKAR: And that, in my opinion anyway, and again this is subcommittee so it's my personal opinion, that conversation ought to in real time involve EPRI.

MR. GUTIERREZ: Yes, I think --

CHAIRMAN STETKAR: Because quite honestly, I think they're way ahead of you.

MR. BIRLA: This is Sushil Birla again, Office of Research NRC. That second last bullet is there just to reinforce what you just told us: that this is future work we have to do.

When Mauricio said that we cannot harmonize the whole world, what he meant was it's a very difficult job, and we cannot get everyone to agree on -- just look at the discussion in this room.

So, how do we deal with that? We are learning how to deal with that, and we have found that there are scientific approaches in dealing with these differences. So many thoughts about mapping of the failure modes.

Mapping is one way. So, people in their own domains and languages and subcultures might use their own vernacular, but if we can at least have an agreed upon mapping; if you say X in our language, it means Y. It is progress in communicating ambiguously.

Now, how do you do that with a science base? We've consulted outside experts. Just a couple of months ago, we consulted experts at NIST who

encountered the same problem in the pharmaceutical patent business between the manufacturers who claim they have a patent and others who say, "No, you don't." It boils down to an argument over the words. What do the words mean?

They find that in technical literature, medical technical literature to research literature, that diseases called by different names and the treatment modality is called by different names, and sometimes even the chemicals are identified by different names, but they have found a science, the science of ontology and computational linguistics to establish relationships across these different nuances and come down to a conclusion, whether it's the same thing or not the same thing.

If it's not the same thing, then what is common and what is different? So, we'll have to go through that. Today we do not have a common agreement on many terms. Even verification, validation, assurance, and I've got a list of about 30 to 40 terms that are fundamental to the business, but every standard has a different set of definitions.

We reference in the NRC regulatory guidance IEEE 1012, IEEE 7032, and these two

fundamental standards don't have the same definitions. So, we recognize it is something we have to try and harmonize, and we recognize that we have a role in it.

What he was trying to say is that it's not an easy road.

MEMBER SCHULTZ: Thanks. We have a long-term colleague who used to say half the problems in the world come from people using the same name for two different concepts, and the other half are people using different names for the same concept.

MR. GUTIERREZ: That may continue, right?

MEMBER SCHULTZ: Well, you're headed in a direction that might prove helpful. I just was hoping you could tell us a little more what you envisioned on that vocabulary harmonization, but it sounds as if you haven't really worked that out yet.

MR. GUTIERREZ: It's in early stages.

CHAIRMAN STETKAR: It's a little bit important though, harking back to some of the stuff that we talked about yesterday in terms of that diagram that had a lot of blue and a couple of white things, and out at the end were regulatory guidance.

If the notion is that development of a vocabulary, if you want to call it, that for failure

modes implies a direction of research, and direction in terms of thought processes that will guide that research developing methods and analytical methods, and a compilation of data to fit that construct that can be quite important. That's not just communication. That's actually developing a conceptual framework.

If that conceptual framework is at odds, and I don't know what the angle between the odds is with a conceptual framework that's being developed in the industry, at least there should be a very clear understanding of, A, that fact, and B, why.

Because especially if the agency is going to embark on developing methods and quantitative ways of treating information data or whatever, to fit this kind of taxonomy that's being developed here, that's really important.

MR. BIRLA: This is Sushil Birla from NRC Research again. So, let's just -- separate from the definition of harmonization in our vocabulary, which was a more general topic, now let's talk about the use of failure modes or the set of failure modes.

Specifically, you had requested in the September meeting to try and harmonize with EPRI. We

put that on the table in our last meeting with EPRI in the research memorandum of understanding, and EPRI has it under advisement but they want some time to think about it.

You asked a question about experience. I think that's partly what they're waiting for: learning from application, what you learn from experience and applying them.

I recognize that the word failure doesn't cover necessarily all kinds of misbehavior. That's part of the hesitancy here in saying that this is the set we want to run with.

The other industry group that we worked with is IEEE standard 7032 working group; that's working group 6.4. They are developing a division to IEEE 743 to Annex D. Annex D concerns hazard analysis.

In Annex D, they have included this very set; what they call set L. So, that's progress towards socialization in industry.

CHAIRMAN STETKAR: Part of what I think we're also dealing with here is some time yesterday, I think it was in EPRI's presentation, there was a slide that develops this notion of failure modes versus -- I

think they use the term failure mechanisms. I'm searching for the slides.

But the thing -- I tend to cause them causes and failure modes, but that's also just vocabulary. Concept at one level -- I mean you might call the -- my example of the valve the corroded stem or the loose bolt a failure mode. Somebody else might call it a failure mechanism.

Now, the aggregation of failure mechanisms at one level manifests itself in terms of failure modes if the valve didn't open. And yet, the valve didn't open failure mode for that valve; you might consider that to be a failure mechanism for the system where the system failure mode is it didn't deliver any flow.

MR. GUTIERREZ: Right.

CHAIRMAN STETKAR: And to make sure that we understand that type of discussion here, when you say the EPRI guide words, they may in their concept think of those as, "Those aren't failure modes. Those are failure mechanisms."

That's okay as long as we all agree that those are the fundamental concepts.

MR. GUTIERREZ: Right.

CHAIRMAN STETKAR: I think that's what we're facing here.

MR. GUTIERREZ: Yes.

CHAIRMAN STETKAR: Okay. Anything more for the staff? You look pensive.

MEMBER SCHULTZ: No, no. I think it's moving forward. That's good.

CHAIRMAN STETKAR: Thank you.

MR. GUTIERREZ: Thank you.

CHAIRMAN STETKAR: What I'd like to do now is ask to see if there are any public comments from anyone in the room, and while we're doing that, we'll get the bridge line open to see if there's anyone on the bridge line. Russ?

MR. SYDNOR: I guess I'm not the public,

CHAIRMAN STETKAR: No, it's anyone in the room.

MR. SYDNOR: Russ Sydnor, Office of Research. I just wanted to thank the ACRS for taking the time. It's a lot of material covered in a day-and-a-half. We're here because you prompted us to come here and talk about these things.

So, I wanted to say thanks for doing that. We're going make our work better. I think EPRI

appreciates that. I think we've been working closely with EPRI and we're going to continue to do that. We're seeing common understanding, but we're seeing development of some things I think can improve not only PRA but digital systems, safety review processes too.

So, I just wanted to say thanks for the feedback. We do take the feedback seriously. I know in the past, ACRS has said, "Involve us in research as you go, not necessarily come and deliver a product at the end that we'll argue about." So, we're trying to do that. So, I just wanted to say to this group thank you.

CHAIRMAN STETKAR: Thank you, Russ. For the record, I always have to say this: We are not the ACRS in this meeting. We are a joint meeting of two subcommittees, and we speak only as individuals here. So, this is -- nothing you heard in the last day-and-a-half is feedback from the ACRS. That's for the record.

No, that's honestly. The ACRS only communicates formally to the Commission through our letters, which is a consensus process. So, these -- anything you've heard are simply a number of

individuals mouthing off.

With that, anybody else in the room have any comments?

MR. BRIAN: Just one quick comment, and it's very quick. I did a -- what Russ said. I totally understand what you're saying, but we appreciate it all. It's very, very useful feedback which we can factor into our processes going forward. Thank you very much.

CHAIRMAN STETKAR: Thanks. I've been told that the bridge line is open. I don't know if anyone is out there, nor do I know actually whether it's open. So, if someone is out there, just please do me a favor and say hello just so we confirm it is open.

MR. ENZINNA: Hello. This is Bob Enzinna.

CHAIRMAN STETKAR: Thank you. Now, is there anyone on the bridge line who has any comments? If so, please identify yourself and speak.

MR. ENZINNA: I'd like to make a brief comment. This is Bob Enzinna at AREVA.

CHAIRMAN STETKAR: Go ahead.

MR. ENZINNA: I'd like to make a suggestion as to where to go. Now, you've got these failure modes, and I think what would be interesting

to me from the PRA perspective is to know how far these failure modes can propagate with respect to common cause failure.

John said earlier - I think it was John - that the most important defense is independence. But I'd like to know -- I'd like to see some assessment of these failure modes with respect to the barriers against propagation.

Compare these failure modes to the defenses; work with EPRI and compare these failure modes to the defenses Ray was talking about so we can judge how much credit these defenses have against preventing propagate to these failure modes. Then you'd have something that would be useful to the PRA.

CHAIRMAN STETKAR: Great. Thank you very much. Anyone else on the bridge line that would like to make a comment? Hearing none, we'll close the bridge line only because it tends to -- you'll still be able to hear us. It tends to pop and crackle in here and be a distraction for us.

With that, as we always do in subcommittee meeting, I'd like to go around the table and see if any of the members have any final comments. Two things I'll ask is -- and think about the second one a

bit.

First of all, think of any comments you might have and should we bring this issue at this time to schedule a full committee meeting? Because Myron doesn't get a chance to answer the second question, I'll let the rest of you think about the second question. Myron, do you have any final comments that you'd like to make?

MR. HECHT: No, I -- no.

CHAIRMAN STETKAR: Thanks. Steve?

MEMBER SCHULTZ: I'd just like to thank the staff and EPRI for their presentations, and for the discussions that we had over the last day-and-a-half.

With regard to whether this is timely for the full committee, I need to think about that. I don't recall whether we had a full committee meeting related to this in 2013. I did not think we did.

CHAIRMAN STETKAR: No, we did not. The full committee has not -- I don't remember the last full committee meeting. It was quite a while ago.

MEMBER SCHULTZ: There are aspects of the progress that I think the full committee would benefit from hearing. I'm just not sure if it warrants a full

presentation at this time.

CHAIRMAN STETKAR: Okay. Thank you. Dennis?

MEMBER BLEY: There's a lot to digest from the day-and-a-half. I haven't digested it all yet. So, I have no further comments beyond those I've made.

For two reasons, I think we should have a full committee meeting. The first is I agree with Steve. It's been a long time and the full committee could benefit from hearing at least a summary of what we've heard in the last day-and-a-half.

The second is it seems to me, and I have to think more about this, but it seems to me we've heard a number of things and made a number of individual comments that would be good to coalesce and do a letter from the full committee putting down a full committee position on at least some of the issue we talking about.

CHAIRMAN STETKAR: All right. Ron?

MEMBER BALLINGER: Yes, I think I look at this from a more ignorant point than most of the other committee members that I found the presentations, especially the EPRI one, very, very good. And so, speaking as a less educated member in this subject, I

think that the other members of the full committee would be -- would gain from hearing something -- hearing something about that.

CHAIRMAN STETKAR: Charlie?

MEMBER BROWN: Yes. I'm trying to organize my comments. You made a correct observation relative to anything we say here as a subcommittee, and therefore it's not the committee.

As you've heard me repeat a couple of times in the last two days relative to fundamental principles, I did want to throw in an observation because I'm aiming this at EPRI and NEI for the most part, and I will relate it to NRC a little bit.

We have internally, as a committee, taken some action relative to those principles. If you look at the previous role of analog equipment, the existing standards and just the characteristic of analog systems, along with the IEEE standards gave you a pretty good barrier relative to -- and I'm talking reactor trip and safeguard systems right now.

The electrical isolation requirement effectively -- I mean you got to work to not have independence if you maintain electrical isolation between divisions. The nature of analog systems with

resistors, capacitors and inductors fundamentally gave you time response and deterministic straight through behavior, and the inability to, from external sources, to come down and modify or alter the set points and other key characteristics of the channels themselves in terms of how they processed or how they tripped, was pretty much under the control of the operators.

And so, those three areas in the analog world were pretty well protected in terms of providing the back stop relative to independence, preventing external access and ensuring repeatable and predictable processing of data.

Computer-based systems have altered that whole picture. Electrical isolation doesn't work from that standpoint. You do have to communicate between divisions for voting and that opens up a vulnerability of, while there are arguments as to whether it can or can't happen, it opens up the thought process of lock up of voting units due to corrupt data from any particular system.

So, the independence does not have the same backstop as the analog systems do. Control of access with network buses, as I mentioned and we talked about during the meeting, provide the potential

if you have access of the in-plant network buses to the external world if it is not blocked totally.

Doesn't mean you can't send in information that you don't run a software controlled data communications path. It should be hard wired one way so that it can't be compromised. So, that one is more vulnerable.

In terms of processing and determinant behavior, software can be very indeterminate depending on how your operating system and your software is configured. It may be not as repeatable and predictable and it would be unpredictable when it would be unpredictable. That's kind of a backwards way of phrasing it.

The committee has made an attempt, based on the new rules being propagated. We have written a letter/report on it where we have made recommendations. I would encourage -- I mean I can't tell anybody obviously. It's not even resolved here within the NRC, but I would encourage the NEI and EPRI, the industry groups, to take a look at that, and say, "Hey, look, gentlemen. The industry really needs to take and re-institute and put those backstops, those preventive measures, back in place the way they

were before."

So, that's the one observation I -- and it was really great. I thought EPRI and NEI, based on other meetings we've had, and the staff as well today, have made really good presentations, and I appreciate it.

They were all very informative, but I would recommend that EPRI and NEI start looking at these particular areas as we have asked the staff to look at, to say, "All right, maybe we ought to take this bull by the horns and do it ourselves."

So, that was -- that's my closing statement.

CHAIRMAN STETKAR: Thank you. Joy?

MEMBER REMPE: I missed prior subcommittee meetings on this topic, and so I appreciated the opportunity to learn from EPRI, the staff and my colleagues. It was more than would've been possible with me reviewing the materials on my own.

As a Member of the full ACRS, I was also pleased, and I think we should acknowledge Russ's and Brian's comments at the end because I do think it helps educate us in advance, and hopefully there's some input that spoke to everyone involved.

I was very interested in hearing about the EPRI approach and how it is progressing, and I hope we get to hear more about it and the document with the results from the Palo Verde effort.

On the NRC effort, I hope that we see some of our suggestions incorporated into the plan that you're updating. I hope we see more tasks identified between and related to the final reliability and risk modeling method, and the guidance. And I believe John mentioned about the need for a pilot plan and a demonstration test to be added to that pilot plan but I wanted to emphasize that again.

I also hope that we get more details about the harmonization included in that program as you go forward.

With respect to the draft NUREG that we were given, I hope before you issue it for the public comment that someone takes a critical look at that document so that you avoid some unnecessary comments that you have to respond to. I mentioned some of my concerns during the meeting, and I'm willing to voice them again if you want to hear about them.

CHAIRMAN STETKAR: Make sure you're on the mic. Talk in the mic.

MEMBER REMPE: I would like to have someone look at it before it goes out. Oh, and with respect to full committee meeting, I vote for it because there's a lot of information that I had not seen before as a full committee member because I hadn't attended the subcommittee meetings. I think it would be useful especially if there's a revised program plan.

CHAIRMAN STETKAR: Thank you. Dennis?

MEMBER BLEY: I thought you were ready to hang up.

CHAIRMAN STETKAR: I gave Myron a chance to talk. He said he didn't have anything to say.

MEMBER BLEY: You're right.

CHAIRMAN STETKAR: It was a long time ago, but indeed -- indeed. I'm sure if he would've thought of something, he wouldn't be bashful and speak.

In summary, I -- again, I'd like to thank the staff and EPRI for all the effort they put in. It's a grueling day-and-a-half and a grueling amount of material to go through. I think I really appreciate the effort that was put in my everyone to organize and focus the discussions.

It was I think a really useful

subcommittee meeting.

Regarding full committee meeting, my -- I've been making notes to myself, and they are, "Gee, should we have a full committee meeting now? Should we wait?" It's an ongoing process. We've heard about some reports that might become available in early to mid 2015.

The question is do we wait until we get those reports? But at that time, it'll still be moving. So, I think I tend to agree with what I've heard around the table. We should probably schedule a full committee briefing.

The practicalities of that are it won't happen until probably the March time frame at the earliest. I've forgotten what our calendar looks like for February, but I think we probably should look some time in the first quarter of next year to have appropriate briefing for a variety of reasons.

I was trying to look back. I don't know when the last ACRS letter was written particularly on the topic of digital I&C PRA. I found one in 2008 that talked about failure modes, but that's -- it's a long time ago. So, I think it's worthwhile to bring the full committee up to speed on what's happening.

With that, if there are no other comments by anyone, we are adjourned.

(Whereupon, the above-entitled matter went off the record at 11:42 a.m.)

