UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

June 25, 2015

MEMORANDUM TO: ACRS Members

FROM: Christina Antonescu, Senior Staff Engineer /RA/
John Lai, Senior Staff Engineer
Technical Support Branch, ACRS

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS, NOVEMBER 18-19, 2014—ROCKVILLE, MD

The Subcommittee Chairman has certified the minutes of the subject meeting, dated November 18 - 19, 2014, as the official record of the proceedings of that meeting. I have attached a copy of the certified minutes.

Attachment: As stated
cc: E. Hackett
M. Banks

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

MEMORANDUM TO: Christina Antonescu, Senior Staff Engineer
John Lai, Senior Staff Engineer
Technical Support Branch, ACRS

FROM: John Stetkar, Chairman
Digital I&C Systems Subcommittee

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS, NOVEMBER 18-19, 2014—ROCKVILLE, MARYLAND

I do hereby certify that, to the best of my knowledge and belief, the minutes of the subject meeting, dated November 18-19, 2014, are an accurate record of the proceedings for that meeting.

/RA/ 06/03/2015
John Stetkar, Chairman Date
Digital I&C Subcommittee

Certified on: June 3, 2015
Certified by: John Stetkar

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MINUTES OF THE ACRS DI&C SUBCOMMITTEE SUBCOMITTEE MEETING
NOVEMBER 18-19, 2014

The ACRS DI&C Subcommittee held a meeting on November 18 - 19, 2014 in T2- B1, 11545 Rockville Pike, Rockville, Maryland. The meeting convened on November 18, 2015 at 8:30am and adjourned on November 19, 2014 at 11:40am.

The entire meeting was open to the public.

No written comments or requests for time to make oral statements were received from members of the public related to this meeting.

ATTENDEES

ACRS Members

John W. Stetkar, Subcommittee Chairman
Dennis C. Bley, Member
Charles H. Brown Jr., Member
Ron Ballinger, Member
Dana Powers, Member
Joy Rempe, Member
Stephen P. Shultz, Member
Myron Hecht, Consultant

Christina Antonescu, Designated Federal Official
John Lai, ACRS Staff

NRC Staff/Consultants
Kevin Coyne, RES/DRA
Russ Sydnor, RES/DE
Ming Li, RES/DRA/PRAB
Tsong – Lun Chu, BNL
George Marts, INL
Kim Kaser, INL
Athi Varuttamaseni, BNL

Other Attendees
Dave Blanchard, EPRI
Bruce Geddes, EPRI
Ray Torok, EPRI

SUMMARY

Russ Sydnor and Kevin Coyne made opening remarks describing history of past efforts and coordination between RES/DE (supporting staff assessment of digital systems) and RES/DRA (modeling of digital systems). While both branches are interested in probabilistic methods, quantitative reliability analysis is not sufficient to provide a "reasonable assurance" finding but can provide insights. RES/DE still relies on deterministic criteria. An ACRS member amplified on this point stating that safety systems should conform to the following principles: redundancy, independence, defense in depth, limited access, determinism, and simplicity. Other ACRS members concurred. The staff agreed that probabilistic results cannot substitute for these design principles but can be used to provide insight. For RES/DRA, a quantitative methodology is the ultimate objective, but the practicality and usefulness of proposed methods is still under evaluation.

Ming Li presented an overview and history of quantitative software reliability research and plans for future activities. Several committee members commented that the plans for future research required more detail. This presentation was followed by two presentations on research conducted by BNL

The first was on the use of Bayesian Belief Networks to assess the fault density and subsequent failure rate of software based on software development practices (requirements, architecture, design, coding, verification, etc.) and was presented by Louis Chu. The work involved identifying the influences on software fault density, developing an influence network of the development practices, assigning weights to the influences, and then calculating defect probabilities. This is work in progress. Thus far, experts were used to create the network. Future work will involve elicitation of their opinions for weights, probabilities, and translation of fault density into failure rates. The subcommittee expressed skepticism about this approach due to the need to carefully account for possible biases of the experts and difficulties in translating fault density to failure rates.

The second presentation was on statistical testing by Louis Chu and Athi Varuttamaseni, and Tim Kaser and George Marts. The objective was to demonstrate how the probability of failure on demand could be estimated using input from accident scenarios that were derived from a probabilistic risk assessment (PRA). The example system was the Loop Operational Control System (LOCS) of the Idaho National Laboratory (INL) Advanced Test Reactor (ATR). BNL modified a RELAP thermal hydraulics model originally created by INL to account for the effects of failures in sensors, actuators, and initiating events (e.g., pipe breaks and sensor failures). The output of this model, which in essence acted as a simulator, was input to the safety and control system, and the responses of the system were recorded and monitored for correct output. There was one test where there was no trip when there should have been one, but the failure was not reproducible. It should be noted that the results of these tests would not be a complete assessment of the probability of failure on demand because they do not consider failures of the underlying hardware or operating system.

Ray Torok, Bruce Geddes, and Dave Blanchard made a presentation on Digital Failure Modes based on their experience analyzing a digital instrumentation and control system. Such failure modes include both "hard failures" and “unintended system behaviors.” The specific failure modes depend on the architectural level of interest. At higher levels of interest, the failure modes are associated with the functions (e.g., high pressure injection), but at lower levels, they are associated with the specific items or equipment. The choice of failure modes is dependent on the lowest level of interest (or depth) of the analysis and the methodology used. For the “top down” analysis at higher levels of interest, effects are traced back to original causes, and the failure modes are function-or context-specific, governed by “guide words” in a manner similar to a HAZOP method used in the chemical industry. For a lower level "bottom up" analysis where the specific equipment are known, the component level failure modes can be used.

Ray Torok, Bruce Geddes, and Dave Blanchard presented EPRI-sponsored work on modeling digital instrumentation and control systems in PRAs. A presentation on Hazard Analysis updated work on six different approaches for hazard analysis that were originally presented in September 2013. Strengths of these methods were compared, and it was pointed out that no single method was sufficient; multiple approaches had to be combined. The four primary approaches were event trees, functional FMEAs, “design” (component level) FMEAs, and System Theoretic Process Analysis (STPA). In functional FMEAs, the analyst starts with effects and traces them back to causes. Effects are defined by event trees. The intent was to come up with a standard set of effects for each type of plant. A demonstration project is underway. For PRAs of digital systems, EPRI defined a 9-step process. The central thesis is that digital components can be modeled like analog systems after taking account for differences. For example, in parallel systems, software introduces a high common cause failure factor. Members of the ACRS agreed with the philosophy that analysts should involve the designers and should not model the system by themselves. However, they also emphasized the need to include human reliability analysts in the process so that the operator actions and the human-system interface (HSI) are properly considered.

The final presentation was an update on digital system failure modes research by Mauricio Guitierrez. The presentation was made in response to comments from the DI&C subcommittee to harmonize failure modes between DE and DRA in the September 2013 meeting. The discussion that ensued covered different concepts concerning “fault mode”, “failure mode”, “software fault”, “software failure”, and “digital system failure” that are contained in NUREG/IA-0254 and RIL 1002. The outcome was that (1) “digital systems” fail and have failure modes, (2) software defects are the cause of some digital system failures, but software does not in isolation have failure modes, and (3) the set of digital system failure modes originally labeled as Set K in RIL 1002 was tentatively selected (now renamed as Set L in the September 2014 version of RIL 1002). It was recognized that this list is tentative and subject to revision. The subcommittee emphasized the need to harmonize the vocabulary with industry and to review related work on failure modes by EPRI.

Public Comment: A public comment was made by Mr. Bob Enzinna of AREVA on 11/18 stating that at the level at which PRAs are done (i.e., a valve malfunction or failure to change position

upon demand), the contribution of the digital system failure to the overall failure probability is small. However, what is also important is the architecture and the design of the digital I&C system itself to prevent failure triggers and features to prevent propagation between different divisions and computers in redundancies. He suggested a taxonomy of common cause failures and defenses. Without that taxonomy, overly conservative assumptions can drive results to counter-productive conclusions. Mr. Enzinna made a similar comment during the comment period on 11/19. Specifically, he said that after identification of the failure modes, the next step for PRA is assessing the effectiveness of barriers and defenses against propagation of common cause failures. He suggested comparing these failure modes to the defenses that EPRI had identified to judge how much credit these defenses have against preventing propagation of failures.

Closing Comments by the Members: All of the ACRS subcommittee members expressed their thanks to the staff and to EPRI for their presentations. Most members (including the subcommittee chairman) felt that an ACRS full committee meeting should be held in the first or second quarter of 2015. An ACRS member stated that the research plan needed additional tasks. Two members suggested performing a pilot study to assess the results of the work on digital system failure modes against a real plant. Another member pointed out that independence (i.e., electrical independence) was relied upon to be the primary means of preventing common cause failures in analog systems, but that is sufficient in analog systems. Digital systems need measures to contain failure propagation such as one-way data paths, and there should not be a "software controlled data path". Several members also stated the need to publish the draft NUREG on the statistical testing approach for public comment, but that it should be reviewed internally prior to its release.

List describing significant issues discussed during the meeting with the corresponding pages in the transcript.

SIGNIFICANT ISSUES	
Issue	**Reference Pages in Transcript**
<u>Opening Presentation</u> Member Brown stated that safety systems should conform to the following principles: redundancy, independence, defense in depth, limited access, determinism, and simplicity. Attempts have been made to answer the basic question of failure modes and failure rates for PRAs and other quantitative analyses but no definitive methods or solutions have yet been developed. Hence, these goals and principles are still relevant and should continue to provide the underlying motivation for the current research effort.	14-20

Members and the staff discussed the complexity of the digital system and how a less complex PRA model can be used to address the design and operation of the digital system.	15-25
Members and the staff discussed what level of detail is used to model the failure modes. It was noted that PRA modeling will generally require a level of detail that is consistent with the available operating experience and data. Deterministic licensing reviews may require more detail.	29-37
Overview of Digital I&C PRA Research Activities Several members took issue with the definition of a software failure. There were two major objections: (1) software can cause not only the failure of a system to perform an action but also perform an incorrect action, much as a human reactor operator could take the wrong action, and (2) software is deterministic and the definition of failure does not seem to take this into account. Chairman Stetkar pointed out that failures are integrated hardware and software; the modeling methods should not get stuck on piece parts, i.e., at too low a level. It's not necessary to deal with the internal state of all components. What is necessary is to determine what constitutes undesired behavior and the frequency at which such undesired behavior manifests itself. Regarding the integration of DI&C research activities shown in the Research Plan Diagram on Chart 7, members pointed out that the way in which the multiple inputs result in regulatory guidance is unclear. The step from research-grade risk and reliability modeling efforts to modeling methods that are sufficiently defensible to withstand regulatory scrutiny is needed. Experience with NUREG/CR-6850 (on fire analysis) showed that it's not a simple transition.	39 – 82
Development of a Bayesian Belief Network (BBN) Model for Quantifying Software Failure Probability Members and Louis Chu discussed the merits of using a BBN rather than truth tables.	89-92
Member Bley requested a copy of a paper by Littlewood	91

Members and the presenters discussed the role of three levels of expert elicitations for the BBN.	102-109
Members, Mr. Hecht, and the presenters discussed the development of the software design phase of the BBN model.	110-115
Members commented that more work is needed to relate the software flaws to system failures. Staff mentioned that the research is ongoing.	115-128
Members and the staff discussed the attributes of the quality nodes in the diagram and how the opinions of expert solicitations are being used in developing the nodes.	133-142
Members and the staff discussed the definition of “function points” and how they are used in the software design diagram	143-148
Mr. Hecht and Louis Chu discussed how calibration may be needed to relate the fault size distribution to a failure rate.	153-157
Members and the presenters discussed how the BBN method is solved at the current stage of the project.	163-175
Overview of Statistical Testing Approach, Results and Insights The presenter stated that there were no loop operating control system (LOCS) trip signal failures for 10,000 simulation test runs. There was actually one case in which a failure did occur. The output showed that no trip signal was generated. INL did approximately 100 runs of the same test case, but they were not able to reproduce the failure.	175-182
Members and presenters discussed the loop operating control system (LOCS) and the INL test loop.	183-207
Members and presenters discussed the Advanced Test Reactor (ATR) PRA model and using the PRA information to generate a realistic operating profile for testing.	208-228
Presenters and Members discussed the results of the statistical testing method.	229-258

Mr. Enzinna of AREVA made comments on the DI&C PRA modeling.	258-260
EPRI's Modeling Digital Instrumentation and Control systems in PRAs Members of the ACRS agreed with the philosophy that analysts should involve the designers and should not model the system by themselves. However, they also emphasized the need to include the human reliability analysts in the process so that the operator actions and the HSI are properly considered. The final presentation was an update on digital system failure modes research by RES/DE/ICEEB. The subcommittee emphasized the need to harmonize the vocabulary with industry and to review related work on failure modes by EPRI.	261 – 394
Mr. Hecht and the presenters discussed the sources of failure modes and hazards.	272-275
Mr. Hecht and the presenters discussed the functional Failure Modes and Effects Analysis (FMEA) method	282-294
Members suggested that EPRI describe guidance for the functional FMEA in a more transparent fashion in the report.	294-299
Presenters discussed the design FMEA method and also how these different FMEA methods may be incorporated in the plant PRA model.	299-309
Industry presenters discussed that lessons learned in activities analyzing specific issues helped shape the method of the most recent EPRI report 1025278.	309-324
Dave Blanchard and Members discussed that some PRA analysts do not model events that are considered unlikely to occur in the internal at-power model, but which could lead to different consequences for digital I&C failure events.	329-333
Members suggested to add more details in Step 1 to guide the PRA analysts and Digital I&C engineers for discussion of the nuances of the digital design.	349-354
Members stated that HRA should be part of the integrated PRA modeling in Step 4.	364-369
Chairman Stetkar stated that uncertainties were not addressed for the quantification in the report.	385
Presentation on Digital Failure Modes by EPRI (11/19)	

Member Brown discussion of system levels reflecting "in plant architecture". Reiterated that the architectural fundamentals of plant protection systems are independence, deterministic behavior, diversity, defense in depth, control of access, simplicity	8-11
Chairman Stetkar's discussion on lack of system level view, too easily combining software unanticipated behaviors with common cause events, clarification of misbehaviors rather than failures as a way of focusing analyst attention. Failures are a subset of all possible misbehaviors	21-26
Member Brown's observation that diversity doesn't always increase reliability. Member Bley's response that diversity does protect against common cause failures	28-29
Member Brown on importance of isolating safety communications from other network traffic	38-39
Member Brown interchange with Mr. Torok on not integrating too many functions (independence) and access control	43-50
Member Schultz on the rarity and hence lack of experience with common cause failures	63-65
Chairman Stetkar's comments on proprietary issues restricting sharing of data on common cause failures	67
Member Ballinger on lack of access to an EPRI report	76-77
Hazard Analysis Demonstration	No significant comments
Presentation from Staff on Failure Modes Research	
Member Brown question that staff actions to revise failure modes were initiated by ACRS comments rather than by a staff evaluation	101
Chairman Stetkar concerned about NRC Staff terminology use	104-106
Chariman Stetkar and Member Brown questions on the intent of terminology harmonization within both NRC and with industry	113-123
Closing Comments	
Chairman Stetkar and Member Schultz on a full committee meeting on topics discussed in the subcommittee meeting	127-129
Member Brown on the need to reinforce independence among divisions in DI&C systems	130-132
Member Rempe on updating the research plan, getting more detail on failure mode harmonization, and reviewing the draft NUREG prior to release	133-134
Chairman Stetkar on a follow up meeting and thanking the staff and EPRI for the presentations	135-136

Documents provided to the Subcommittee

1. Draft NUREG/CR-xxxx, “Development of a Statistical Testing Approach for Quantifying Software Reliability and Its Application to an Example System,” October 15, 2014
2. Research Information Letter (RIL) 1002, “Identification and Analysis of Failure Modes in Digital Instrumentation and Controls (DI&C) Safety Systems—Expert Clinic Findings, Part 2”
3. EPRI TR - 1025278, “Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments,” July 2012
4. EPRI TR - 1019183, “Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants,” December, 2009

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 18, 2014

Work Order No.: NRC-1229 Pages 1-377

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

Washington , D.C. 20005
(202) 234-4443

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

JOINT DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

AND RELIABILITY AND PRA SUBCOMMITTEES MEETING

+ + + + +

TUESDAY

NOVEMBER 18, 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

DANA A. POWERS, 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

P R O C E E D I N G S

(8:33 a.m.)

CHAIRMAN STETKAR: The meeting will now come to order. This is a joint meeting of the Digital Instrumentation and Controls and the Reliability and PRA Subcommittees. I'm John Stetkar, Chairman of the Subcommittee meeting.

ACRS members in attendance are Steve Schultz, Dennis Bley, Ron Ballinger, Charlie Brown and Joy Rempe. We're also joined by out consultant, Myron Hecht. Hi, Myron.

ME. HECHT: Good morning.

CHAIRMAN STETKAR: Christina Antonescu of the ACRS staff is the designated federal official for this meeting. The purpose of this meeting is to review research related to the effort of modeling digital instrumentation and control systems and probabilistic risk assessments.

We've been following this work for a few years and will learn about progress that has been made since our last briefing in, I think it was September 2013, if I got my dates right.

The meeting is scheduled for a day and a half, and we have a lot of material to cover. We'll

hear presentations from the NRC staff and their contractors and the Electric Power Research Institute.

The subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions as appropriate for deliberation by the full committee.

The rules for participation in today's meeting have been announced as part of the notice of this meeting, previously published in the Federal Register. We received no written comments or requests for time to make oral statements from members of the public regarding today's meeting.

I know that we have some people on the bridge line listening in to the discussions. To preclude interruption of the meeting, the phone line will be placed on listen-in mode during the presentations and committee discussions. We'll open the bridge line at appropriate times during the meeting to allow anyone listening in to make comments.

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

the subcommittee. The participants should first identify themselves and speak with sufficient clarity and volume so that they may be readily heard.

Also, please check and silence all of your personal little electronic beefy devices. We will now proceed with the meeting. I believe that Mr. Russ Sydnor from the Instrumentation Controls and Engineering branch and Mr. Kevin Coyne from the Probabilistic Risk Assessment branch have some opening remarks. Russ?

MEMBER REMPE: Mr. Chairman, just quickly, because of organizational conflict of interest concerns, I will need to limit my participation and comments in certain portions of this meeting. And I see it in the statement. Sorry for that.

CHAIRMAN STETKAR: Thank you very much.

ME. SYDNOR: Thank you. Good morning, everyone. So I first wanted to just go over a purpose that we're here for a day and a half. We have several different areas of research we wanted to discuss. We believe these research areas are complimentary, and we hope to demonstrate that to the ACRS over the next day and a half. So we're here to present status and some results, some status. I think you'll be interested in

all of it.

In another meeting, like we had about a year ago, we asked PERI to participate in this meeting too, because the industry is doing complimentary research in this area. And we've been collaborating with them under our MOU in the Office of Research.

So we're really looking for, we're not requesting a formal letter or anything at this point. We want to discuss and obtain insight from ACRS members. And as you'll see as we go through this, a good portion of what we're discussing today is we're coming back because of concerns you raised in the past meetings, issues and concerns.

And the other purpose today is the NRC staff, because we have been working closely with PERI under the MOU, we want to support their presentation and be available to, you know, answer any questions that might pertain to how their work relates to our work.

Just some quick background, the last briefing of ACRS Digital I&C Subcommittee on the Brookhaven work looking into methods for digital system PRA was on June 7th, 2011. And at that time, you may remember Alan Kuritzky was the project

manager.

Ming Li, who'll be presenting today is now the current project manager of this work. They presented quantitative software reliability methods that they had reviewed and plans to implement a BBN and statistical testing methods based on the methods, the reliability methods they'd selected.

MEMBER BROWN: What's a BBN again?

ME. SYDNOR: Bayesian Belief Network.

CHAIRMAN STETKAR: Bayesian Belief.

MEMBER BROWN: Oh, Bayesian, that fancy word again. For us non-PhDs. Thank you.

CHAIRMAN STETKAR: I don't have a PhD.

MEMBER BROWN: I know, but you're smarter than I am. So there.

ME. COYNE: It's essentially an influence diagram.

(Laughter)

ME. SYDNOR: Some ACRS feedback at that time, which Kevin and his staff will be addressing in his time, trying to achieve an appropriate balance between system complexity, and PRA modeling and understanding digital system failure modes. And that's where there's significant crossover to our work

in my branch, especially with regards to completeness of PRA context and dependencies.

And as you mentioned, John, about a little over a year ago we came to the committee to talk about several different topics, failure modes and also some new work we were doing on hazard analysis. And again, as I mentioned before, at that same meeting we had PERI. And they did a presentation on work they had completed on hazard analysis.

So some feedback from that meeting, which this feedback is probably one of the primary reasons we're here today. Because we've been, Kevin and I, I came back from that meeting, Kevin and I started meeting. We set up routine meetings.

We felt we'd always been aligned, but, you know, you raised valid questions though, we decided to tackle that issue head on. So you raised concerns about the research related to failure modes as being performed by different groups, and might be divergent and have different understandings of how digital hardware and software fail.

Members also requested, in relation to the PERI work, that we pursue harmonization of failure modes identified by NRC and PERI. And some of what

we'll talk about today, hopefully you'll see how we believe it does harmonize.

But the final presentation at the end of the half, morning tomorrow, we'll come back and revisit that and tell you some very specific things we did in the work we presented at that time in September. Because we presented the draft research information letter which is now complete. And we've made significant changes to it based on ACRS feedback. And also we told ACRS we'd come back and brief on our mutual work.

One thing I wanted to stress, and Kevin will stress too, is that the research activities we're talking about today, including the PRA work, are all under the same research plan. Kevin's efforts in digital system PRA are covered in our research plan. And we're looking at updating that plan, because we're getting to the end of the five years. And so even in the future, that'll pertain. We've agreed to that.

So our research objectives under that plan is to understand digital system behavior and develop guidance, whether it's in PRA or in deterministic licensing reviews, develop guidance that supports that mutual understanding.

So in my area, we developed staff positions and review guidance to support safety reuse by the licensing offices. And in Kevin's area, he's working on developing methods and associated guidance for including digital systems in nuclear plant PRA. Kevin's going to continue here with the --

ME. COYNE: Okay. So as Russ said, we began communicating more in earnest after the September 2013 ACRS meeting. We had been talking prior to that, but we realized as we talked more we haven't done a good job communicating how we are aligned and how our research programs are complimentary and covered by the same integrative plan.

So it forced us to start thinking a little better about how we could communicate that. So the next few slides go through a few areas where I think there's been, and probably fostered by the staff, some perception that we haven't been fully aligned, and we might be diverging somewhat.

So I wanted to go through a few areas and just highlight some of the differences and similarities between what we're doing, between Russ' program, and the research division of engineering and

my program in the division of risk analysis.

So to start breaking things out, we thought about the role of qualitative reliability analysis. And from the deterministic licensing viewpoint, that directly supports their system assessment and how they view the systems.

From the PRA standpoint, it provides modeling insights. It isn't the end goal for us, but it's providing insights in how we want to model these systems in a quantitative PRA. And that moves over to the quantitative reliability analysis.

And I think the first bullet is really a key point, because I think this is one area where we haven't always spoken with a unified voice externally. I think we were aligned internally, but I don't think we've done a good job communicating this.

Quantitative reliability analysis doesn't support a deterministic licensing finding. We don't license any system based on its reliability target. We license it based on deterministic licensing criteria, compliance with quality assurance programs, general design criteria, things like that.

So although that's good insights for the deterministic licensing process, the quantitative

reliability of the system isn't something that they can make their safety finding off of. They don't look at it and say it's got 99.99 percent reliability, so therefore it's good to implement in the system.

And so I think when we said things like we can't use quantitative reliability for licensing, we haven't clarified that in the right context. But it does provide insights. It's just not the final result you need. You need to look at other criteria to actually do the licensing process.

MEMBER BROWN: Can I ask a quick question on the quantitative part? One of my underlying, you've probably heard several times my standard comment relative to the principles of reliable digital instrumentation control systems, the redundancy, independence, deterministic behavior, defense in depth, diversity, et cetera, et cetera, simplicity of design.

And I guess one of my concerns has been going around when we talk about the quantitative, and trying to tie the quantitative type PRA methods to our protection systems and safeguard systems, and I'm really, I'm kind of harkening back to some early comments when I first arrived here six years ago, six-

plus years ago.

There was communication between divisions, software type communications, proposed in many circumstances, which really compromises or threatens to compromise independence.

And I guess one of my concerns is that somebody comes along with a quantitative reliability analysis and says, oh gee, this things good for 99.99 percent reliable, it'll always work, that now we start compromising fundamental principles such as independence and/or some redundancy that we might have.

And I don't know what's downstream in your thought processes. I don't view, I have no problem with this, don't take this the wrong way, I would find myself hard-pressed to have these types of methodologies used to compromise the fundamental, or override or supersede the fundamental principles. So I just wanted to, I don't know what you all's thinking is. That's my thinking. I'm just --

ME. COYNE: I couldn't agree with you more, actually. And I think a theme that might emerge over the next day and a half is, and this goes back to the last ACRS meeting we had 2011 on this, in that the

issue of complexity, and I think the concern, and Dr. Bley was one who was advocating this, is you've got to be careful of using simplified PRA methods.

Because the systems themselves may be more complex, and you may not get a good match between, you know, a simplified modeling approach and the actual complexity of the system.

My personal view is I turn that around and say there has to be a limit on the complexity of the digital system you're trying to put in the plan, because you may not be able to model it in a PRA.

There may be limitations that you need to oppose on what the system can look like and the communication between divisions and things like that, that if you allow the sophistication and complexity to become too great, it may not be possible to really do an effective PRA model of it.

So I think that's a balance we have to meet between the design of the system and the PRA modeling. That's a challenge. I don't have an answer for it.

MEMBER BLEY: Before we leave this, and you might not believe me, Charlie, but I don't think if you do, excuse me, if you do a good model, I don't

think you can find the reliability in the system if it doesn't meet --

MEMBER BROWN: Well, that's my --

MEMBER BLEY: -- this criteria.

MEMBER BROWN: -- yeah, I agree. That's my --

MEMBER BLEY: And if you find one that way, you ought to start digging and figure out either there's something wrong with my principles or there's something wrong with the analysis.

MEMBER BROWN: Yeah. Well, I look at it based on our earlier discussions of trying to identify where our systems have gotten more complex, but it doesn't add value, or it runs into compromising potentially the fundamentals of the thing. So it's just a matter of how we use them and how we apply them. And that probably applies somewhat to the level at which you model them in your methodology --

MR. COYNE: And a challenge for us is there may be levels of complexity that we just can't do a practical PRA model for. I do worry about that, and I think that's a challenge looking forward, as we move forward with the research.