ELECTRIC POWER RESEARCH INSTITUTE

Update on Digital Instrumentation & Control Projects

- Digital System Failure Modes
- Modeling Digital I&C in PRA
- Techniques for Failure Prevention and Mitigation
- Status of Hazard Analysis Demonstration Project

Ray Torok
EPRI
Bruce Geddes
Southern Engineering Services
Dave Blanchard
Applied Reliability Engineering

Advisory Committee on Reactor Safeguards
Subcommittee on Digital Instrumentation & Control Systems
November 18-19, 2014

Update on EPRI Digital I&C Projects
Contents/Purpose

Purpose of presentations

Update ACRS on EPRI research activities around understanding, preventing, and/or mitigating digital failure modes

Four topics

- Digital System Failure Modes – Bruce Geddes
- Modeling Digital I&C in PRA – Dave Blanchard
- Techniques for Failure Prevention and Mitigation – Ray Torok
- Status of Hazard Analysis Demonstration Project – Bruce Geddes

Consistent treatment of failure mechanisms, modes and effects throughout

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Update on EPRI Digital I&C Projects
Key Points/Conclusions

- Problem statement: Potential digital failures, including common-cause failure, that result in loss of critical system functions (e.g. as expressed in SECY 93-087)
- Much progress in recent years:
  - Improved understanding of digital system failure modes and measures to prevent / mitigate them
  - Application of PRA to develop risk insights that help identify and address potential vulnerabilities
  - Advanced failure/hazard analysis techniques to identify and address potential vulnerabilities
- Time to apply updated knowledge and tools in plants
- Work ongoing by industry to update their guidance and plant procedures – EPRI supporting with technical guidance and tech transfer

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Update on Digital Instrumentation & Control Projects
- Digital System Failure Modes

Bruce Geddes
Southern Engineering Services

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Digital System Failure Modes
Contents

- Key points
- Historical perspective
- Levels of interest
- Hazard analysis methods
- Example - Functional failure modes and effects analysis (Functional FMEA)
- Taxonomy of low level failure mechanisms and defensive measures
- Conclusions

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Digital System Failure Modes / Misbehaviors
Key Points

- Purpose of presentation
  - Extend failure modes discussion from September 2013 presentation on hazard analysis
  - Clarify application of failure mechanisms / mode / effects at various levels of interest
- Technical points
  - Failure mode treatment is consistent with PRA principles
  - Important to consider failure modes at the appropriate level of interest – hazard analysis “guide words” can apply at any level
  - Understanding low level digital failure modes/mechanisms is useful in assessing protection against undesired effects at higher levels

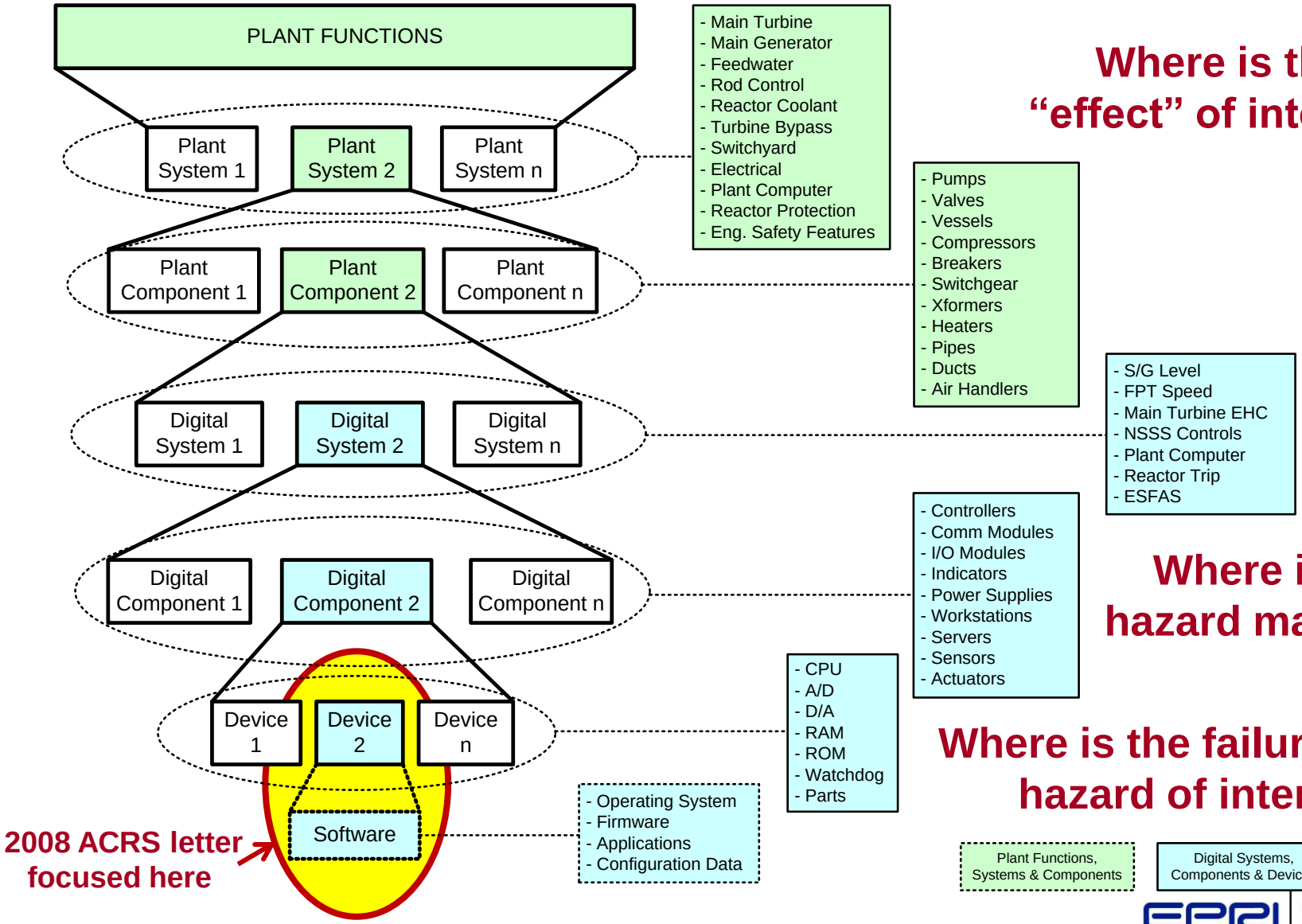
© 2014 Electric Power Research Institute, Inc. All rights reserved.

Digital Failure Modes
Historical Perspective

- ***"Digital I&C may introduce new failure modes that are not well understood."*** – Letter, Chairman ACRS to Chairman U.S. Nuclear Regulatory Commission, April 29, 2008
- Failure mechanisms produce failure modes which, in turn, have effects on plant system operation (NUREG 0492 – Fault Tree Handbook, January 1981)
- EPRI hazard analysis guide (EPRI 3002000509)
  - Presented to Subcommittee in 2013
  - Provides useful framework for considering mechanisms, modes and effects at appropriate "levels of interest"

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Key to Focusing Failure / Hazard Analysis - "Levels of Interest"



© 2014 Electric Power Research Institute, Inc. All rights reserved.

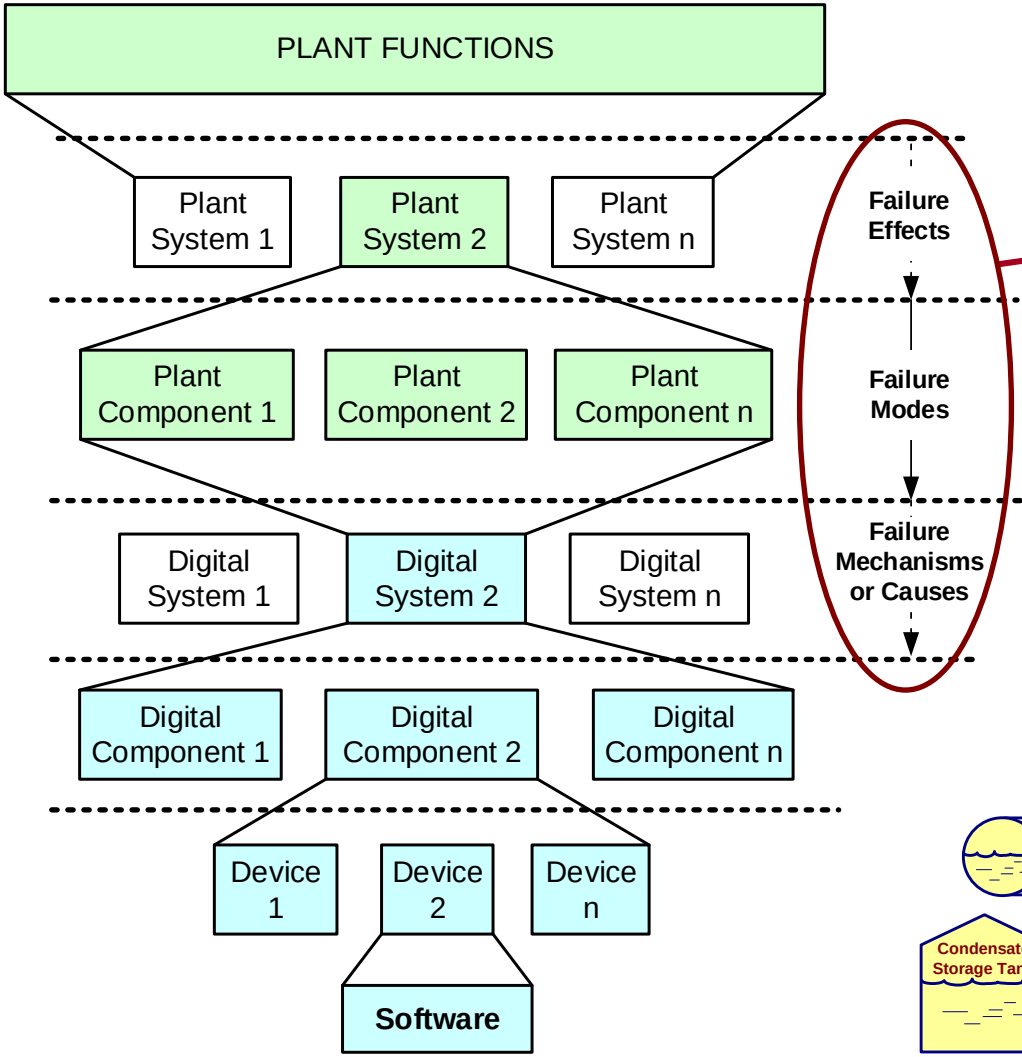
Hazard Analysis Methods for Digital Instrumentation and Control Systems (EPRI 3002000509)

Six Methods Investigated	'Top-Down' or 'Bottom-Up'	Strengths		
		Identifies Hazards Beyond Faults/Failures	Integrated View of Plant Design	Mature, Well Documented
Functional FMEA (Failure Modes & Effects Analysis)	Top Down		X	X
Design FMEA	Bottom Up			X
Top-Down using FTA (Fault Tree Analysis)	Top Down		X	X
HAZOP (HAZard and OPerability Analysis)	Top Down	X	X	X
STPA (Systems Theoretic Process Analysis)	Top Down	X	X	
PGA (Purpose Graph Analysis)	N/A	X	X	

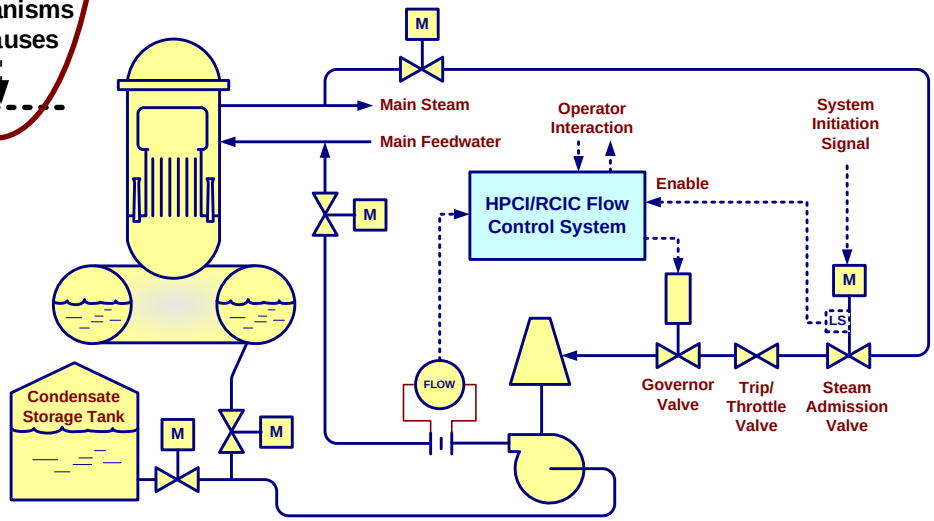
Blended approaches may combine strengths of multiple methods

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Example of the Functional FMEA Method: High Pressure Coolant Injection (HPCI) System



Example in 3002000509 evaluates postulated functional failures at the plant system level & their potential *causes* due to digital control system failures or misbehaviors



© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Functional FMEA Worksheet for HPCI Example

PFMEA Number: **Example 4-1** | **Prepared by/Date:** | **Sheet: 1 of 3**

High Level Process/Functional Area (check one):
(X) Safety
( ) Equipment Protection
( ) Power Generation

Equipment: **HP[illegible]rol System**

Checked by/Date:

Lifecycle Phase: Conceptual Design

Rev: 0a

Row No.	Function	Process	Requireme[illegible]	Potential Failure Mode	Potent[illegible] Effect(s) of [illegible]	Possible Cause(s)/ Mechanism of Failure	[illegible]rent/Detect Method	Detection	Recommended Action
1		Turbine/pump provides required coolant flow	5000 gpm (HPCI) 500 gpm (RCIC) @ 1000 psi, on demand, within 60 seconds	No coolant flow	Loss of Rx inventory, lea[illegible] to core damage	[illegible]	[illegible]e V&V [illegible]S PM 3. Turbi[illegible]e PM	1. ESFAS Test 2. System Flow Test	Evaluate flow control [illegible]des
2				Less than 5000 gpm (HPCI) or 500 gpm (RCIC)	Less than adequate Rx inventory, possibly leading to core damage	1. HPCI starts, but turbine trips 2. Turbine speed too low 3. Incorrect setpoint	1. Software V&V 2. ESFAS 3. Turbin 4. Setpoi Control P 5. Human Performa		
3				More than 5000 gpm (HPCI) or 500 gpm (RCIC)	Too much Rx inventory, possibly leading to Rx overfill	1. Turbine speed too high 2. Incorrect setpoint			
				5000 gpm (HPCI) or 500 gpm (RCIC), but after 60 seconds	Less than adequate Rx inventory, possibly leading to core damage	1. Late initiation signal (or late response) 2. Ramp rate too slow			
				No steam flow	Loss of Rx inventory, leading to core damage	1. Steam line break 2. Inadvertent isolation	1. H_2O Chem. 2. Human Performance	1. Section 11 Test 2. Alarms	
			ty at	Poor steam quality (high moisture)	Turbine degradation, eventual loss of Rx inventory	1. High carryover from Rx	Rx PM	1. System Flow Test 2. Turbine PM	
				Steam pressure too low	Less than adequate Rx inventory, possibly leading to core damage	1. Steam line leak 2. Steam line partial blockage	1. H_2O Chem. 2. FME Program	1. Section 11 Test 2. Alarms	
				Steam pressure too high	Relief valves lift, steam pressure/flow transients	1. Steam hammer 2. Rx pressure transient	1. Ops Procedures 2. Human Performance	Alarms	
				No water flow	Loss of Rx inventory, leading to core damage	1. Empty CST or Torus 2. Inadvertent isolation		1. Alarms 2. CST/Torus Surveillance	
			ate	Foreign material in water	1. Pump damage, less than aequate flow 2. Clogged strainer, low NPSH, less than adequate flow	1. Inadequate FME controls 2. Material degradation	1. Human Performance 2. H_2O Chemistry	1. System Flow Test 2. Chemistry Samples	
				Less than adequate NPSH	1. Pump cavitation, eventual damage, less than adequate flow	1. Low water level in CST or Torus 2. Pipe obstruction	1. Ops Procedures 2. FME Program	CST/Torus Surveillance Test	
12		Coolant Flow Path to Rx	Maintain pressure boundary integrity, capable of 5000 gpm @ 1000 psi	Loss of pressure boundary	Loss of Rx inventory, leading to core damage	1. Pipe break 2. Interystem leak	1. H_2O Chemistry 2. Human Performance	Alarms	
13				Capacity less than 5000 gpm	Less than adequate Rx inventory, possibly leading to core damage	1. Pipe leak 2. Intersystem leak			
14				Less than 1000 psi	Less than adequate Rx inventory, possibly leading to core damage				

What can go wrong?

Guide Words:

- **No Function**
- **Partial Function**
- **Over Function**
- **Degraded Function**
- **Intermittent Function**
- **Unintended Function**

What can cause the problem?

© 2014 Electric Power Research Institute, Inc. All rights reserved.

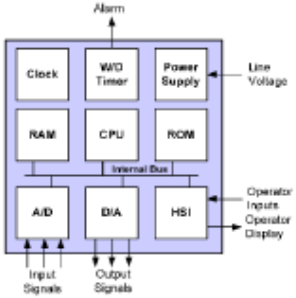
EPRI ELECTRIC POWER RESEARCH INSTITUTE

EPRI 3002000509 Appendix B: Taxonomy of Failure Modes, Failure Mechanisms & Defensive Measures

Functional Level		Diagram	
System	HPCI, RCIC	See Figure 5-	
Subsystem	Positioner		
Component Identification	Function(s)	Failure Modes	Failure Mechanisms
Governor	Provide automatic governor valve position demand signal to digital positioner to compenate for error between actual turbine speed and demanded turbine speed	Output Fails Offscale High	1. CPU Data Corruption 2. CPU Logic Error 3. D/A Device Error 4. Lost or corrupted RAM data
		Output Fails Offscale Low	
		Output High Rate of Change	
		Controller Lockup	1. CPU Halt 2. CPU Crash 3. Stopped internal clock
		Failure to Boot or Reset	1. CPU Data Corruption 2. CPU Logic Error 3. Lost or corrupted ROM data
		Dead Controller	1. Failed internal power supply 2. Line voltage below spec

Design FMEA Worksheet

Sheet B-4a
Type 1 Controller Component Failure Modes



This is a basic layout of a standalone controller, labeled "Type 1" in this guideline. A Type 1 controller is capable of performing typical I&C loop functions without the need for any other modules.

A Type 1 controller typically contains CPU, RAM, ROM, A/D Converter, D/A Converter, HSI, Clock, Watchdog Timer, and internal Power Supply devices (see related Taxonomy sheets).

Failure Mode	Failure Mechanisms	Defensive Measures
Controller Lockup	1. CPU Halt 2. CPU Crash 3. Stopped internal clock	See CPU Device Taxonomy Sheet B-1a See Clock Device Taxonomy sheet (TBD) Configure W/D Timer to detect, alarm, and force outputs to preferred state
Dead Controller	1. Failed internal power supply 2. Line voltage below spec	See Power Supply Device Taxonomy Sheet (TBD) Implement redundant, uninterruptable line power
Outputs Fail High Outputs Fail Low Output High Rate of Change	1. CPU Data Corruption 2. CPU Logic Error 3. D/A Device Error 4. Lost or corrupted RAM data	See CPU Device Taxonomy sheet B-1a See RAM Device Taxonomy Sheet B-2a See D/A Device Taxonomy Sheet (TBD) Implement "loopback" signal by connecting outputs to spare inputs and check for deviations via SW logic Implement redundant controller, validate output from primary controller, takeover if needed
Loss of Input Signal Processing	1. CPU Data Corruption 2. CPU Logic Error 3. A/D Device Error 4. Lost or corrupted RAM data	See CPU Device Taxonomy sheet B-1a See RAM Device Taxonomy Sheet B-2a See A/D Device Taxonomy Sheet (TBD) Implement redundant controller to takeover if needed
Loss of Operator Interface	1. CPU Data Corruption 2. CPU Logic Error 3. HSI Device Error 4. Lost or corrupted RAM data	See CPU Device Taxonomy sheet B-1a See RAM Device Taxonomy Sheet B-2a See HSI Device Taxonomy Sheet (TBD) Implement redundant controller to takeover if needed
Failure to Boot or Reset	1. CPU Data Corruption 2. CPU Logic Error 3. Lost or corrupted ROM data	See CPU Device Taxonomy sheet B-1a See RAM Device Taxonomy Sheet B-2a Implement redundant controller to takeover if needed

Taxonomy Sheet

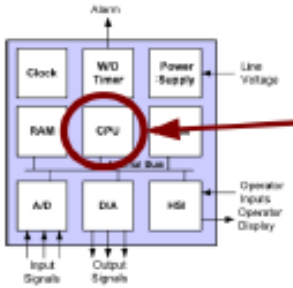
© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

EPRI 3002000509 Appendix B: Taxonomy of Failure Modes, Failure Mechanisms & Defensive Measures (cont.)

A Digital Component

Sheet B-4a
Type 1 Controller Component Failure Modes



This is a basic layout of a standalone controller, labeled "Type 1" in this guideline. A Type 1 controller is capable of performing typical I&C loop functions without the need for any other modules.

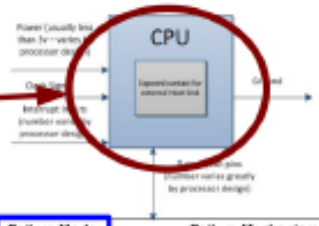
A Type 1 controller typically contains CPU, RAM, ROM, A/D Converter, D/A Converter, HSI, Clock, Watchdog Timer, and internal Power Supply devices (see related Taxonomy sheets).

Failure Mode	Failure Mechanisms	Defensive Measures
Controller Lockup	1. CPU Halt 2. CPU Crash 3. Stopped or [illegible] clock	See CPU Device Taxonomy Sheet B-1a See Clock Device Taxonomy sheet (TBD) Configure WD Timer to detect, alarm, and force outputs to preferred state
Dead Controller	1. Failed internal power supply 2. Line voltage below spec	See Power Supply Device Taxonomy Sheet (TBD) Implement redundant, uninterruptable line power
Outputs Fail High Outputs Fail Low Output High Rate of Change	1. CPU Data Corruption 2. CPU Logic Error 3. D/A Device Error 4. Lost or corrupted RAM data	See CPU Device Taxonomy sheet B-1a See RAM Device Taxonomy Sheet B-2a See D/A Device Taxonomy Sheet (TBD) Implement "loopback" signals connecting outputs to spare inputs and check for deviations via SW logic Implement redundant controller, validate output from primary controller, takeover if needed
Loss of Input Signal Processing	1. CPU Data Corruption 2. CPU Logic Error 3. A/D Device Error 4. Lost or corrupted RAM data	See CPU Device Taxonomy [illegible] See RAM Device [illegible] See [illegible] Implem[illegible] if needed
Loss of Operator Interface	1. CPU Data Corruption 2. CPU Logic Error 3. HSI Device Error 4. Lost or corrupted RAM data	See C[illegible] See R[illegible] See HS[illegible] Implem[illegible] needed
Failure to Boot or Reset	1. CPU Data Corruption 2. CPU Logic Error 3. Lost or corrupted ROM data	See CPU [illegible] See RAM [illegible] Implem[illegible] takeover to takeover if needed

Assess for Available Defensive Measures!

A Digital Device

Sheet B-1a
Central Processor Device Failure Modes



The number of input and output connectors and bits can vary greatly by the processor design. Also, some low power processors don't have the Heat Sink contact in the center because heat generation is not as much of a problem. Commonly the processor clock speed runs at a multiple of the input clock signal. Data I/O is commonly handled using various protocols, implemented by on-chip peripherals.

Common bit widths* of processors: 16, 32, and 64-bit

Failure Mode	Failure Mechanism	Defensive Measures
CPU Halt	1. Power Supply Off 2. Power Supply Dip	Do not turn off power Supply. Do not let power dip.
CPU Logic Error	1. Power Supply Dip 2. Bit Errors (radiation, EMI) 3. Design Flaws 4. Manufacturing Defect 5. Failed Connections (including internal bond-wire and lead free solder interconnect failure) 6. Overheating 7. Part Wear Out (e.g., due to various age-related degradation mechanisms, exacerbated by small feature size)	Do not let power dip. Quality testing. Ensure proper shielding around controller to protect against radiation and EMI. Integrity tests before and while running.** Use of diverse microprocessor Architectural diversity/redundancy Integrity tests before and while running ** Quality testing of processor cooling systems. Temperature monitors on or near the processor. Ensure cooling systems are properly mounted
CPU Data Corruption	1. Bit Errors (radiation, EMI) 2. Design Flaws 3. Manufacturing Defect 4. Failed Connections (including internal bond-wire and lead free solder interconnect failure) 5. Overheating 6. Part Wear Out (e.g., due to various age-related degradation mechanisms, exacerbated by small feature size)	Quality testing. Ensure proper shielding around controller to protect against radiation and EMI. Integrity tests before and while running..** Use of diverse microprocessor Architectural diversity/redundancy Integrity tests before and while running. ** Quality testing of processor cooling systems. Temperature monitors on or near the processor. Ensure cooling systems are properly mounted Use devices with feature size >= 350nm Specify devices with ceramic packaging Specify components using leaded solder
CPU Crash	1. Manufacturing Defect 2. Failed Connections (including internal bond-wire and lead free solder interconnect failure) 3. Overheating	Integrity tests before and while running. ** Quality testing of processor cooling systems. Temperature monitors on or near the processor. Ensure cooling systems are properly mounted
Permanent CPU Damage	1. Overheating 2. Part Wear Out (e.g., due to various age-related degradation mechanisms, exacerbated by small feature size)	Use devices with feature size >= 350nm Architectural diversity/redundancy Specify devices with ceramic packaging Specify components using leaded solder

Without *Defensive Measures*, Device Failure *Modes* Can Become Component Failure *Mechanisms*

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Summary / Conclusions

- Framework for understanding and assessing digital failure modes is in place
  - Failure mode treatment is consistent with PRA principles
  - Important to consider failure modes at the appropriate level of interest – hazard analysis “guide words” can apply at any level
  - Understanding low level digital failure modes/mechanisms is useful in assessing protection against undesired effects at higher levels
- Work remains to be done
  - Develop detailed guidance that would help utilities update plant processes to improve digital failure mode understanding and treatment
  - Incorporate lessons learned from tech transfer activities (e.g., Palo Verde demonstration project)

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Together…Shaping the Future of Electricity

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

ELECTRIC POWER RESEARCH INSTITUTE

Update on Digital Instrumentation & Control Projects

Modeling Digital Instrumentation and Control in Probabilistic Risk Analysis – EPRI Report 1025278

Dave Blanchard
Applied Reliability Engineering, Inc.

Advisory Committee on Reactor Safeguards
Subcommittee on Digital Instrumentation & Control Systems
November 18-19, 2014

Modeling Digital in PRA
Contents

- Key points
- EPRI research projects related to modeling digital I&C in PRA
- Modeling basis – reflects lessons learned
- *Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments.* 2012. (EPRI 1025278)
  - Overview of process
  - Insights and lessons learned
    - Sensivity of PRA results to modeling assumptions
    - Defense-in-depth and diversity considerations for I&C
- Conclusions

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Modeling Digital in PRA
Key Points – Guideline Principles

- Modeling digital I&C in PRA should be a collaborative effort involving both I&C and PRA experts
- Context
  - Identify the functions performed by the I&C given the integrated plant design as considered in the PRA
  - Key input to the level of detail needed in the model
- Defensive measures
  - Design practices and features should be considered when incorporating I&C models into PRA
  - Key input to developing reasonable ‘failure probabilities’
- Software is different – behaves deterministically, doesn’t wear out
  - PRA models the effect of encountering unexpected conditions for which software response results in adverse consequences.

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Modeling Basis Reflects Lessons Learned
Insights

- The I&C can be designed such that the PRA is insensitive to its misbehaviors
  - Context

    The defense-in-depth and diversity (D3) in the mechanical and electrical systems dictates the level of D3 that may be of value in the I&C.

  - Defensive Measures

    The digital system reliability need only be similar to that of a comparable analog system to manage risk adequately.

© 2014 Electric Power Research Institute, Inc. All rights reserved.

EPRI Research Topics Related to Modeling of Digital I&C in PRA

- 2004 – 2009 – Specific issues/scoping studies
  - Risk-informed defense-in-depth diversity analyses (1002835)
  - Risks and benefits of automated diverse actuation systems (1016721)
  - Value of defense-in-depth and diversity in digital I&C (1019183)
- 2009-2012 - Guidelines
  - Estimating failure probabilities for digital systems, December 2010 (1021077)
  - Modeling digital I&C in PRA using current techniques (EPRI 1025278, July 2012)

Lessons learned in activities analyzing specific issues helped shape the method of 1025278

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Modeling Basis Reflects Lessons Learned

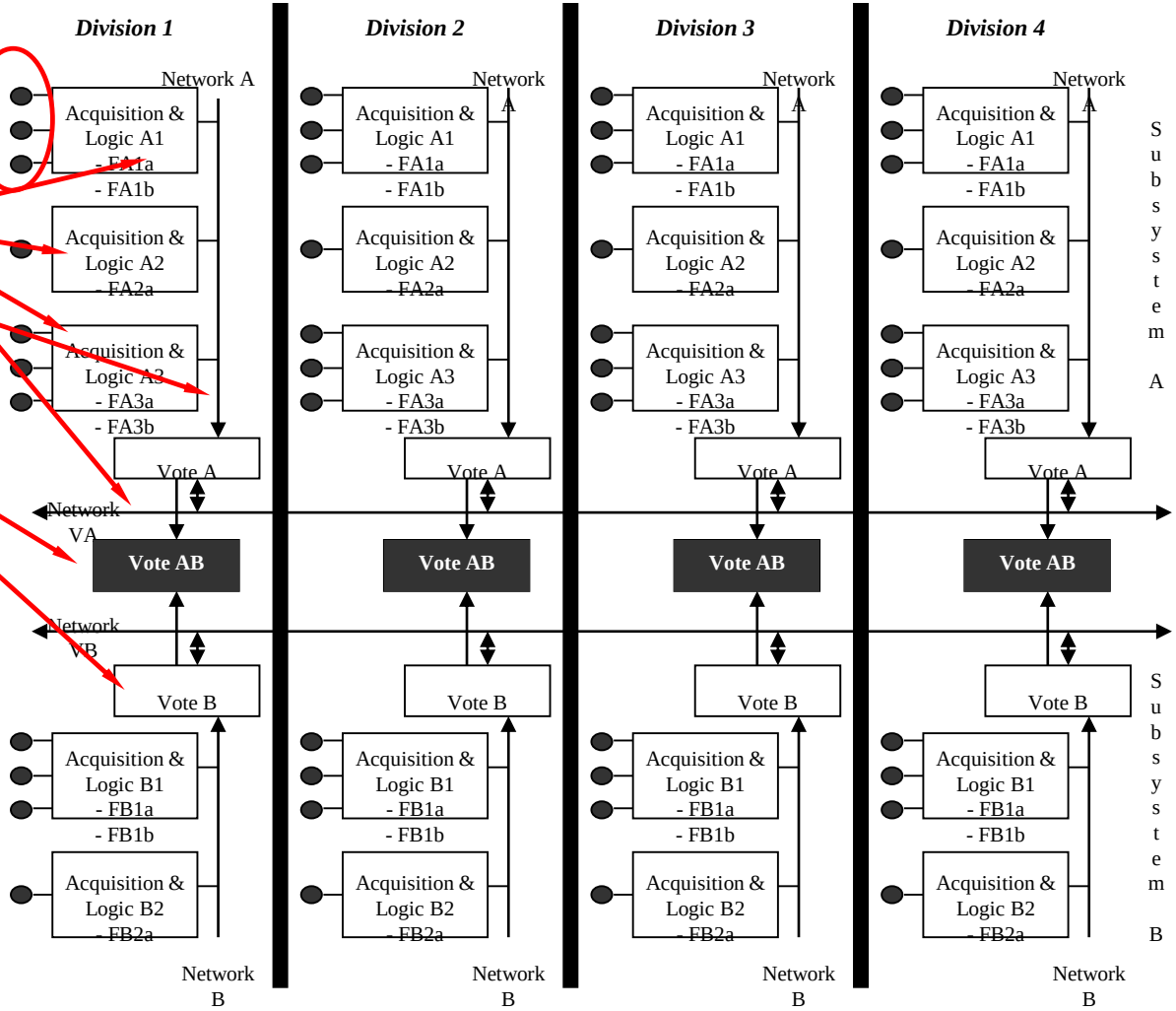
What are we trying to model?

Sensors

Signal processing

Communication

Voting



Functionally similar to analog I&C.

Modeling components having

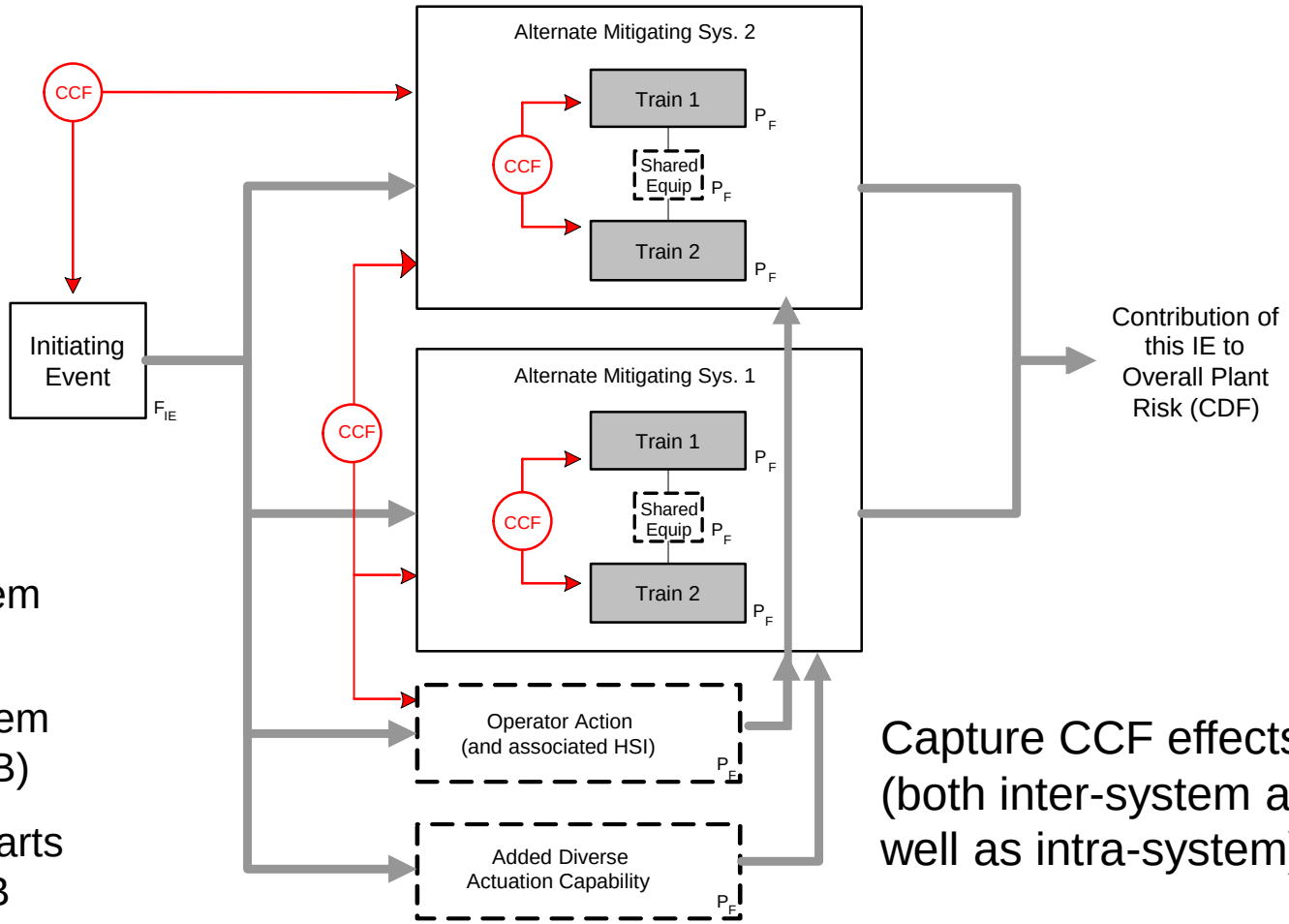
processors vs relays, acquisition logic vs signal converters, etc.

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Basis Reflects Lessons Learned

How are we trying to model it?



<u>Example</u>

Initiating event-
loss of feedwater

1st mitigating system
AFW

2nd mitigating system
PORVs/HPSI (F&B)

Operator action starts
AFW, initiates F&B

Diverse actuation
AMSAC

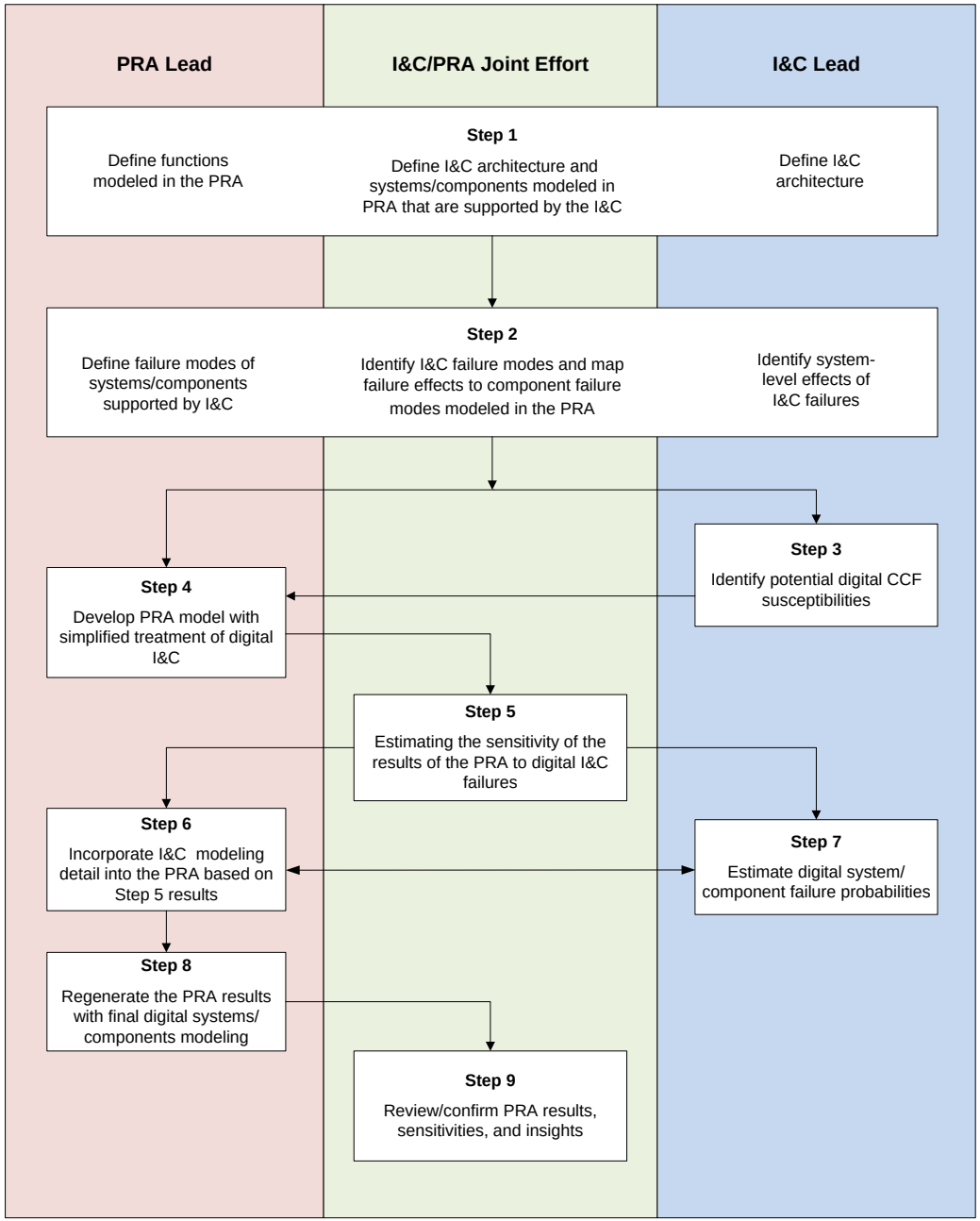
Capture CCF effects (both inter-system as well as intra-system)