Second bullet, for us, you know, the

ultimate goal is the quantitative reliability. We want to get these systems modeled in a nuclear plant PRA. And the whole purpose of doing that is to get the quantitative reliability model. So that's the end goal for us, contrary to the more deterministic view.

MEMBER BLEY: Before we let this one go --

ME. COYNE: Although insights are important too. I should say that.

MEMBER BLEY: I kind of wish some of you had been at yesterday's session where we saw the PERI response to this open phase problem on power systems, and very complex problem, very hard to solve.

But when you get clever enough, you find a way to analyze parts of it that can solve your problem. And I just hate for us to get in the spot, we hint that we ought to be designing our systems so that they're easy to model in PRA land. Enough on that.

ME. COYNE: Right.

MEMBER BLEY: It that's a problem, we ought to get more clever about how we do our modeling.

MEMBER REMPE: I agree. It almost sounded like, if I can't model it, I don't want to put it in a plant. And that didn't sound quite right.

MEMBER BROWN: On the other hand --

(Simultaneous speaking)

MEMBER BROWN: I think there's a balance.

MEMBER BROWN: I could Roger up to that.

MEMBER REMPE: Well, sometimes it sound a little strange, I mean --

(Simultaneous speaking)

MEMBER BROWN: If you dig down into a channel of I&C today, digital I&C, it's very, very complex. Software is complex, the interactions inside the software are complex, the interaction of the software with adjacent other hardware pieces within its own division are very complex and not time predictable unless you follow certain sets of principles.

But that doesn't abrogate the ability to go use that, that technology, to your benefit. And that's the key. You want to use it to your benefit and where it adds value. So I agree relatively with my colleagues comment here to a certain point. It depends on what you're looking at and where that level of complexity exists.

MR. SYDNOR: I think you just keep those questions in mind as you hear both what we're doing

and what the industry is doing.

MEMBER BROWN: I will be listening.

CHAIRMAN STETKAR: I think, I might as well weigh in a little bit here, that instrumentation and control, anything to do with electrical stuff, instrumentation and control being part of that, and now digital instrumentation and control with the added joys of software, always raises the aura of complexity.

And I hate to say this, but the folks who design and build this stuff are enamored by the amount of complexity of these things. And they know in their hearts that the only way that you can model this stuff is to model each bit and bite of all of that complexity. You have to do that. Because that's the way we, as engineers, think about all of these things.

I harken back to 30 years ago when people first started to model analog, nice relay, click, click, click, protection systems, where some guy who had spent his career designing and building these things, took it upon himself to develop a model of these things.

And he had the model down to corrosion on contacts, and resister open circuits, and capacitor

degradation and built a model that was so big that the computer software at the time could not solve the model.

But he knew that that model had to be that complex to solve the problem. He had no data to support the model, because no data were -- I mean, you could look at, you could find numbers anywhere, you can look in the phone book and find numbers.

He finally was convinced that he could simplify the model to not a single black box that said it works or not, with some likelihood, but some intermediate level of detail, if he got clever and thought about at what level is the information available, that's compatible information, and actually got the model to a size that, A, could be solved and, B, provided reasonable results that were sort of consistent with operating experience.

But he couldn't do that without the help of people who were professional modelers. And my point is that you need both of those skill sets when you're developing a risk assessment. You don't need the modeling skill set when you're designing and building a system. And you don't necessarily need to know every iota of a design when you're trying to

model it.

Because in many cases, as Dennis mentioned, you can be clever about ways to model things when you look at where's the information available, what are the functions, what are the outputs that you need?

So this notion of, well, it's so complex that I can't model it, you can model anything regardless of how complex it is. It's just a matter of selecting the right level of detail that's consistent with the available information.

And, you know, if something is really complex, and I'm not trying to downgrade, digital instrumentation control systems are pretty doggone complex when you start thinking about all of the details. But I think there are ways to solve the problem.

And some of the stuff I've been reading lately, I think seems to be pretty encouraging in terms of the direction it's going.

MR. SYDNOR: I think you mentioned a couple of things there that I'd ask you to listen for, especially in EPRI's presentation, a level of concerns with the system. Where is your level of concern?

Where's your level of ability and skill sets?

MEMBER SCHULTZ: And, Kevin, going back to your original comment in terms of design complexity and ability to model that complexity, when we do come upon examples in the presentation today, tomorrow, if you could elaborate regarding those examples, either you or Ming Li --

MR. COYNE: Right. We'll do that.

MEMBER SCHULTZ: -- whenever that comes up, that will be very helpful.

MR. COYNE: Okay. Yes, we'll do that. And I also want to add, to follow on to the comments, over the last several years this has evolved to me. If you recall a few years ago, I mean, there were pockets of resistance saying we couldn't even model digital systems in PRA, some very senior people in the agency actually making statements like that.

I've always believed we could. I think it comes down to, and we will echo an earlier comment we gave you, I think it comes down to the practicality and usefulness of it. Is it going to be practical to model these systems? And if they become so complex, yes, we can model them, but it's just, you know, cost prohibitive to practically do it.

Or the uncertainties associated with the parameter estimations I have to do for some of these things might overwhelm the insights and results you get. So I think that's the balance we have. We'll hold that thought. Ming is going to touch on it later as we go through the presentation.

But, let's see, so it's failure modes. So, John, your thoughts were a good set up for the failure modes and the complexity. So this has been a topic that we've actually been having a lot more discussion on.

In fact, most of the monthly meetings Russ alluded to have been focused on failure modes. And it's been good. So I think the comments from the ACRS have helped us get some better alignment in this area.

So clearly, failure modes provide insights into the behavior of the system. One of the key things, and it's a theme that you'll hear from us and EPRI, is that the insights depend on the level of detail you're considering in the analysis, function level systems, training component and sub-component level. The deterministic review obviously uses the failure mode information for failure modes and effects analysis, hazard analysis, system design reviews.

I struggled with the second bullet. I'll say loosely it characterizes the basic events in the PRA model. There's additional things failure modes do for you, but that's one high level, simple way to look at it.

And then going to the next slide, I couldn't help but put a line from NUREG-0492 on the fault tree handbook. And this vocabulary is very important as we go through it. And that's one of the key lessons we've learned as we've gone through this research program, is failure mechanisms produce failure modes, which in turn have a failure effect on the system.

And as you change the level of detail you're looking at from train component, sub-component, for example, these things shift. So this is actually, it isn't exactly from NUREG-0492, but it's close proximity to an example that that NUREG gives of a valve failing to open and how it affects the train component, and sub-component and the mapping between failure mechanisms, failure modes and failure effects.

MR. HECHT: Kevin, can I ask a question about that?

MR. COYNE: Sure.

MR. HECHT: In September of 2013, EPRI presented, as part of their work, a basically standardized seven-level, I believe, hierarchy for a nuclear power plant. And, of course, you show that. They called it levels of interest. You're calling it levels of detail here. Is there any thought about harmonizing and standardizing on the levels of analysis?

MR. COYNE: I'm staring at Ray Torok right now. But we've discussed this concept. I think, and you're going to hear a very detailed presentation from EPRI on this. I don't think this concept is inconsistent with their view of the system. They have a little different way of looking it and a little different way of talking about it. But the concepts are very similar. Ray, do you want to add anything?

MR. TOROK: Yeah, this is Ray Torok from EPRI. Yeah, I agree with what you said. And we will continue to talk about this during our meetings with the research guys under the memorandum of understanding we have where we continue to compare notes from our projects.

MR. HECHT: I'd like to suggest that is you can standardize on that, then you will find the

challenge a lot easier, including but not limited to terminology and the concepts behind it. The vocabulary is extremely important to agree.

MR. COYNE: We have painfully become aware of that. It's a great point, in that the thought of having PRA modelers work more closely with the digital system designers, and that vocabulary is a huge barrier to overcome.

And Ming is going to talk about an international project we had through OECD, and that was one of the biggest challenges of making sure everybody was on the same vocabulary.

MEMBER BROWN: Before you go on, I mean, the little box that you say you had to throw in from the NUREG, the levels of detail, which is, I understand that. That's simple enough for me to understand.

Have you tried to take that model of how you describe it and translate it into what's the level of detail in a digital microprocessor-based division, channel, whatever you want to call it? Say, you know, where, following that thought process --

MR. COYNE: Right.

MEMBER BROWN: -- can you, it would have

been nice if you used a I&C level of detail box for that instead of a valve box.

MR. COYNE: Yeah, I'm not smart enough for the I&C example. The valve, I could barely get.

CHAIRMAN STETKAR: Actually, it's better not use it, quite honestly. Because it's a concept rather than getting into the minutiae of details of -- it's a concept.

MEMBER BROWN: Yeah. No, I understand that. But if you look at the I&C systems at a higher level on a concept basis, you can think of detectors, you can think of IO inputs. You can then think of the box, the computer, you can think of a hardware monitor, and you can think of various pieces that are part of that component level, subcom.

But they're not down in the minutiae. And then how does that flow through there? And so that's what I was thinking, if they had started to translate to that level.

ME. COYNE: I tried --

MEMBER BROWN: The answer is no.

ME. COYNE: I tried for a simple example. And I couldn't come up with one.

CHAIRMAN STETKAR: I think EPRI's

presentation will walk you through that in your vernacular.

MEMBER BROWN: Okay.

MR. COYNE: And Ming is going to talk about this international OECD WG risk project. And that was to look at failure mode taxonomies. And one of the initial tasks that people rapidly realized is they needed to define what an I&C system looks like.

So there was an example system that was developed. It didn't represent any particular system, but it tried to capture the attributes of a typical digital I&C safety system to try to show, you know, system level components, sub-component level and how that maps. He'll have a few slides on that to try to illustrate this point a little more with an I&C example.

A couple of key points here is that, you know, multiple failure mechanisms map into the failure mode. So, you know, corrosion of the stem is one way to get stem binding, but there's other ways to get stem binding.

The other thing is failure mechanisms can go into multiple failure modes. A bound stem is going to cause the valve to fail to open and fail to close.

So there is this mapping process between the mechanisms, and the modes and the modes to the effects.

The other issue is, depending on the level of detail, you change what your failure modes are. So you need to have that context of what level of detail in the system you're looking at to be able to understand what the modes actually mean. Because if you change the level of detail, you shift what you're talking about.

But this mapping remains. And that's one of the key features that Mauricio Gutierrez is going to talk about in, I think, our last presentation of the failure mode work that the Division of Engineering has done.

And although there's many different ways to define these failure modes, there is a mapping that exists between them which is reassuring. So it does add to the number of sets that are out there.

MEMBER BLEY: How far has that work gone now? Have you tried to put data in your boxes?

ME. SYDNOR: No. The research information letter, or the draft, when you reviewed it about a year ago, it has been published now.

MEMBER BLEY: Okay.

ME. SYDNOR: But it's the third in the series of research. The next one deals more with quantification. We'll talk about --

MEMBER BLEY: I suspect, when you start trying to apply it to data, it gets rearranged somewhat.

CHAIRMAN STETKAR: Well, I think, that's what I was going to mention, that this third sub-bullet under the first bullet is really important. I mean, we learned that with your valve example, that trying to, you would think, I mean, this again is the engineer versus the modeler versus the practitioner, you would think the data would be available at the smallest piece part.

Because, my God, you would know how resisters work. But the fact of the matter is often that's not the case. It's often that the best available information is at a higher level, because that's the level at which people actually fix things.

And my example, the guy who was modeling this system was appalled to know, to find out that people at plants could tell him how many cards they had taken out and thrown away. But they didn't know

what failure occurred on each card, you know, whether it was a resister, or an open circuit or something like that. Because they didn't care.

So you could have, you had pretty good failure data at the level of a card. But at a lower level, it became much, much, much more difficult to try to quantify things. And that's, I think, part of what Dennis is saying. When you try to marry the concept with the actual availability of information, you may find that you need to rethink things a little bit.

ME. COYNE: And I want to, just a real quick point. I meant to make this. So in a, and this will help with the next slide too, for a PRA, I wouldn't rule it out. But I doubt you're going to find many PRAs that have a basic event for corrosion of a valve stem.

You're going to find most PRAs have a basic event for a valve failed to open or a valve failed to close. That doesn't mean that, from the PRA perspective, we don't care about valve stem corrosion. That has to be, we have to assure ourselves that those failure modes are captured in the operating experience data we collect.

But from somebody doing a deterministic review of, you know, the material selection for that component, you know, the NRC still cares about that the material selection is appropriate for the valve stem. We may not see that level of detail in the PRA modeling, presuming that we're able to capture it with our operating experience data.

CHAIRMAN STETKAR: And it's important, though, going forward, Kevin. Because now that the PRA has identified and reasonably, I hate to use the term standardized, but kind of state of the practice is you have --

Thank you for silencing your little beefy devices.

Oh, sorry, a big beefy device. The -- I lost my whole train of thought here. No, it's important that now we've sort of developed this syntax of failure modes.

People going forward now compile data into those failure mode boxes. They still know the underlying causes. You know, it's important to know that 73 percent of valves failing to open may come from stem corrosion. It helps you to better design or maintain valves, for example.

But you don't have now people compiling data at 37 different levels that have different taxonomies associated with them. So it's important to establish those failure modes going forward so that, when people start to collect data, the data are compiled at the appropriate level and people understand what they're talking about.

MEMBER BLEY: But two, and I apologize for tautologies, but two tautologies, one is don't let the structure you've built force people to do things that don't make sense. And you see that way too often. I've got to put everything into one of these boxes. When you start looking at the data, this stuff doesn't fit, and you've got to rearrange it.

So it seems obvious, but all too often I've seen reports come out of well respected institutions. And when you go talk to them it's, well, we had to put it in one of these, because that's the structure we were given. And it just doesn't make sense.

And the other is going back to what John said. Forty years ago when we first started doing this stuff in the nuclear business, it had been done before in others, very often people do their first

modeling kind of copying things they've heard at the high level. And then they get these wonderful insights.

And they do go in and try to model corrosion and all these other things. And their second models turn out to be intractable, and they give up. So you may run into that. But that's a year, or two or five away.

ME. COYNE: I think we cover the highlights in this slide. And I realize in hindsight we should have given this probably more time --

CHAIRMAN STETKAR: We have a day and a half. And, you know, it's cold outside. What are you going to do this evening anyway?

(Laughter)

ME. COYNE: So today's presentation, it has been awhile since we talked to you on the PRA aspects of digital monitoring. It has been since 2011. And largely, it's because we wanted to come back when we had some substantial results to discuss with you and we had reached some level of fruition on the concept we talked about last time.

And I think we're at this point. So we do have a pretty full agenda. But we're going to have

presentations just to review the overarching framework for our digital I&C PRA research program. We'll talk about some recent results we've gotten from a statistical test method that we applied to an actual digital I&C system.

We've made some good progress on Bayesian Belief Network modeling for software. We have colleagues from South Korea here to also assist us in this. We've been having a very fruitful collaboration with Korea for many years now on the software reliability issue. It's been very beneficial to our program. I hope it's been beneficial to South Korea too. But they came in with a lot of knowledge and experience in this area.

We have PERI coming in to talk about digital system PRA, their failure modes work, failure prevention, mitigation and hazard analysis. I think, and I hope, that you'll see some common themes develop amongst the staff presentations and the PERI presentations. I think there's some good alignment between how we're viewing the problem and the modeling that we're doing.

And then finally, we'll wrap up with Mauricio, and then we'll talk about the failure modes

work that's been going on in DE. And I'm glad that Ming is listed with that, because that is a testament to the fact that we are talking more. And I do appreciate the ACRS forcing our hand on that a little bit more, to be a little more formal in our interaction between the groups. And that certainly helped us.

MEMBER BLEY: I didn't see one, but have you sketched out a graphic, or a flow chart or something that kind of ties all these pieces together, where we want to end up and how all these pieces fit together to reach those various goals at the end?

ME. COYNE: Ming has a picture that Alan Kuritzky first developed. And it's kind of --

MEMBER BLEY: A lot of it seems bottom up to me right now.

ME. COYNE: Well, I think it's actually Ming's first presentation, and he's going to talk about that.

MEMBER BLEY: Good. Okay.

ME. COYNE: So we'll see how that part goes. And then we can answer the questions from there. So some key messages. And I apologize for my typo on complimentary, although I think Russ does a

great job. We also --

(Laughter)

ME. COYNE: -- are more holistic in our views. So I think these are complimentary also, that we're working to the same end. It's just different aspects of the same problem.

So I think we are aligned. I hope we're able to communicate that, because I don't think we've done a good job communicating the alignment between our groups in the past. So we're hoping today and tomorrow will help with that.

And again, EPRI's doing a fine job here too, but I think you'll see that our work here is also complimentary. And I think all of us, Research, PRA, DE and PERI agree on the basic concepts. You're going to see some differences between how we view things, but I think that the big picture items, we do have agreement and alignment on the basic concepts. And there're some differences in focus, and intent and objectives that may highlight some differences in how we view certain things.

I apologize for running over a bit. But we'll do a switch here. And we'll bring Ming up to continue on.

CHAIRMAN STETKAR: Thank you. Anything else for Russ and Kevin?

ME. HECHT: Can I just ask one question? On the presentations on failure mode, is that going to cover RAO-1002?

ME. SYDNOR: It's not a total representation of that material. Because you heard most of it before. But it will discuss the changes we made to it based on comments, feedback.

MR. HECHT: Okay, thank you.

(Pause)

MR. LI: Good morning. This is Ming Li. Kevin, thank you for the introduction. I'm here today to provide an overview of the research on the digital I&C PRA. This digital I&C PRA research is formulated in the digital I&C research plan, and in particular in Section 3.1.6, the digital system PRA section.

The objective of this research are to identify and develop methods too in the reg guides to include the digital system failures into current NPP PRAs and ultimately to incorporate digital systems into NRC's risk-informed licensing and oversight activities.

In order to achieve these goals, this

research area identified, research area includes the failure mode identification, failure effect determination, the hardware components for the data support and the common cause failure modeling, the uncertainty modeling, the modeling of design features such as the self diagnostics, reconfiguration and the surveillance.

This digital I&C PRA study also supported by other research covered, for instance in Section 3.1.5, the analytical assessment of digital systems. This research is about to identify analyzed digital system failure modes and to discuss the feasibility that applies these failure modes to assess the safety impact of digital systems.

And this research, I mean, the digital I&C PRA research, also supported by the research covered under 3.4.5, operating experience analysis. So the operating experience analysis study is to analyze an operating experience of digital systems to identify credible failure modes and to establish data collection rules to assure that data collected are credible, are useful and are adequate.

Also operating experience analysis is to improve the efficiency and effectiveness of a

regulatory review using the data and the knowledge obtained through this research.

The key to include digital system failures in N.P. PRAs is to construct a probabilistic or reliability modeling of the digital system. Although the digital system hardware reliability has been well-established in theory and widely practiced in industry and other government agencies.

Whether software can fail or whether software reliability can be modeled, still in big arguments. Staff believe software can fail, software does fail. And software reliability can be modeled. Software fails due to their defects in software, and the use of the software triggers these defects. And the defects, by the way, I use the term defects and fault interchangeably in my presentation.

CHAIRMAN STETKAR: But, by the way, Ming, you also use the term fail. Software really doesn't fail. It does exactly what it's supposed to do. It doesn't --

MEMBER BROWN: What it's told to do.

CHAIRMAN STETKAR: Well, I'm sorry, what it's, you're right, excuse me. What it's told to do. It's not a failure, it does what it's told to do.

Occasionally that's not necessarily what it was supposed to do.

This is important because we talk these days about understanding human behavior. And humans very often don't fail. They do exactly what they thought was appropriate under the circumstances.

So these aren't really software failures. It's identifying the conditions where the software behavior is not what the designers or the users of the software expected it to do. That's not a failure, it's just what it does.

MR. LI: Well said. Here, just follow the definitions popular in the literature. So we define software failure here, a triggering of a defect of the software which result in occurrences to the whole system failing to accomplish the intended function or initiating an unwanted action.

CHAIRMAN STETKAR: But see, my point is that failure to accomplish the desired function is only one thing that the software might not do. It also might do other things which are not failures, it's just what it does. And if you focus on only not opening that valve, you're going to miss the other things that the software might do. Like it might open

the valve when you don't want it to open it.

MR. LI: Yeah, I agree.

CHAIRMAN STETKAR: That's the notion of focusing in on this notion of failure, because you then say failure to do what? Well, failure to open that valve. Because that's what I wanted it to do in my model for this particular event. And that's okay.

Under other conditions, it might open that valve when you didn't want it to, which also wasn't a failure. It was just an effect that was not what you wanted to occur at that time.

MEMBER BALLINGER: Even more so, by not opening the valve, it might do something else --

CHAIRMAN STETKAR: Well, no. That's --

MEMBER BALLINGER: -- completely unexpected --

CHAIRMAN STETKAR: -- that's, my point is that it's --

MEMBER BALLINGER: -- by not opening the valve.

CHAIRMAN STETKAR: -- for a given --

MEMBER BLEY: Just like people.

CHAIRMAN STETKAR: Just like people.

MEMBER BLEY: We've been fighting 20 years

to stop using human error. We haven't succeeded. We'll probably not succeed here either. But at least the concept you have in blue is the one, almost the one we would like. But it's still focused on failing to accomplish what the modeler wants it to do. The modeler needs to think of, well, you've got an unwanted action. So what's in blue is pretty good.

MEMBER BALLINGER: But this is a little more insidious actually. With human error, if somebody fails to do something, that's it.

MEMBER BLEY: No, I'm sorry.

MEMBER BALLINGER: No?

MEMBER BLEY: People don't fail to do, people do.

CHAIRMAN STETKAR: People do.

MEMBER BALLINGER: Okay. So people does something wrong --

MEMBER BLEY: Just the same.

MEMBER BALLINGER: It is the same?

CHAIRMAN STETKAR: It's exactly the same.

MEMBER BLEY: People do, and not always what you think they ought to do or might do.

CHAIRMAN STETKAR: What the designer of procedure thought that they might do because they

designed the procedure for a certain thing.

MEMBER SCHULTZ: They may do something different or additional.

CHAIRMAN STETKAR: You know, why did your grandmother drive the car through the window? Was that a human error or was she triggered by something that somebody didn't expect? Maybe it was a perfectly rational decision on her part.

MEMBER BALLINGER: But when my grandma drove through the window, she stopped. In this case the software might do something else.

MEMBER BLEY: So might your grandma.

MEMBER BALLINGER: Well, she might be dead.

CHAIRMAN STETKAR: No, I mean, there was something on the news the other day where a person actually drove in, backed up and drove in again. So it's, you know, I don't know what they were thinking. But apparently, you know, it made sense at the time.

MEMBER BALLINGER: I like the word corrosion, but that's as far as I got.

ME. HECHT: Can I suggest a framework here? And maybe I've struggled with this for about ten years before I came to the conclusion. Software

as it's used from the development context, from what people get paid to do, is a list of instructions.

You get source code. That gets compiled. So long as it's not running, it's never going to cause a failure. It only causes a failure when it's running and it's integrated on the hardware.

And so when one thinks about a failure, a software failure, what one is really thinking about is an event which happens in time. It's not a defect. It just happens, if you will, in space, or in text or something like that. But it is an integration of the hardware, the execution platform on which it's running and the instructions.

So when we use the term software failure, people get confused on that point. Because they do think of software as that list of instructions. And what I try to tell them is it's the function that's failing. And the function failure is due to a defect in the software if it's a digital I&C complement and it's not due to other circumstances.

But thinking about software in that context, of what it is at run time rather than what it is on paper, or what it is the NRC inspects, or what it is that a program manager pays for might be a

better way to think about it. So software has two manifestations, if you will, its static manifestation and its dynamic manifestation. And it fails in its dynamic manifestation.

CHAIRMAN STETKAR: But it doesn't fail. It does what it's instructed to do.

ME. HECHT: Well, it's a system, the system deviates from its requirements due to --

CHAIRMAN STETKAR: That's one way to think about it. Another way is it does what it's instructed to do. Sometimes that's what you want it to do, sometimes it's not what you want it to do. Our challenge is, in PRA, is to identify conditions that cause both.

MR. LI: Staff take a position that the failure is similar to Dr. Hecht=s. So the failure in terms of the function in software does not have a physical, you know, it's not a physical matter. So software is not break, not like a weld, not like a pipe.

But software execution is a logic series of the instruction. So that does produce some unintended function or produce some unwanted consequence to either downstream or sometimes even

upstream component. So that's what we mean by software failure, from the function perspective and not of a physical statement like broken. So that's not what staff means. So let me continue here.

ME. COYNE: Ming, just, Kevin Coyne from the research staff. A little more context on the definition in the blue box. Several years ago the ACRS had asked us to look at a specific issue about software failure. It was back when Alan Kuritzky was the main project manager for this. And we formed an expert panel of software experts to look at this.

The definition of software failure, I'd say, is not settled law across, you know, every practitioner in this area. And even that expert panel noted many of the things you're talking about. Software is deterministic in how it behaves.

But they felt that you could apply a failure definition like this. This is the definition that that group came up with. A different group of experts could come up with a different definition. But that's where this one came from.

I do want to note that we do include the unintended action as part of the failure. So the valves, firstly, opening would be, under this

definition, would be software failure.

But going back to the comment on the vocabulary, this is a case where we can get very tied up in the vocabulary, but we're all really talking about the same concepts we want to capture in the modeling.

CHAIRMAN STETKAR: And, Kevin, you're right. As Dennis mentioned, the blue box is, when viewed in that context, is what we're talking about. It's just that too many people too quickly start thinking of software failure in the same sense as a valve failing to open and software failure only in the context of not doing what we as modelers or we as designers intend it to do. So the blue box is right.

MR. LI: Let me --

MEMBER BROWN: Before you go on, I'm just going to milk this a little bit more, okay. It's not always a design issue that gets reflected in this. In other words, the code does what it's supposed to do. You step through the code, whatever the op code is, develop the ones and zeros. That's what goes out and that's what it does.

You can get bits flipped for other reasons. It can be compiled once, you can put it in,

it can be working just fine. You can come back a year and a half later and find a bit got flipped for some reason. And you now issue an instruction, because now it doesn't mean what it's supposed to. It locks the whole thing up. You don't know how that, now, is that a defect? Is that a failure?

CHAIRMAN STETKAR: It's like corrosion --

MEMBER BROWN: We get wrapped up in that level of detail. We've got to be careful because it's not --

CHAIRMAN STETKAR: It's like corrosion on a valve stem.

MEMBER BROWN: Yeah, exactly.

CHAIRMAN STETKAR: That's one thing that can cause the thing to not behave --

MEMBER BROWN: But it's not a design issue.

CHAIRMAN STETKAR: -- as you expected.

MEMBER BROWN: That's all I'm saying. And you can't fix that by getting a better material that, it's an external influence. It could be noise, it could be gamma rays. I mean, we've found bits get flipped and the memory of the stuff. Now, does it happen all the time? No. It doesn't happen all the

time.