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA (1025278)

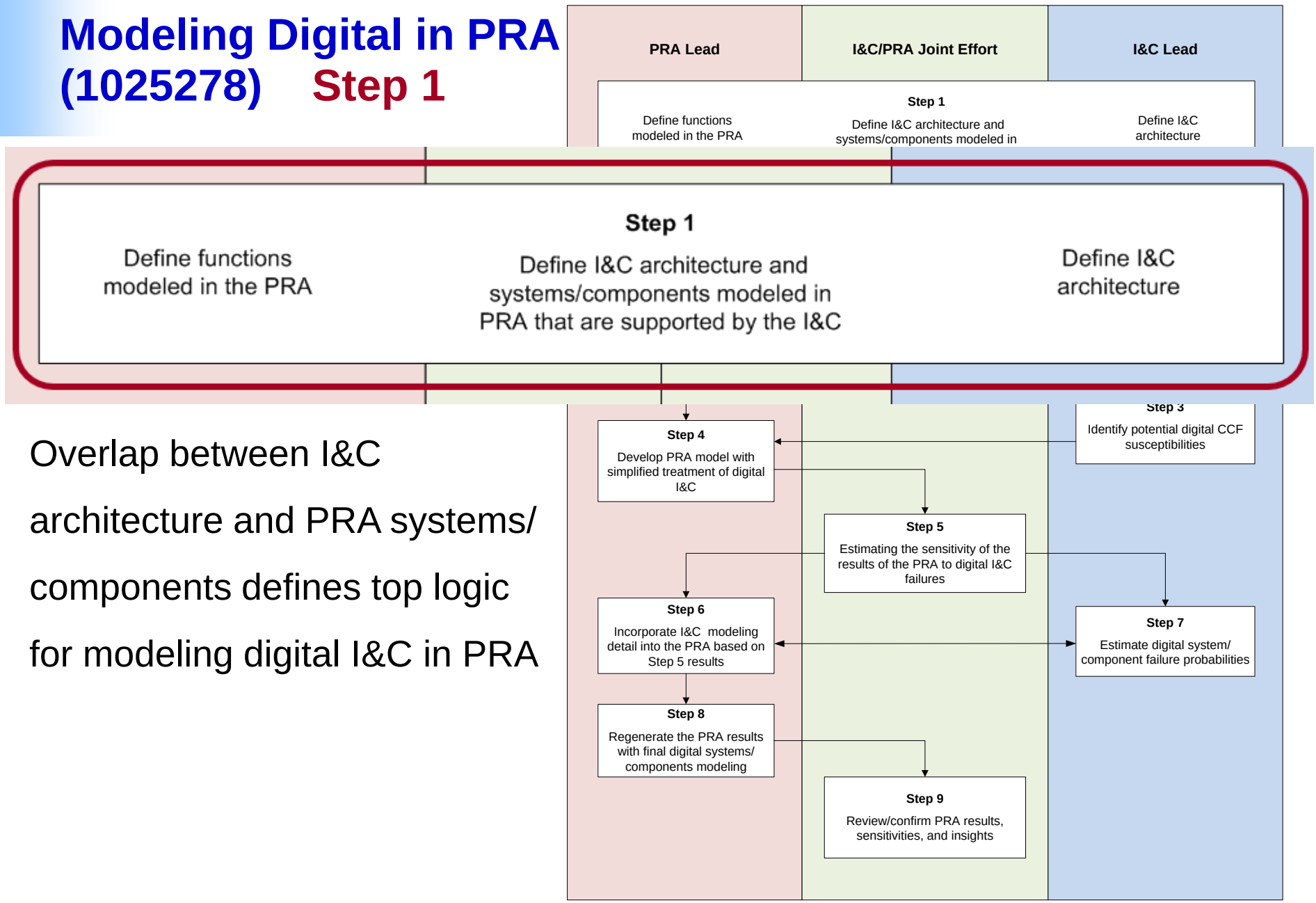
- Joint effort between I&C specialists and PRA analysts
  - Develop, quantify and apply digital system models
- Consider:
  - Context of I&C in system and integrated plant
  - Defensive design features in I&C components and architecture



© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital in PRA (1025278) Step 1



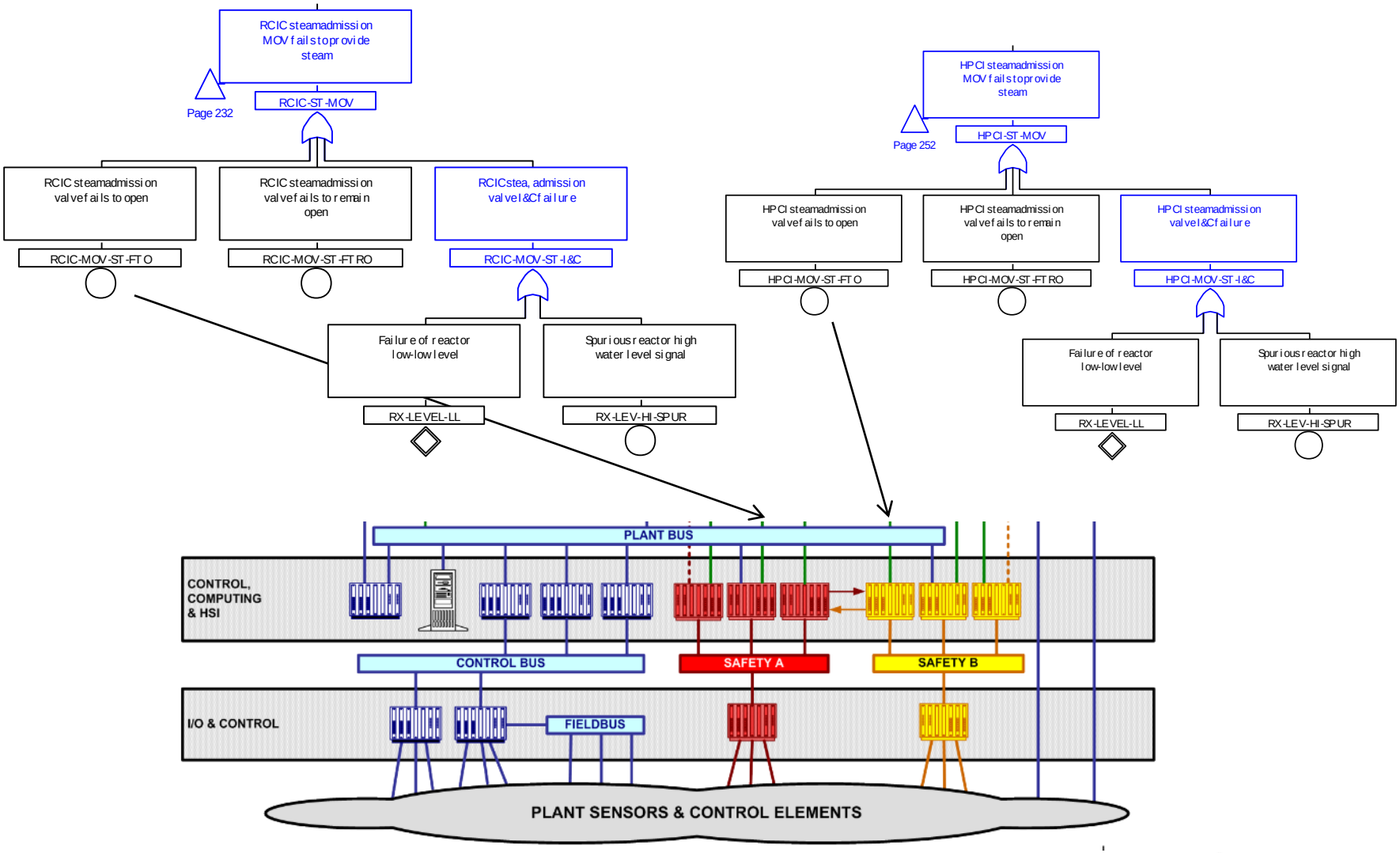
Overlap between I&C architecture and PRA systems/ components defines top logic for modeling digital I&C in PRA

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA

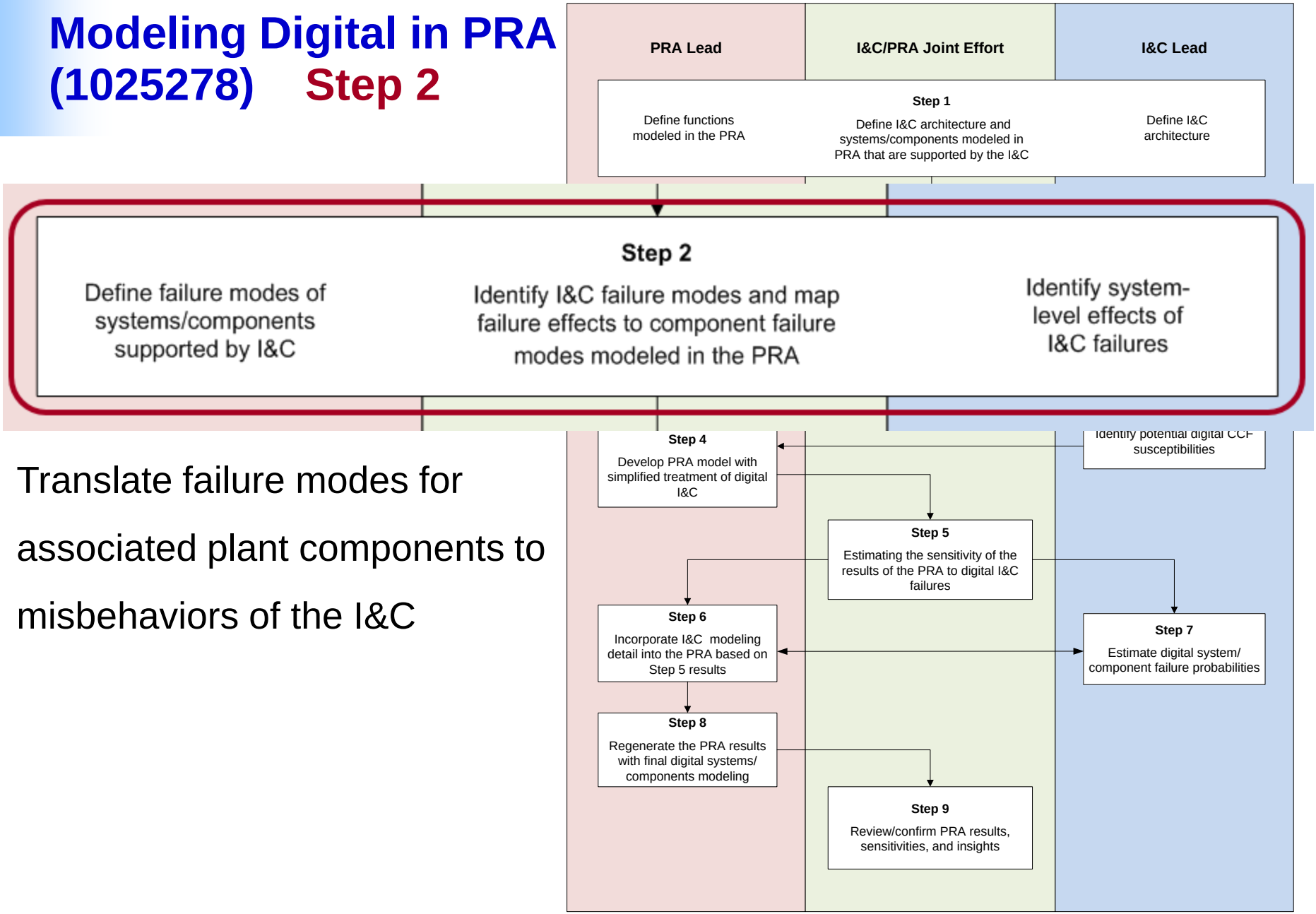
Step 1 – Interface between I&C and PRA components



© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital in PRA (1025278) Step 2



Translate failure modes for associated plant components to misbehaviors of the I&C

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA
Step 2 – Identify I&C 'Failure Modes'

- Identify failure modes for electrical and mechanical components that are actuated or controlled by the I&C (e.g., valve fail to open, breaker fail to close, pump failure to provide adequate flow,…)
- Translate plant component failure modes to undesired misbehaviors of the digital I&C system

I&C System Failure Mechanism	I&C System Failure Mode	I&C System Failure Effect (on plant systems)
Output of 1 instead of 0	Protective action when none is warranted	Spurious operation of (pump, valve,...)
Output of 0 instead of 1	No protective action when needed	Failure of component to operate (pump FTS, valve FTO, ...)
Delayed output	Delayed protective action	Delayed component operation

controls.

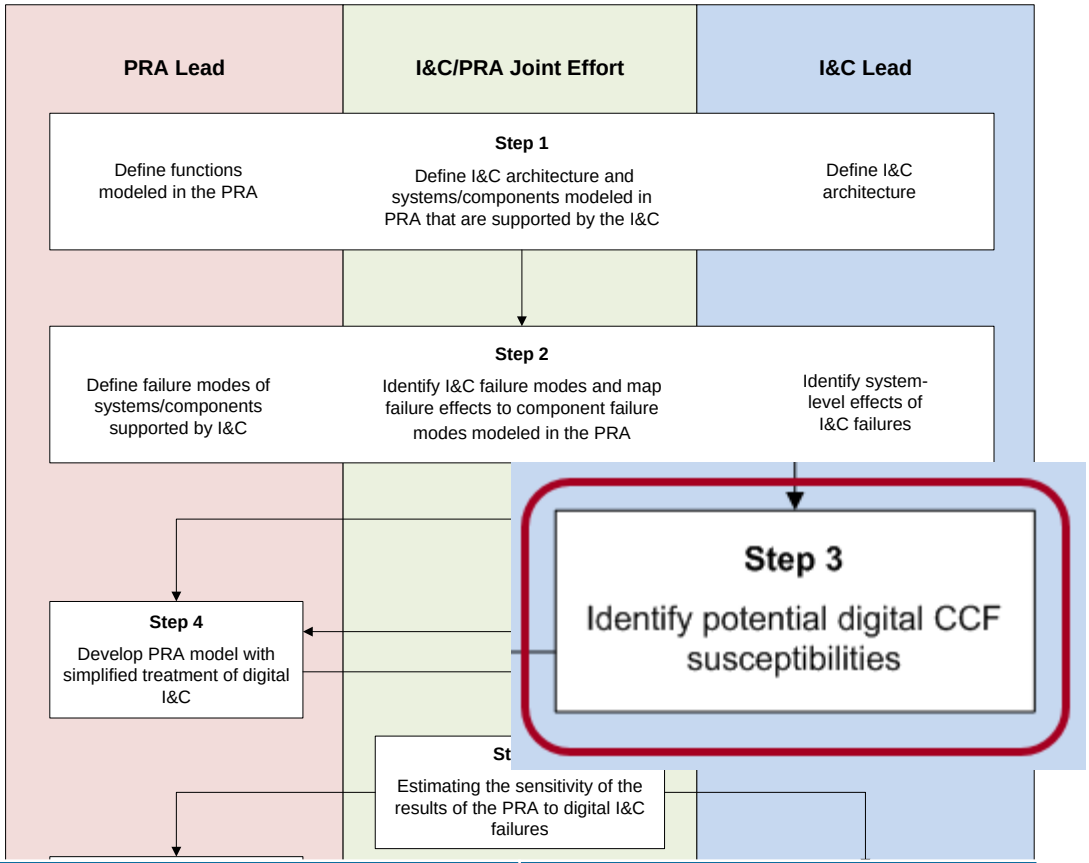
© 2014 Electric Power Research Institute, Inc. All rights reserved.

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital in PRA (1025278) Step 3

Preventive measures for CCF

- Hardware – Different:
  - Component type / failure mode
  - Manufacturer
  - System (different operating conditions, environment)
  - Maintenance practices
- Software defensive measures:



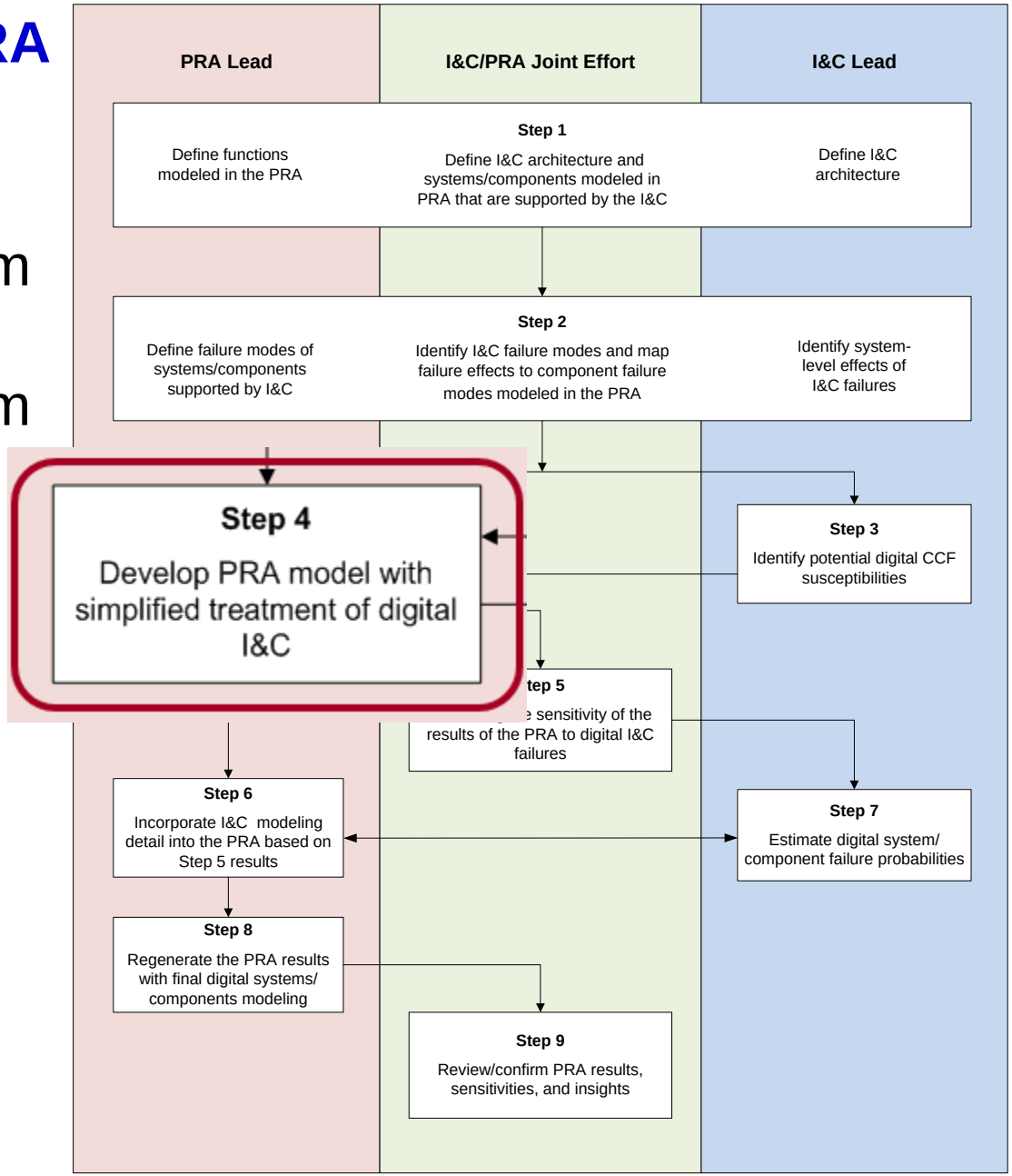
Operating System	Application Software	Communications
Cyclic operation	Functional diversity	Cyclic operation
Few interrupts	Signal diversity	Transparent to plant conditions
Transparent to plant conditions		

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital in PRA (1025278) Step 4

- Incorporate intra-system and inter-system CCF dependencies at system level
- Estimate failure probabilities

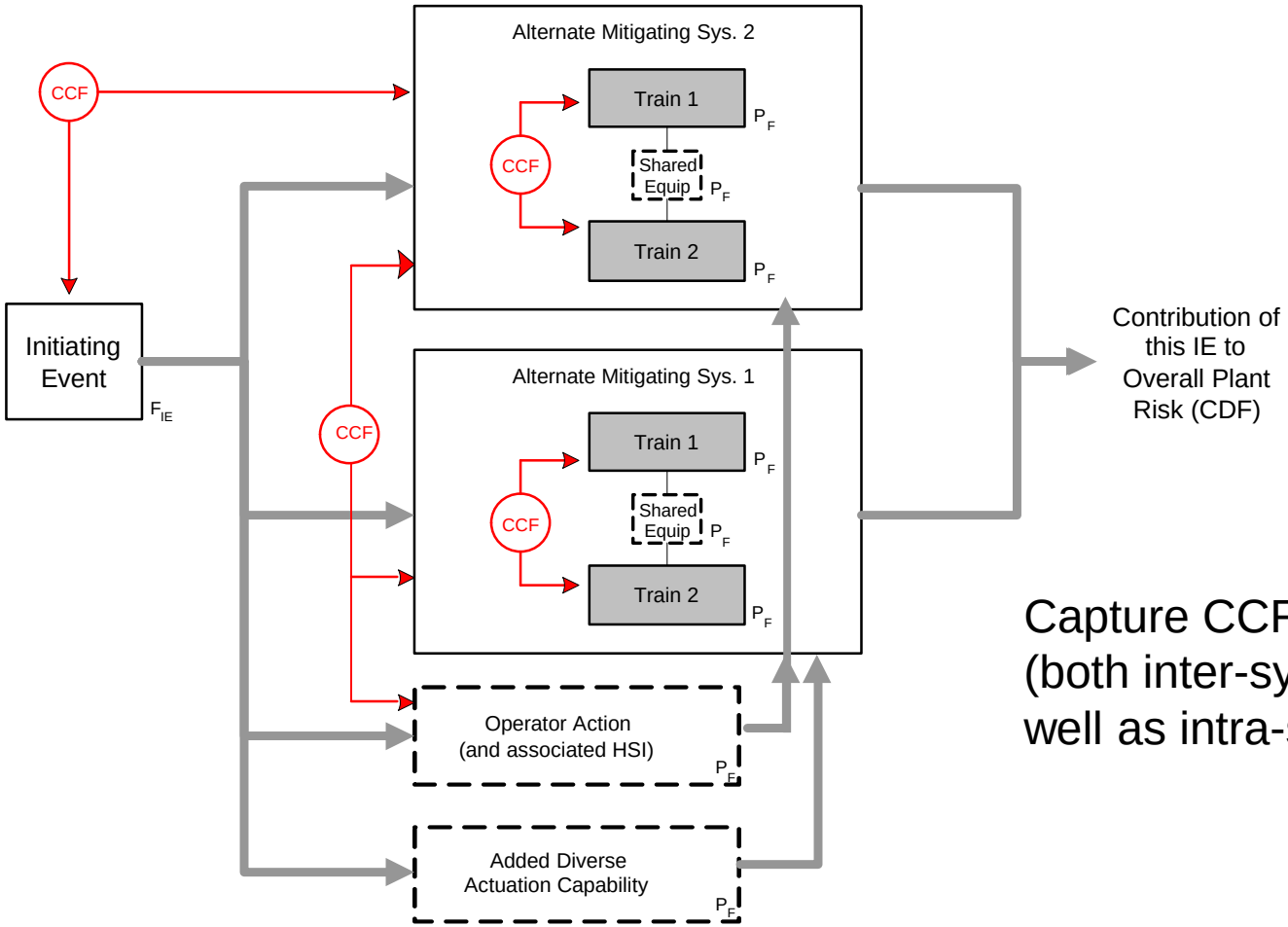


© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA

Step 4 – Incorporate the I&C Factors into the PRA



Capture CCF effects (both inter-system as well as intra-system)

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA
Step 4 – Parameter Estimates

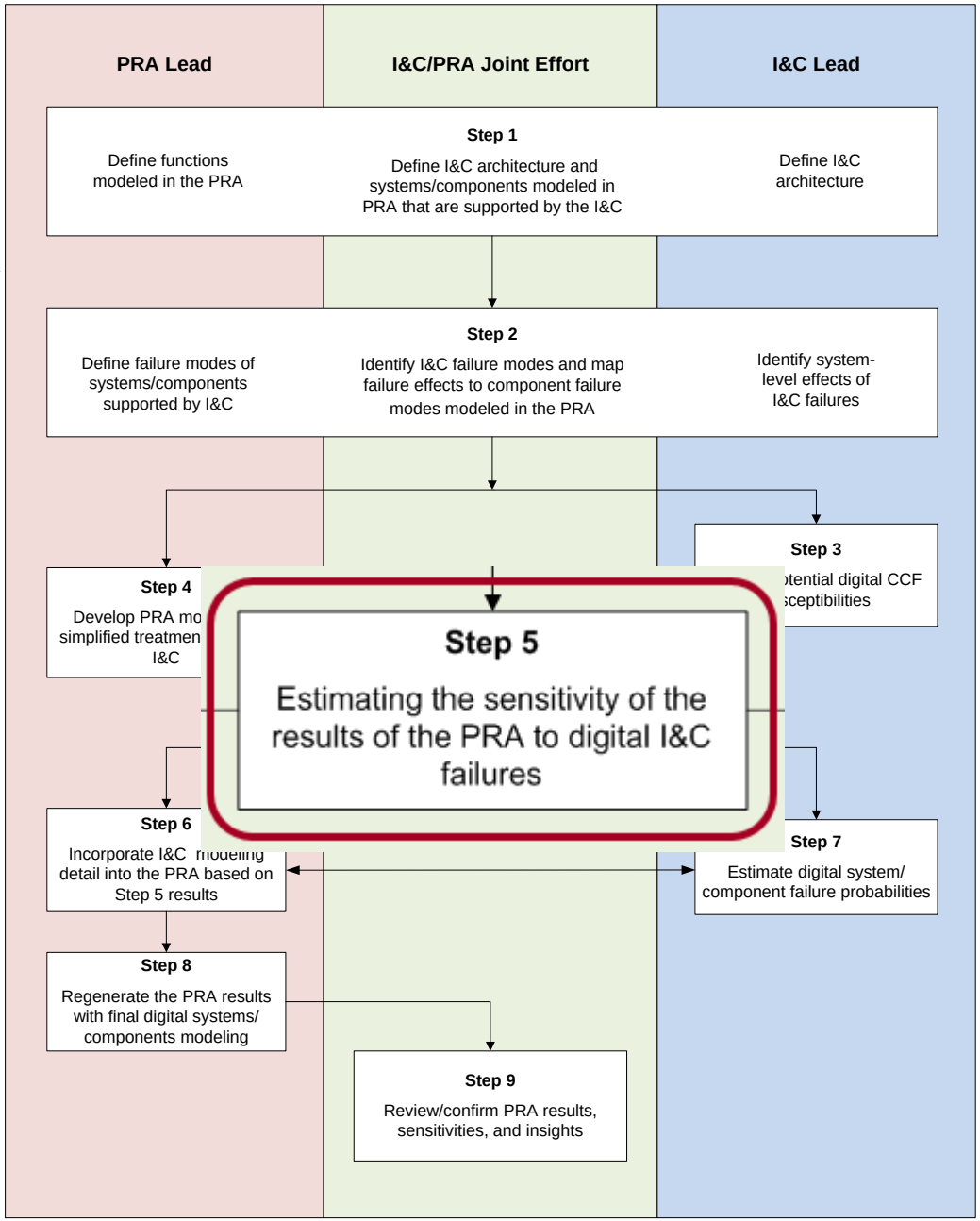
- Inputs to failure probability estimate
  - Vendor operating experience
  - Expert opinion based on presence/absence of defensive design measures
  - International standards, e.g., IEC 60880 (software) and IEC 60987 (hardware)
    - "For an individual system which incorporates software developed in accordance with the highest quality criteria (IEC 60880 and IEC 60987), a figure of the order of 10^{-4} failure / demand may be an appropriate limit to place on the reliability that may be claimed." Ref IEC 61226
- It is suggested that an initial failure probability be applied assuming high quality design processes and then sensitivity studies performed on assumptions for:
  - Failure modes
  - Failure probabilities

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Modeling Digital in PRA (1025278) Step 5

Determine sensitivity of PRA to I&C

- Approach
  - Assign low sensitivity I&C a high failure probability
  - Review PRA results to confirm that low sensitivity systems do not affect PRA conclusions



© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA
Step 5 – Sensitivity Study

- Why a sensitivity study?
  - It's to influence the I&C design where practical
  - In the current generation of plants, I&C is not a significant contributor to risk
    - for individual systems
    - for accident sequences

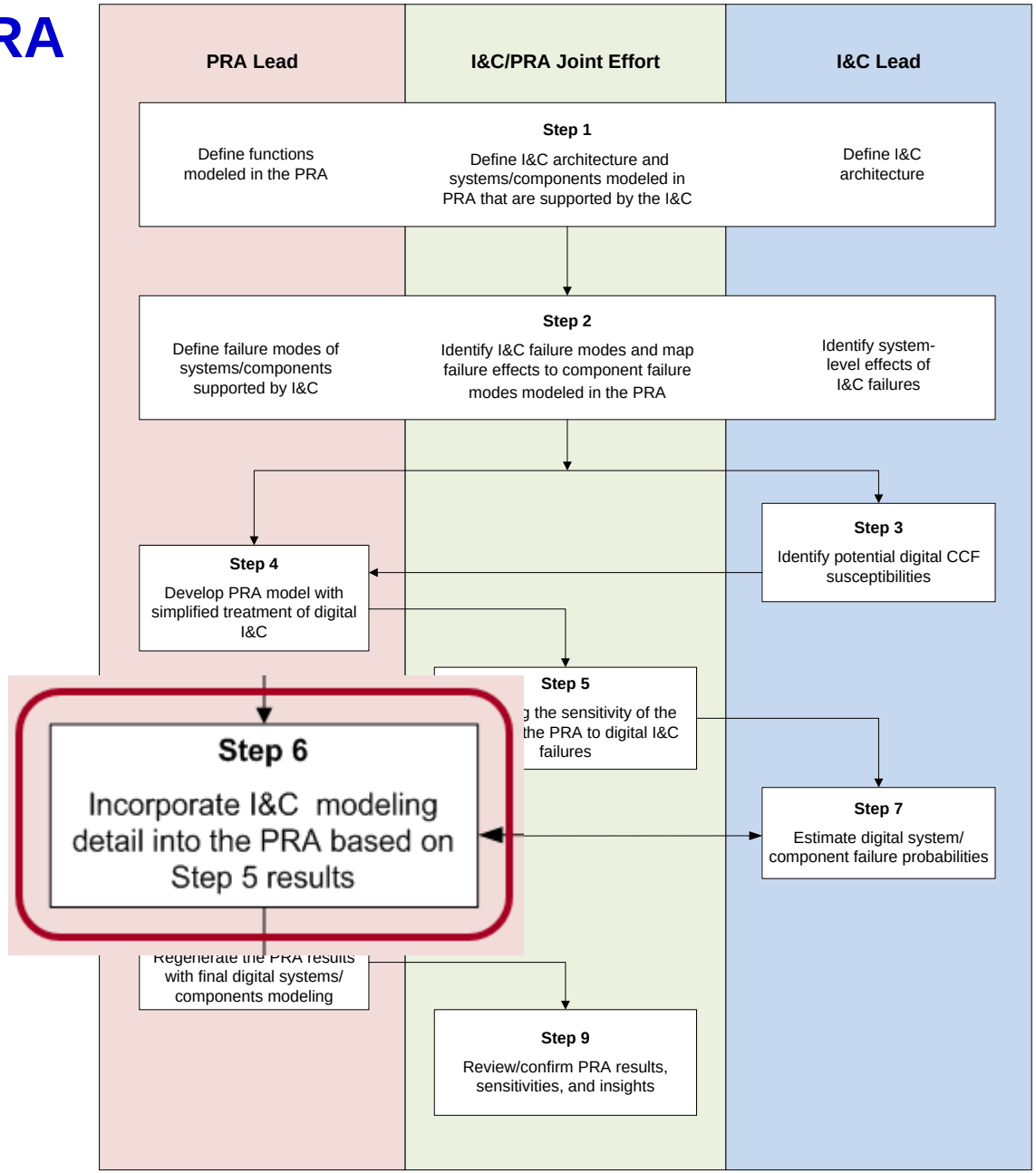
    <u>We want to keep it that way</u>

  - In upgrading I&C in the current generation of plants, we have the opportunity to incorporate risk insights into the design <u>before</u> the plant is modified – just like the new plants

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Modeling Digital in PRA (1025278) Step 6

Different levels of detail for low and high sensitivity systems

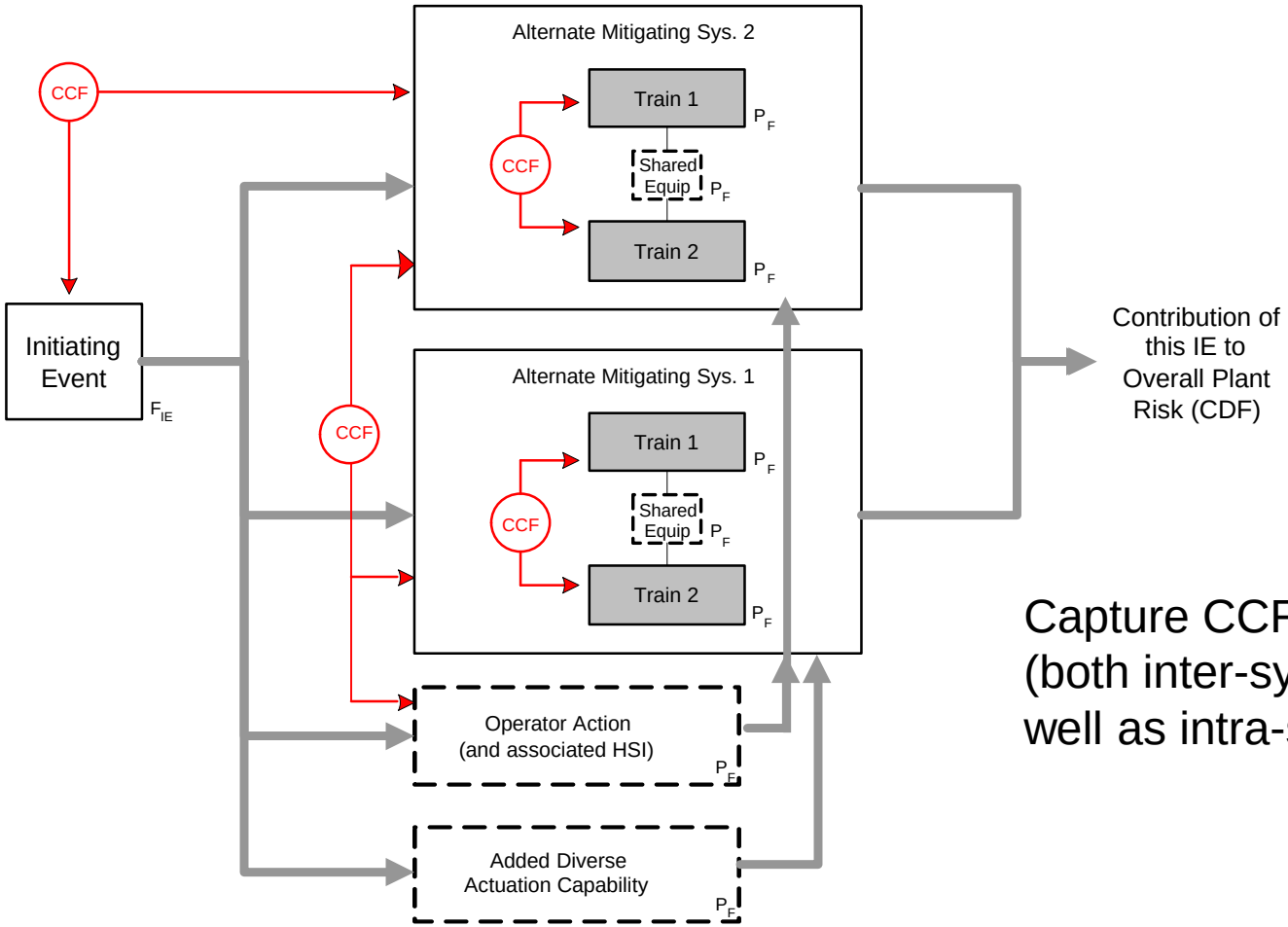


© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA

Step 6 – Level of Modeling Detail for Low Sensitivity Systems



Capture CCF effects (both inter-system as well as intra-system)

© 2014 Electric Power Research Institute, Inc. All rights reserved.