MEMBER BLEY: And more up there than down here.

MEMBER BROWN: Exactly. But, I mean, there are circumstances. And that's a relaying from personal experience, where we actually found some of the compiled code got, for some reason, we never knew what the exact reason was, but we found we had to recompile and redo some stuff occasionally just to reinitiate, re-baseline it, I guess, would be a better terminology.

Anyway, I just wanted to make that distinction. Be careful how you design. It's not always design, there can be other external causes that the code gets corrupted.

MEMBER BLEY: And there can be random errors in the coding that don't show up in your testing until --

MEMBER BROWN: You can compile it and come up with errors and not know it.

CHAIRMAN STETKAR: But that, again, comes back to the analogy of a bolt not quite torque right or corrosion --

MEMBER BROWN: Exactly. I don't disagree

with you.

CHAIRMAN STETKAR: You know, it's in many cases we don't care about it at that level of detail. We care about how frequently does the undesired behavior manifest itself. Can we identify what the undesired behavior is?

MEMBER BROWN: Exactly.

CHAIRMAN STETKAR: And how frequently does it, if you want to dig down into the causes, that's fine.

MEMBER BROWN: That's why I was trying to bring other point up. Because I wanted to accomplish the same goal you have. I don't want to get down to that level. I think that's not the right place to go.

MR. LI: Before I go ahead, can I add something to that? We're talking about, to me we're talking about the interaction between the hardware and the software. You are talking about an event where similar things offset.

So some relation called a single bit flip, flop, and then crash the entire system. So this is because of hardware failures integrating the software execution. And I agree with you, this is not a design error. This is a random hardware failure.

MEMBER BROWN: If a bit flips, that's a hardware failure, necessarily, due to the, you know, interference?

ME. HECHT: It's a transient hardware failure.

(Simultaneous speaking)

CHAIRMAN STETKAR: Hold on, hold on.

MEMBER BROWN: It can be a hardware failure, it could not be a hardware failure. It could be an external event that causes the bit to flip.

CHAIRMAN STETKAR: This is good discussion. But we've already established that the hardware and the software are integrated. And I don't particularly care if one camp wants to call it a hardware failure and the other camp wants to call it a software failure. I care that this behavior occurs at some frequency --

MEMBER BROWN: I agree.

CHAIRMAN STETKAR: -- from my box.

MEMBER BROWN: I agree.

CHAIRMAN STETKAR: Okay. So that's why I want to stop this discussion about one camp might call it a hardware, one might call it a software. I might call it corrosion. Somebody else might say I don't

know anything about materials, and I ought to call it something else.

MEMBER BROWN: I just want to end it on your thought process not on some other more detailed level thought process. That's all.

CHAIRMAN STETKAR: Yeah, thanks.

MEMBER BROWN: All right.

MR. LI: I just brought that up because that's related to the failure, you know, mechanism of the digital system. So let me continue here.

PARTICIPANT: Sorry.

MR. LI: Defects, software defect includes the requirement defect. And the manifestations of the developer and the user, mistakes made if you're in the software development life cycle. And the software defects, in nature, if that static and deterministic software fails because there're defects, First, there're defect in the software.

And second, the use of the software triggers this defect. And this failure mechanism is actually deterministic also. So by that I mean if we can repeat the same input, and if we can repeat the same execution environment, then we are definitely sure that we can repeat the same failure.

And that execution environment includes any input from the human beings, any hardware input, sensor, from sensors, and even the memory leaks accumulated during the long term execution process.

So if we can repeat everything, then we can repeat the failures. So from that perspective, the software failure mechanism is deterministic. But this software use, which we call operational profile, is probabilistic.

So from that perspective, we can claim that the use of the software which is probabilistic modulates the failure mechanism. So the failure, software failure, behaves probabilistically. So that's a staff position that it's reasonable to model software probabilistically because of that.

Modeling software, modeling digital system reliability, and in particular modeling software reliability, entails great challenges. Because, as I mentioned, software fails because there're defects. And the use of the defect triggers those, the user of the software, I'm sorry, triggers the defects.

So think about the estimate of the defects, the number of defects, location of the defects, and the different types of the defects and

providing the user of the software, they're all big challenges.

There are no agreement now even in academia, industry practice, there are no agreement. There are many methods, there are many models try to resolve this issue. But there are no agreement.

And furthermore, all the software defects are commonly, they're design errors. And the PRA are not good as, we did not have a logic appearance to model design errors in PRAs. And also, the development --

MEMBER BROWN: Well, your first state -- we don't have a lot of experiences of design errors, it's really experience modeling. You stuck a different word in there, another word in there when you said that.

Because I would have said we have a lot of experience finding design errors when you go see it yourself in a test room. That's what you do initially when you try to run the system. Run the system, and you find the stuff you have to fix --

MR. LI: Right.

MEMBER BROWN: -- gradually decreases to a --

MR. LI: But not model that in PRA context.

MEMBER BROWN: Yeah, okay.

MR. LI: Yes. That's what I mean. Thanks. Also, another big factor needs to be considered is big development and changes. If we think about ten or 20 years ago, the common practice to design digital system is to use a general purpose CPU. And you'll see language to design the digital system.

Now things all changed. For example, AREVA start using, I call it the fourth generation language to design their TELEPORT system. And some vendors I heard, and I saw some presentations, they started designing the old S.G.-based system.

So those designs, I call the variabilities, makes the modeling process more difficult and more challenging. And we also, this committee already brought up at what level the modeling needs to be. And also the data to support this modeling process, there're also big challenges.

So staff believe that modeling digital system in PRA is possible. Now, it's a matter of whether it's practical and useful to the regulatory

review activity.

This chart overviews the digital studies. And in the past, NRC sponsored a number of research on this area that were summarized in this NUREG report. And this research, supported by the MOU, between NRC, EPRI, NRC and NASA and also supported by international collaboration from OECD and also from South Korea, KAERI.

The ongoing research, the so-called Statistical Testing Method and Bayesian Belief Network and also area such as the dependency and common cause failures, system design features, modeling, and a human reliability analysis and a revised PRA framework are identified as a future research. Those research are also supported by the Division of Engineering study, such as the failure mode analysis and all operating experience analysis.

CHAIRMAN STETKAR: Ming, go back to that. This is a picture, and I guess my ultimate objective would be to write a regulatory guide. This would show how I might pile up a bunch of reports, and read through them and eventually write a regulatory guide.

It really doesn't tell me how the research is supporting the real objective of developing

coherent, practical models for digital I&C systems. Could you expand on that a little more?

MR. LI: Sure. As Mr. Chairman mentioned, the ultimate goal of the research program is to establish reg guides which can help the regulatory review process.

And in order to achieve that, we have to come up with, we call them final reliability and risk modeling of the digital systems. And we identified that there are challenges there. And the ongoing research and the future research are devoted to achieve that goal, to come up with the final reliability and risk modeling.

And the areas to achieve that goal for the final reliability and risk modeling include the fault reliability modeling which the ongoing work, the ongoing research about. We're not seeing that the STM and the BBN going to be the answer. But those are the two possible methods we are trying.

CHAIRMAN STETKAR: I guess what I'm struggling with is that I see a lot of arrows pointing into this blue box and a lot of bullets. But they don't seem to be, they don't seem to be really organized at all. In other words, a process by which

you have kind of a concept of how you get to that final goal, it just seems to be, well, we have a lot of people doing a lot of research.

And miraculously, it's all going to come together, and we're going to have a model at the end. And then we're going to tell people how we did it or how you ought to do it.

So I think what Dennis was looking for, and I don't want to put words in his mouth when he's not here, but was a better, some more detail in that middle part there that says, well, we want to identify, you know, what are the basic things that we need to identify to build this? And how are each of these elements of the research programs feeding into those fundamental things that we want to identify, rather than, yeah, obviously we want to identify the end goal of modeling. But that's too broad.

And the inputs are diverse, but I don't understand how they're working together to achieve that. So that's sort of, you know, the genesis of my comment.

MEMBER SCHULTZ: The way this is depicted is, well, is that you have an end point out somewhere in the future that is the regulatory guidance. And

given all of the input and all of the machinations inside the blue box, I'm afraid that's way out there.

CHAIRMAN STETKAR: Well, yeah, and if we had a better structure to say where are we on this basic element right now?

MEMBER SCHULTZ: Right. So what happens inside the blue box is really, I think, what Dennis was interested in achieving. What are the interconnections, what are the feedback --

MEMBER BLEY: And what are the goals?

MEMBER SCHULTZ: -- elements that would be important, and what are the intermediate goals that is going to lead to the reliability and risk modeling and then the regulatory guidance? And is that one product? I don't think it is. I think it's intended to be an active and developing program.

CHAIRMAN STETKAR: And something you mentioned, you know, you said, well, maybe the Bayesian Belief Network approach will not be the final way to support the quantification. Well, okay, quantification is one of those elements, you know, the availability of information. I won't call it data necessarily, information to support quantification is one of those interior elements.

But that's not in isolation. That's also directly integrated with developing, I'll call it failure modes for the time being, for the modeling framework. And if we had that, you could then say, well, where are we in the Bayesian, do we have confidence that the Bayesian Belief approach is going to achieve what we need to do in the context of these other elements?

And if the answer is, well, no, maybe another approach seems to be better at the moment. That's important information to guide both these kind of presentations so we understand better what's happening and to guide kind of resource allocation for future research.

But as Steve said, with some sort of, you know, is that regulatory guidance 2015? Probably not. Is it 2016? I'd hope so. Is it 2040? I mean, if it is, fine. I don't need to worry about it. I'm not going to be here.

ME. COYNE: Kevin Coyne from the staff. It's a good comment. And, you know, as I was looking at it in light of Dennis' question, this really shows the other influences and interfaces with other groups. It doesn't really show the art. So that's a point

well taken.

And actually, the comment comes at a really good time, because as Russ mentioned, we are updating the digital I&C research plan. And I should have stated it earlier. The timing of this meeting is perfect. Because this gives us good feedback in how to better show this in the plan.

Just as a reminder though, we were on a development arc here that we started with hardware modeling. So D&L had done a good project using a feedwater control system to do the hardware modeling.

We made some broad assumptions about software. We didn't try to model it. That was a fairly successful project. We used surrogate data. We didn't use the, you know, the actual data. We just used representative data from, I guess, the MIL standard is where we got it from.

But we had some confidence we could develop tools and techniques to model the hardware associated with, at least, the feedwater control system. And then we had a belief that a safety system, a demand actuation system would be more straightforward to model than the control system.

Once we had that done, and that was some

of these earlier NUREGs that Ming had mentioned like, I think, 6901, and 6962 and 6997 had talked about some of this earlier work, we tabled the hardware to focus on the software.

And so the more recent effort has been looking at quantitative software reliability methods. There's many out there. We tried to bend them. And we'll talk about that in the next presentation of potential methods to explore further.

It's not one is better than the other. It's just ones that we thought would have some benefit to us. And so we decided to pursue the statistical testing and BBN approaches. Ultimately this will fall back into the hardware and try to bring it back together. And we need to show that better --

CHAIRMAN STETKAR: But a bit of the structure, as we were mentioning earlier, if you think of not necessarily the hardware and the software as two distinct absolutely square black boxes, if you think of it as an integrated system of hardware and software that produces a desired or undesired effect, and that the models need to account for it at that level, that might be a different way of thinking and structuring the research, rather than saying, well,

let's focus, you know, we've checked off the box.

We understand how to model hardware. And now let's focus a lot of effort on software and then suddenly find out that, well, these are not parallel and distinct paths that indeed it's all part of the same problem. And, you know, that type of thought process may help a little bit.

ME. HECHT: Can I offer possibly a clarifying thought or maybe a distracting thought? What you have there, I think, is enough to help you estimate parameters. But is it direct, from what I hear, particularly when I heard about you describing the hardware model into the feedwater control system?

Would it be correct to say that right now what's missing is the modeling methodology for how you would take that, those parameter estimates or that information that you got from the bottom, and then put that into a combined, integrated hardware/software model? Is that a good restatement of --

MR. LI: I personally believe yes and no. So we have channeled it from both the modeling techniques and the data collection. As we mentioned earlier, we don't have taxonomy yet. So we don't have a lot meaningful data to use to estimate the

parameters.

And also, from the modeling perspective, some of the failure mechanism like hardware/software interaction, common cause and those type of design features, first of all, I don't see any clear description, explanation on those interactions and what exactly the issue is. I don't see any of the clear, let's say, technician from that perspective.

And there are no good research, there are no credible without, out in the literature. So that's from the modeling perspective. So to me, there's still a long way to march to --

CHAIRMAN STETKAR: We need to move on and keep in with the schedule. I'll just make a comment. That's a traditional, bottom up, detailed oriented approach to life. And I'm challenging you to not take that approach to life, okay.

I'm challenging to think more like a modeler and say what do we need to achieve a reasonable model for the integrated hardware and software. And you may find out that there's better information available and better techniques than trying to build everything out of fundamental piece parts and hope that it comes together at the end.

MR. LI: Okay. All right. That's a -- go ahead. I'll quickly go through the previous research hardware or system reliability modeling.

A joint effort conducted by Ohio State University, ASCA, University of Virginia, they surveyed a series of reliability modeling methods and came up with two methods, Markov chain, and the dynamic flow graph methodologies.

And they applied those two methods to a digital feedwater control system. And the BNL did something similar but using failure mode and an effect analysis method applied to the same digital feedwater control system.

From the fault reliability modeling perspective, the University of Maryland research team came up with so-called metrics-based studies. So this work basically ranked over 40 software metrics in terms of their capability of estimating software reliability. And they selected 12 of them and constructed models to link the metrics to the number of defects remaining in the software. And --

MEMBER BLEY: Is that the Carol Smidts report?

MR. LI: I'm sorry?

MEMBER BLEY: Is that one Carol Smidts --

MR. LI: Yeah, Carol Smidts.

MEMBER BLEY: Okay.

MR. LI: And then they convert the number of defects remaining in the software to the failure probability using the Finite State of Machine simulation method. And also they embedded the original profile in that simulation.

BNL conducted an expert panel on software reliability and came up with a conclusion that software does fail, and software reliability could be modeled. And they are continuing in the survey as a software reliability methods.

And they pick up two of them, Bayesian Belief Network and the Statistical Testing Methods to estimate software reliability, apply them to example systems which are the HR loop operating control system. I'll discuss that later in my next presentation. The international --

MEMBER BROWN: I was going to ask, but you're saying you're going to cover results of these at some application --

MR. LI: Yes, yes.

MEMBER BROWN: But your results from

looking at that --

MR. LI: Right. So we are going to cover STM and the BBN.

MEMBER BROWN: Okay.

MR. LI: I'm going to talk about the NUREG/CR-7044.

MEMBER BROWN: Okay. Thank you.

MR. LI: Thank you. International collaboration from OECD and from bilateral agreement from South Korea also supports this research effort.

OECD identified the need to model digital I&C PRA model digital system in PRA. And they started two initiatives. One, failure mode taxonomy, and another one database, the data collection effort which called COMPSIS.

Later, I'm going to talk about the fenimal taxonomy work and present the results. South Korea provide a large technical support for the STM and especially for the BBN. So the two ongoing research projects are Statistical Testing Method and the BBN, Bayesian Belief Network.

Statistical Testing Method use the PRA and existing PRA to define the operational profile, as I mentioned, the software failure probability, the

function of the software use.

So in order to model software failure in the PRA sequence, the test cases need to reflect the use of the software which defined by the PRA sequence. And the BNL takes the PRA and extracts the COMPSIS, which represents the plant conditions, and use that to define the thermal hydraulic boundary conditions, then generate test cases through the thermal hydraulic stimulation, then deliver those to Idaho National Lab.

And INL did the actual testing on the real hardware and the software combination. And the BBN is coming from a different route. BBN tried to link, build up a covert relationship from the software development process and software product characteristics, which we called attributes in this case, link those attributes to the number of defects remaining in the software and then convert those number of defects to the failure probability or probability per demands. Dr. Chu of BNL is going to go through those two research in detail.

So in the near future, we're going to publish the STM results in the NUREG report. And BNL is going to complete the BBN research and publish the result in another NUREG report.

And the staff is going to collect all the feedback from committee and then update the digital I&C research plan to reflect the next phase of the work. And this concludes my first presentation. Any questions?

MEMBER REMPE: So if I go back to Figure 7 and where you're at right now, you're in the additional research portion on this?

MR. LI: Yeah, the ongoing. Yes.

MEMBER REMPE: And do you envision you're going to have, it says final reliability and risk modeling, you're going to have recommendations for the best practices for a model and things like that? Or are you going to have -- you're not going to have just a, because there're so many different applications, one type of model, those have recommendations for modeling, and then there'll be regulatory guidance for the modeling, is what you're going to issue?

MR. LI: Yes.

MEMBER REMPE: Okay.

MR. LI: We're going to summarize all the lessons learned, pros and cons for each approach, then it's up the later phase to pick up the right one they feel comfortable.

MEMBER REMPE: Okay. And I know Steve mentioned time frames. Do you have an idea of how much longer? Not really?

MR. LI: No.

(Off microphone discussion)

CHAIRMAN STETKAR: I thought there might be somebody on the side who would want to say something.

(Off microphone discussion)

MR. THOMAS: These are all very good comments. And in fact, this is a great slide that puts together a number of things that we're doing in different venues.

But we still have not embarked upon an effort to lay out a better plan, you know, that goes further, meaning a plan that establishes, as you were saying, a top down approach, looks at what are our ultimate goals, what are our objectives and then what are the things that we need? And how do all of these pieces come together to feed into our recommendations to the regulatory program office?

Do you see that box that says final reliability and risk modeling? That's more of a set of recommendations of best practices that would then

be provided to the program office. And it would be incumbent upon the program office to then look at that to see, you know, what could they decipher from that in terms of acceptance criteria that would be used to provide guidance to the licensees and to the staff?

So, you know, I really like it, there's a lot of work to be done. And these are why questions are being asked of the staff in many areas at this point in time.

CHAIRMAN STETKAR: Brian, when you think about that, and again, it's not our role here. Certainly, you know, this is only a subcommittee meeting. I have to always emphasize that so you're hearing individual opinions from individual members. And we don't, even as a committee, get involved, except when we review the research plans at that level.

One of the things I think is important here is to look at that goal. But somewhere between the white box that says final reliability and risk modeling and the white box that's hanging out on the end that says regulatory guidance, there really needs to be a process of, whatever you come up with, there needs to be a realistic piloting of those methods.

And you will find that they're not going to work perfectly. And not piloting on a simple digital feedwater control system, piloting on a real plant, you know, and looking at it.

This is the lesson that we learned from NUREG/CR-6850 on the fire analysis and that we're learning on other things, is that it's not a simple transition from that box that says final reliability and risk modeling to regulatory guidance.

There's going to be iteration in there. And you need to plan for that, which if you do indeed have, you know, a date associated with that regulatory guidance within plus or minus a year or so, you need to back all of that out. That's really important. Because otherwise, you're never going to get there.

MR. COYNE: And this harkens back to Ming's earlier slide that we're still determining whether it's going to be practical or useful to apply any of these techniques.

So it's, well, I think the no for the final date was the accurate answer. It may leave it a little too open ended. We are diligently working on an active track here to solve those questions.

CHAIRMAN STETKAR: My personal opinion --

ME. COYNE: I couldn't give you a day right now when that would happen.

CHAIRMAN STETKAR: Okay. That's, I realize you guys are working on that. But my personal opinion, is it practical? Yes. Is it useful? Absolutely. That's my own personal opinion. I don't understand why it would not be useful to understand how these things might get you into trouble in a power plant under conditions that you didn't expect.

MEMBER BLEY: Yeah, that bothered me too. Even if you have trouble getting to a quantification that you find meaningful, just the understanding that you develop along the way puts us miles ahead of where we are already.

CHAIRMAN STETKAR: Remember, we didn't know about reactor coolant pump seal LOCAs until we asked those questions in the earliest PRAs. We didn't know about them.

MEMBER BLEY: They weren't on anybody's radar. Nobody'd ever talked about them.

CHAIRMAN STETKAR: Now they're suddenly, everybody knows that reactor coolant pump seal LOCAs are really important contributors to risk on pressurized water reactors.

ME. COYNE: So one of our big challenges right now, not to take up too much time here, is finding an example system was extraordinarily difficult for us because of the proprietary nature of these systems.

So getting software life cycle development information so that you could crunch it through a reliability model, getting actual data is very difficult because of the proprietary barriers that we have to face in this area. That could change over time. But that is a very large obstacle for us to practically build a reliability model right now.

MEMBER BLEY: One thing, I'm not sure it'll be helpful at all to you, but you might want to look at. Idaho, for many years, has been doing some reliability studies that have a whole series of reports. I think they looked at digital I&C.

They also were maintaining a common cause models and database. And I know those had gathered a fair amount of failure data on cards and digital I&C systems. You might look at those and see if there's something there that you're not aware of.

MR. LI: They are all hardware data, right?

MEMBER BLEY: They're linked to hardware. This card failed. But when you dig in, you find out why the card failed. And they did some of that. So I think it's worth taking a look at what they were able to find. Because they went back to maintenance records out of the plants to do that.

So yeah, definitely they're linked to hardware. But as we said earlier, you know, that's what we really care, is when these problems lead to failures somewhere that manifest itself in hardware. So it gets linked to hardware. But it tracks back.

ME. COYNE: All right, thanks.

MEMBER BLEY: It's worth a look. I don't know if it's worth a lot of time, but it's worth a look.

ME. COYNE: Thanks.

MR. LI: I just want a clarification here. By practical and useful mean that how much effort need to put to model the system and whether it is worth it to proceed. So for instance, the BBN work, we heavily rely on the expert opinion. And the size of the model could be huge and amount of data could be accessible. So that's what we mean by practical or useful.

CHAIRMAN STETKAR: My analogy for the poor guy who spent nine months, I didn't mention that, of his life developing the model that was so big it couldn't be solved, we now know that you ought not to do that. We don't need to learn that lesson again.

MEMBER BLEY: I think we've learned it many times.

CHAIRMAN STETKAR: And we've learned it many times.

MEMBER BLEY: If you look back at WASH-1400, the largest systems analysis chapter in the whole PRA was the section on containment isolation, by far. We don't do that anymore.

CHAIRMAN STETKAR: Anything else for me, at least on this topic? Because I think we all need it, I'm going to call for a break now so that we don't have to break into the next presentation. So let's recess until 10:15.

(Whereupon, the above-entitled matter went off the record at 10:01 a.m. and resumed at 10:17 a.m.)

CHAIRMAN STETKAR: We are back in session. And I've been alerted to the fact that apparently the agenda that was printed out, and is available in the

back of the room is not the agenda that we're going to follow.

So, let me just, for the record, and for the folks who might be listening in on the bridge line, go through the agenda, just so we're sure about the order of the topics. Right now we're going to hear about the overview of the Bayesian Belief Networks.

We're going to break for lunch. We're then going to hear about the statistical testing approach from the staff. We'll hear about the OECD/NEA work. After the break this afternoon EPRI will come up. We'll hear about digital system failure modes, and modeling of digital systems in PRA. And that will end today's session.

And then tomorrow morning we'll pick up with EPRI again, on techniques for failure prevention. And the final two presentations will be EPRI on the hazard analysis methodology. And then finally, the staff coming up and update on digital system failure modes. So, I hope we're now all oriented in terms of the agenda.

We do indeed have the folks up front who are prepared to talk about the Bayesian Belief

Network. And I believe that all of our slides are in the order that I just laid out. So if, with that, and I apologize for the confusion, it happens, the good news is, it's a subcommittee meeting, and we are flexible in subcommittee. So, with that I'll turn it over to, I don't know, Ming.

MR. LI: Mr. Chairman, we're now at Session Number 4, which is not the BBN. So, I'm okay to skip with Number 4 and go to Number 5.

CHAIRMAN STETKAR: Okay.

MEMBER BROWN: Okay. You're going to pass the Insights? You're going to skip this?

MR. LI: It's up to the subcommittee.

CHAIRMAN STETKAR: We'll pick this up after the Bayesian Belief.

MEMBER BROWN: Okay.

CHAIRMAN STETKAR: Or maybe, there's a method --

MEMBER BROWN: Oh, sure. And I noticed --

CHAIRMAN STETKAR: There's a method here. I'm trying to establish context and input to the context for both the staff and EPRI. And that's the way the --

MEMBER BROWN: I'm just --

CHAIRMAN STETKAR: And that's the way that that agenda was laid out.

MEMBER BROWN: I just felt that the new agenda we got had the insights and results now, and then the Bayesian Belief.

CHAIRMAN STETKAR: That's right. The new --

MEMBER BLEY: Adapt.

CHAIRMAN STETKAR: Adapt. We're going to -- let me put it this way. I'm the Chairman. We're going to talk about Bayesian Belief Networks now. Make sure that the folks up front are ready to do that. Find it in your slides.

MEMBER BROWN: I got it.

CHAIRMAN STETKAR: Got it?

MEMBER POWERS: He's using his command voice, Charlie. Look at it that way.

CHAIRMAN STETKAR: No. You don't want to hear the command voice.

MEMBER BROWN: Probabilistic approach to running a meeting, right?

CHAIRMAN STETKAR: This is not a probabilistic --

MEMBER BROWN: We'll probabilistically do

this, or maybe we'll probabilistically do that. But we don't have a Bayesian or systemic or --

CHAIRMAN STETKAR: Charlie, you don't know whether this is --

MEMBER BROWN: -- statistical blah, blah, whatever it is. And just wake me when you're ready.

CHAIRMAN STETKAR: It's 10:20 a.m., Bayesian Belief Network team, start speaking.

MR. CHU: I'm Louis Chu, Brookhaven National Laboratory. I'm presenting the status of the progress we made on developing this Bayesian Belief Network model for quantifying software reliability, or software failure probability.

This project is done in collaboration with KAERI. And I have two gentlemen from KAERI sitting with me, Dr. Kang and Dr. Lee. And Athi recently announced that he's working with me on the digital projects.

First I'll give some objectives and background. And the second bullet is the key subject. I try to explain how we developed this BBN model for estimating software failure probability. And that's a big bullet. I have quite a few slides that go into more detail.

And then I'll try to talk about the issues, limitations, kind of the difficulty we encountered. And talk about how uncertainty consideration comes into play in our model. And the project status.

The objectives are simple. Basically we want to develop a BBN model for quantifying software failure probability of safety-critical systems. I think that's a subject that we just debate among ourselves a little bit, that is, I guess it's obvious we want to develop a model for safety-critical systems, because that's what NRC is interested in.

CHAIRMAN STETKAR: Louis, what's a safety-critical system?

MR. CHU: I guess I tried to use, I assume there's a more generic term, instead of the safety related system.

CHAIRMAN STETKAR: Okay.

MR. CHU: I guess in NRC framework. Because we work with some expert who are not grouped here. And safety-critical may be more meaningful to them. I guess could not use --

CHAIRMAN STETKAR: Okay.

MR. CHU: -- safety related. And we want

to develop such a model for safety-critical system, and apply it to example system. And the example system is the new operating control system of the advance test reactor.

That is, we have two projects. One on BBN, the other on status of testing. In both project we're using the explicit, this loop 2A of the ATR as our example system. As Kevin earlier point out, you know, we had a hard time finding that example system. And we certainly appreciate that Idaho National Lab was willing to help.

In the case of this project, the BBN project, INL provide information about the system, about the next project you'll hear about statistical testing, INL now actually collaborating with us in performing this testing.

And the intent of the BBN model is that we use the BBN model to evaluate the quality of software development. And using that quality then valuation can come up with a prior distribution for probability of software failure. And this distribution can be further updated using the test data that we get from statistical testing.

This slide is, it's just a background of

the BBN theory. I probably don't want, I don't know. I'll try to go through it. It's the, it gives you some basic theory of BBN. It's a probabilistic graphical model depicting a set or random variables and relationship.

A basic assumption of BBN model is that it has a structure. What comes with that structure is the conditional independence of some truth. And also, the root nodes of the basic network are supposed to be independent. So these are kind of basic assumptions of the BBN model.

The third bullet shows how the joint distribution of the random variables modeled by the BBN model can be expressed. It's a part of a lot of the conditional probabilities. And in the BBN model the relationship between the random variables are expressed using conditional probabilities.

As given Variable A, what is the distribution of then the Variable B? And the Node Probability Table represents that relationship. And one thing I want to point out is that Bayesian Belief Network is a math model. And it is a quantitative model. That's what makes it difficult in a sense.

You can positively say there is some

relationship. But the BBN require you to put that relationship in a quantitative form, while in our project, no. There's an issue of how much data you have to quantitatively represent that information.

And then, we developed this model for supposedly the class of safety related systems. Therefore, in developing such a model we used data from safety-critical and safety related systems.

When we applied this model to a certain software, like the mock system at ATR that we need to collect specific data from, this system to evaluate the quality of its development. And in addition, we tried to collect data, you know, the number of bugs detected in the development process. And these go into the BBN model.

We used basing updating to come up with the specific failure probability for the software. This is a slide, a simple example showing the relationship between a cloudiness when our sprinkler is on. Whether or not it is raining, and whether or not the grass is wet.

So these tables show us the conditional probability of one node state as a function of the state of its parent node. You can see this, I guess

qualitatively you can easily say, if its quality is more likely that it would rain, and if the grass is wet, it may be caused by the rain.

So it is this model trying to express that kind of relationship. You see the nice long numbers. I think they are probably just, someone made it up to illustrate it as an example. But in the real application you need to look at the applicability of the model.

Say one collect data from New York to fill this model. And in say, Southern California, that never rains. Then this model may not be applicable to it. In an extreme case when you want to use model data, some places that don't use sprinklers. And the structure itself may not be right.

So when we develop model we're to keep that in mind, what is the applicability of the model in which we are supposed to collect data, gather information to build a model based on the scope of the intended application of the model.

MEMBER BLEY: So, since you drew that picture, illustrated by truth tables, can you quickly tell us what the advantage is of using a Bayesian Belief Network, as opposed to a set of truth tables?

MR. CHU: I guess this is a model. And then, say you're interested in if it rained. And someone tells you the grass is wet. So the grass is wet is an evidence. You put that into the model. You get a updated probability on the rain. I guess in this particular case it relates that given the grass is wet there's a higher chance it rained.

MEMBER BLEY: Okay.

MEMBER POWERS: You distinguish between the truth table and exact values the way these do in a truth table that edits distributions?

MEMBER BROWN: I didn't hear that.

MEMBER POWERS: He's asking what relative advantage of the network over a, just a set of truth tables. And to my mind the Belief Network allows me to take those nodes and make them distributions, rather than exact values fairly easily.

But I was wondering if Dennis distinguished between these two. I mean, you might say a truth table could have a distribution as well as an exact value.

MEMBER BLEY: You might. I've never seen anybody do that.

MEMBER POWERS: I've never seen anybody do

that either. But the network, the advantage there is, rather than say, if it's cloudy it's raining with a probability of .5, I can say, it's cloudy, but therefore the variance in my distribution is narrower by X amount, and the mean is shifted as well.

MEMBER BLEY: I'm not sure that you can do that.

MEMBER POWERS: And I can make it fairly complicated with the network. Whereas, with truth tables, you know, it gets hard to write it all out. But the network I could make those transitions just as complicated as I want to make them. In particular, I can use expert opinion, and a bunch of experts to do that in a network very easily.

MR. CHU: In that simple example it has only two states. So you have more states --

MEMBER BROWN: That you can make instead of a truth table. It can be a multi-dimensional matrix.

MR. CHU: Right, right. When you have too many states for the nodes, that's the complexity issue that arises.

MEMBER BROWN: So what, this could be really wet, or it could be a little bit wet?

MR. CHU: In that sense you can --

MEMBER BROWN: I'm just trying to relate to your comment --

MR. CHU: Right.

MEMBER BROWN: -- about the --

MR. CHU: You can define --

MEMBER BROWN: -- complexity of the node.

MR. CHU: Right. You can define finer.

MEMBER BROWN: Okay. All right. I just --

MR. CHU: Right.

MEMBER BROWN: I understand what you're saying. Well, I vaguely understand what you're saying.

MR. CHU: Right. And this slide is kind of some background on using BBN method to assess software reliability. It shows some of the early work that people used BBN. Johnson, who is Gary Johnson of Lawrence Livermore Lab, I think they have a team of people working for NRC for quite some time.

But that was awhile ago. In his report he pointed out BBN is potential method. But he didn't really fully develop it. And Littlewood also had suggested BBN be used, and later he further explored

its application to software. And then he became somewhat negative.

He was our consultant for the project. So he mentioned the concern of the complexity of the model. In addition, he has a paper that shows somehow you can get counter-intuitive results. It's somewhat like, you do more tests with no failure in his example.

You do more tests with no failure, you tend to think that shows the system is reliable. But then somehow the model shows you miscounted it. But that be right model. And he tried to come up with possible explanation, like, you know, assumptions that went into the model.

MEMBER BLEY: I'd be interested in seeing that. Is that the paper listed here?

MR. CHU: Not this one. Not this one. I can give you --

MEMBER BLEY: If you can. Because that doesn't make any sense to me. So I'd like to see what he's talking about. And somebody could --

MR. CHU: It is actually probably in that NUREG CR 7044. That mainly was supposed to have been sent before this presentation. I'm pretty sure that's

one of the references, that NUREG CR 7044. The next bullet, Gran, as a part of the Halden reactor project developed a BBN model.

I think they used the standard DO 170C, which is a avionics standard to evaluate the quality of software. And then in that project they actually used expert to directly estimate software failure probability.

It's somewhat like in a general sense, given good quality, quality level 3. What do you think the failure cause that it is? So it's a table that he came up with.

(Off microphone comments)

MR. HECHT: Just a point of information on DO 178. The levels of software assurance going from Levels A through E correspond to hardware failure probabilities that the FAA established for, well, for hardware in a directive that they call 25.1309.

So the point is that Level A corresponds to the catastrophic event. And that's ten to the minus nine for flight hour. Level B corresponds to the hazardous event, which is ten to the minus seven for a flight hour.

And the point is, is that the assertion

was made without any empirical evidence that if you did all of the objectives that were stated, all the 66 process objectives that were stated in the DO 178B, that your software was good enough to be Level A. And then there were a couple less for Level B. And about ten less for Level C, and so on.

So, the, I assume that the conditional probabilities that they got for that software were based on the mapping that the FAA made between levels of assurance.

MR. CHU: No, no. I made up my example. When I say quality I have, and I said Level 3, and made that up as no direct connection to what you said. What I have in mind is, within their modeling they have different type of quality, which have no direct connection to what's in the standard. I was speaking in general term, you know, given you are of certain quality level, then what is the failure probability.

Actually, their table of failure probability is more complicated than that. There are some three, four measures that -- And each one has different levels. These are different levels. And given any combination of those levels the X will come up with some figure of probability. It has no direct,

as far as I know, it has no direct connection.

Plus, actually coming up with numbers you, it's hard to map from one to the other. And I also echo your concern, you know, to come up with numbers there's really no strong basis. But that's the basic difficulty that you're facing.

And as you will see in our, later in the presentation, we had suggest we factor in, calibrate our model. From that we can come up with reasonable numbers, whatever the word reasonable means. That's also a subjective term.

The last bullet, Mr. Eom of KAERI developed a BBN model. He adopted the method developed by Norm Fenton. And in that model he estimated the number faults remaining in the software. He used the BBN model. And this worked. In fact, the starting point of our effort.

A simple way of looking at what we did is, we revised the model somewhat. And then we came up with an estimated number of faults remaining in the software. And then we convert that number in the software table probability. And some kind of theoretical reasoning for doing so is not very strong one.

But again I, well, earlier in the discussion I heard people talking about the analogy between human error and software failure. I really appreciate the knowledge between the two. And in case of human reliability analysis, we used HEPs in PRA basically. You can also caution how much basis you really have.

I know the HRA people did not like what I said. But you don't have data, right, especially in accident condition. What is the probability that an operator will do the wrong thing? There's just no data.

And the similarity that software, it will, that's the argument, that software doesn't failure. Similarly, you can argue, human don't fail. It's the context that the operator sees. He sees certain indications based on his training, he can do certain things. And what he did may turn out to be the wrong thing.

But you can argue that's, determine this in process too. So, I guess I talk too much. This is the five phases of software development that we considered. It includes software requirements, software design implementation, testing, installation

and check out.

And for each phase we developed a BBN model, trying to estimate the number of faults inserted in the phase. And also the number of faults detected in the phase, such that they can be removed. So at the end of the model we have the remaining faults.

Some of the inserted faults go undetected. So they stay in the software. And we have such a model for each phase. So that interaction between the phases is that an earlier phase may pass faults to the next phase. But those faults can possibly be detected and removed in later phases. So essentially, the BBN model, in terms of number of faults, tried to model that. This slide is --

MEMBER BLEY: Before you leave that last slide, does that summarize everything you've looked at in this project?

MR. CHU: That's the part we spent more effort on. The other part is the fault size distribution that we used to convert the number of faults to a failure probability. That part, we looked into, you know, if there's any data available. And we fine tune.

MEMBER BLEY: So you formulated that. But you haven't --

MR. CHU: But we haven't tried to pin it down in terms of coming up with numbers. But the idea is -- one thought is that maybe we can assume that software failure probability is a fraction of the hardware probability.

Same for the current nuclear power plant. And they have a hardware failure probability of ten to the minus five. And then we may assume software failure probability as a goal of say, ten to the minus 5 or smaller, assume some goal. And then you can use that to do the calibration. Or you can call it back calculate the fault site's distribution.

MEMBER BLEY: I guess I'll wait until you go through what you've got here. Because I'm --

MR. CHU: Okay.

MEMBER BLEY: Something about what you're trying to do on that last slide, coming up with something like the number of faults in the code, smells a lot like what people did with reliability growth models for software 40 years ago. And counting coding errors. I'm not sure that gets us very far. But let's go ahead and hear more.

MR. CHU: Okay. I guess --

CHAIRMAN STETKAR: The reliability models, it used to do a piece part count in the number of --

MEMBER BLEY: Yes.

CHAIRMAN STETKAR: -- you know, widgets that you had in an engine, or something like. And you somehow infer that you then knew how reliable the engine was going to be.

MEMBER BLEY: But go ahead.

MR. CHU: Okay. This slide is a kind of high level description of the overall approach. And I have more detailed slides explaining each of them.

MR. HECHT: Question. Is it, in response to Dennis' comment. As I recall from reading Fenton's work, which was awhile ago, didn't he make some attempt to translate bulk density into a failure rate? Or was it all in terms of fault density?

MR. CHU: I am not aware of his attempt in doing so. I don't know if our collaborators know it. I think that he only worked with a number of defects. Or maybe he separately have work on reliability fault method earlier. He may have.

So a important part, since our model is try to evaluate the quality of software development.

Therefore, we developed attributes. And associate activities for these activities. I guess later I will have an example showing what all the attributes are in general.

Say, in the case of software development. In the face of software development there are two basic tasks. One is developing the software architecture. The other one is develop the software. So, each one of these two make the attributes that is effectively asking, how good a job have they done in developing software architecture? Or how good a job have they done in software development.

And each such attribute don't just describe what they are. Like I said, our software architecture, to develop the software architecture where we actually list, come up with a list of detailed activities. And that are the required activities for the developer to carry out.

So we spent significant effort in developing these attributes and activities. And the purpose is to evaluate how good a job they've done on individual attributes. And then we make assumptions.

The second bullet. By evaluating those attributes we can come out with some quality of the

development of V&V activities. We further make the assumption. We say, a good software development should lead to lower defect. And similarly, a good V&V will lead to high defect detection probability.

And it's easy to say that qualitatively it makes sense to everyone. But the model calls for quantification, how you express this qualitative relationship quantitatively. And this is where expert elicitation come in.

In our project, the third bullet, we plan to have three different expert elicitations. The first one is on our BBN structure. Later I will show the BBN structure. And it has to do with the assumptions made in building the BBN model.

And this elicitation is completed, and we have a summary of what the expert provided. And we, based on their comment of suggestion we modify our model somewhat to address the comments. That's the first elicitation that's completed.

So in that sense we hope that currently structural, our BBN model is a reasonable one that we can continue using. The second elicitation is probably more commonly done to estimate the parameters. There we will get experts, we ask them

specific questions. Given V&V quality is high, what is the fault detection probability?

MEMBER BLEY: So you did gather a group of experts to do this?

MR. CHU: We have a group of experts that we used in the first one, first elicitation. And then it's in one of the backup slides, a list of them. And then the second elicitation we essentially used the same list of experts.

These are what I call generic experts, in the sense they are experts who have extensive experience in software development, or management of software development and V&V.

MEMBER BLEY: And when you did this you were having them look at some V&V program that exists in the nuclear business?

MR. CHU: We, okay, we --

MEMBER BLEY: Or did you just say it was a good V&V program?

MR. CHU: We, yes, that relates to the first quality development of the attributes. We look at all kinds of guidance of V&V or software development, and come up with these attributes associated to those.

In that sense we can kind of claim that it is a more complete list of guidance of software development. And then we use these attributes plus the means for evaluating the quality.

MR. LI: Can I add to that? The standard they used to the V&V attribute is IEEE standard 2012 which is endorsed by NRC. So that's the V&V procedure, follows.

MR. CHU: Yes. I have a slide that gives more detail. Later I'll --

MEMBER BLEY: Okay. I'll wait for that. Then you can tell me how your experts used these attributes to --

MR. CHU: Okay. We provided those attributes to the experts. And, I don't know, 13 pages or more of those. And I kind of doubt that they really have enough time to go through all those tables. But in our questioning, you know, we had more specific questions.

MEMBER BLEY: Okay. Are you going to show us some examples of this?

MR. CHU: Okay. An example will be, like I mentioned, develop the software architecture is one attribute. And then we have a list of detailed things

that they have to do in developing the software architecture. I myself, I'm not a software expert. So, in developing this --

MEMBER BLEY: What I was trying to get at, if you have some examples of the questions you asked, and the kind of responses you were looking for from your experts, based on your 50 pages of attributes you gave to him. I'm hoping to understand what you did.

MR. CHU: Our emphasis is on the structure of the model. So, our questions are, again, later I have a slide that shows example of question. I asked them if they agree the model captures all the causal relationship. That's, I guess a very general statement.

MEMBER BLEY: I'll wait until you get to that.

MR. CHU: Okay.

MEMBER BLEY: And then I'll ask you the kind of questions I want to get into.

MR. CHU: Okay. So, I talk about using -- So, the generic actually has two roles. One is looking at our BBN structure and provide comment. That that part is done.

The second role they have is to come up

with estimates, quantitative estimates of numbers, like detection, fault detection probability and fault density. And that's probably the harder part. Because it's kind of the core of developing our model.

And the third expert elicitation is a different type, in the sense it uses a specific expert, that is, use experts who are familiar with the software development of the LOCS system at ATR. And we have, I think one of the expert is sitting here, George Marts is sitting here.

And he's the INL guy who's in charge of this system. So he knows the detail of the system development. And the other expert that we'd like to get is the vendor who actually developed this system for the LOCS system.

By using these experts they can, based on their experience, score the software development activities. And so, that's the third elicitation that's specific to the LOCS system.

And in addition we hope, or we're sure data is available, what's collect, due to the number of faults detected during the software development project. These are the key software specific, or specific software data that's needed to specialize the

BBN model.

MEMBER REMPE: Isn't there a conflict if you have the vendor who developed the software being an expert assessing quality of the software development?

MR. CHU: That's possible. Everyone claimed one, you know, once all work is good. That's where I think it would be nice to have a regulator, an NRC guy who are involved in reviewing the development of the software. Then they can kind of paint the other side, the more critical one of the work. Yes. But

MEMBER BLEY: But that's --

MR. CHU: He only --

MR. COYNE: Louis --

MR. CHU: He consult with him, so --

MR. COYNE: To be clear though, you used George Marts for the first expert elicitation panel, which was the general influence in the BBN, not the application to the actual LOCS system. That's correct, right?

MR. CHU: Right, right.

MR. COYNE: So it was more the general --

MEMBER REMPE: But I was referring to, he

said he was going to have some of the software vendors on the second panel that hasn't occurred yet. And that would seem to me to be a bit of conflict if you have the vendor who developed the software assessing the quality of the software. Did I misunderstand?

MR. COYNE: Maybe this didn't come across. The first panel was developing the structure of the BBN. The second expert panel is developing the probability tables that underpin the quantification of the BBN. So it's given a quality attribute set at a certain level, how does that influence the next node in the BBN. So that's what the second panel is doing.

MEMBER REMPE: Okay.

MR. COYNE: The third panel will then take that completed general BBN and apply it to the LOCS system. And look at the various quality attributes associated with the LOCS system. And then get an estimate of reliability for the LOCS system based on that.

MEMBER REMPE: Okay.

MR. COYNE: Is that --

MR. CHU: Yes. So the third elicitation we have to use experts who are familiar with it. So, these are the experts.

MEMBER REMPE: Okay.

MEMBER BLEY: I'm -- Just a comment. I mean, when you put the other expert panels, when the National Academy puts together one of its panels you can either have nobody who knows anything, or you can have the people who do. But try to balances the biases within the panel.

One would hope you tried to do that in a case like this, which you really have to go to people you know. And then temper that with other knowledgeable people.

(Off microphone comments)

MEMBER BLEY: It's a good point. But it's one that has to be --

MEMBER REMPE: I can deal with it. Okay.

MEMBER BLEY: -- balanced.

MR. CHU: And then the last bullet is on use of fault size distribution.

MEMBER BLEY: Can you define that for me. I've gone all through your report trying to find what that means. I don't find the words even in your report.

MR. CHU: Shall I skip to -- I have a slide or two on that.

MEMBER BLEY: Okay. I'll wait. You can get there if you're going to get there.

MR. CHU: Okay, yes. I'll get there.

MEMBER BLEY: Because I don't see it in your report.

MR. CHU: If we --

MEMBER BLEY: That's why I --

MR. CHU: If we have time, I guess there's time, I think. This slide gives a high level view of our model, kind of I have already explained it. It will, it has five phases. Each phase we developed some model. And the interaction between the phases is the faults.

The faults get passed from one to the other. So, after installation and checkout there are certain remaining faults. And we use the fault size distribution to compare to failure probability.

MEMBER BLEY: There isn't much of a network here. It's just a straight path.

MR. CHU: But you have to look inside, which is shown in the next one. This one is a model for the design phase. That is the second phase of the development. Let me try to explain that. It has two quality nodes. This, oops. Two quality nodes.

This one is quality of development in software development phase. This node is quality of V&V in this phase. And as I described earlier the quality of the development will affect the defect density. And the quality of V&V will affect the fault detection probability.

In this phase we considered two type of faults. One type is those faults that was passed along for earlier phase. And another type, the second type is the faults that are inserted in the current phase.

And the reason we treat them differently is because during the first expert elicitation the expert saying the probability of fault detection for the three type of faults should be different. So we see them in the same way. But they should have different detection probability.

And another, this now represent a measure of the size and complexity of the software, that is, it is function point, number of function point in software. And the defect density is expressed in terms of the number of faults, the function point. Therefore, the number of function point multiplied by the defect density give you the total number of

faults.

And then, given this number of faults there's some probability that faults are detected and removed, which is given by this node. They joined, they basically use a binomial distribution to estimate what is the number of faults detected and removed, which is given by this node. And this node basically is the difference between the total number of faults inserted and those that were detected and removed.

We have the similar treatment for those faults that were passed along on earlier phase, which is shown here. And so, the number of faults that were generated in the current phase, and were not detected, is here. And this is the number of faults that were passed on the earlier phase, and went undetected. The sum of the two is the total number of remaining faults.

And I again describe the structure and the qualitative, I describe it as everything in this model needs to be quantitated at the center, so that we are relying on expert elicitation.

MEMBER BLEY: It almost looks like you're asking the questions to support this network in the absence of knowledge about the size of the software

we're talking about. That can't be true, I guess.

MR. CHU: The size of the software is represented by this node. And so, for a specific software we will count, or we will estimate the number of function points. And the number of function points multiplied by the defect density, the function point gives you the total number of faults. And that says you account --

MEMBER BLEY: Okay.

MR. CHU: -- for the size or complexity.

MR. HECHT: Getting back to Dennis' question about size. In larger projects you have a certain amount of requirements, volatility. You have a certain amount of staff turnover. You have a schedule, which causes some mismatch between development phases.

That's not accounted, is that accounted, it looks as if that's not accounted for in this model. Is that correct? You assume that every stage is completed before you move on to the next stage?

MR. CHU: Yes. This also relates to the fact the real development involved iterations. It's not just a sequential form. I think our model, we want to apply our model after the software is

installed in checkout.

Kind of like, for a PRA purpose technically you look at, you know, its reliability during its operation. So the times when we do the assessments is after the system is installed and checked out, and it's operating. And so, at that time all the process, development process is completed.

Whatever interface happening, or whatever interactions have taken place, has taken place. But we do our assessment at that time. I'm not sure if it answers --

MR. HECHT: Okay. Well, I'll just give you a personal observation, if I might. That what we've seen, that if, for example, you change requirements. Let's just say you add an interface --

MR. CHU: Yes.

MR. HECHT: -- during the later stages of design, and you don't account for all of the interfaces, all of the influences that that additional interface may have. That things may be forgotten. You may not trace everything back in your integrations tests.

And that some things may be overlooked that cause defects to exist. Because the requirement

change wasn't totally traced throughout the design. It wasn't, it was just not completely accounted for.

CHAIRMAN STETKAR: I'll bring you back to, a valve could have failed because the bolt wasn't torque, or it could have been a little bit corroded. In many cases all of that doesn't make any difference when we're trying to model the end result.

MR. HECHT: Well, I --

CHAIRMAN STETKAR: So, those are good comments about the way things can go wrong. And there could be a bazillion of them. And we can't model explicitly each of the bazillion, because you never get to the end.

MEMBER BLEY: I think there's something in what Myron's saying that's important for these guys, though. If you're putting together an expert panel --

CHAIRMAN STETKAR: Right.

MEMBER BLEY: -- to come up with their best judgments, based on whatever evidence they have of these parameters in this model, those kind of things --

CHAIRMAN STETKAR: Right.

MEMBER BLEY: -- need to be on their mind.

CHAIRMAN STETKAR: If you're trying to

build it --

MEMBER BLEY: Which is what --

CHAIRMAN STETKAR: -- from piece parts, which is what they're trying to do.

MEMBER BLEY: -- they're trying to do.

CHAIRMAN STETKAR: Right.

MEMBER BLEY: So, if you aren't thinking about those kind of things, that puts into question --

CHAIRMAN STETKAR: The vessel.

MEMBER BLEY: -- whatever you come out with is an answer from this process.

CHAIRMAN STETKAR: Indeed that's right, if that's the approach you're taking to try to build it. So this, and that is a fundamental question. That if you're trying to take this approach if you've assumed those away, then you're wrong.

MR. KANG: Well, what --

CHAIRMAN STETKAR: Then you're wrong.

MR. KANG: At the specific timing of this method application, the previous tests will be categorized to the basis. So if you make a small change in requirement then it will cause huge change in the down coming flow. So, those activities will be re-categorized to the basis. We have five phases.

And then we will evaluate the activities in each phase.

MEMBER BROWN: Then you go back to the beginning again?

MR. KANG: We don't have to really go back to the beginning.

MEMBER BROWN: But if it's a new requirement.

MR. KANG: Yes. For example, we, during the software development process let's say 50 activities were done. And then we made a small change in the requirement. Because of that change we did 30 more small sub-activities.

Then in total we have 80 activities here. We categorize 80 activities to five activities, five, I mean, phases. And then we quantify the quality of each phases. That's the process.

CHAIRMAN STETKAR: I hear what you're saying. And, by the way, I understand what you're saying also, Myron. But what I'm trying to get back to is, why are we doing all of this? I can, you know, instead of an 832 machine screw I needed a, I don't know, a 624 machine screw.

Does that make a difference in terms of

what we're trying to do in modeling a valve? Does that make a difference? If somebody put it together and decided that, oh, my God, it's not going to work with an 832, I need a 624. So they went back and redefined that. You're trying to infer that somebody, that that 624 might have wrong?

I'm interested in, did the valve work? Did it open or close? If you're trying to build it through all of those little decision processes, from the point of having a valve design that looks like this blank piece of paper, through the point that I have in installed valve in the plant that I can look at for failure modes, I'm not sure how you're getting to that end through this process.

MR. CHU: I think our attributes, you know, we have a pretty complete list of attributes and associate activities. In that sense I think it captures like a missing requirement that's added later on.

I think the requirement, they will be required to go through, kind of iterate through the software development process, to make sure that new added requirements treated correctly. But if it is not treated correctly in our assessment we do have an

attribute called traceability.

So the experts who are familiar with the development process may recognize we didn't do a good job here in tracing this new requirement. Therefore, they should get a low score. In that sense, it can be captured. So, when it come to, you know, the attribute themselves, I think we have a pretty good list.

MR. LI: A few response to Dr. Hecht's question. Those back and forth going to be reflected in the input to the model. So, if you have many requirements the new part added to your product. So, that's a reflection of the true quality of your product.

And admittedly, the number of defects calculated using this model is going to be higher. So, this reflects in the input to the model. Now, you response to Mr. Chairman's question. This work, it tried to estimate the number of defects. And tried to quantify the fault or failure rates.

MEMBER BLEY: But the gap there between the number of defects and the next step, where John's hanging up, and from what I heard Louis say earlier, it's the part you haven't --

MR. LI: Fault --

MEMBER BLEY: -- been able to get across.