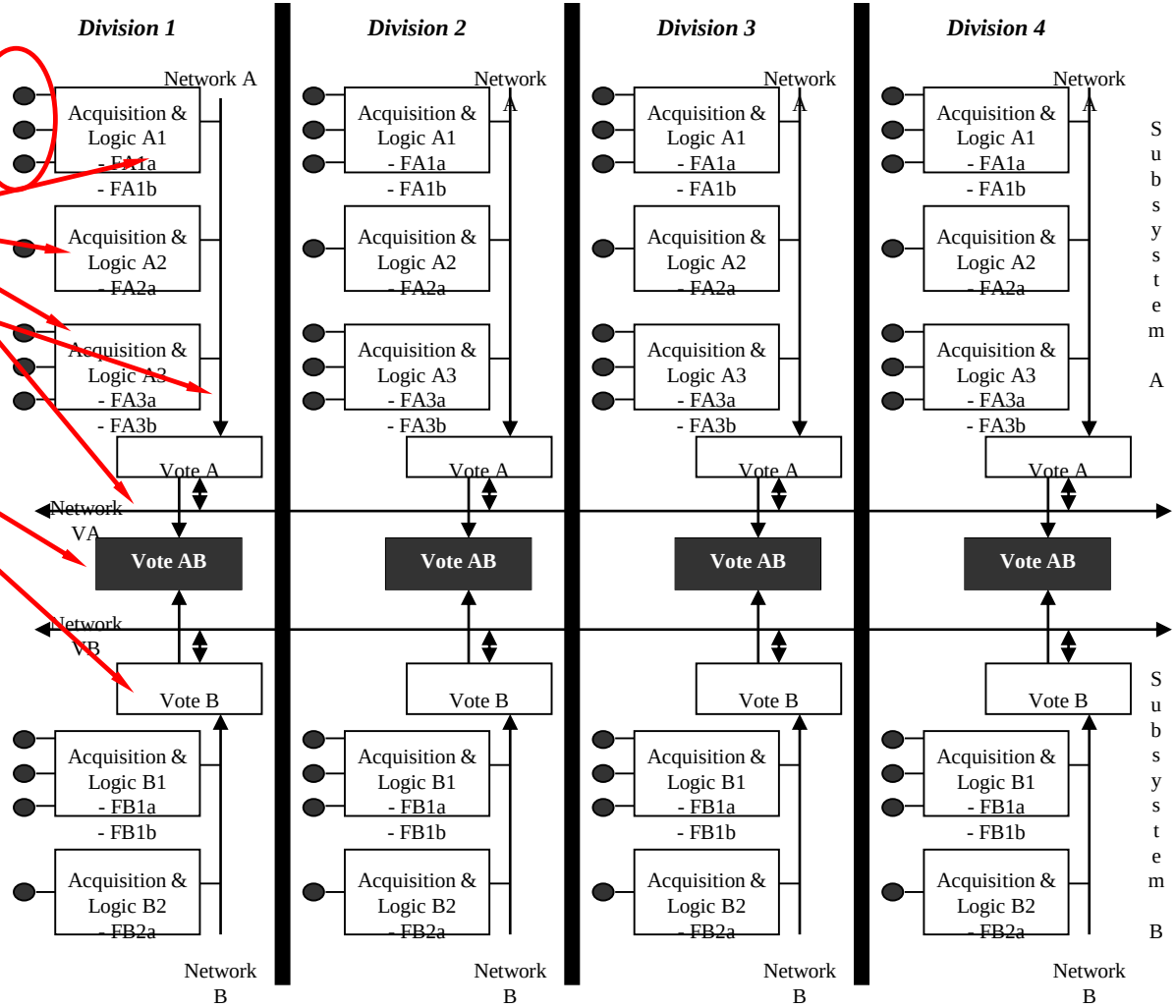
ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA

Step 6 – Level of Modeling Detail for High Sensitivity Systems

Hardware

- Sensors
- Signal processing
- Communication
- Voting



Components, their failure modes and effects

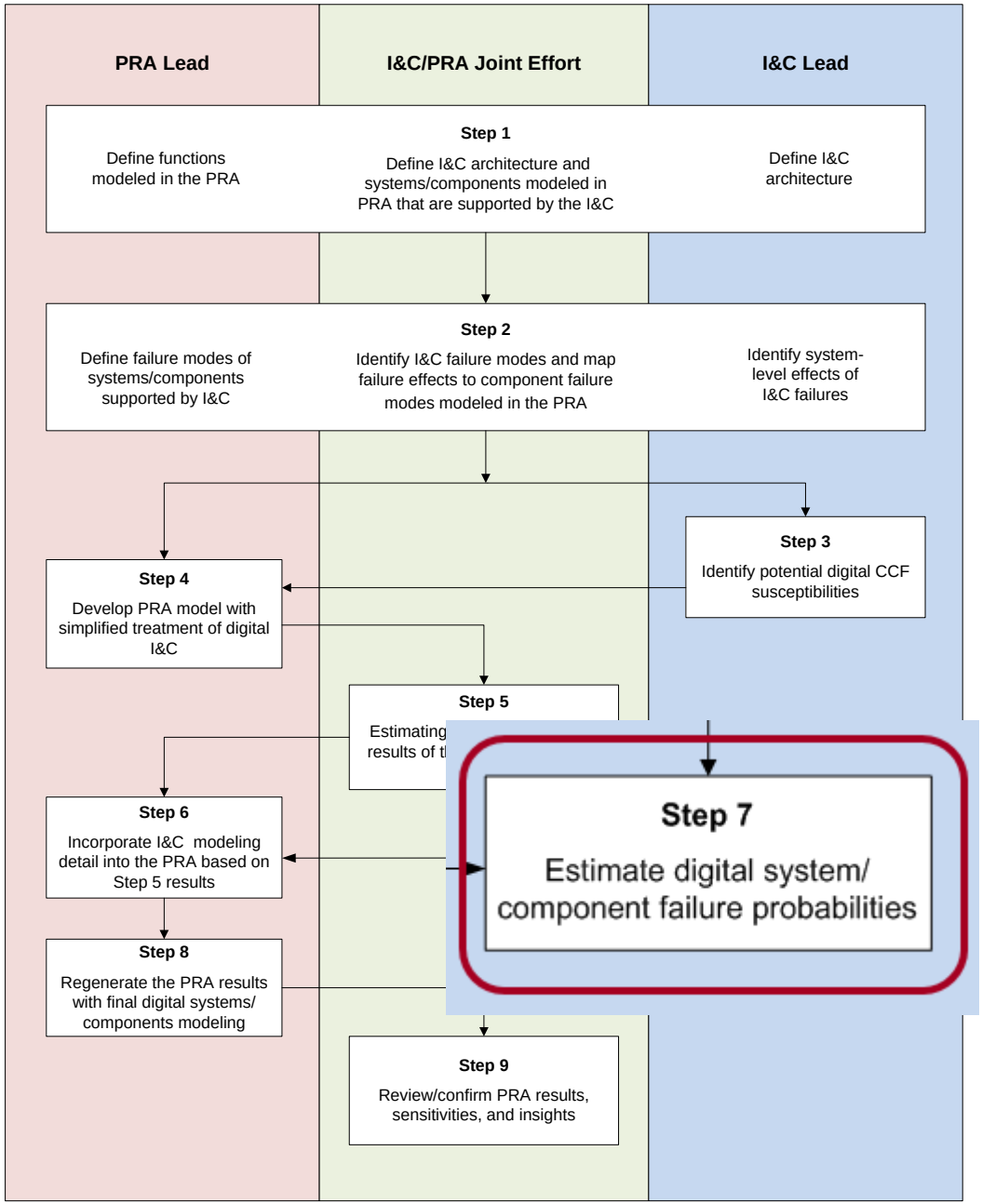
Note: Unavailabilty and maintenance errors modeled separately

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital in PRA (1025278) Step 7

Different parameter estimates for low and high sensitivity systems



© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA
Step 7 – Parameter Estimates for Low Sensitivity Systems

- For both hardware and software, approximations can be made ('black box' approaches)
  - Holistic approaches

    Conformance with Standards (e.g., IEC-61226)

    "For an individual system which incorporates software developed in accordance with the highest quality criteria (IEC 60880 and IEC 60987), a figure of the order of 10^{-4} failure / demand may be an appropriate limit to place on the reliability that may be claimed."
  - Analytic approaches
    - Statistical testing
  - Operating experience
    - Vendor
    - Industry

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Modeling Digital I&C in PRA

Step 7 – Parameter Estimates for High Sensitivity Systems

- Analytic approaches
  - Statistical testing
  - Design review combined with operating experience
    - Software
    - Hardware

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Modeling Digital I&C in PRA

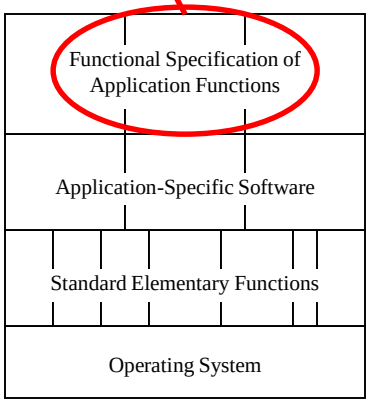
Parameter Estimates for High Sensitivity Systems (Software)

In reviewing the digital system design, develop simple reliability models of digital system computing units.

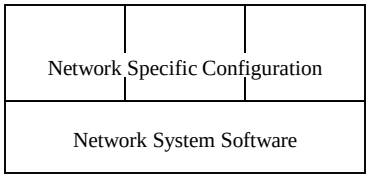
Failure mechanisms are reviewed for the various units of the digital system as input to the development of failure probabilities.

Recognize that not all failure mechanisms can be completely screened

Defensive measures implemented by the designer can be used to screen failure mechanisms for these subelements and help in estimating failure rates



Acquisition and Logic Units, and Inter-Division Voting Units



Communication Units

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA
Quantification of Residual Failure Modes

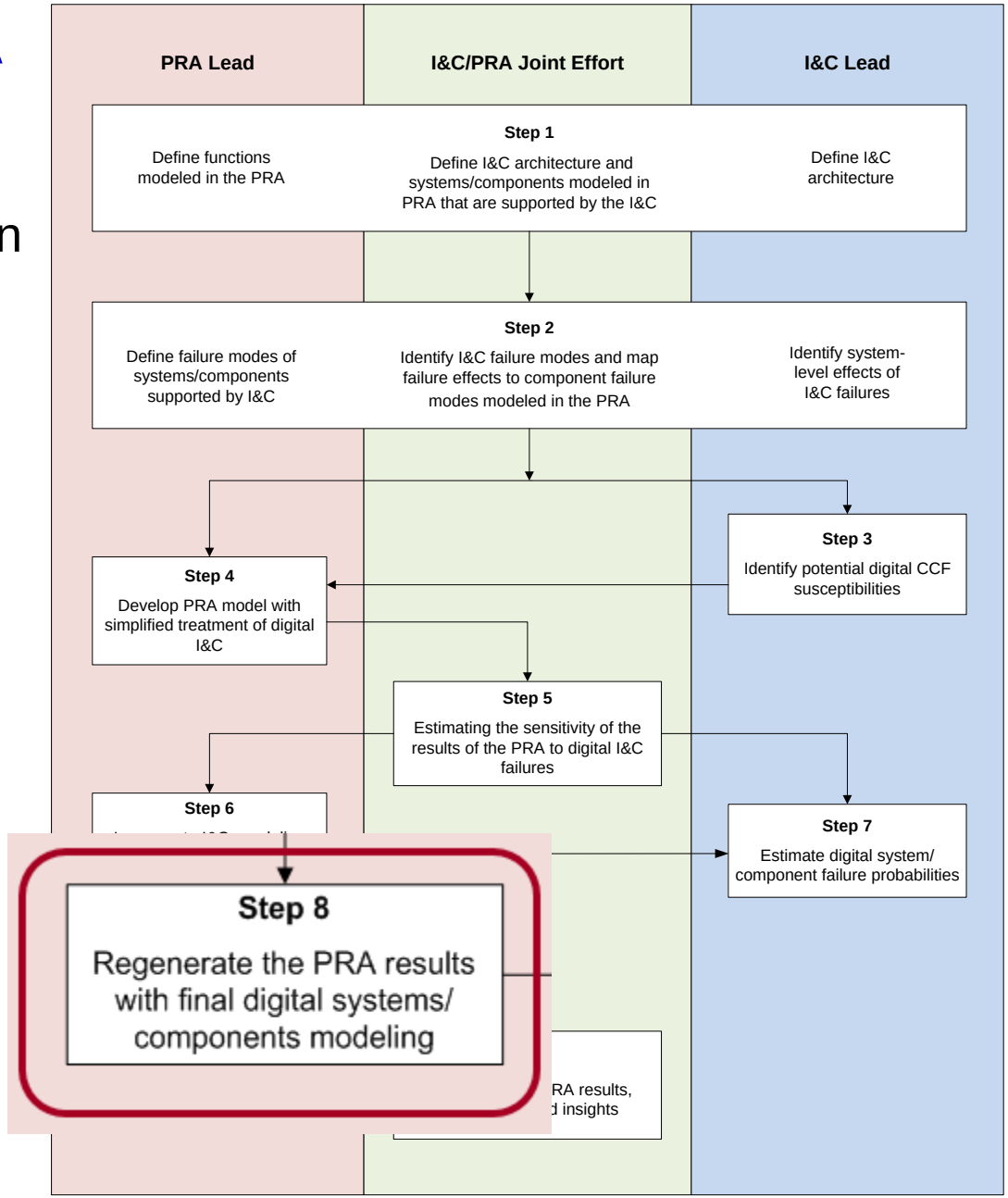
- For well designed digital systems with defensive measures that eliminate, reduce the potential for or tolerate known failure mechanisms and modes
  - Dominant contributors to failure likely will be limited to functional specification and design errors
  - Operating experience was used to quantify the potential for functional specification and design errors (‘unknown’ failure mechanisms/modes)
    - EdF has over 500 reactor operating years of experience with digital protection systems on their 1300 MWe units.
    - See EPRI 1021077, ‘Estimating Failure Rates in Highly Reliable Digital Systems’, December 2010

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Modeling Digital in PRA (1025278) Step 8

Accident sequence quantification

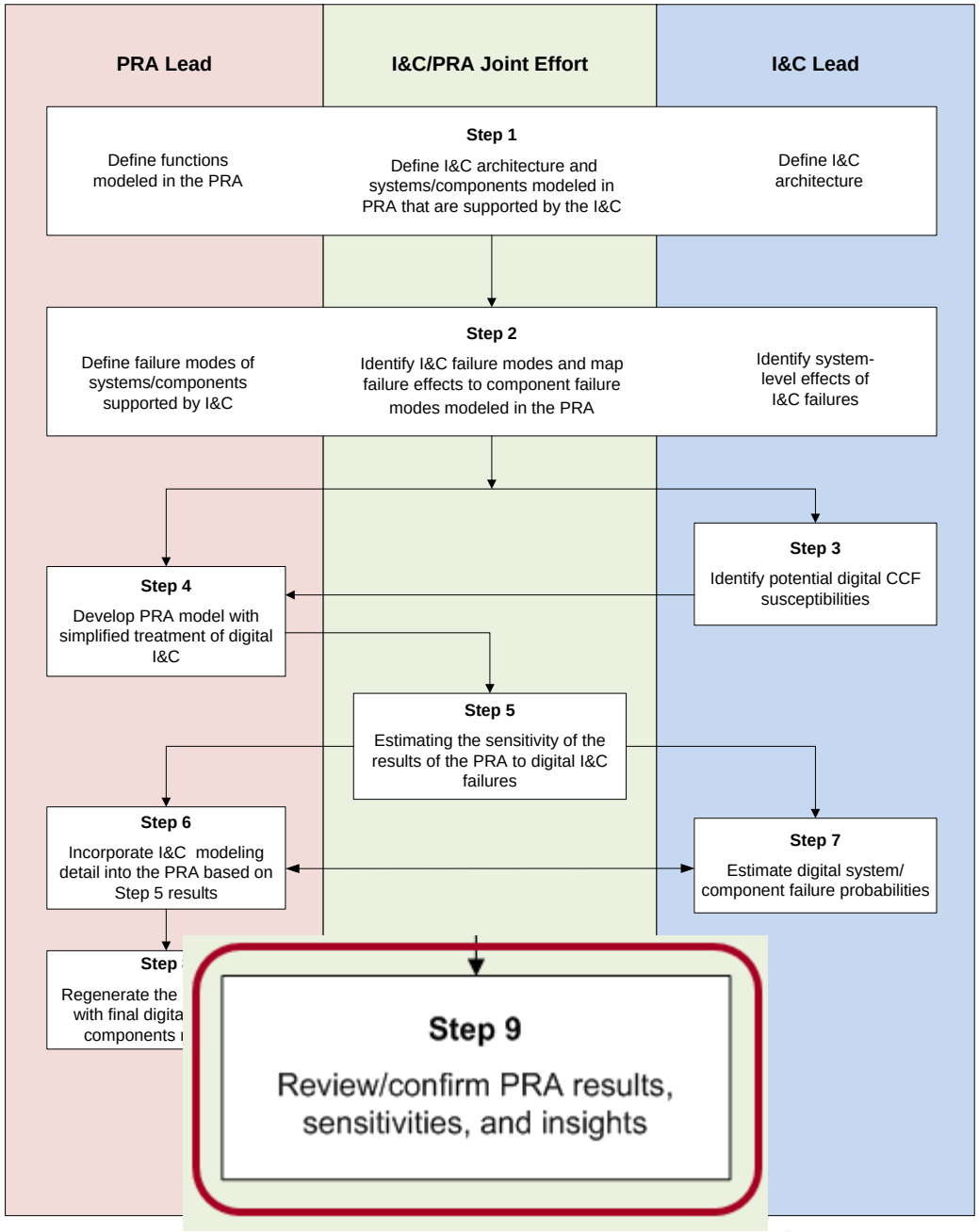
- Regenerate accident sequence results using:
  - Models from Step 6
  - Parameter estimates from Step 7



© 2014 Electric Power Research Institute, Inc. All rights reserved.