MR. LI: Yes. He's going to discuss that in Page 19.

MEMBER BLEY: And for me, coming up with the number of faults hidden somewhere in the software, I mean, people have been doing that for 40 years in different ways, not with the BBN.

MR. LI: Right.

MEMBER BLEY: And they've counted, they've tracked, they've come up with reliability growth models and other things to extend beyond where they've tried. And, you know, those are hidden in all kinds of places.

And they're not in the places you've tested. And they might be in places that never get actuated. We're back to your earlier slide, when you actually fall in that spot. And it's a problem.

MR. LI: Right.

MEMBER BLEY: So it seems like we're doing an awful lot of work to come up with something for which there are estimates that might be every bit as good as you get from this, out there in the literature. But it's that next step, the hard part,

that you're --

Well, if you're going to get there, from what I heard Louis say earlier, you haven't been able to pull that off. Is to get from some density of flaws in the software to how that relates to the systems failing.

MR. COYNE: Ming, is it fair to say that we haven't gotten to that stage of the research? You're certainly putting some preliminary thought into what that would look like. But that hasn't been a strong focus. And I guess as this -- This is very good feedback, by the way.

And this project is very much a work in progress. So this is actually an ideal time to get the feedback, because we can work it back into the research project.

Dennis, to your point, there is, you didn't get a document on this part of the project yet. The document you got was on the statistical testing method.

MEMBER BLEY: Yes.

MR. COYNE: So we didn't --

MEMBER BLEY: That's right.

MR. COYNE: We haven't actually given you

a write up on this.

MEMBER BLEY: I was wrong when I said earlier I could --

MR. COYNE: Well, and I --

MEMBER BLEY: -- put it in the wrong --

MR. COYNE: We should have been clear when we started to let you know that --

MEMBER BLEY: That's okay.

MR. COYNE: -- you didn't have that. One of the points of feedback we got early on, and maybe Louis mentioned this. I can't remember. But Bev Littlewood had been one of our subcontractors to BNL. He had pointed out that they did do the development of the BBN. But at best it would give you a weak prior.

MEMBER BLEY: Yes.

MR. COYNE: So, South Korea has far more experience developing it. We're very interested in entering this collaborative arrangement. It's been very fruitful to us. It remains to be seen how strong of evidence we'll be able to get from the BBN in the end.

And this question of how to convert defects to the final reliability is still an open

research question. But I do want to say, one of the very attractive things of the BBN approach is the ability of the BBN to take additional evidence beyond. We're focusing on quality attributes.

But there's other attributes that we could certainly bring in, as Louis mentioned, the complexity of the software, some of the quality attributes. And the potential to link the quality activities that we would review as part of a licensing action, to the ultimate reliability of the software is, if we could do that I think that would be a very beneficial thing to be able to do, to more formalize that link up.

We know these quality attributes are important. We know that you need to do them to have high reliability software. But as far as the quantification, and the actual numerics that underpin that, it's something that we hope to get more insights on as we go forward with this particular project.

MEMBER BLEY: I would mention though that if this doesn't pan out to be real helpful at this level, getting some experience with the BBNs you might find useful in some other areas.

I've seen things people are playing with in using it to kind of overlay on a PRA to figure out

how to use the guts of that analysis in notable ways. There are lots of places it might be useful. But thanks for your comment.

MEMBER POWERS: I want to just make an observation on the translation fault density into failure rates. This has been a, how shall I say it, the holy grail of software reliability work for the last, well, 35 years I think.

MEMBER BLEY: Easily. I've seen it for even longer than that.

MR. HECHT: Well, the work I'm thinking of specifically is the work by Rome Laboratories somewhere around 1980. And if there's interest, I can get you the specific research, the specific report number.

And the basic theory was that you had the fault density, the execution rate, the number of times the fault would be triggered, or that it might be triggered. And that turned into a rate. And I think there were three or four other parameters that I don't remember that were in that model.

The point is, it's very attractive, but was found to not be terribly, have a terribly high predictive value. It's very difficult. It might be

possible within a very restricted domain. For example, if you were to work on CE System 80 plants.

To say that, given this experience that we've had over the past 30 years developing the software, that we may know something about the future software within that limited domain.

MEMBER BLEY: I think where you began with the comment of the holy grail is something not to be forgotten. I don't think we're going to get there in that.

MR. HECHT: Okay. But you're observation is well taken. And the thing about reliability growth models is, what they're really useful for is to tell you when your test program can be ended.

MEMBER BLEY: That's right.

MR. HECHT: Given, and what it says is that given the profile of pass failures that you've discovered in your test program, this is how many your test program is going to discover. Not necessarily the residual defect rates, but, you know, just be careful.

My recommendation would be, suggestion would be that to be careful that you're not going down the same seductive blind alley that other people have

tried over the past --

CHAIRMAN STETKAR: Thirty years.

MR. HECHT: Yes, plus.

MR. CHU: Regarding the reliability growth method, you know, we spent some time looking into that. And in comparing with what we are doing here, I think significant difference is some reliability growth method is basically driven by data. You collect some data on fault detected.

MEMBER BLEY: Yes.

MR. CHU: And you kind of use the data to fit some curve that you have. While our model, you know, the main emphasis is really on the quality. You evaluate the quality. Our model try to estimate defect as, that is, in case of LOCS it may well be the case if no data reported. But --

MR. HECHT: Okay. Well, you --

MR. CHU: -- still the model can give you an estimate. And how good that estimate is we may see.

MR. HECHT: Okay. And then, of course, there is the final question that if you predict the defect density of X per thousand lines, how does that translate into failure rate per hour, or failure

probability for a year.

MR. CHU: Right. That's where we plan to use that so-called fault size distribution, which is somewhat similar to the ratio used in the software reliability --

MR. LI: So, in response to your comment, I couldn't agree more. You mentioned RADC, the Rome Lab, our 85th study published in 1992.

And they come up with like over 12 tables, magic number. You fill in the tables, check this, mark that. And then at end you add them up. Then there are magic coefficient there. Then you convert that to the failure probability. But we tried to avoid that approach. We tried to open that box here.

So, we collect the set of attributes we believe relevant to a number of defects and failure to the failure probability. But we might be wrong. So, if we're wrong then we can replace with a different set of attributes and rebuild the structure.

And regarding the conversion from number of defects to failure probability, I agree with you, an open issue. So we don't have a clear answer. So, so far in the literature you can find when the fault by distribution, which in 1980 something, very early.

And then Musa, John Musa, 1987 published the so-called fault exposure ratio.

Later UMB and even Sergio Gurro came up with some different approach. But, you know, those are just one method could be used. Are they the final solution? We don't know. So here we can have a pilot say all the possibilities, whether that one works or not. So that's the current status.

CHAIRMAN STETKAR: We should go on. I have a goal to finish this section by noon. So we will finish this section by noon. Louis, make sure you finish --

MR. CHU: Okay. I'll try --

CHAIRMAN STETKAR: -- this section by noon.

MR. CHU: -- to go faster.

MEMBER BLEY: And I would suggest, if you need to cut some stuff, I would cut the development of the flaw, number of flaws down, and talk more about where you're headed with flaw size distribution, and why that might be useful to you.

MR. CHU: Okay. This slide shows, you know, the previous slide is a simplified one, because it doesn't show the attributes connected with these

quality nodes. So, this slide shows different attributes. And there are three types of attributes.

The first type is those basic activities that you need to carry out the phase. The second type is the analysis type attribute, that is, these are traceability, risk, criticality, security analysis.

The third type is what I call management related attribute. They are review and audit, and configuration management. And note that this is in a divergent configuration, because there's practical difficulties using the convergent configuration.

MR. LI: Louis, before you go on, can I go back? Mr. Bley, you were looking for example, the attribute example. And this chart provide you some example. For instance, configuration management. So, this is one attribute.

MEMBER BLEY: So, critical analysis is an attribute.

MR. CHU: Criticality analysis --

MEMBER BLEY: In the right corner.

MR. CHU: -- yes.

MEMBER BLEY: I'm sorry?

MR. CHU: Criticality analysis.

MEMBER BLEY: Oh, that's not what it says.

Okay. So that would only be applicable if you were looking at something for which criticality was --

MR. CHU: We abbreviate.

MEMBER BLEY: -- was an issue.

MR. CHU: I'm sorry?

MEMBER BLEY: Yes. Oh, that's criticality of --

MR. CHU: Of the software --

MEMBER BLEY: An element of the software.

MR. CHU: -- is component modules. The safety integrity level --

MEMBER BLEY: So, given criticality analysis, what would you have provided your experts with regard to that, to help them --

MR. CHU: We have a --

MEMBER BLEY: -- develop judgments?

MR. CHU: -- reasonably detailed description of what they need to do in doing the criticality analysis.

MR. LI: May I add to it? Criticality analysis is basically activity here in the two elements. So, the way put it, the way we put it to evaluate the quality of that activity. So, whether the development did a great job or an okay job in term

of this criticality analysis.

MEMBER BLEY: You gave them the standards to look at to say --

MR. LI: Right.

MEMBER BLEY: -- what is a good --

MR. LI: Right. There --

MEMBER BLEY: What are the boxes you check off to do an okay job?

MR. LI: Right. There are definition of different levels. So, excellent, so how we define excellent? So you need to achieve this goal, that goal. And there are a list of goals. If you achieve that then you can claim your activity is excellent for the moderate and --

MEMBER BLEY: So, did you ask your panel a question based on the quality was average, or the quality was good? Or, what did you give to the experts to get their opinions back, to use in your analysis?

MR. LI: For the generic experts. So, we provided them the definition of the levels.

MEMBER BLEY: Okay.

MR. LI: So, assume --

MEMBER BLEY: So, they have the

definitions, what it means?

MR. LI: Right. With the definition. So, assume the development did a wonderful job on the criticality analysis. What's the contribution to the number of defects? So there we ask the generic experts either contribute whether there's a causal relation, and also what's the quantitive relation to that.

MEMBER BLEY: I take it what you're asking them for is to give you estimates of the probabilities of certain things along --

MR. LI: Right.

MEMBER BLEY: -- this Bayesian Network.

MR. LI: Right. That's second phase of expert opinion. The first phase we asked them whether they're linked there.

MEMBER BLEY: Okay.

MR. LI: Whether --

MEMBER BLEY: Did you draw the picture right?

MR. LI: Right. Exactly.

MEMBER BLEY: Okay.

(Off microphone comment)

MEMBER BLEY: And that's the part you've

done?

MR. LI: Right.

MEMBER BLEY: Have you done the second part?

MR. LI: No.

MEMBER BLEY: No.

MR. LI: The second part is ongoing.

MEMBER BLEY: Okay. So, what you've done so far with your experts is --

MR. LI: Just --

MEMBER BLEY: -- really develop this --

MR. LI: -- this diagram.

MEMBER BLEY: -- the diagram.

MR. LI: Whether --

MEMBER BLEY: Develop the basis --

MR. LI: -- that diagram or this diagram. What of the two diagram looks right.

MEMBER BLEY: Okay. Okay, go ahead.

MR. CHU: This slide gives some detail of how we can follow up the attributes and associate activities. I guess to save time maybe I should skip this one. The main point is --

MEMBER BLEY: Yes. I think you can skip that one.

MR. CHU: -- to look at a wide class of items to come up with the attributes and associate affirmatives. In that sense, you know, it's a reasonably good compilation, using information from different sources.

MEMBER BLEY: So, before you leave this slide, the top part I don't think we need to talk about. We know most of that stuff. An attribute is modeled as a node representing qualities. And this picture, that's that little node way up here. And that node is over these 18 or 20 things over here.

MR. CHU: No. The attribute is one of those 18 nodes on the --

MEMBER BLEY: One of those.

MR. HECHT: So, you ask that question to prove each one of the nodes on the, for the diagram on Page 10.

MEMBER BLEY: And possibly for each of the levels of reaching one of these things.

MR. CHU: The middle, each of these nodes on the outside is an attribute node.

MEMBER BLEY: I almost wish you wouldn't call those nodes. But those are attributes of quality.

MR. CHU: Yes. And then the ones in the middle effectively is a aggregation of those qualities. That is, the overall quality.

MEMBER BLEY: It's somehow aggregated there from all the --

MR. CHU: Right.

MEMBER BLEY: -- ones around the outside.

MR. CHU: Right.

MEMBER BLEY: And is that overall aggregation of quality the thing in the upper left corner of your BBN?

MR. CHU: Right. Right.

MEMBER BLEY: So, you have to go through and set levels of meeting each of the attributes on this picture with your experts. Given all of those they then do some kind of aggregation.

MR. CHU: Into the --

MEMBER BLEY: And that puts in here --

MR. CHU: Right.

MEMBER BLEY: -- a question they have to answer. Like, what is the probability of, what's the number of flaw, the flaw density? What are you asking them to put in here?

MR. CHU: It will be the --

MEMBER BLEY: I'm trying to figure out what you're asking your experts to do.

MR. CHU: Given high quality of the development --

MEMBER BLEY: Right, which is the sum of all, some kind of aggregation of all of the things on this paper.

MR. CHU: Which is this node.

MEMBER BLEY: Which is the aggregation of all the stuff on the other picture.

MR. CHU: Right.

CHAIRMAN STETKAR: Do you have an algorithm to show how all of those 15, or however many there are, attributes determine whatever metric goes into that box that you're using?

MEMBER BLEY: Or is that a judgment by your experts then?

MR. CHU: There will be some judgment on relative importance of those attributes. So some expert already express their opinion. They're saying certain analysis has no effect on quality, or on the numeric box.

MEMBER BLEY: The ones around the outside of this picture?

MR. CHU: Right. So, in the second elicitation one set of question will be related to importance, relative importance of those attribute nodes.

MEMBER BLEY: And then are you going to run that through an arithmetic machine to generate the aggregate? Or do the experts do that?

MR. CHU: That is, we, I think we, our current question we basically ask them to rank those attributes on a scale of five or ten, I forgot. And so, in that sense the expert will just check off a table, you know, indicating its, the importance of those attributes.

MEMBER BLEY: Of the ones around the outside.

MR. CHU: And then we plan to further aggregate, use that expert information to come up with a parameter needed in the --

MEMBER BLEY: Is there a claim that these are independent? Or have you asked your experts to decide if they're independent?

MR. CHU: Those attributes, some experts do express concern that the other one, these attributes --

MEMBER BLEY: Yes.

MR. CHU: -- may be.

MEMBER BLEY: That's the one I'm holding up. Maybe you can't see that far.

MR. CHU: Yes.

MEMBER BLEY: But it seems fair for me to hold that up if I had to look at this one.

MR. CHU: Yes. They have comments saying, you know, some nodes are, should be dependent. So, in terms of those --

MEMBER BLEY: Seems to me that they might even tell you it's more complex. If this one is super good, then it doesn't matter about this one. But if this one is average, then this one becomes very important. Have they talked about that?

MR. CHU: No.

MEMBER BLEY: Or have you wrote them about --

MR. CHU: The only --

MEMBER BLEY: -- that kind of independence or dependence?

MR. CHU: Not to that kind of level of detail. They have commented certain attribute may not be that important.

MEMBER BLEY: Are you finished with that round of elicitation? Or are you still collecting.

MR. KANG: Second round elicitation.

MEMBER BLEY: I'm sorry.

MR. KANG: In the second round elicitation we will ask the kind of --

(Simultaneous speaking)

MEMBER BLEY: Okay.

MR. CHU: But it happen --

MEMBER BLEY: I'm just trying to figure out where you are too.

MR. CHU: Right.

MEMBER BLEY: So, okay. I'm getting a little bit of a --

MR. CHU: It happened we did the first elicitation. The purpose of that was not to relate it to the importance. But it happened that they provided that kind of comment.

MEMBER BLEY: And to help me a little further. I don't know if it's the third or the fourth, or the fifth round of elicitation. But at some point you will have an aggregate value here giving us a certain set of values on those attributes.

And then they're going to give you a

judgment on something to put in here. And what kind of something is that? Is it an estimate of number of flaws, or flaw density? Or something altogether different?

MR. CHU: Well that, no. We have three possible state, high, medium, low.

MEMBER BLEY: So, they'll put in high, medium or low?

MR. CHU: Right. And then --

MEMBER BLEY: So then, that's just something that conditions everything that comes after it?

MR. CHU: Yes.

MEMBER BLEY: Is that right? Okay.

MR. CHU: And basically the next expert elicitation will ask, given that overall quality is high for a safety critical software, what do you think the defect density is? Or similarly, what do you think the fault detection probability is?

And of course, you can also have questions how the experts are good in providing answers with this type of question.

MEMBER BLEY: And that covers only the things that are daughters of this path? So, the only

things that quality, high, medium, low will effect are the next box, the box after it, the two after that, and the final one.

MR. CHU: Yes.

MEMBER BLEY: Because you're independent of things that aren't fathers in this, parents in this line.

MR. CHU: But I --

MEMBER BLEY: By your model.

MR. CHU: Right.

MEMBER BLEY: Okay.

MR. CHU: Yeah. That's the conditional independence.

MR. HECHT: I'm a little bit confused here. Because things, these 15, the importance of those 15 parameters varies by the design stage, you know. For example, the software integration test plan is going to impact the number of defects remaining.

And it's going to impact the number of defects that are detected. And your criticality analysis is probably going to effect the number of defects introduced into the design. And security analysis may be the same thing.

So, I guess my question is, don't you have

to ask the question about how these factors influence each one of the boxes? That's, I'm confused about that.

MEMBER BLEY: I think. I'm going to try something in response. And then you comment on it. My understanding of what they claim they're doing is, they've already asked their experts to make sure that that quality box up there is only important to the things in its direct line. That it's, the other things are independent of that.

Because when they crunch numbers through their model that's the assumption. That everything that you can't track by arrows from that box to the end is independent of that box.

CHAIRMAN STETKAR: Such that the --

MEMBER BLEY: So you're saying, I don't think that's true, which would say the model's not drawn right. And supposedly your experts have --

CHAIRMAN STETKAR: Judged that you're wrong, and --

MEMBER BLEY: They're right.

CHAIRMAN STETKAR: Such that the quality of V&V is completely independent of the quality in development. Because that's the way this --

MEMBER BLEY: That's the way the picture's drawn right now.

CHAIRMAN STETKAR: -- model is structured. Despite the way an organization might work in practice, or anything. It is presumed that it is fully independent, and that any attribute that you evaluate for one is fully independent of the attributes for the other. that's the way this is modeled.

MEMBER BLEY: It's only parents that affect daughters.

MR. CHU: I guess --

MEMBER BLEY: That's right, isn't it?

MR. CHU: -- one reason is that for safety related systems they're supposed to have independent V&V. In that sense when they argued that the quality of independent teams may be independent.

But I, again, also see, you know, they have interactions. And the interaction, you know, someone doing a good job in V&V may tell the development team that they would correct certain things, such that the development team corrected, and ended with a good job.

I don't, in general there's type of

insurance. You look at the dimension of any two nodes and you can ask that question, are these two nodes, do they affect each other directly?

So the BBN assumption is if one node affect the other node directly, not through the structure, then you should have an arrow connecting them.

But in the case of the attribute nodes, okay, the expert did mention, or assert, that we consider that kind of dependency is weaker than, such that we are going to ignore them. Otherwise, it becomes messy, or becomes unmanageable.

CHAIRMAN STETKAR: Let's, I do need to keep us on track here. So, if you could, Dennis, if you're interested in the things about what they learned from the expert elicitations so far.

MEMBER BLEY: I think they may have told us a fair amount of that.

MR. CHU: Kind of. Let's see. Expert elicitation on structure. The outcome is that these two bullets show the, as a result of the expert comments we changed our structure.

The first one is use of separate default detection probabilities for the two type of faults.

The faults are the current phase, and the faults passed from the previous phase. And the second change we made is the number of function points. Originally in our model we say it affect --

MEMBER BLEY: I'm sorry. I lost the language. What's a function point?

MR. CHU: It is a measure of the complexity of the software. There's a concise definition of it that I do not know. But there's a flaw that is generally, there's a way of counting it.

MEMBER BLEY: But, I mean, it's not in your BBN picture.

MR. CHU: The function point is. It's in the --

MEMBER BLEY: Is it?

CHAIRMAN STETKAR: I think it affects this thing here.

MEMBER BLEY: Oh, size and complexity. So, somehow that affects the size and complexity one.

MR. CHU: I'm sorry?

MEMBER BLEY: One of these is called size and complexity.

MR. CHU: Yes. That's the --

MEMBER BLEY: So, the function points,

whatever they mean, affect that. But you can't quite tell me what they mean.

MEMBER BROWN: I made an assumption that a function point was where something actually got calculated or determined based on data, or an if then, or an algorithm, or a whatever. The more function points you have, the more possibilities of defects you could occur. If that's wrong --

(Off microphone comments)

MEMBER BROWN: I made an assumption that that was --

MR. LI: That, function points are the replacement of random code for software size. Initially, if you use random codes to measure software size. And later on the industry developed concept of measure called function points to do that.

Function points measure the piece on the software interface and the internal logic. And the data support that. So there are rigorous algorithm. And there are people, rigorous people, certified people to do the counting. So, this becomes the de facto industry standard to measure software size.

MEMBER BLEY: And what you asked your experts were, is function point a suitable measure for

size and complexity?

MR. LI: Yes.

MEMBER BLEY: And they said, yes.

MR. CHU: They said yes. But some --

MEMBER BLEY: But it also affects detection from them.

MR. CHU: Yes. So, following their advice we joined arrow from function point to detection probability.

CHAIRMAN STETKAR: This arrow.

MEMBER BLEY: Yes. Because it will also affect that. Okay. So that's your conditional, that they're conditionally related.

MR. CHU: Related, right.

MEMBER BROWN: But just to have the argument, you know, not all lines of code are equivalent.

MEMBER BLEY: Right.

MEMBER BROWN: it's a little arbitrary.

MEMBER BLEY: Right.

CHAIRMAN STETKAR: Thirty two versus 24 --

MEMBER BROWN: yes. When you got 552,000 lines of code you don't have to worry about whether it's arbitrary or not. It's just a hell of a lot of

code that has to be executed. And it's a matter of how that code gets stuck together.

In other words, which pieces function, I'm not using that word interchangeably. How pieces of that code create an operational picture of something. Whatever that is is more important than necessarily the lines.

If I've got a function that I got to accomplish that takes 50 lines of code with all kinds of data and a bunch of calculations, and I've got another function that only takes two calculations, it's a considerable difference between the complexity. And a considerable difference in terms of what can go wrong in --

MEMBER BLEY: I understand everything you said. I'm still not sure --

MEMBER BROWN: But that's --

MEMBER BLEY: -- how they're --

MEMBER BROWN: I'm not sure either.

MEMBER BLEY: -- using what this means to them.

MEMBER BROWN: That's what --

MEMBER BLEY: Is it a standard thing out there if I --

MR. LI: Function point -- it's going to count the difference. Because of their internal logic, their amount of input output. So function point measure from the function perspective side.

MEMBER BLEY: So it mirrors? What did you say, mirrors that?

MEMBER BROWN: Measures.

MR. LI: Measures.

MEMBER BLEY: Measures that, okay.

MR. HECHT: Function point is an industry accepted term --

MEMBER BROWN: Which is undefined.

MR. HECHT: -- that --

MEMBER BROWN: For which nobody can define.

MR. HECHT: There are function point conferences every year, where all the people who count function points get together.

MEMBER BROWN: Oh, God.

MR. HECHT: There are formal people who count lines of code, that count function points. But it is a measure of software size. And it's used often to predict, you know, the software development effort, and the schedule, and things like that.

MEMBER BROWN: But that, you have to have a specific package of software --

CHAIRMAN STETKAR: Makes me glad I took the career path I did. Can we get --

MEMBER BROWN: Well, I've got another, I could make another comment.

CHAIRMAN STETKAR: WE have about 12 minutes.

MEMBER BROWN: I could make another comment relative to that. But it's not going to useful, it's not going to add value to this, other than --

CHAIRMAN STETKAR: But that gives you a hint.

MEMBER BROWN: -- to say we ought to object to this whole approach, okay.

(Off microphone comments)

MR. CHU: This slide shows the changes that we made due to the expert elicitation. This slide shows other comments the expert provided. And we didn't make any change because of their comments. So, in that sense, you probably can look at these comments made, in some cases indicate, you know, some unique points of our modeling.

We sampled the dependent, this potential direct dependency between the attributes. And we just cannot, putting, you know, a complex network to try to capture that kind of dependency.

The model, the way it is now, it's already quite complicated. But I always say, it's complicated because the attributes of the guidance are numerous. There are so many guidance on it, that's why we come up with so many attributes can make the model difficult to handle.

Function point, for example, is one issue. Some expert indicates that, you know, the data available in the literature may be on the lines of code and function points relatively new.

MEMBER BROWN: It sounds like it's vague. I'm sorry. Go on.

MEMBER REMPE: It is to me, while we're stopping.

MR. CHU: And then the intent of definition. I think lines of code or function point, they all have variations in definition. In case of function point, I think we picked one that seemed to be a popular one. But there are variations in those different definition. They will give you different

numbers.

Maybe I'll go on to the fault size distribution. I guess that's a subject of interest. I have two slides trying to explain what it is. And how we plan to use it.

A similar way of describing it is, as indicated in the first bullet, the software rate of probability is equal to the number of faults in the software times the fault size distribution. And the word "size" in the second bullet represent the probability that a fault will be triggered.

And the distribution, the fault size distribution represent the variability of this probability among the faults. So, you have N faults. Each may have a greater probability. This fault size distribution supposedly represent that, the distribution of those probabilities. And --

MEMBER BLEY: Well, at least the way the words are. For a single fault the flaw size distribution represents the likelihood of that fault becoming a, what you're calling a failure, right?

MR. CHU: Right.

MEMBER BLEY: Okay.

MR. CHU: Different fault, they have

different probability in this probability --

MEMBER BLEY: Different flaw size distributions.

MR. CHU: Yes. And this term was first introduced by Littlewood. And it's also used by Delic in his more recent work. But that wasn't as many years ago.

MEMBER BLEY: It's a probability distribution. I don't know why it needs a special new name. But, okay.

MR. CHU: I guess to try to give the meaning of this thing to make sense. That is, people doing software reliability tend to say, you know, you have fault in the false states. And that to a failure. But they're mapping is associated probability likelihood, and kind of this fault size distribution captures that.

MEMBER BLEY: Is that --

MR. CHU: And the third bullet just point out the similarity to fault exposure ratio that's used in reliability growth methods. In the, in software reliability growth method people work with failure rates.

So they have this equation, that's that

failure rate equal to the number of faults, times the failure, fault exposure ratio. So you compare the two equations, and they look alike. Kind of, it's the same theory, and the same concept. But, you know, you can always question it. But it really makes sense.

And also, I just want to point out the similarity to failure likelihood index method for human reliability. This shows the equation of human error probability is A + B times the failure likelihood.

And the failure likelihood index for human reliability is calculated as weighted scores on human perform, human, what's the word, performing shaping factors. That is, the performing shaping factor could be the training of the operator. Whether or not it is good procedure. Whether or not there is a good indication of those factor that can affect operator action.

And in this failure likelihood index method it effectively convert the failure likelihood index into a human error probability. And the equation shows the parameters A and B. They are estimated using calibration.

That is, they were estimated by using some

well recognized or formally accepted HEPs. In that sense what we propose to do, using fault size distribution similar to the failure likelihood index.

MR. HECHT: So, are you saying that for calibration you might say that you might do it by vendor, or something like that? How would you calibrate that, other than --

MR. CHU: I don't have the, we haven't formulated detail. Just by now it's common sense. That is, as you mentioned, the CE plant or core plant protection calculate, they have some operating experience. I think in John Bickel's paper he talk about maybe it's possible to have, they may have found one fault, or something like that.

MR. HECHT: Yes.

MR. CHU: But the operating experience is not long enough to justify a, let's see, a ten to the minus five count of numbers. So, that may be one place that we have some data but that's not enough. I think the Calvert Cliff operating experience may justify say, a ten to the minus three type number.

But for a reactor protection system you kind of expect ten to the minus five as a number. And in order to come up with that, and also, I think when

people do PRA technical analyses I assume there are goals, reliable goals for that.

Therefore, the idea I have is, let's assume the goal is met by the software. You can back calculate this fault size distribution. If we, you know, our model can estimate the number of faults, or apply the (coughing) to estimate the number of faults. And assume the software is the goal.

Then we can calculate the fault size distribution. I have to say, you know, this is not enough data. You cannot generate, you cannot get something out of nothing. Therefore, you have to make some assumptions to develop.

MR. HECHT: Well, let me ask it another way. If you don't have enough information to develop the fault size distribution in general, then how would you be able to determine the failure rate, based on the quality factors?

MR. CHU: I don't see a way of doing that. That's why I propose we do some kind of calibration.

MR. HECHT: Okay, well, okay. So, I guess, what does calib -- I guess we have a misunderstanding on what calibration means.

MR. CHU: Okay. Say there are ten, we are

seeing about ten faults. And we, there's a goal of ten to the minus five. Then the fault size distribution should be ten to the minus four. It is ten to the minus five divided by ten, or multiplied by ten.

Because we don't have real data. It's similar to human reliability analysis. People put in a human error probability. There's no data to just -- And, but we are comfortable with what the people, in the sense we are used to. And you can make the same argument instead. You don't have really, you have no way of allocate it.

MR. HECHT: Okay. So, let me say, should be. You mean, it's been measured to be on the order of ten to the minus five, based on Bickel's work. And you estimate that there is, that the FSV is ten. Therefore, you calibrated that. Is that the --

MR. CHU: Right. Right. Because we don't know, we really don't have solid data to come up with it.

MR. HECHT: Okay. So if you went to another system, you know, by another vendor, I won't name one. But if you went to something by another vendor then you would have to come up with another

calibration, right? Because you couldn't take the CPCS data and apply it to a BWR or a --

MR. CHU: Well, maybe we could look at that calibration as a way of estimating a generic fault size distribution. For lack of additional information we want to apply it to a different software. I will end up using that as using the fault size distribution estimate that seem important there.

MR. HECHT: Do you expect that any of the vendors will, or anybody's blind nuclear quality software will have anything other than the very highest number, the very highest quality levels?

MR. CHU: I do expect. In our scheme we have three levels. Basically we say, those safety critical systems following the guidance captured in our attributes, if they carry out those activities successfully, it should get a medium rating.

MR. HECHT: Medium?

MR. CHU: That's how we define the medium.

MR. HECHT: I see.

MR. CHU: And then we specify a high state by saying, if they do something extra, more than what is required, and in the evaluator's mind this additional activity would increase the quality. Then

the evaluator can choose to give them a high rating. But it is left with the evaluator to make that decision.

And for our attribute development we did provide a few examples. See, we have a list of activities that are required, based on, you know, the providers of this attribute. And we provided an example of additional activity that can potentially raise the score from medium to high.

So we are leaving that judgment to the person who does the evaluation. And that's another point that some expert pointed out, you know, by being an additional activity, you know, it's not that clearly defined. So they do a little bit, it said, does that deserve a high rating. So, the way we will address it is it's up to the evaluator to make that judgment.

MR. HECHT: So, if, let's just say there's a vendor that uses SysML as an example, to do their design, as opposed to other vendors that don't use SysML, but just use manual or rely on what's in people's memory to do the design.

Do you expect that you would give that vendor a higher score in design? And that that would

eventually correlate to a lower failure density through the BBN model, that would then, after calibration be associated with a failure rate? Is that the idea?

MR. CHU: I'm not sure, I don't follow what you said. Somehow you talk about some kind of standard, or a way of developing software. But in general --

MR. HECHT: Sign methodology. That's different.

MR. CHU: Sign method, okay. But in general, we're saying our model can be used to assess a software that's developed based on that methodology. And hopefully, having these attributes on the quality we have enough resolution to capture the differences of the two design method that you seem to be talking about. How, you know, how well the model can capture that is a --

(Simultaneous speaking)

MR. COYNE: One of the issues we had early on is we tried to use Branch Technical position 714 --

MR. HECHT: Yes.

MR. COYNE: -- as a basis for the nodes. And there wasn't that variability that we can. It was

either go, no go. And so, everything would have been set at the same level. So that actually was a bit of a setback.

And we started looking at these other areas on Slide 12 to try to find attributes with more variability, so that you could get safety critical software that still had some variability in how the nodes were set.

CHAIRMAN STETKAR: We need to finish by 12:15, or --

MR. CHU: I'm sorry.

CHAIRMAN STETKAR: And I don't care what time we finish, because I don't need to eat. But we're going to reconvene at 1 o'clock. So, we need to get through this section. My comment is, because I've used this failure likelihood method for human reliability analysis for about 25 years.

Observations. If you put in too many attributes, meaning too many performance shaping factors, you get the same result no matter what you do. So, you have to be careful.

Over specifying the number of attributes sounds like good engineering, like my example with the poor guy who spent nine months out of his life because

he needed to have the finest structure possible. You will get the same answer regardless of what the problem is.

MEMBER BLEY: We haven't proved that. But we observed it.

CHAIRMAN STETKAR: We've observed this. Seems to be some sort of central limit theorem. The issue of calibrating these curves is indeed very, very important. It doesn't necessarily do vendor to vendor. It's having data points to anchor the correlation. And you need some data points.

It could be from expert elicitation. But you need some good parameters. The other thing is, that all of this is done in the context of a particular scenario. It isn't like the software didn't work.

What's the likelihood that the human did not open a particular valve within 45 minutes, given this event progression? So, this is not a generic people didn't do what they were supposed to do.

It's all within the context, which means that we run through this process perhaps 100 different times for 100 different operator actions in a particular PRA. So, be aware of what you're walking

yourself into here and what might be the implications of that.

MEMBER BLEY: Louis has some experience in that.

CHAIRMAN STETKAR: He does. Let's see if we can finish up here. I'd like to hear what you're talking about the next two slides.

MEMBER BLEY: At least this one.

CHAIRMAN STETKAR: The treatment of uncertainty, and the issues and limitations of the BBN model. Treatment of, let's skip the uncertainty, in the sense of time --

MR. CHU: Okay.

CHAIRMAN STETKAR: -- and get the one you're on there.

MR. CHU: Then the issues and limitations. First one I have repeatedly said, you know, one can easily see that they are qualitative in relationship between two things. While trained operator will do better job and work, how you translate that quality information into a quantitive model is the problem.

And the answer we have to it is basically expert elicitation. We hope the expert will come up with a reasonable estimate of the numbers that we see

in our model. And the second bullet talks about dependencies. And I talk about it also.

In general it is difficult to show for every pair of nodes. They do not affect each other directly. That is, you can, if you look at our model you're looking at an attribute. The definition of them when they are, you know, these two nodes back each other.

Therefore, you should put in a direct connection in your structure. But that will make the network even more complicated. So, our argument is, the dependency is a weak one. Therefore, we choose not to do that in the model.

But the third bullet has to do with solving of the BBN model. We are using the AgenaRisk software tool. This is the software tool developed by Norm Fenton. Using this tool we have tested in that Figure 3 with all the attributes in a diverging configuration.

You know, we have a dozen or more attributes. If you use a convergent configuration that means the node in the center, the overall quality node will be a function of the combination of all the parent, of the states of the parent nodes. That is,

each parent node has three states.

And if you have a dozen such attributes, the number of combination of the states will be three to the twelfth power. That makes it difficult to come up with estimates for such a complex table. Plus, there's a computational difficulty.

Essentially this issue of state explosion that makes the processing possible. We play with the AgenaRisk model. And we found it's not able to handle it. As the reason, instead of using convergent we use divergent configuration.

CHAIRMAN STETKAR: I'm sorry, Louis, I'm violating my own rule here.

MEMBER BLEY: Yes, I think you --

CHAIRMAN STETKAR: But it sounds like what you're saying is different from what I thought you answered Dennis earlier. And make sure I understand this. This drawing again, the one with the 15, or however many they are, it sounds like the algorithm for combining those attributes to determine something is now wired into software? is that true? I thought you were saying that the experts did that.

MEMBER BLEY: Did that aggregation.

MR. CHU: The model is entered into the

software.

CHAIRMAN STETKAR: Which model?

MR. CHU: The picture that you --

CHAIRMAN STETKAR: This picture is in the software?

MR. CHU: Right. In the AgenaRisk tool. But it just help with the processing --

CHAIRMAN STETKAR: But --

MR. CHU: -- of the numbers.

MEMBER BLEY: Let me just say, so for a given Bayesian Belief Network each node has associated with it an attribute picture that is aggregated through software, not through expert judgment. That's what I think you just told me.

MR. LI: Oh, man, that's --

MEMBER BLEY: Told John.

MR. LI: Page 11, that diagram.

MEMBER BLEY: Yes.

MR. LI: What we get from the experts in their opinion. For instance, criticality analysis. If criticality analysis is high then what the, let's say distribution contribute to the quality of the development. And if the criticality is medium then what the contribution to that? So we get that number

from the experts.

MEMBER BLEY: Okay.

MR. LI: But --

MEMBER BLEY: Wait. Stop. I don't know what number they're giving you, if you're asking them for the contribution. I don't know what that means.

MR. LI: Well, if it's high --

MEMBER BLEY: If I'm the expert --

MR. LI: If it's high --

MEMBER BLEY: -- and you tell me that's fine --

MR. LI: -- then the quality is high. So there's probably 80 percent likelihood that the quality is high. If it's medium, the criticality is medium, and the quality of the development to be high might be only 40 percent.

MEMBER BLEY: Independent of all the other 20 things on that chart?

MR. LI: Yes. So that cause a node probability table, a NPD table.

MEMBER BLEY: Wait a minute. So you're ask -- They're giving you the answer, the center answer, given just the condition of one of the attributes?

MR. LI: Right.

MEMBER BLEY: Okay. And then you'll ask them for all of the attributes?

MR. LI: Right.

MEMBER BLEY: And now you'll get a set of numbers that might add up to anything.

MR. LI: That's the generic model. And later we applied to specific software. Then for the specific software --

MEMBER BLEY: I don't --

MR. LI: -- you know that the criticality --

MEMBER BLEY: You just lost me. I don't know what the generic model is. Is this picture the model?

MR. LI: The picture is the model.

MEMBER BLEY: But then it says you need all 20 of these things, not just one of them --

MR. LI: That's right.

MEMBER BLEY: -- to do the aggregation.

MR. LI: That's right.

MEMBER BLEY: But you're asking them one by one --

MR. LI: One by one.

MEMBER BLEY: -- to give an aggregated --

CHAIRMAN STETKAR: No, not that, just the input to that.

MR. LI: Just the input. Not aggregated yet.

CHAIRMAN STETKAR: To see how those -- If it's high, let's say if it's high it's .8. And if it's medium, whatever you said, is .4.

MEMBER BLEY: Yes.

CHAIRMAN STETKAR: I don't know, but someplace in the middle, in this magic software, is where all of those get aggregated into some sort of ranking of this quality thing.

MEMBER BLEY: But our experts have also told us the ranking of these, I'm saying 20, I don't how many there are, these 20 attributes. So they give you a ranking of the 20 attributes. And then an estimate of the overall quality, given the condition of each one of the attributes separately.

MR. LI: Right.

MEMBER BLEY: And then somehow you've got software that's turning those two sets of answers into an aggregate.

MR. LI: We aggregate to a specific

application. By that I mean, you have a piece of a software you want to evaluate. Then I have this model. I have all the quantitive relationships there. So, for each aggregate to that software you're going to have a specific input.

Criticality is going to be medium. The traceability analysis is going to be excellent. So you have a, you know, a combination of input specific to that software. Then your AgenaRisk, that software going to run, take that input, and come up with final quality evaluation.

MEMBER BLEY: That gets used in the BBN.

MR. LI: Yes.

MEMBER BLEY: This isn't part of the BBN, this is input to the BBN.

MR. LI: No. This is the model of the BBN. The input --

MR. KANG: How do BBN estimate layered approach?

MR. CHU: Let me try this. This --

MEMBER BLEY: I'd sure like to see a picture of the whole BBN, or a segment of it.

MR. CHU: This node represent the overall quality. And the same --

MEMBER BLEY: Which on the previous slide is the box in the upper left corner.

MR. CHU: Right.

MR. LI: The group, yes. Yes.

MR. CHU: Right. So, we don't have enough space to put all these on that slide. So we put it separately on this slide.

MEMBER BLEY: So, if that's true, then at least for me the arrows on this little thing are drawn in the wrong direction.

CHAIRMAN STETKAR: That's what he was saying.

MR. CHU: That's the issue of convergent as opposed to divergent configuration. If you have the, change the direction of the arrow, the number of combination of the states of the parents will be like half a million. There could be half a million of such states.

In principle, we would like to estimate this huge matrix. What's a number to put in that matrix? It becomes unmanageable. It's impossible to try to come up with that kind of number. Not to mention, the computer's capability in processing.

MR. COYNE: It's equivalent to saying, if

you flip the arrows all those nodes are completely dependent. Or, you're allowing the model to allow you to assume they're all completely dependent.

So you would have this like 20 nodes, or three to the 20 power entries on this probability table. By doing the divergent configuration you're effectively assuming they're independent of each other.

And you just look at the one influence from each of those attributes on the final answer. It's a way to make it tractable at this point in the research project.

MEMBER BLEY: But there isn't a path through the network going that way. Because the middle is the thing that's --

MR. COYNE: It's a numerical construct. So you can still set those nodes in the -- And there's plenty of different types of BBN software. But the software will, when you set those attribute nodes, will grind it through the BBN network to give you the final answer on the quality node you're looking for.

MEMBER BLEY: Okay. Okay. Okay, I sort of get it. It's a, somewhere in the software there's a thing, if the arrows don't go anywhere you assume

it's this other arithmetic game that you're playing. And it generates an aggregate number to stick into the rest of the network.

MR. CHU: It's an alternative way of aggregating this. Because the other way is --

MEMBER BLEY: None of this stuff is in your earlier this year NUREG, right?

MR. CHU: No, this is the --

MEMBER BLEY: None of that.

MR. CHU: -- one we've been doing the past three years, I guess, since the last one.

MEMBER BLEY: And we're already past.

CHAIRMAN STETKAR: I don't think that, unless, Louis, you can think of anything that is really important to stress, given the time constraint. Do you have anything more that --

MR. CHU: I think I want to draw the analogy to human reliability again. I want to point out there's a lot of similarity. And we got used to the human reliability analysis. But the issues --

MEMBER BLEY: I'm sorry. We're still fighting that tooth and nail. But go ahead.

MR. CHU: After 30, 40 years? And so, in case of software reliability, you know, people

challenge, caution, way, how you call it by example reliability. But I think what make it more complicated is, software has much wider interest from nuclear industry, for people in different fields.

And if the nuclear industry come out with something like, well, we developed, people in other industry, they find it not usable to them. Or they need to --

What we did, what we do, defend it or challenge their model. So, there are political consideration too. It's difficult to come up with a model that's accepted by all the industry. So, what will make our work a little unique is that we will get failure probability, not failure rates.

While other industry tend to look at failure rates, for whatever reason or purpose. Again, you know, we need to be fair to software reliability. We are still at the early stages compared to human reliability.

And it's better to develop some method. It may not be perfect. But it's better to have a method and try to use it. So, that's my message related to the BBN model.

In fact our, the next presentation, the

statistical testing, I think, it's much less controversial and it's pretty straightforward. And I know we are happy with what we did. So, after lunch we'll have more detailed presentation on it.

CHAIRMAN STETKAR: Let's break for lunch. For you, since the same group is presenting after lunch, I do want to make sure that we leave -- We're already scheduled to go to 6 o'clock tonight. And I don't really want to challenge that end time. I want to make sure that we leave absolutely enough time for EPRI.

Given the fact that you have 30 some odd slides in this afternoon presentation, make sure that you have it organized so that you're done with that section by 2:30 p.m., okay. Otherwise, I'm going to cut you off. Let's break for lunch and return, I'll be as generous as I can, 1:15 p.m.

(Whereupon, the above-entitled matter went off the record at 12:24 p.m. and resumed at 1:15 p.m.)

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

(1:15 p.m.)

CHAIRMAN STETKAR: We are back in session. And, as I mentioned before lunch, I would appreciate if you could, you know, shorten up your planned presentation a little bit so we can keep somewhat on schedule. Because I do really want to make sure EPRI has enough time to present. We'd all like to get out of here by 6:00 tonight.

So with that, it's yours, Ming. I don't know, Louis, I'm not sure which of you two are going to take the lead here.

MR. CHU: My name is Louis Chu. I'm with Brookhaven National Lab. I'm reporting on the second project on software reliability that has its own statistical testing of the LOCS system.

This work is done in collaboration with Idaho National Labs. The key guys are sitting here. Idaho guys are Tim Kaser, George Marts. And at the end me an Athi, Athi has been working on the digital project in the past three years.

And in this presentation, I think I'll give the introductory part of the presentation and then some detailed presentations will be given by Tim Kaser of INL and Athi of BNL.

This is an outline of the presentation.

Essentially, it kind of shows the steps that we followed in doing this testing project. But again, the loop operating control system is our example system. And we are happy that Idaho Lab was willing to help with it.

And in this case, they actually carried out, they set up a test configuration and carried out the test. In addition, things like, it's on the LOCS system. Also, we see the PRA of the evidence test reactor in order to simulate the scenarios, generate the test cases.

We also got a redefined model of the Loop 2A. That is, this the thermohydraulic model of this loop. This loop is somewhat similar to pressurized water reactor.

And in this study, we make use of PRA to generate cutsets that lead to a reactivity insertion accident. And the LOCS system's function in this situation is it needs to detect the overall condition and generate a trip signal.

So using the PRA to generate cutsets, and we sampled on the cutsets, a total of 10,000 tests was done, that is each sample from the list of cutsets that we sent end up, you know, becoming a test case.

In addition, for each sample cutset, in order to model the failure effect of the cutset, we developed what we call probability failure model, basically such a model captures variability of the failure effects.

For example, the cutset may say you have a small LOCA. But it doesn't say where the small cut LOCA is located and what size it is. So the probability failure model accounts for the variability and specifies the possible locations and possible size.

So given with sample of cutset and further sample from the probability failure model, such that the scenario is better defined and can be simulated using the RELAP5 model of the loop.

So the test case generation essentially involves sampling from the cutset and, for each sample, further sample from the corresponding probability failure models. And then use that to specify the RELAP runs to simulate the thermohydraulic condition that is seen by the LOCS system.

What we are going to mention is the probability failure model, it should be something that the dynamic PRA people try to account for, basically

in a dynamic modeling they try to account for timing, they try to account for different timing they have on the scenario and the human performance. So I tend to think the probability, the model has its general efficability besides just statistical testing.

And after the test cases were simulated into the RELAP model, we sent it to Idaho Lab. And Idaho Lab has a test configuration, basically has test a computer that interfaces with the LOCS system. It feeds the test cases one by one to the LOCS system and records the output from the LOCS system.

For each such run, they generate the output, they provide the results to BNL. And BNL, after we've seen the result, we basically look at the input, and we try to estimate, based on this input, when a true signal should be generated. And we compare this expected time when a trip should be generated with the actual time when the trip is generated.

So this is how, essentially, we evaluate the results. And one thing that we run, one difficulty we ran into this reproduced civility of test results. I think partly because the test computer and the LOCS system are not synchronized,

that they each have each cycle point.

Therefore every time you run it or try to run a test case, the LOCS system may be in a different part of its cycle point. Therefore, its response to the input may have some variability. That's one reason that we have difficulty introducing exact same result.

And people tend to say, you know, software, you give it the same input you always give it. So in output, but this in our case, we are not able to show we have reason that we can vary simulation why.

And the test results basically show we did 10,000 tests with no failure. Based on this data, we use to send a method of quantifying separate reliability to estimate a failure probability.

And we mentioned that, when we first did the test, there was actually one case in which a failure did occur. That is the output is such that no trip signal was generated. But when we tried to reproduce it, we were not able to. We did probably 100 runs of the same tape, but we were not able to reproduce it.

CHAIRMAN STETKAR: So is the one percent

chance, given that set of input conditions, that you would not get a trip?

MR. CHU: I guess the reason, we're still, we don't have a solid explanation for what happened. But I kind of --

CHAIRMAN STETKAR: We have evidence.

MR. CHU: Right. But on the other hand, it's how we reproduce one.

MR. MARTS: One of the things that happened is when the test was run we weren't there to see what happened. And what you're looking through the data, it looked like the distributed control system didn't change at all. So it's kind of like it didn't see the input file, you know.

But in all the other previous cases, we would see the inputs change to like the input file. In this one we didn't. And so we can't explain, not being there, you know, did something not turn on, or did we lose power, that kind of stuff?

MR. KASER: We had scenarios that varied from 30 seconds to half an hour. These tests are all run sequentially, 24/7. And so there're parts of the day that we are not there to monitor and babysit the system. And occasionally, we did have situations

where we had power outages where the system reset. And of course, when it does that, it doesn't fire back up and then continue running.

CHAIRMAN STETKAR: Of course, that never happens in the real world.

MR. KASER: It never happens in the real world.

CHAIRMAN STETKAR: No, my point is that you do have some evidence that there may be conditions --

MR. KASER: Yes.

CHAIRMAN STETKAR: -- where you won't get a trip signal. But you, for some reason, have thrown those away and said you didn't have any failures.

MR. KASER: Well, something went wrong there, and so --

CHAIRMAN STETKAR: Well, things go wrong in the real world.

MR. KASER: And Louis is guiding here why we went back and retested it many times to see if that one case had something about it and could not get it to fail anyway. And I assume that something happened in the middle of the night.

MR. CHU: Okay. I have two more slides I

can cover. And then other times we're going into more detail. I think this one, I have pretty much covered the key stat of this that we start testing.

Basically, we tried to simulate the real conditions that a LOCS system sees on the real demands on the LOCS system, such that the test results is effectively the same as the data collected from operating experience. In that sense, this way of doing statistical testing appeared to be a pretty sound method for estimating the reliability.

The only limitations is the realism of different things that we did in the analysis. How realistic is the PRA model, how realistic is the RELAP model, and how realistic is the test configuration?

But it's just like any other modeling. You can ask the same question, how realistic are you modeling what you're modeling? So in that sense, I don't consider that as a limitation method.

This slide shows the interaction between BNL and INL. In addition to, you know, running the test cases, Idaho Lab also provided the RELAP model and the PRA model that we make use of. In terms of performing the test, BNL generated test case input that we provided to Idaho Lab. Idaho Lab put together

a test configuration.

MEMBER REMPE: So in your draft NUREG there's some statements, and I didn't pick up the page and all that. But there're some comments sometimes about, that imply that Brookhaven didn't quite have all the details of the loop design, so you had to make a few assumptions. And it almost implied we're not quite sure we got it right here and there. But yet you guys are all here today.

Was there enough interaction that you feel confident in your model now of what you're doing in your analysis now? I can dig up specific quotes if you want me to, from get the report, but again, maybe this is just a documentation thing. But it almost conveys that you weren't real confident with some of your modeling effects.

MR. MARTS: Can I talk to that? One of the ATR, the Advanced Test Reactor, the PRA is official use only. And also, so was the RELAP model. And so what we did is we took parts of that out that we were willing to share with Brookhaven National Lab.

And so they didn't get the complete picture. We gave them enough so that they could run, that we could go forward with this analysis. But we

didn't give them the entire picture. Like we didn't give them the PRA for ATR. We didn't give them the RELAP model for ATR itself.

MEMBER REMPE: Well, I can understand that. And they made a comment about things being proprietary or whatever. But still, did they not have you review it afterwards and say, yeah, those changes you made look okay for what you're doing or something? I mean, was there a follow-up so you had confidence in the way the analysis was done?

And perhaps the report should convey that confidence, do you see where I'm coming from, in the draft NUREG? See what I'm saying? Do you still have some uncertainty about some of the assumptions that you made? Or would you talk to --

MR. CHU: We did provide our report to Idaho Lab. But I'm not sure how much time or how much resources to have to thoroughly review our report. But I think, for the purpose of demonstrating the method research, that was really an important, you know, the model may not be realistic, may not truly represent the ATR. But regardless, using the model will demonstrate how you apply this approach to quantify software reliability.

MEMBER REMPE: So that'd be good to convey in the report. The other thing was that I'm aware that an older version of RELAP was typically used at ATR. Which version of RELAP did you run the model in? Was it the ISL RELAP version?

MR. CHU: All I know is RELAP5. I don't know -- RELAP5 --

MEMBER REMPE: So you have them the INL, or the NRC, the older version?

MR. CHU: NRC, right.

MR. MARTS: The one that NRC could run, yes, BNL could run.

MEMBER REMPE: Okay.

MR. CHU: So I guess this concludes my presentation. There are details out of all that, and Athi will present, at this point on out, try to help answer any questions.

MR. KASER: I am going to defer to George to explain the ATR complex and how we implemented our system there. And this slide is for you, George.

MEMBER BLEY: As you go through this part, are you going to describe how the test was actually run? And then maybe we can understand a little better about that case that you couldn't --

MR. KASER: Yes.

MEMBER BLEY: -- that didn't work right.

MR. KASER: A little bit of background to start with. I'll --

MEMBER BLEY: That's good.

MR. MARTS: ATR is a test reactor that is operated by or for the Department of Energy and our regulator. There're six pressurized water loops at ATR. Five of them support the Navy Nuclear Program. The sixth one is one we just currently installed primarily for the commercial industry.