Modeling Digital in PRA (1025278) Step 9

- Provide to the plant staff
  - Results and conclusions
  - Key assumptions
  - Sensitivity study results
  - Explanation of results in terms of plant design features and operating characteristics
- Plant staff conclusions
  - Validity of classification of digital system effects on the PRA (sensitivity of the PRA application results)
  - Confirm assumptions and plant design features that drive the results



© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital I&C in PRA

Conclusions

Key Points

- Model development and estimating failure probabilities should be a collaborative effort between designers, I&C personnel and PRA analysts.
- Level of detail needed in the model is dependent on the context of the system within the integrated plant design.
- Consider a blend of diversity and defensive measures in developing failure probabilities.
- Software behaves deterministically. It is the effects of encountering conditions for which the software was not designed that is modeled in the PRA.

Additional Insights

- Important to model digital systems in the PRA before they are installed in order to understand the full scope of the effects and influence the design

© 2014 Electric Power Research Institute, Inc. All rights reserved.

EPRI References

- *Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades: Applying Risk-Informed and Deterministic Methods,* EPRI 1002835, 2004
- *Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions*, EPRI 1016721, 2008
- *Effects of Digital I&C Defense-in-Depth and Diversity on Risk in Nuclear Power Plants*, EPRI 1019813, 2009
- *Estimating Failure Rates in Highly Reliable Digital Systems,* EPRI 1021077, Dec 2010
- *Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments,* EPRI 1025278, July 2012

© 2014 Electric Power Research Institute, Inc. All rights reserved.

EPRI References, cont'd

- *Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems*, EPRI 1016731, December 2009.
- *Protecting Against Digital Common-Cause Failure - Combining Defensive Measures and Diversity Attributes*, EPRI 1019182, December 2010.
- *Digital Operating Experience in the Republic of Korea*, EPRI 1022986, 2011.
- *Hazard Analysis Methods for Digital Instrumentation and Control Systems*, EPRI 3002000509, June 2013.

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

NRC Research References

- *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments*, NUREG/CR-6901, February 2006.
- *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, NUREG/CR-7007, ORNL/TM-2009/302, ORNL, 2009.
- *Traditional Probabilistic Risk Assessment Methods for Digital Systems*, NUREG/CR-6962, October 2008.
- *Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods*, NUREG/CR-6997, September 2009.
- *Review of Software Quantitative Reliability Methods*, BNL-94047-2010, September 2010.

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Other References (data sources)

- NUREG/CR-5500, Vol. 2, INEEL/EXT-97-00740, 1999.
- NUREG/CR-5500, Vol. 10, INEL/EXT-97-00740, 2002.
- Bickel, J., “Risk Implications of Digital Reactor Protection System Operating Experience”, *Reliability Engineering & System Safety*, 2006.
- Yastrebenetsky, M. “Operating reliability of WWER NPP Digital I&C Systems”
- “Electronic Reliability Design Handbook,” Military Handbook 338B, 1998.
- RAC, “Nonelectronic Parts Reliability Data”, NPRD-2011, 2011.
- RAC, “Electronic Parts Reliability Data”, EPRD-97, 1997.
- RAC, “Failure Mode/Mechanism Distributions”, FMD-97, December 1997.

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity

ELECTRIC POWER RESEARCH INSTITUTE

Update on Digital Instrumentation & Control Projects - Techniques for Failure Prevention and Mitigation

Ray Torok
EPRI

Advisory Committee on Reactor Safeguards
Subcommittee on Digital Instrumentation & Control Systems
November 18-19, 2014

Techniques for Failure Prevention and Mitigation

Contents

- Key Points
- Focus – Extend failure mode discussion to prevention and mitigation
- Current EPRI project on assessing and managing digital failure susceptibilities
  - Overview / Goal
  - Approach / concepts
    - Key terms
    - Prevention & mitigation
    - Defects & triggers
    - Common-cause failure
    - Defensive measures
    - Diversity
    - Assurance of adequate protection
  - Project status
- Conclusions

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Techniques for Failure Prevention and Mitigation
Key Points

- Purpose of this presentation
  - Inform ACRS about current EPRI project to develop guidance on assessing and managing digital failure susceptibilities
  - Extend failure mode discussion to practical treatments and solutions
- Concepts
  - Protection consists of prevention and mitigation
  - Software “failure” needs both a defect and a trigger
  - Protection can be accomplished at different levels of interest in plant architecture
  - Common-cause failure (CCF) has several contexts and initiators
  - The goal: reasonable assurance of adequate protection against effects of failures

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Focus – Extend Failure Mode Discussion to Practical Treatments and Solutions

- EPRI ‘digital’ research topics over last 20 years
  - Hazard analysis
  - Modeling digital I&C in PRA
  - Estimating failure rates for digital
  - Evaluating critical digital equipment
  - Digital operating experience
  - Defense-in-depth and diversity
- Products, standards and guidance have evolved
- Current project is applying earlier results to develop practical treatments and solutions

Our ability to ensure high dependability of critical digital systems has improved significantly since the SRM to SECY 93-087

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Current EPRI Project - Assessing and Managing Digital Failure Susceptibilities (aka "EPRI CCF Project")

- EPRI developing technical guidance for digital implementations
  - Assess susceptibilities to potential failures, including CCFs and unintended behaviors
  - Manage vulnerabilities using preventive and mitigative measures
  - Show adequate protection against undesired consequences
- Nuclear Energy Institute (NEI) to address regulatory implications
  - Application of 10 CFR 50.59 and industry guidance (NEI 01-01)
  - Potential for malfunctions with a different result
  - Likelihood of malfunctions
  - Heavy CCF emphasis

EPRI project to provide guidance for utility engineers and technical input to licensing effort

© 2014 Electric Power Research Institute, Inc. All rights reserved.

EPRI Project on Digital Failure Susceptibility
Key Terms

- *Failure* - Inability of a structure, system or component to function within acceptance criteria
- *Common-cause failure* - Failure of two or more structures, systems or components due to a single specific event or cause
- *Defense-in-depth and diversity analysis* – two components
  - *Susceptibility analysis*:
    - identifies potential vulnerabilities and the measures in place to prevent them
    - qualitatively assesses the likelihood of failure, including CCF
  - *Coping analysis* – shows whether the mitigative measures are adequate to avoid the undesirable effects of a failure / CCF

© 2014 Electric Power Research Institute, Inc. All rights reserved.

EPRI Project on Digital Failure Susceptibility

Approach

- Apply and extend results and lessons from earlier EPRI projects, industry standards, and industry guidance
- Expand the conversation –
  - It's not just about equipment diversity or 100% testability
  - It's about protecting against plant level CCF effects
- More holistic approach
  - Assess susceptibility to failure and CCF
  - Credit design features that address vulnerabilities (including diversity)
  - Consider both prevention and mitigation
  - Use coping analysis where appropriate
  - Apply engineering judgment to assess CCF protection

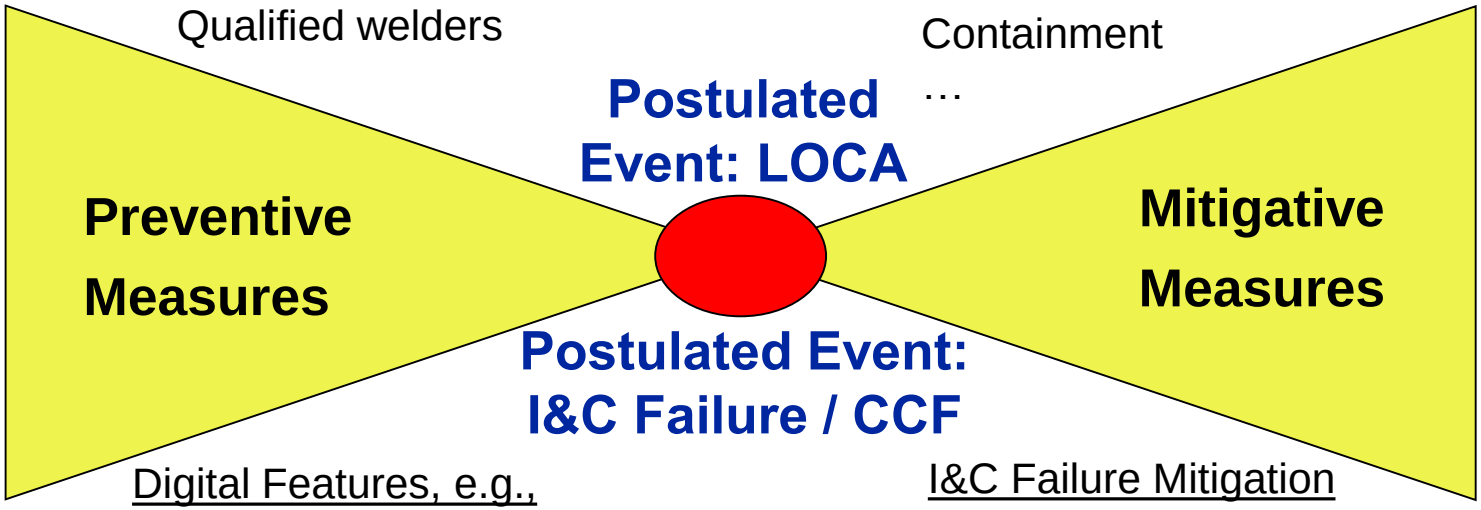
© 2014 Electric Power Research Institute, Inc. All rights reserved.

Approach / Concepts
Prevention and Mitigation

Causes/Sources

Piping Attributes, e.g.,
- Qualified materials
- ASME code
- Inspections
- Qualified welders

Piping Failure Mitigation
- Isolation valves
- Emergency core cooling
- Low pressure safety injection
- Containment
- …



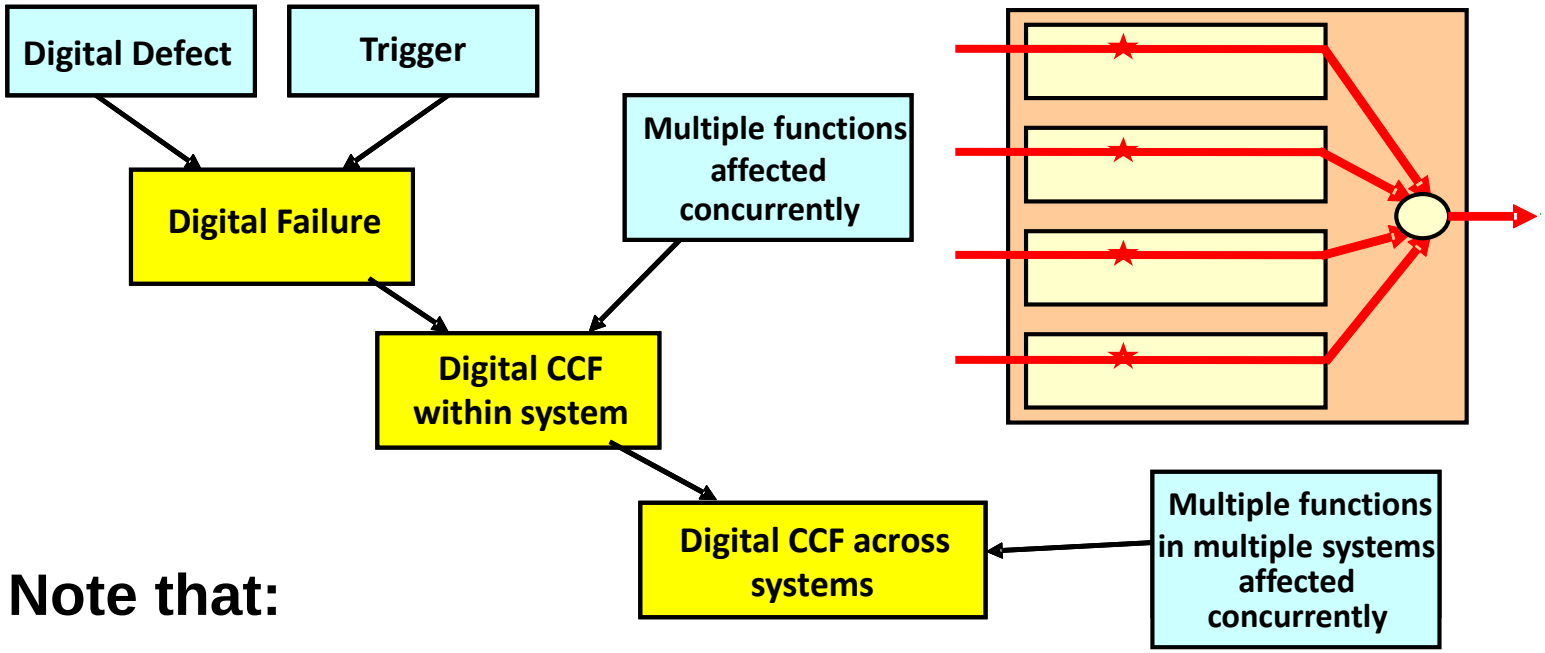
Consequences

Digital Features, e.g.,
- Watchdog timers
- Data validation
- Cyclic processing
- Minimal interrupts
- Functional diversity
- Segmentation

I&C Failure Mitigation
- Watchdog Timers
- Reactor trip
- Non-safety control actions
- Operator action
- Diverse actuation for RPS & ESFAS
- …

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Approach / Concepts
Defects and Triggers



Note that:

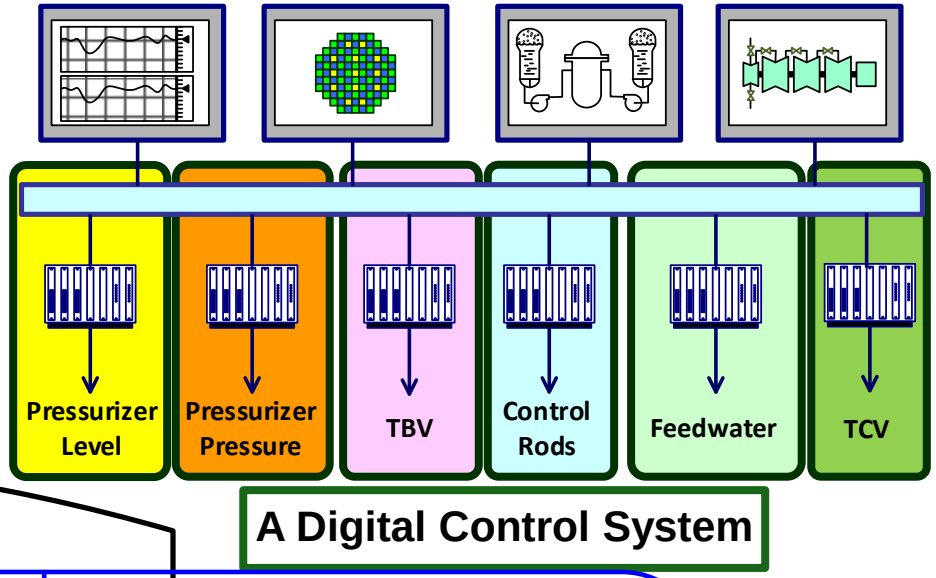
- Not all digital defects/failures can become CCFs
- Not all digital failures are safety-significant
- Defect-free software is neither expected nor needed
- Eliminating defects and triggers reduces likelihood of failure / CCF

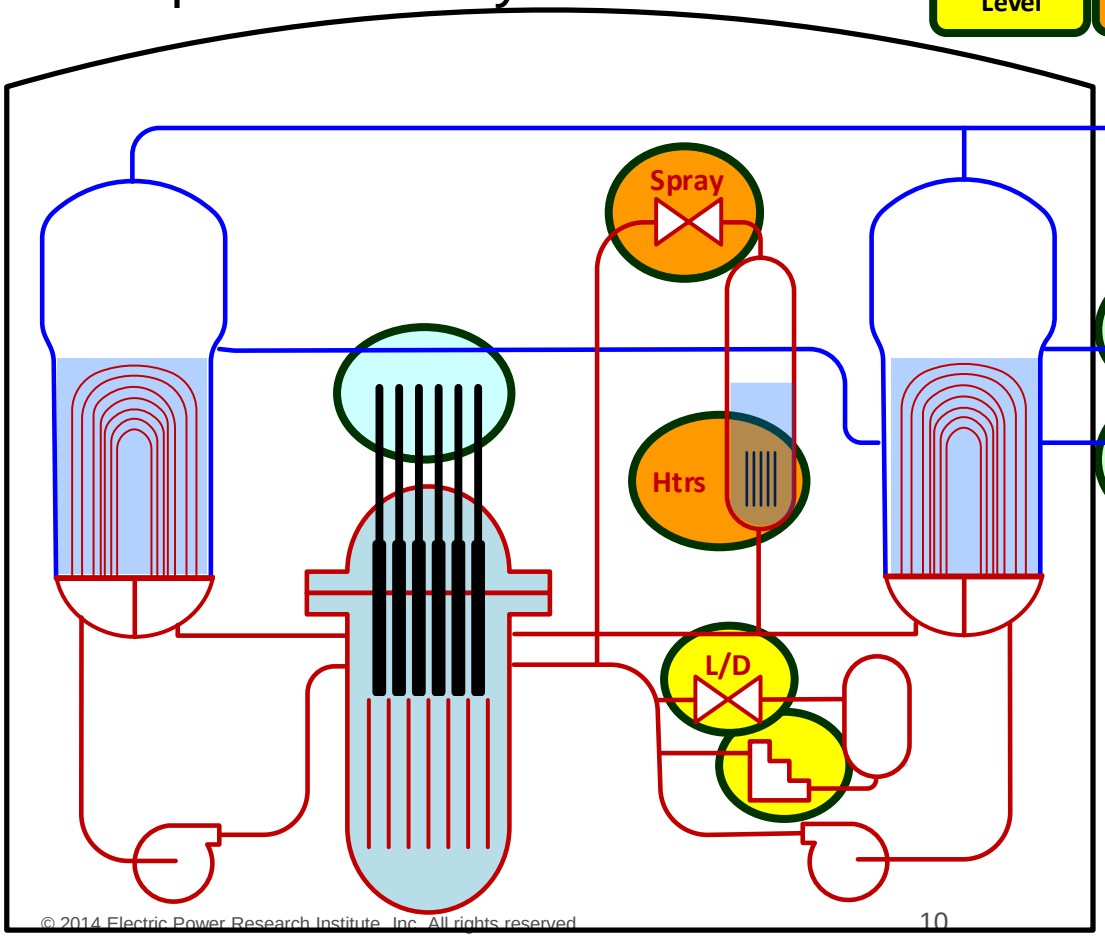
Failure/CCF susceptibility evaluation looks for design measures and practices that reduce the likelihood of defects and triggers

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Approach / Concepts
Common-Cause Failure Contexts