We are currently, well, we have run two EPRI experiments, and we're getting ready to run our third. Anyway, the pressurized water loop at 2A can run at prototypical commercial industry. The design conditions, 2,500 psig, 650 degrees F and 60 gpm.

ATR's been operational, since 1970 we've been running experiments. And 1990 we upgraded all the experiment control systems from pneumatic controllers and that kind of stuff, stuff you expect from, you know, the technology in the 70s to a digital control system.

At that time, we were looking at doing a separate system for control and a separate system for

plant protection. We went to DOE and said we didn't think we needed a system, a plant protective quality system, you know. And they agreed with us.

And so we were able to mesh it into one system, you know, which saved us a lot of money and grief. Because nobody else had a digital control system that would, you know, act as a PPS system on a reactor.

And so, at that time, we went with a digital control system. The vendor at the time was Leeds and Northrop. They've since separated and that kind of stuff and now owned by Metso Automation.

And so we have a digital control system that has two CPU-based redundant controllers, reads the IO, does the math and all that stuff and then sends out what we'll need to control.

This is a simplified schematic of Loop 2A. The reactor vessel's on the left. And so water just goes around the circles. We have three primary coolant pumps, some line heaters. We don't show the pressurizer on there. But it does show the instrumentation that we modeled, that we used in the RELAP code as outputs that feed into our control system. Let's see --

(Off microphone discussion)

MR. MARTS: Yeah, that group and the flow instruments are part of our protective system. It's a two-out-of-three system. We added two more indications, pump suction pressure and pump suction temperature, so that if the RELAP, you know, the input said, hey, the pumps are tripped, the pumps would trip using those inputs. And so that's why those were added to our system.

MEMBER REMPE: Again, when I was reading the report, a lot of places I see ATR has a positive void coefficient. Is that the proper way to say it or is it the loops in the ATR?

MR. MARTS: Probably the loops in the ATR.

MEMBER REMPE: Yeah. I guess I was, you know. And so I think we ought to be ought careful about some of the documentation.

MR. MARTS: Okay.

MEMBER REMPE: Yeah.

MR. MARTS: This is kind of a busy, this is the software and hardware portion of the logic for one of the protective channels. This happens to be our impulsive inlet temperature. We also do outlets, impulsive outlet temperature, impulsive inlet flow and

impulsive inlet pressure as our four protective channels.

And so this is the temperature. The temperatures, there are three separate modules. And those modules have 16 inputs, and so it's a mixture of inputs on those three separate modules. You know, it's not just input temperature coming into a module.

And then we have a point that reads that signal from the analog input, converts it into engineering units. And then there's another block that we configure. It takes that value and does the logic on it. In this case, it would create a high alarm showing a trip.

And then those three, the three different channels go to a, we'll call it a two-out-of-three comparator, that if any of the two of the three channels trip, then it'll go through an or gate, and that goes through an and gate and then an inverter, it goes to our digital outputs. And then the digital outputs interface with the plant protective system over there on the left.

MR. KASER: Right.

MR. MARTS: On the right.

MR. KASER: Yeah. Repeat, yes. Same as

me.

MR. MARTS: The PPS channel. So this is, the loops at ATR are a little bit different than a normal commercial facility in that we have these trips that aren't specifically required by our safety documentation. But they act as a backup to our safety, oh, what's that word, they're a backup to our reactor plant protective systems.

And meaning that if we fail to scram the reactor, there's other things that will happen to trip the reactor. If we don't, if there's an event in the loop, like a high temperature event, and we fail to scram the reactor, there are things within the reactor side that'll scram the reactor and make is safe. So it's not really necessary. It's defense in depth, was the word I was looking for.

So like I said, we have three sensors for each of the -- we do some weird things, because we're allowed to. Like our flow Venturi has one set of taps. We tap that into three things instead of having three separate flow Venturis. That was sort of the stuff we were able to get away with.

So we tried to make it a two-out-of-three system, primarily for production so that we can keep

the reactor running instead of having a single input trip, just like the instrumentation before.

This is showing our best bet. The computer on the top is just the human to machine interface that we use to configure the Meso hardware and software.

And so down, what we did is there's three analog input modules that we provided input from the simulator. And then there's three digital outputs that the simulator monitored to see when the reactor, you know, when the LOCS was sending the trip signal. Do you want to --

MR. KASER: And I'll continue with this. We actually did not use our reactor in the production facility. We used the facility that we develop things on which is running a nearly identical version of the same software that runs out at the plant. And the nearly identical is limited by the fact that we can actually change inputs into a simulated or a stagnant set point as opposed to causing them to change.

And so many of the non-safety related inputs that go to the control of this loop were set at those values, simply for holding in place and making it look like things were happening normally.

And then the 14 items that we were simulating, if you will, from the simulator down here at the bottom, this is our whole physical simulation system that's connected up to the CPU, interfaced directly in our lab there with the control system.

This is pretty straightforward stuff in the fact that we, you know, all of the pressure temperature instruments are handled via transmitters, four to 20 million of transmitters. And therefore we simply recreated a four to 20 million amp signal that simulated that, which corresponds to the RELAP model output that Louis and his group provided to us.

MEMBER BLEY: So what I didn't remember, I didn't study the report carefully enough. In each of your tests, did you have a different set of parameter inputs?

MR. KASER: For the 14 values, 14 different items?

MEMBER BLEY: Yeah.

MR. KASER: Yes.

MEMBER BLEY: Okay. So you continually varied those?

MR. KASER: It varied according --

MEMBER BLEY: The tests.

MR. KASER: -- according to what he chunked out on his RELAP model.

MEMBER BLEY: Okay.

MR. CHU: The time set is 21 seconds. Every 21 seconds you have a new record.

MEMBER BLEY: A new record.

MR. CHU: Yeah.

MEMBER BLEY: And that one failure was a case where you put in the 12 inputs, and you got no trip.

MR. KASER: Yeah, it did not trip. Or it did trip and it wasn't supposed to. It didn't trip on time.

MR. CHU: It didn't trip at all.

MEMBER BLEY: It didn't trip.

(Simultaneous speaking)

MEMBER BLEY: And then what you did later was go back and put in that same set of 12 signals and it tripped.

MR. CHU: Right.

MEMBER BLEY: So you don't have any idea why it didn't generate a trip signal, but you saw something else that was funny, you said.

MR. MARTS: Going back on the history on

the LOCS system, I was able to, at that time we ran that test, none of the inputs changed. And so it's like it wasn't getting, and so we can't explain, you know, was it the DCS not updating like it should be, or was there a problem with the simulator?

MR. KASER: It could have been a power glitch, you know, that reset things and didn't start things back up.

MEMBER BLEY: Or, what you first said, there could be --

MR. MARTS: Yeah. You know, and so I don't --

MEMBER BLEY: It could be an actual failure.

MR. MARTS: It could be an actual, you know --

MR. KASER: The system at the plant, though, is on a backup power system. So it never goes down.

MEMBER BLEY: Yeah, but you don't know that's why you got that signal

MR. KASER: That's true.

MR. MARTS: That's true. And, you know, because we weren't, we can't explain it. And one of

the things I didn't, and I want to say it goes back to, the allowable failure of this system is ten to the minus two.

CHAIRMAN STETKAR: The allowable crash rate for airplanes is zero.

MR. MARTS: Yes. And so it, and so --

MEMBER BLEY: So you meet that even if it was a failure.

MR. MARTS: Yes. And looking at the --

MEMBER BLEY: Now, if I read the report right, you look two ways. You said if I'm going to have a ten to the minus four failure rate for this thing, I need 10,000 tests. And you did run 10,000 tests.

But then you also looked and said, looking at my PRA, if I have 134 tests I know it's an insignificant risk contributor. And that's kind of where your ten to the minus two thing comes from.

MR. MARTS: Right, yes.

MEMBER BLEY: Okay.

CHAIRMAN STETKAR: And they were targeting a seven times ten to the minus three or some sort of number that --

MR. MARTS: Right.

CHAIRMAN STETKAR: -- would have suppressed this in terms of the contributors.

MEMBER BLEY: But it kind of bothers me saying that failure didn't occur. I mean, it doesn't kind of bother me.

MR. KASER: Yeah.

MEMBER BLEY: I mean, you can't say for sure that it wasn't a failure.

MR. KASER: But we could reproduce it. But you're right.

MEMBER BLEY: But other things in that box can lead to this problem, other than just those inputs coming --

MR. KASER: It's in our box here too. It's not what you would call a fully certified box. It's an emulator.

MEMBER BLEY: Well, but that's what you're using. Go ahead.

MR. MARTS: Yeah, we didn't go, if this is a for real --

MEMBER BLEY: If you'd been there, well, you would have known if you lost power.

MR. MARTS: We would have known it.

CHAIRMAN STETKAR: You would have known

it.

MEMBER BLEY: You would have known if you lost power.

MR. MARTS: Yeah.

MEMBER BLEY: You wouldn't have known if it was something else.

MR. MARTS: Right.

MEMBER BLEY: But go ahead.

MR. MARTS: You know, it's easy to look. When we're running the test when we're there, it's easy to tell whether or not it's working. Because you could see the values change.

One of the slides, I think probably the next slide, this is what the simulator looks like. And so when it's running, you could see the output values going to the LOCS system change. And then we could look on the LOCS screen and go, yes, we've seen the same things.

MR. KASER: This is our LabVIEW layout for controlling the National Instrument hardware.

MEMBER BLEY: So could then, I guess it could have been the test system like LabVIEW, which is not --

CHAIRMAN STETKAR: What you're testing.

MR. MARTS: Yeah.

MEMBER BLEY: But it could have been what I call the infrastructure, the operating system, the device drivers --

MR. MARTS: Easily could have been that.

MR. HECHT: And that leads me to a question that I asked Bruce about. And maybe I can ask it for the record. It seems that the results that you have here are under the assumption that the hardware is working and the infrastructure software is working. In other words, what you've measured here is the probability, or the failure probability or the success probability, given perfect hardware and infrastructure software. It seems a good assessment.

MR. CHU: In doing this test, we actually used actual certain hardware and software. So in that sense, we are testing the system, not just the software but also hardware. And --

CHAIRMAN STETKAR: In that sense, if they'd had, you know, 30, 40, 50 failures, they could have tracked it back to see, you know, what were the cause.

MR. CHU: You can question whether or not the way test is done. Similarly, the real condition

in the sense like you're concerned about memory leak, as once I know when Idaho ran the test cases, you know, ran 10,000 of it, one case after another without saying it's setting the LOCS system, I assume.

CHAIRMAN STETKAR: That's correct.

MR. CHU: Right. So in that sense, it was running for long hours. But the staff represent the real condition where it is operating at a plant, you can still question it.

MR. HECHT: Well, let me ask you this. If you were running the test, and all of a sudden one of the DPUs just suffered a, you know, a fuse blew or something like that, would you accept that result, or would you say that that's a non-relevant failure and exclude the result?

MR. CHU: Because it has redundancy, right, supposedly the other BP will take over. Then our test may not be the record. Our test only look at the outputs. It should signal what's generated at the right time. If it does fail, then we may try, we try to look back to see what's causing it. But that's not an easy task.

MR. HECHT: Well, I guess what I'm trying to ask is, in terms of the measurement that you're

doing, I'm not questioning the result that you got. You just need to characterize what the result was.

So if, for example, you were, I mean, it was an integrated test. But it was checking only the logic or the correctness of the implementation of the safety software. It wasn't checking that the hardware was correctly implemented or that the hardware wasn't failing. And it wasn't checking that the operating system, and the device drivers and the other parts of the infrastructure --

MR. KASER: That's true. We were only simulating signals, analog signals, that you would see.

MR. MARTS: For the control system, we did, for the LOCS, the digital control system, externally, of the transmitter and the interface, we did test all that. Because the input module was there, you know, our configurate.

For this particular system, we don't need it. The DPUs can run without any supporting computers or anything like that. You know, once they're configured, they'll run forever.

MR. HECHT: Yeah. But, okay.

MR. MARTS: But, yeah.

MR. HECHT: I think I got the answer --

MR. MARTS: Yes.

MR. KASER: This screen here just shows our monitor to allow us to watch the real time effort that's going on. Then we have a setup screen there too and an error screen. So in our initial software go-around, building this software, we had some things to straighten out.

And so that helped us to do that debugging. And once we got it right, then we did a test on this also to compare what the signals, the value of the signals that we're sending out from our simulator was as expected on the DPU.

So we did a number of runs there with our own INL scenarios, if you will, to see how well it mimicked that signal that we were feeding it and compared both magnitude and timing. And within our initial acceptance of what we were going to simulate, it did a very good job of that.

Limitations, the test cases were loaded in memory as electrical values. In order to improve the system throughput, RELAP produces an engineering unit output. So the reason that we did that, put it into electrical units, is simply so you don't have to

convert, save some time on the process. So that way we're expediently emulating, if you will, as opposed to having more overhead to do that conversion.

The second thing is Windows is, the system we were using was not exactly a real time system. Windows does not support real time match natively. And so if you want that, you're going to have to enhance the system.

That would be one thing to, a place that we could go with this is to take the variable execution time of the emulator out of the picture. And thereby, you're looking solely then at the test article, the DPU, the LOCS that you're trying to stimulate and understand its variabilities a little better probably.

To prevent the apparent timing issues that we had, we thought that maybe changing or adjusting the timing cycle a little bit might help. This problem of the timing of simulation is such that you've got two non-synchronized running systems.

And, you know, you've got things happening. And sometimes things get missed. And we're very much of the same crazy domain, if you will, of each system, you know, where you're sub-second but

not sub-millisecond. And so you're going to have some occasions where things could get missed, completely missed, if it's only one record out of the scenario that comes through and trips the reactor, and then it goes back again.

We also had histories to the effect that, in resetting the scrams, if it occurred only in one record, and we're assuming that we would catch that on the output so would see that it's scrammed, if there were occasions where initially that that was a problem.

MR. HECHT: So could that have been the explanation of why you missed --

MR. KASER: It could have.

MR. HECHT: I'm familiar with one AR4 system where it's a software-defined radio where the signal processing aspect of it is being done using the real time operating system. And the user interface is, which also displays the theater from the radio which is done in Windows, and they had similar problems.

MR. KASER: But we only had one scenario that created that problem.

MR. HECHT: Well, it didn't happen very

often.

MR. KASER: And like I say, it's a rare event. And so --

MR. HECHT: It could have been the antivirus run.

MR. KASER: It could have been anything on that PC, yes. So what we're suggesting is that there's two different types of approaches to this, both fixed cycle time where you're real time, if you will, and one that's a variable system that allows things to kind of move in its natural state. George, you guys want to add to this?

MR. MARTS: One of the things I forgot to address is this particular system, the way it's designed is that you have points that you could say I want this point to update every tenth of a second, which it will. But it's not a fixed update. It will meet at least a tenth of a second, but it's probably faster.

And so the input to output of the LOCS varied up to 300 milliseconds. Sometimes it was in the 100 milliseconds and sometimes it was in the 300 milliseconds. And so that added some complexity, especially to Louis looking at the data. We picked

100 milliseconds so that we can gather all the stuff. But because we picked it faster than what the system could respond to, it created a lot of records.

CHAIRMAN STETKAR: Back to you, Louis.

MR. CHU: Yeah. I guess the next part will be the part that BNL did. And I'm going to ask Athi to give the presentation. Athi did a lot of the detail work on this project. And he's more familiar with the detail work. And I will try to support him in answering any questions you may have.

(Off microphone discussion)

MR. VARUTTAMASENI: Okay. So in this slide, I will basically give just highlights of the PRA model of the ATR that is important to our work. So basically what we are interested in is the fault tree that looks at the events that can cause reactivity insertion that originated from Loop 2A. And in that fault tree, the events are through --

MEMBER BLEY: Just to make sure I got this, because I've never seen the ATR before. But I've seen results from experiments. These test loops, I was trying to resolve it, at least have it in my own head, these test loops are arranged so that you can, as you put whatever you put in there to test, it can

be fissile material or anything else, you can get them within reach of the flux of the reactor. Is that right?

So what the protection system we're looking at is trying to do is if something goes wrong in the test loop it'll shut down the reactor to protect the test loop and the whole machine then.

MR. VARUTTAMASENI: Yes.

MEMBER BLEY: Okay.

MEMBER REMPE: So one question I didn't ask, but I was curious, is how much data are there to support that voiding of an experimental loop will really result in a reactivity insertion?

MR. VARUTTAMASENI: We know that from just keeping a loop up. We change the temperature, the reactivity goes up. And so we have to counteract that with our control, the reactor control system.

MEMBER REMPE: Over-moderated in that region --

MR. VARUTTAMASENI: It's over-moderated --

MEMBER REMPE: -- or those regions of the port.

MR. VARUTTAMASENI: -- in those. Yes.

MEMBER REMPE: Okay.

MEMBER BLEY: And you can change the temperature in any loop independent of the other?

MR. VARUTTAMASENI: Any, yes. Okay. So the cutsets are approved into three separate fault trees, if you will. One deals with loss of pressure control. The other is for loss of temperature control. And the third one is for loss of flow control.

So these events include both failure of the LOCS components which include sensors and analog input modules as well as events not related to the LOCS such as pipe break or pipe plugging.

And in the actual event tree that looks at the possible core damage sequences, there are three different systems that can mitigate the reactivity insertion by LOCS. One is the LOCS protection function itself. If that fails to trip the reactor, then there's always the plant protection system.

And finally, there's something called a slow insertion. And my understanding is that that is basically a drum that is half coated with neutron absorber. So if you want to initiate that system, then the drum would rotate. And that will introduce negative reactivity into the ATR. And that doesn't

necessarily shut down the reactor, but it can be enough to mitigate some of the scenarios that the PRA is looking at.

Now that manual insertion or the slow insertion can take up to several minutes to work. And so in our RELAP simulation, we tried to find the cutsets that, in the worst case, will not generate conditions where the trip set point is reached within, say, three minutes. So for those sequences, the slow insertion should be sufficient to mitigate whatever scenario causes the reactivity insertion.

MEMBER BLEY: So if you fail the slow insertion, you still can have a successful strand?

MR. VARUTTAMASENI: Yes. Because --

MEMBER BLEY: In the model?

MR. VARUTTAMASENI: Right. In the event tree, LOCS is basically given the first opportunity to trip and then followed by the PPS. And slow insertion is the last --

MEMBER BLEY: Well, and if those two trip, they cause a scram.

MR. VARUTTAMASENI: Yes.

CHAIRMAN STETKAR: Either one.

MEMBER BLEY: Either one.

MR. VARUTTAMASENI: Either one, right. The slow insertion doesn't cause a scram --

MEMBER BLEY: Is the manual scram part of the model?

MR. VARUTTAMASENI: Yes. It is. So in the original PRA model, all cutsets credit slow insertion as a possible mitigating event. But in our RELAP5 simulation, we actually tried to classify the cutsets according to whether slow insertion would be sufficient to stop the accident condition.

So we modified the PRA sample to add in a separate branch for events that can be, that slow insertion can mitigate those events where slow insertion cannot mitigate. And so that is one modification that we made to INL's original PRA model.

The second type of modification that we made is to add in some of the components that are important for LOCS. We noticed that, in the original PRA model, things like sensors and DPUs are not included in the reactivity insertion fault tree. And we talked to INL a little bit about that.

And I think, in that analysis, the failure mode associated with those components will not lead to reactivity insertion. But for our work, we want to

expand the scope of that somewhat and introduce the possibility that those components can fail in such a way that it will cause positive reactivity. So we added those components into the fault trees.

So the reactivity insertion frequency for Loop 2A is about 0.97 per year. And that is within the system reliability criterion of one per year. And that includes both failure of LOCS component and non-LOCS component failure like pipe break and pipe plugging. In our analysis we only, well, basically only looking at the first 200 cutsets, and that makes up for more than 99 percent of the 0.97 per year frequency.

And the table on this side basically shows the breakdown of the cutsets. About 90 percent of the cutsets involve some type of failure of secondary loop components. So this is the components in the secondary side of the heat exchanger to the Loop 2A.

Only about four percent of the cutset involve LOCS component failure. So when we do the sampling, most of the cutsets that we obtained are basically just some variations of failures that involve the loss of heat exchanger cooling. And only a few involve failure of the primary LOCS components

themselves.

CHAIRMAN STETKAR: So only because of what numbers were in there for the LOCS components?

MR. VARUTTAMASENI: Right.

CHAIRMAN STETKAR: Go on.

MR. VARUTTAMASENI: This slide basically shows a simple calculation to estimate, you know, how many tests we would need to perform in order to meet an acceptable failure rate. So the total core damage frequency for the ATR is about three times ten to the sixth per year.

Now, LOCS hardware failure contributes very little to that, an order of three times ten to the minus 13. So that means that, well, and also the LOCS hardware failure probability is on the order of seven times ten to the minus three.

So before performing any tests, we can say that, assuming that the LOCS software is only performing the protection function, then we can say, even if LOCS software fails at the same frequency as, well, fails with the same probability as the hardware, seven times ten to the minus three, then if we get a result that shows less than one failure in 10,000 tests, then we would still meet the, it will still be

an acceptable failure probability.

MR. HECHT: That last statement, is that based on some assumption about a 99 percent confidence integral using some distribution or something like that?

MR. VARUTTAMASENI: This is the --

MR. HECHT: Or where does that result come from?

MR. VARUTTAMASENI: Which result?

MR. HECHT: The test showing less than one failure in 10,000 test cases, in other words --

MR. VARUTTAMASENI: Okay.

MR. HECHT: -- ten to the minus four --

MR. VARUTTAMASENI: This is based the Bayesian, so we don't assume a uniform prior with a binomial likelihood function. And if we do a posterior calculation, this result is the mean of that distribution. The 95 percent confidence level will, I guess, be a little higher.

MR. HECHT: So it's a uniform prior, a binomial posterior?

MR. VARUTTAMASENI: Binomial likelihood.

MR. HECHT: Likelihood, okay.

MR. VARUTTAMASENI: And later on, I will

have a slide that, I think, has some equations that support this.

CHAIRMAN STETKAR: That was a Bayesian analysis using a presumed half a failure and dividing by, I don't remember, 5,000 or --

MR. VARUTTAMASENI: Right. It's --

CHAIRMAN STETKAR: That doesn't strike me as a Bayesian analysis.

MR. VARUTTAMASENI: It's just using, you know, a --

CHAIRMAN STETKAR: It's a number trick. It's not a Bayesian analysis.

MR. VARUTTAMASENI: But I think that --

CHAIRMAN STETKAR: It's okay. It's a number they came up with somehow. And it doesn't have any uncertainty distribution on it. It's a half a failure divided by something with a denominator.

MR. CHU: No. We did go through the Bayesian update. The crux of the issue seemed to be on just a choice of prior distribution. As in our report, we used a uniform prior distribution and updated the 10,000 cases. And because we have done 10,000, this is pretty strong evidence.

So regardless what prior distribution you

use, then you end up with a relative narrow distribution. And so this last bullet kind of is looking at the mean. But even the 95th percentile is not much larger than the mean value.

CHAIRMAN STETKAR: Okay.

MR. CHU: We also did some sensitivity calculations using the, what's called, Jeffrey's file which is --

CHAIRMAN STETKAR: That's what I read. That's where you put the half, presumed half failure.

MR. CHU: That's, I guess, with that prior distribution, effectively it's counting as you have a half failure.

CHAIRMAN STETKAR: Yeah.

MR. CHU: But this is the, you know, the end of the result analysis, not a key part of the work --

CHAIRMAN STETKAR: I just get upset with people throw around the term Bayesian analysis.

MR. VARUTTAMASENI: This shows the nodalization of the RELAP5 model. So I wanted to point out here is that the model doesn't have the details of the secondary loop. So the heat exchanger is, basically, it's modeled as a constant temperature

surface. And likewise, the ATR loop is modeled as a constant heat source. So those assumptions basically impose some limitations into the situations in which RELAP, this particular RELAP5 model can handle.

The control functions present in the model have some basic flow and temperature control. But it doesn't have a pressure control. So the pressurizer has no control mechanism, and it doesn't respond to pressure changes.

Originally, this model was provided to us by INL. And I guess their use is to look at large LOCA accidents. So in those cases, we don't really need too many control functions. But for our use, we probably would like to have some control functionality model in here.

But the way we use it, we didn't have information to make modification to this. So we just used it as is. So that means that some of the results may or may not be the actual behavior of the ATR.

MEMBER BLEY: Nevertheless, they generated time sequences on parameters that you could feed into the experiment.

MR. VARUTTAMASENI: Correct.

MEMBER BLEY: Now, did you do a large set

of those, or did you run that same transient over and over, I mean, to the tests?

MR. VARUTTAMASENI: The input are different for all 10,000 cases.

MEMBER BLEY: So they're actually different transients that you --

MR. VARUTTAMASENI: Correct.

MEMBER BLEY: So you have 10,000 different transients. Okay.

MR. CHU: Yeah. All the simulators, 10,000 transients. We set up our RELAP model on four different computers and ran them overnight. So you started running before you leave work. Coming back in the morning they're done.

So when it comes to actually running the test cases, Idaho Lab, they have to simulate in real time. So that whatever the simulation time that comes out of RELAP model, they have to follow that. So in that sense, their simulation, I think it was taking a couple of weeks or something.

MR. MARTS: There is one that's, I think, 15 minutes.

MR. VARUTTAMASENI: Per case.

MR. MARTS: Per case.

PARTICIPANT: And you ran 10,000 of those.

MR. VARUTTAMASENI: Yeah. Yes, it took us only about three days running, using four personal computers in parallel to generate the RELAP5 input cases that we sent to INL, so much faster.

MEMBER BLEY: Now, I think what I heard Tim say earlier, I'm still thinking about that one failure. So that was one transient, and you pushed that transient through a bunch of times.

MR. KASER: Pushed it back through 100 times.

MEMBER BLEY: But, let me just draw a picture in the air. The parameter that would cause a trip's going up. And it could keep going up, or it could go up and just pass the trip point and come back down.

Is there any, I think what I heard you say, that there was some chance it could have actually done that. But that wasn't when you sampled the data. And you might have missed the peak that should have caused the trip.

MR. VARUTTAMASENI: But in this particular case, I think the parameters just kept going so --

MR. MARTS: They just kept, if I remember

--

MEMBER BLEY: In the one that went bad?

MR. MARTS: If I remember right, this was

--

MEMBER BLEY: That's what I was asking? But it really couldn't have been that?

MR. MARTS: Yeah. Our large break LOCA, I think, is --

MR. VARUTTAMASENI: I think this is a, one of the larger secondary --

MR. MARTS: Okay.

MEMBER BLEY: In any case, it should have generated --

MR. MARTS: It should have.

MEMBER BLEY: -- a solid signal, no matter when you sampled. Okay, thanks.

MR. VARUTTAMASENI: Okay. So in this slide, I am basically introducing what we call the probabilistic failure model. So once we have a cutset that is basically not enough to predict what the trajectory of the system state would be, so if you have, you know, the cutset says a pipe break at the pump, just a pipe break, then we need to know the break size and the break location.