Failures and misbehaviors could affect single or multiple components or systems



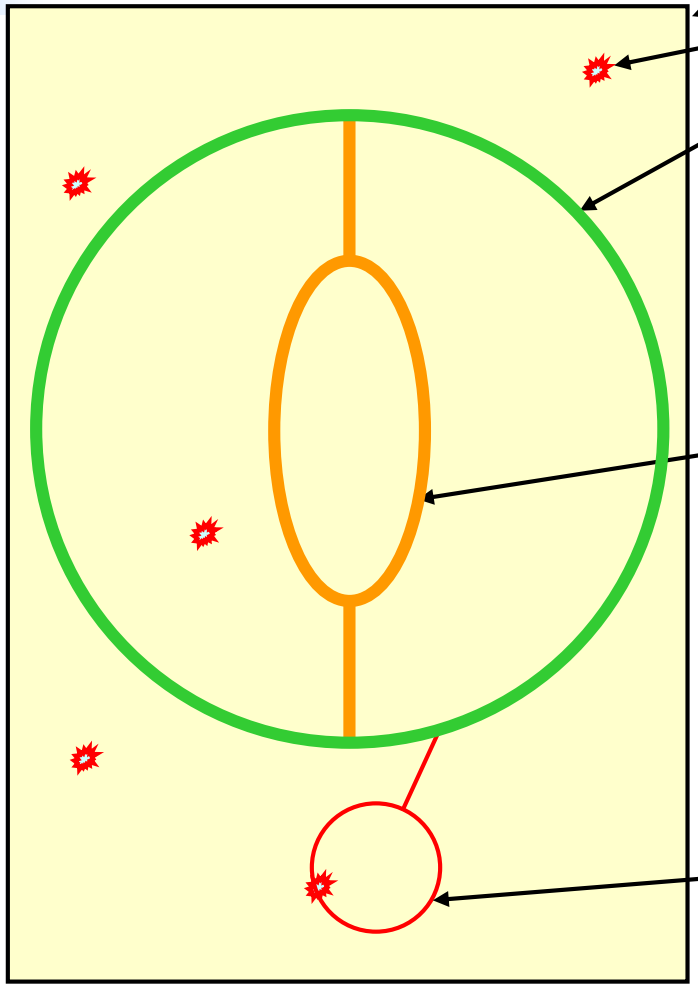


© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Approach / Concepts - Defensive Measures Example

System Constrained to Well Understood and Tested Trajectories



Complete domain of behavior

May contain residual digital faults

Path exercised continuously in normal situations

Influence factors during continuous operation:

- normal process inputs (validated before use)
- short-term memory (as little as possible)
- clock interrupts (thorough verification)
- (process-related interrupts: none)
- (resource management: static)

Path exercised in occasional but tested situations

Influence factors that could disrupt cyclic behavior:

- initialization (only once)
- operator requests (single channel)
- hardware failures (single channel)
- exceptions (very simple)
- codified dates & times (e.g., Y2K)
- plant transients: affect all channels

Path exercised in unanticipated or untested trajectories

A robust system avoids unanticipated and untested trajectories

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Approach / Concepts
Defensive Measures - Examples

- Watchdog timer (hardware-based, independent of microprocessor)
  - Protects against ‘task crash’ - ’task hang’ – ‘no response’ etc.
  - Notify operator - impose safe state
- Cyclic ‘infinite loop’ software architecture
  - Minimal branching
  - Constrain system to known, tested conditions
  - Limited sensitivity to plant transients
  - Avoid latent defects in software
- Data validation
  - Detect sensor problems
  - Protects against software reacting incorrectly to abnormal or unexpected data values

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Approach / Concepts
Defensive Measures – Examples, cont'd

- No times, dates
- Minimal, well controlled shared resources
  - Power supplies
  - Timing signals
  - Communications networks
- Segmentation
  - Limit scope of CCF
- Diversity
  - Functional
  - Signal

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Approach / Concepts
Diversity - Not Always the Answer

Can be effective in preventing or mitigating CCF

- Many types – design, equipment, human, software, etc. - effectiveness varies
- Functional and signal diversity shown effective in EPRI studies on nuclear plant digital operating experience

However

- Can add complexity – training, maintenance, switchovers, resolving conflicts, etc.
- Limited value against requirements errors, especially for redundancies with identical functionality
- Diverse backups increase risk of spurious actuation
- Diversity does not guarantee that CCF cannot still occur

Appropriate types of diversity should be implemented where they can be shown to be beneficial

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Approach / Concepts
Diversity - Not Always the Answer, cont'd

And in the regulatory context…

"Of course we do not argue that diversity is always bad – only that a diversity requirement imposed by the NRC demands more justification than a flat assertion that diversity is desirable in the abstract……..We wish only to supply some of the cons that must be balanced against the pros, so the outcome is not decided by a slogan."

Chairman ACRS to
Chairman USNRC
February 16, 1994

© 2014 Electric Power Research Institute, Inc. All rights reserved.

The Goal:
Reasonable Assurance of Adequate Protection

Many potential contributors to assurance, e.g.,

- Traditional hardware practices - quality assurance, qualification testing, etc.
- Software development practices – e.g., standards, coding practices, etc. (Does not ensure good design)
- Defensive design measures in software, hardware, architecture, procedures, operation, etc. (OE suggests that this is being done well – project team is consulting experienced designers)
- Mitigation and coping capability
- Extensive test coverage
- Performance records
- Risk and safety analysis insights
- Simplicity of digital platform and application

Consider the evidence and apply engineering judgment to make "reasonable assurance of adequate protection" determination

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Reasonable Assurance of Adequate Protection
Different Contributors for Safety and Non-Safety

Attribute	Safety Systems	Non-Safety Systems
Redundancy	Independent Channels	Master/Slave
Qualification Testing	Yes	Varies
Formal SQA* Methods	Always	Varies (Improving)
Functional Complexity	Low	High
System Interactions	Low	High
Operating Experience	Low	High
Defensive Design Measures	Varies (Improving)	Varies (Improving)
Test Coverage	High	Varies
Risk Significance	Varies	Varies

Consider the evidence and apply engineering judgment to make "reasonable assurance of adequate protection" determination

*Software Quality Assurance

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Project Status –
EPRI Project is Developing a Guidance Document

- Target audience:
  - I&C design engineers, safety analysis engineers, licensing engineers, PRA analysts
- Guidance to be applied in design activities
  - Design measures and practices that:
    - Reduce likelihood of defects, triggers and failures
    - Increase protection against effects of failure/CCF
  - Assess susceptibility to digital failure and CCF
  - Coping analysis to demonstrate adequate mitgation
  - Qualitative assessment of adequacy of protection
  - Examples to illustrate principles
- Technical update published November 2014 (3002002990)
  - Download free from epri.com
- Final report mid-2015

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity

ELECTRIC POWER RESEARCH INSTITUTE

Update on Digital Instrumentation & Control Projects
Status of Hazard Analysis Demonstration Project

Bruce Geddes
Southern Engineering Services

Advisory Committee on Reactor Safeguards

Joint Meeting of the Subcommittee on Digital Instrumentation & Control Systems and the Subcommittee on Reliability and Probabilistic Risk Assessment

November 18-19, 2014

Hazard Analysis Demonstration

Project Objectives

- Trial application of EPRI guideline:
  - *Hazard Analysis Methods for Digital Instrumentation and Control Systems* (EPRI 3002000509)
  - (Presented to I&C Subcommittee in September 2013)
- Capture lessons learned
  - Efficacy of methods
  - Learning / applying novel method

Approach

- Plant takes lead in performing hazard analysis
- EPRI team provides training, coaching and reviews

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Palo Verde Exciter Replacement Project

Replacing main generator exciters on three units (non-safety, but critical to generation):

- Each exciter system (controller, rectifiers and peripherals) to be in its own new building, adjacent to turbine building, with dedicated HVAC
- Building HVAC is critical to generation (i.e., less than 10 minutes before rectifiers overheat on loss of HVAC)
- Each exciter system building is equipped with three redundant HVAC units, each sized for 100% heat load

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Hazard Analysis Steps (from EPRI 3002000509)

1. Determine scope and objectives
2. Function analysis
3. Identify the level(s) of interest
4. Determine appropriate method(s)
5. Consider a blended approach
6. Determine resources and schedule
7. Preliminary hazard analysis (PHA)
8. Perform the detailed hazard analysis
9. Hazard analysis acceptance, documentation and maintenance

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Palo Verde Exciter Hazard Analysis

1. Scope and Objectives
   - Main generator exciter system
   - Exciter building HVAC system
   - Identify and resolve potential hazards that can cause loss of HVAC (leads to main generator trip)
2. Function Analysis
   - Functions for exciter, exciter controls, exciter HVAC and HVAC controls defined
   - Function/Process map for exciter HVAC developed

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Palo Verde Exciter Hazard Analysis

3. Identify Level(s) of Interest
   - Exciter, controls and operator interface
   - Digital control system in all three redundant HVAC units
     - Interfaces between redundancies
     - Human-system interfaces
   - Electrical power supplies to HVAC units
4. Determine Appropriate Method(s)
   - Functional FMEA for exciter system, including controls and operator interface
   - STPA (systems theoretic process analysis) for exciter HVAC control system
   - Fault tree analysis for electrical/mechanical portion of exciter HVAC system (EPRI scoping study)

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Palo Verde Exciter Hazard Analysis

5. Consider a Blended Approach
   - Using Functional FMEA results to help identify hazards to be assessed using STPA method
   - Functional FMEA, FTA, and STPA view the control system in the context of the integrated plant design
6. Determine Resources and Schedule
   - Palo Verde Staff performing the hazard analysis
   - EPRI coaching on hazard analysis methods and reviewing results via email and on-site workshops
   - Resolve identified hazards prior to exciter system installation

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Palo Verde Exciter Hazard Analysis

7. Preliminary Hazard Analysis
   - Functional FMEA performed to identify the ‘must do’ and ‘must not do’ functions of the exciter HVAC control system
8. Perform Detailed Hazard Analysis
   - HVAC control system hazards organized in worksheets using *A-STPA* tool developed by University of Stuttgart
   - Detailed hazard analysis results to be reviewed in next workshop at Palo Verde (December 2014)

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Palo Verde Exciter Hazard Analysis

9. Hazard Analysis Acceptance, Documentation and Maintenance
   - To be determined

© 2014 Electric Power Research Institute, Inc. All rights reserved.

Hazard Analysis Demonstration Results

- Project ongoing
  - On-site workshop in May 2014
  - Palo Verde performing hazard analyses
  - 2nd on-site workshop planned for December 2014
  - EPRI lessons learned report in 2015

© 2014 Electric Power Research Institute, Inc. All rights reserved.

ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity

United States Nuclear Regulatory Commission

Protecting People and the Environment

NRC
Failure Mode Related Research

Mauricio Gutierrez
RES/DE/ICEEB

Ming Li
RES/DRA/PRAB

November 19, 2014

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Objectives

- To respond to ACRS comments and feedback from the Sept. 2013 I&C Subcommittee meeting.
  - Changes, based on ACRS feedback, were made to RIL -1002, "Identification and Analysis of Failure Modes in Digital Instrumentation and Controls (DI&C) Safety Systems – Expert Clinic Findings, Part 2,"
- To demonstrate that the Division of Risk Analysis (DRA) and Division of Engineering (DE) in the NRC Office of Nuclear Regulatory Research
  - have a common understanding of how digital systems fail, and
  - have conducted research efforts related to digital system failure modes that are complimentary and aligned.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Agenda

- Background
  - Summary of NRC Digital System Failure Mode Related Research Efforts
  - ACRS Feedback
- Summary of Staff Follow-up Actions
  - PRA and Deterministic Assessment Perspectives
  - Digital System Failure Mode Terminology and Common Concepts in Selected Definitions
  - Digital System Failure Modes Mapping
- Conclusions and Next Steps

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Background

- Advisory Committee for Reactor Safeguards (ACRS) has long standing concerns that software based DI&C system failure modes are not well understood. ACRS brought concerns to Commission attention in 2008.

- June 26, 2008 – Commission issued SRM-M080605B
  - Directed staff to "report the progress made with respect to identifying and analyzing digital I&C failure modes …"
  - and "discuss the feasibility of applying failure mode analysis to quantification of risk associated with DI&C…"
  - Direction rooted in NRC efforts to risk inform licensing process.

NRC Digital System Failure Mode Related Research

- DRA – PRA Methods for Digital Systems
  - Brookhaven National Laboratory NUREG/CR reports
    - Traditional Probabilistic Risk Assessment Methods for Digital Systems (NUREG/CR 6962 and NUREG/CR 6997)
    - Quantitative Software Reliability Models for Digital Protection Systems (NUREG/CR 7044)
  - WGRisk
    - International effort to establish failure mode taxonomy for PRA related research.
  - Draft "Development of A Statistical Testing Approach for Quantifying Software Reliability and Its Application to an Example System" (NUREG/CR-xxxx, BNL-NUREG-yyyy-20zz)

- DE – Analytical Assessment of Digital I&C Systems
  - RIL-1001 and NUREG/IA-0254
    - Software Related Uncertainties and Software Fault Modes and Effects Analysis
    - Completed on May 4, 2011, ML111240017
    - ACRS Briefed on June 22, 2011
  - RIL-1002
    - DI&C safety system failure modes
    - ACRS Briefed on September 19, 2013
    - Completed on September 3, 2014, ML14197A201
  - RIL-1003 (scheduled for early 2015 completion)
    - Feasibility of applying failure mode analysis to quantification of risk associated with DI&C systems.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

ACRS Feedback

- September 19, 2013 – ACRS I&C Subcommittee Updated on Research Information Letter 1002.
  - ACRS members offered overall positive feedback on RIL-1002 research and content.
  - Members raised concerns that NRC research related to failure modes was being performed by two groups (DE and DRA) and the research was divergent due to different understandings of how hardware and software fail.
  - Members requested harmonization of failure modes identified by NRC and EPRI.
  - Members suggested altering negative conclusions of RIL-1002 to more positive uses.
  - Staff agreed to provide ACRS a briefing by both DE and DRA staff to address concerns.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary of Staff Follow-up Actions

- DE and DRA staff have been meeting regularly to consider ACRS feedback.
  - Considered Technical Objectives and Perspectives
  - Considered Digital System Failure Mode Terminology used
  - Considered Failure Modes Sets Identified by each division
- Changes made to RIL-1002
  - Executive Summary re-written.
  - Added a set of failure modes identified by reviewing EPRI research.
  - Conclusions Section of RIL-1002 re-written.
  - Removed language implying that the synthesized failure modes in RIL-1002 are not applicable to PRA.

PRA and Deterministic Assessment Perspectives

	Technical Objectives	Involves asking:
Deterministic Licensing	Review how consequences of pre-determined bounding accident sequences are addressed. [NRC Glossary, Adapted] Determine the level of safety of a DI&C safety system [RIL-1002].	1. What can go wrong? 2. What are the consequences? [NRC Website: Risk Assessment in Regulation]
Probabilistic Risk Assessment	Support quantification of system reliability. Estimate Risk by computing real numbers [NRC Public Website: How We Regulate]	1. What can go wrong? 2. How likely is it to go wrong? 3. What are the consequences? 4. Which systems and components contribute the most to risk? [Apostolakis Presentation]

Digital System Failure Mode Terminology

Term	WGRisk/DRA	DE
Fault	Defect or abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function (IEC 61508; "defect" added) [WGRisk].	The state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources (IEC 60050-191: IEC Vocabulary) [RIL-1002].
Failure	Termination of the ability of a product to perform a required function or its inability to perform within previously specified limits (ISO/IEC 25000:2005) [WGRisk].	The termination of the ability of an item to perform a required function. (IEEE Standards Dictionary, IEC 60050-191: IEC Vocabulary) [RIL-1002].
Failure Mode	The physical or functional manifestation of a failure (ISO/IEC/IEEE 24765:2010) [WGRisk].	The effect by which a failure is observed to occur (modified from definition 1 in IEEE Standards Dictionary) [RIL-1002]. The manner in which failure occurs. (modified from definition 4in IEEE Standards Dictionary) [RIL-1002].

Common Concepts in Selected Definitions

Term	Common Concepts
Fault	Unintentional impairment of desired or correct functioning. Faults are often revealed when triggered by a condition that was not considered or not thought possible to occur. Faults are systemic.
Failure	The termination of the ability of an item to perform a required function.
Failure Mode	The manner in which failure occurs.

Digital System Failure Mode Mapping

RIL-1002 Set L	WG Risk Survey	EPRI Guidewords
No output upon demand	Loss of function No actuation signal when demanded	No function Partial function
Output without demand	Spurious actuation	Over function Unintended function
Output value incorrect	Failure to actuate	No function Partial function Over function
Output at incorrect time	Failure to actuate in time	Unintended function
Output duration too short or too long.	Loss of communication	Partial function
Output intermittent	No actuation signal when demanded	Intermittent function
Output flutters	Spurious actuation	Degraded function
Interference	Adverse effects on other functions	Degraded function
Byzantine behavior	Other	Degraded function

Conclusions and Next Steps

- DE, DRA, and EPRI have a common understanding of how digital systems behave and how digital systems can misbehave.
- DE and DRA staff;
  - Agree that Failure Mode Set L is an acceptable set of failure modes that could be useful for both DRA and DE.
  - Agree that Failure Mode Set L is incomplete; it is uncertain how many unidentified failure modes remain.
  - Are considering potential uses for Failure Mode Set L
- DE and EPRI will continue sharing information from digital system failure mode related research.
- Vocabulary Harmonization project is being considered for inclusion in I&C Research Plan FY 2015-2019.
- RIL -1003 – will address technical limitations and feasibility of traditional quantification methods use for digital system assessments.

Backup Slides

Mauricio Gutierrez

Ming Li

RIL-1002 Cites DRA Research

- Set I and Set J in RIL-1002 were generated by DRA sponsored research projects.
- Set J: WGRisk Failure Mode Taxonomy
  - Classify and organize digital I&C failure modes for the purposes of NPP PRAs or PSAs
  - No complete set of failure modes is developed
  - This taxonomy was demonstrated by an example study
    - Failure to actuate
    - Failure to actuate in time
    - Spurious actuation
    - Adverse effects on other functions
    - Loss of function
    - Loss of communication
    - No actuation signal when demanded

RIL-1002 Cites EPRI Research

- Set K was added to RIL-1002 per ACRS comments.
  - No function
  - Partial function
  - Over function
  - Degraded function
  - Intermittent function
  - Unintended function
- Set K was found in EPRI report: Hazards Analysis Methods for Digital Instrumentation and Control Systems.

RIL-1002 Synthesized Failure Modes

- Set L:
  - No output upon demand
  - Output without demand
  - Output value incorrect
  - Output at incorrect time
  - Output duration too short or too long.
  - Output intermittent
  - Output flutters
  - Interference
  - Byzantine behavior