So that's where the probabilistic failure model comes in. So we sample from a distribution which is, in our case, it's just a uniform distribution. The break size, and also we sample for the break location, and the break size and the break location together will go into the RELAP5 model input.

So the cutset, in this case, is a pipe break. And the probabilistic failure model gives the actual break size and break location. The actual distribution can be anything. But for simplicity for our work, we are assuming a uniform distribution for most of the failure effects.

This slide gives, we have a total of 13 failure effect groups. So the cutsets that, the 200 cutsets that we obtained from the PRA are assigned to one or more of these groups.

As I said earlier, the loss of heat exchanger cooling, or Group Number 1 here, it basically explains about 90 percent of the 200 cutsets. And since we have no way of modeling the secondary side in RELAP5, we approximate the impact of this group by varying the heat transfer coefficient, the time at which the heat transfer coefficient reaches zero.

So the secondary side is modeled by a constant temperature surface. And there's an associated heat transfer coefficient with that. In the RELAP5 model, we basically reduce that heat transfer coefficient in a linear manner to zero.

But we introduced randomness into those events by changing the rate at which the heat transfer coefficient decreases. So it's a way of approximating the loss of heat exchanger cooling cutsets that we can do using the RELAP5 model that we have.

MEMBER BLEY: So let me paraphrase what I think I understand about this. You used the PRA to see what were the most likely failure modes that could occur in the system, in the whole system, including the whole ATR. And from that, you ginned up mathematics to make the RELAP runs look like it was, the situation was caused by these cutsets.

MR. VARUTTAMASENI: Pretty much, yes. But the different cutsets --

MEMBER BLEY: So once we run this whole thing, we've got a test on a large set of RELAP runs that says, for this set of RELAP runs, we haven't seen any problems in the logic system hardware and software that caused a failure, probably, except for that one

case.

But Mother Nature may give you a different transient that we haven't tested that takes the software into regimes that we haven't yet tested. And if that's where our holes lie, those are still laying out there. From the PRA, you think those are much less likely than this group, but --

MR. CHU: It seems you are pointing out the completeness.

MEMBER BLEY: Well, I'm really pointing out how I personally think these software systems are going to fail. It's when they get, either the transient that puts the parameters outside of where we've tested, you've got a pretty nice set of tests here, or something in the monitoring systems itself generates a bogus signal that takes the software outside of the range where we've tested it.

So that's why I was pushing on that point, to understand what you did and how you did it. So we think that you've covered 90 percent of the failure modes the PRA says are the important ones. But there's another ten percent. And there's a whole range of detailed differences and scenarios that would look a little different.

MR. CHU: We sample based on the probability of the cutsets.

MEMBER BLEY: That's right, but --

MR. CHU: In that sense --

MEMBER BLEY: But the whole system --

MR. CHU: -- we had the probability of --

MEMBER BLEY: I'm sorry. But the whole system's sitting there. This is our model of the minimum things that go wrong. But the real world's always got some other things that are wrong. And you never get a clean set like this. You get something else in the real world. So those are the ones that I think are the ones that we'll eventually --

CHAIRMAN STETKAR: I'll give you examples of what Dennis talking about. If I look at the cutsets, there are large numbers of cutsets that contain things like instrument inverter fails.

Now, in the real world, instrument inverters sometimes fail clean, sometimes they fail dirty. When they fail dirty, you tend to get a lot of noise out in a bunch of stuff. You've modeled that effect as sometime at which the heat transfer coefficient reaches zero, because all of that stuff is out in what you're calling the secondary part of the

plant, which is replicated in all of these other cutsets.

But in the real world, noise happens. And it may not necessarily manifest itself as some variability in time at which a heat transfer coefficient goes to zero in a thermohydraulic model. And I think that's what Dennis is saying.

MEMBER BLEY: Well, it's kind of that. The other piece of what I'm saying is when we do the PRA we calculate the minimum set of plants. And that's a good set.

But if I ask you to calculate, at any point in time, what's the probability in that transient, if it should happen, that those and only those things are failed in the plant? It's pretty low. There's almost always things failed around the plant that could affect the heat transfer and some of these other things. So we'll never get a complete test. But on the stuff you've run, we think you haven't seen any failures.

MR. CHU: Yeah. I guess this type of issue has been pointed out to us when we were working on the previous NUREG/CR. In the way of, you know, non-minimal cutsets, that is first we truncate. So

those cutsets that were truncated never get sampled.

And then there were arguments that non-coherent, I mean, non-minimal cutsets may generate unique input that's going to be missing. But I guess the basic approach we have is we let the probability determine what gets sampled. That is, we work with 200 cutsets. We could, in general, extend to, say, 2,000 cutsets. Or even include some --

MEMBER BLEY: I don't care how far you go, you won't get them all.

MR. CHU: Right, right. You won't get them all. But if you did, that probability will determine what sampled those, you know, lower lying cutset mean never gets sampled. But it seems that's the nature of the problem. That is --

MEMBER BLEY: No, no. A specific non-minimal cutset is less likely. But the chance that there's something out there failed other than the things in your PRA model is pretty high. Because there are always things failed out there. And they can be things in the secondary that affect the transient.

So, you know, when we build a PRA model and say we're taking the most likely things, well,

they aren't quite the most likely, they're the most likely of the things that are important to the model we developed. But almost surely, there are other things that affect the progress of the scenario that aren't, that actually are sitting there.

So I think you can go ahead. But I'm just making that point. And I think I'm not surprised by your results, because I suspect, when you developed this instrument system, you tested it for many of the conditions that you expected it to work under.

CHAIRMAN STETKAR: Yeah. I mean, they're essentially constrained, I believe.

MEMBER BLEY: Yeah.

MR. COYNE: I think it's most important --

MEMBER BLEY: March ahead.

MR. COYNE: -- to put this into perspective. What they're trying to show is that I can use the PRA to generate a realistic operational profile for the testing. They're not trying to demonstrate that the PRA was complete. That's a whole other series of meetings to talk about the completeness of the PRA and whether it covers everything.

MEMBER BLEY: I'm not --

MR. COYNE: The idea was the PRA, can they use that as a tool to generate a realistic operational profile? And that's what they were trying to demonstrate, is that, given the PRA and the constraints associated with it, they could use that information to get some approximation of what a realistic operational profile in that system should be subjected to. So I'm not just doing the same test 10,000 times. I'm doing a realistic spectrum of tests for the software.

MEMBER BLEY: And I think that's a nice step forward.

MR. LI: Well, I completely like Mr. Bley's points. Are you too involved in research cost, accelerated software testing.

MEMBER BLEY: Yes.

MR. LI: Because software normally fails. If you look at the operational profile, you feel an integral part which is a rare event. And the one way to do that is we kind of skew, you know, the distribution. And if you follow the normal random sampling, you will not sample the point for the very remote event. But if we skew that distribution purposely, in the sample there, so we can, you know,

sample some of the rare events and challenge the software from that perspective.

MEMBER BLEY: You will reduce the chance that we get hit with one of things outside of the range we tested.

MR. LI: Exactly.

MEMBER BLEY: Exactly for --

MR. LI: But that purpose is, I'll call it for functional testing. But if we know the magnitude we skew that, then we can also calculate the failure probability. But if we put that back in the PRA sequence, there might be a very remote, ten to minus 15, then get cut off.

CHAIRMAN STETKAR: So go ahead with your presentation.

MR. VARUTTAMASENI: Okay. The only new information in this slide, I guess, is that the 10,000 RELAP5 input cases were generated using a script. So we basically have a master file that contains comments indicating which lines need to be changed to reflect the particular input that we want.

And then the script, just basically do a text search for the comment, and then we place the appropriate number of the input file with whatever

results that were obtained from the sampling.

MR. HECHT: The last point there says you also added noise. Is that noise that's in --

MR. VARUTTAMASENI: Oh, yes.

MR. HECHT: -- a single value or noise in the sense that Dennis was talking about where you had oscillations in the --

MR. VARUTTAMASENI: So the RELAP5 output well, you know, it's a deterministic output.

MR. HECHT: It's only a single value.

MR. VARUTTAMASENI: So it's just a single value, it's not, the LOCS system has three sensors that's used as input. So we basically sampled a unit from distribution, sampled the noise from the unit from distribution based on sensor accuracy and then add that to the single deterministic output from RELAP5 to generate the input values that the three sensors would see. So that is the noise that we are referring to here.

So the evaluation of the test results, I guess we have two separate criteria to evaluate whether the output on the testing is a success or failure. One is based on the channel response time. And the other is based on the expected window.

And the reason that we came up with two separate criteria is that, because of the difference in cycle time between LOCS and the test computer, it's hard to determine what values LOCS is actually responding to when it generates a trip. Because the cycle time of LOCS is not a constant 0.3 seconds. It's around 0.3 seconds, but it can vary.

And also because of the hysteresis where, you know, if you reach a trip set point and the threshold is exceeded, then the next cycle, if the actual input is slightly below the set point, the trip may not be reset because of the hysteresis that's built into the system.

So in that sense, it's very important for us to know what values LOCS is actually responding to. And that's not easy to do not knowing the exact cycle time of LOCS. So we came up with two different criteria to evaluate the results. And they give us a somewhat different outcome.

So the first is the channel response time. This is the specification that INL has. It's basically the time from the occurrence, the trip condition at the sensor to the time that the LOCS protection system outputs the trip state. So it

includes the delay of the DPU and everything in between.

And the flow temperature and pressure channels have different channel response time. Now we, in using this channel response time criteria, we are assuming that the trip condition exists for at least three consecutive records.

And that is because if, you know, if the set point is exceeded in only one record, then there's about one-third chance that LOCS will actually see that record.

So our criterion is that once a trip set point is reached, then we add it in the channel response time, say 0.78 seconds would correspond to about seven input records. So we added that to the first occurrence of the trip condition. And if the actual trip occurred within this window, then we call it a success. If the trip occurred after this window, then we call it a delayed trip.

The second criterion that we use is based on the observation that sometimes a trip condition exists for only one record. And in that case, if we were to use the channel response time criterion, then that one record will not be counted as a valid trip.

But in reality, LOCS sometimes did respond to that trip. And in order to capture that sometimes, we came up with the trip window criterion. So the lower bound for our window is the occurrence, the first occurrence of two-out-of-three channels being in a trip state, even if we lost one record. And the upper bound for the window is based on the cycle time consideration.

This slide presents the result using the trip window criterion. So we see that there are 27 cases where we saw that the trip was delayed. Twenty-six of those cases have a delay less than 0.5 seconds. The largest delay that we saw was 1.2 seconds.

And the table on the right shows cases with early trips. So these are the trips that occur before any of the channels reach the trip set point. And we --

MR. HECHT: Is that the same thing as the spurious trip?

MR. VARUTTAMASENI: Well, it could be a spurious trip. But we actually manually went through some of those cases. And we saw that the system was in a trip state for just one record. So that wasn't caught in the criterion that we were using.

And also some of the channel values came close to the trip set point. So if you have, you know, a trip set point at five, ten degrees Fahrenheit, then in some of these cases the values come to within 0.2 or 0.1 degrees.

And we thought that maybe noise in the system or some channel accuracy causes might, you know, might be sufficient to push that to the natural -- so the system will interpret that as a natural trip, that the value has actually been exceeded.

So this slide is basically -- so the noise I was talking about is probably an important part of the consideration, because the RELAP5 values that we use as an input is actually a digital system, a digital signal. And that gets converted to analog signal that is then sent to the analog input module which is converted to a digital signal which LOCS processes.

So there are multiple conversion steps. And those steps can definitely introduce noise that can push cases where the ratings are very close to the trip threshold that actually causes a trip. So that is a big part of why we see what we are seeing.

MEMBER BLEY: What good does it do to use

white noise in the digital format?

MR. VARUTTAMASENI: Well, the --

MEMBER BLEY: I wouldn't have expected, I would have expected an output in the analog side more than on the digital side. So I --

MR. VARUTTAMASENI: The noise was added to the RELAP output. So that's used to simulate the actual noise in the sensor. The sensor has a set accuracy value. And so you have three sensors that are actually looking at some actual temperature. The output from the sensors are expected to be different. So we added noise to the deterministic output, to the actual temperature to simulate.

MEMBER BLEY: All right.

MR. VARUTTAMASENI: So this slide shows some of the anomalies that we observed. Then you talk about the one failure to trip in 10,000 cases, there were a few cases where the LOCS output actually changed very fast within, say, 0.1 seconds. And I guess we called that anomalies because LOCS is expected to have a cycle time to about 0.3 seconds.

So each cycle should last about three records. But for some cases, we actually saw that LOCS was responding to signals much faster than 0.3

seconds. Sometimes it actually changed every 0.1 second. But that could be caused by the fact that LOCS cycle time is not constant at 0.3. It could be as fast as 0.1 seconds.

And there were also some cases where the three digital output modules don't actually show the same trip status. So in ideal cases, we expect all three output modules to show the same trip status. But in 398 cases, those outputs were different.

MR. HECHT: Would that be an artifact of LabVIEW not collecting the inputs at --

MEMBER BLEY: I couldn't hear you. I'm sorry.

MR. HECHT: Could that be an artifact of LabVIEW not collecting the inputs at the same time?

MR. KASER: I assume it will be a timing issue of some sort between the yellow CSN of you doing that, yes.

MR. HECHT: Because LabVIEW can only take one of those at a time.

MR. KASER: It's cycling in one time, and the yellow CS is cycling in another time. It turned out that I didn't bring it with me. I ginned up kind of a layout of what the possibilities might be, you

know. And it covered everything under the sun, you know, up to about 0.3 seconds, at which time everything works.

MEMBER BLEY: Can you back up? I don't see any anomalous cases where one of the channels never got a trip signal, and only redundancy got you the trip signals for the others. Is that true? You didn't list anything like that?

MR. VARUTTAMASENI: Only one channel --

MEMBER BLEY: We have three channels, right?

CHAIRMAN STETKAR: Two out of three.

MEMBER BLEY: And you need two out of three to generate a real trip.

(Simultaneous speaking)

MR. VARUTTAMASENI: Right.

MEMBER BLEY: Were there cases where you only got two and the third one never came in?

MR. VARUTTAMASENI: Yes.

MEMBER BLEY: Oh, there were?

MR. VARUTTAMASENI: Yes.

MEMBER BLEY: Do you know why?

MR. VARUTTAMASENI: So that's included in the 398 cases where I said that --

MEMBER BLEY: Yeah, when I read that I just assumed one of them was a little late compared to the others. But late was like never.

MR. KASER: Everything on the simulator, if you'll read those scram signals back, is in a sequential fashion, okay. And so when I say it's sequential fashion, I mean the first channel scram is read. The second and the third, we could have missed them.

CHAIRMAN STETKAR: But were there cases where the third one came in like never?

MR. KASER: I don't believe so.

MR. VARUTTAMASENI: Oh, no. Oh, never. I guess there was --

MR. KASER: Yeah.

MR. VARUTTAMASENI: There were cases where the third one was delayed but I guess never, we didn't see any.

MEMBER BLEY: Okay. That's a different answer. I liked the other answer.

(Laughter)

MEMBER SCHULTZ: You were looking for it and didn't see it.

MR. VARUTTAMASENI: We did, right.

MEMBER SCHULTZ: Okay.

MR. HECHT: I guess what that also means is that obviously RELAP5 didn't cover the I&C system, right? So in other words, the failure scenarios, if you will, the input scenarios might have included sensors, because you could emulate sensor failures with the RELAP input but didn't include actual failures within the hardware, of the DPU hardware or the output. Is that correct?

CHAIRMAN STETKAR: What he's saying, there were always input signals from all three channels.

MR. KASER: And output, yeah.

MR. HECHT: So in that regard, I just wanted to say that there was another artifact or modeling artifact that wasn't considered. And that was the Rosemount transmitter, which is something that I discussed earlier because of the digital aspects of that device as well over the network. And I assume that that would be true in most modern instrumentation systems as well, Rosemount's again. And it's not only in Rosemount, it could be any smart --

MEMBER BLEY: Most of the others have Rosemount guts in them.

MR. VARUTTAMASENI: So this slide shows, we ran several cases multiple times just to test the reproducibility of the results. And the failure to trip case. And so we ran that 100 times. And the trip was successful in all 100 times. So we were not able to reproduce that failure to trip case. You also will notice that sometimes the trip window is fairly large. And that is because for some cases we have situations --

MEMBER BLEY: Is that seconds, or what do those numbers mean?

MR. VARUTTAMASENI: These are records numbers, and they correspond to 0.1 seconds. So to translate these numbers to seconds, I guess you multiply it by 0.1.

MEMBER BLEY: Okay.

MR. VARUTTAMASENI: So for the --

MEMBER BLEY: I got 40 seconds.

MR. VARUTTAMASENI: For the first case, eight out of ten times LOCS tripped in 0.5 seconds. And in two cases, the trip was actually at 40 seconds. And we manually went in and looked at the input. And it turns out that, in that case, in the first few seconds the trip actually, trip set point was ranged

for one record.

And so that means that in two out of ten times LOCS didn't see that single trip record. So it actually tripped at a much later time, at 40 seconds where the trip was sustained, that the trip condition was sustained and it's a lot of --

MEMBER BLEY: Oh, I'm sorry. The last column then isn't the window between two and 417. It's at two you've got a trip, should have had a trip signal. And then at 417 and later you would have a trip signal.

MR. VARUTTAMASENI: Right. Using 417 as for our sustained trip, two is the first occurrence of a single record.

MEMBER BLEY: So it's not a window. It's two different occurrences, and the second one keeps going?

MR. VARUTTAMASENI: Yes. You can say that.

MEMBER BLEY: And that's true for the other sets we see there?

MR. VARUTTAMASENI: Yes. And this is the slide that contains the information for how we calculated the probability of failure on demand. So

we assume a bigger distribution which, you know, if you set the two bigger parameters, A and B, to one, then you effectively have a uniform distribution. So you observe --

MEMBER BLEY: I don't know my distributions well enough, but that is really true. So it's uniform between what and what?

PARTICIPANT: Zero and one.

MEMBER BLEY: Zero and one.

MR. VARUTTAMASENI: So if you observe X failures in end tests, then the posterior distribution becomes what's given here. And we just plugged a number in. We didn't consider a delayed trip to be a failure. So we say zero failure in 10,000 cases, not huge concern of posterior, a mean of the posterior distribution of one times ten to the minus four.

(Pause)

MR. VARUTTAMASENI: And I guess we, this is the last slide. And I want to talk about some of the limitations and challenges that we saw. I think Louis talked a little bit about the fact that if you have non-minimal cutsets, or we have events that are not covered in the PRA, then obviously they're not going to be in the samples and will not be tested.

And so the question is, you know, how complete are the cutsets? And we can definitely add, if we identify scenarios which are not in the cutsets, we can definitely add that in to the list, you know, with some appropriate frequency. But the method will still be the same.

And also the possibility of having transient hardware failure to cause some of the observed delays in the trip was discussed a little bit. And I guess the testing method itself cannot distinguish between software failure and the transient hardware failure. Because we are only looking at the failure of the actual system to generate a trip signal. So it's hard to tell whether that's from software or just from transient hardware failure.

And for all our tests, we assumed that the initial condition is the full power. And, you know, if needed, we can always have a distribution for the initial condition and use that as the starting point for the simulation.

Another issue is that the actual LOCS system has many input values. I guess 14 are important, corresponds to parameters that are important to safety. But the other inputs are dummy

values we used.

And we hope that by doing that, we didn't, you know, change the load that system sees in the test system compared to the actual LOCS system. But, you know, that could cause the difference in CPU load and may cause some delays. But that can always be changed in reruns of tests that we may do. Okay. So --

MR. HECHT: I just wanted to add that there's one limitation that you didn't mention that we did talk about before. And that was that you didn't consider internal failures of the DPU itself. And that would be either hardware or software, right? We spoke about that in several contexts.

(Off microphone discussion)

MR. HECHT: By software I mean the non-application part of the system, the operating system.

MR. VARUTTAMASENI: Right. So in possible --

MR. HECHT: -- developed stuff.

MR. LI: By the operating system, or you mean the test computer --

MR. HECHT: Oh, no.

MR. LI: -- or the LOCS --

MR. HECHT: I mean the operating system of

the DPU, and the device drivers and the Rosemount transmitter software.

MR. CHU: I would say like the Rosemount transmitter is just outside the boundary of this business that we have. But in terms of not fully simulating the control part of the DPU function, that's the, you know, practical limitations in the sense that I think the real system has many more IO modules. And if we want to, we'll listen to, really reproduce the system that is installed. You need to pull in many more IO modules which cost money of trying to put in place.

MR. HECHT: Well, I was talking about something separately, even within the, you know, restricted system that you had, one of the, you know, operating systems do slow down. They do crash. Hardware does fail.

And we discussed before that it was assumed that the system was, that the system execution platform was perfect. And that's okay, but I think you should have stated that in the --

MR. CHU: In the limitation --

MR. HECHT: -- limitation.

MR. CHU: -- of the work. Yes, I agree

with that. But I also want to point out something that was discussed in the morning in terms of, you know, reliability modeling of digital systems. Three or four years ago now we did the modeling of the digital feedwater control system, and I think that ACRS likes it.

And it has some, you know, it requires some more detailed modeling. But it has that capability of, you know, you posture your hardware failure, and you actually run, effectively, the actual software to propagate the failure effect. To some extent, it actually captures the interaction between software and hardware. So that's kind of another way of looking at the advantage of that method and in capturing software and hardware interaction.

MEMBER BLEY: And maybe you should look at extending that in the future here. I remember your presentation of that, but I don't remember the details of that DSCS system that you've been --

MR. CHU: Right. For example, find a real protection system. But Kevin had pointed out in the model that, you know, there are problems getting the vendor or utility to cooperate in providing that information. But in general, I think that method is

the favored method.

And now think of the statistical testing, although there are limitations of the demonstrated method, we can argue that some of the things we did are not realistic. But in general, that's not a limitation of the record, which includes those failures, to do a better job. But then how much more is proven can you afford to do? But it's more of a strain under resources available.

In addition, I guess, I want to mention that something special this morning that relates to the objective of PRA. So I'd like to give my opinion. And it's, it represents assessment. So in a sense, PRA guys' role is to assess a system so that we can quantify its reliability so that we can put it in our model.

And it is not our objective, main objective, to find software bugs. That is, in doing our work, say, statistical testing, we may stumble upon, you know, some problems. Or in general, when we develop a PRA model, we may happen to discover some weaknesses of the plant.

But that's the side benefit of doing PRA. The key thing the PRA does is assessing, come up with

a reasonably probabilistic model to model the plant, or the system or the software.

CHAIRMAN STETKAR: That's your opinion. There are others of us who have different opinions about the usefulness of PRA. Nobody thought about reactor coolant pump seal LOCAs until we modeled them in PRAs. That wasn't something assessing the safety of the plant. It was systematically looking for problems.

MEMBER BLEY: I can go back before that. WASH 1400 emergency auxiliary feedwater systems were absolutely non-safety and not under any consideration. They turned out to be very important. And that really changed the direction.

I think one thing, John and I were mumbling, your last bullet, if you look at a PRA of either an older plant that's had PRA done and has been modified to reduce the risk to some extent, or you look at a new plant that was designed to have PRA being done and tried to get rid of the big lumps, you find lots and lots of cutsets or contributors to get to 90 percent. You've got a cart-load of them, because there aren't any big contributors. And when you have that problem you were talking about, of how

much can you afford of this to do, it becomes improbable.

CHAIRMAN STETKAR: And buckets of those tend to be large numbers of things like support system transients. And, you know, you don't have the large LOCA that you can model necessarily cleanly, either in terms of your RELAP models.

MEMBER BLEY: Things that aren't even built in to them yet. But you might find ways to, like you did --

CHAIRMAN STETKAR: Yeah.

MEMBER BLEY: -- around that for some things. Your report calls itself a draft. Is it essentially done, or have you been evolving the product here? And do we expect major changes in that report?

MR. LI: The report coming today is a draft. So --

MEMBER BLEY: I couldn't --

MR. LI: The report is a draft report for now.

MEMBER BLEY: Yes.

MR. LI: So we're going to make it public to collect public comments and then to make it a NUREG

report.

MEMBER BLEY: So you're pretty comfortable with it right now, if you're going to go for public comment?

MR. LI: Right, right.

MEMBER BLEY: Okay. You're not envisioning any changes unless something comes in?

MR. LI: Nothing major.

MEMBER BLEY: Okay. That's what I was asking. Thank you.

CHAIRMAN STETKAR: Thank you. A couple of logistics issues here. First of all, do any of the members have any other questions --

MEMBER BROWN: Yeah. I have one question because I --

CHAIRMAN STETKAR: Good.

MEMBER BROWN: -- wanted to make sure I understood, since I'm not a PRA person or anything else on this last round on this -- I saved this to the end because I didn't want to interrupt your flow since you were on a roll.

The statistical test method, and I'm looking back at your, again, recalibrating myself on figures and then how you tried to verify whatever

other analysis you were doing that did -- the way I understood it, you did the RELAP to generate test cases for the various accident conditions or other type things you're concerned about. You had, I don't know, over 13, I remember, scenarios.

MR. CHU: I was going to say failure models.

MEMBER BROWN: Okay. Well, all right, whatever they were for the system itself, the ATRs, Loop 2A, or whatever it is, the system operationally. And then you generate those test cases in what are the profiles of the transients that you get out of them. And then you put it into this host computer as models of the actual reactor performance, then fed them up. Did you feed them right into the LOCS actual hardware and software?

MR. CHU: Yes.

MEMBER BROWN: So you disconnected physically from the reactor stuff --

MR. CHU: No. What's done in a lab setting, not the system that's operating at the plant, but I think --

MEMBER BROWN: Is there an identical LOCS system set up?

MEMBER SCHULTZ: Yes.

MEMBER BROWN: Same one that's in the plant? That's fine.

MR. MARTS: Pretty close.

MEMBER BROWN: Well, I'm not going to argue about --

MR. MARTS: But, you know, just to make sure --

MEMBER BROWN: -- not going to argue pretty close or not.

MR. MARTS: Yeah. You know, same operating system --

MEMBER BROWN: But we've got the operating system, the software and then, so you actually had the digital, the software-based digital representations of the plant.

MR. MARTS: Yes.

MEMBER BROWN: And it converted those signals to, I don't know if we talked about it, conversion back and forth.

MR. MARTS: Yeah, yeah.

MEMBER BROWN: So you need it to go, how did you feed into the LOCS system, via analog equivalent or digital equivalent?

MR. MARTS: Analog.

MEMBER BROWN: So you took the RELAP digital, converted it to analog, then went into the, whatever the inputs, IO, to converge analog to digital converter system and then to the output. And then you ran your test cases, and you develop all the statistical performance of the actual software performance of the LOCS system. Is that correct?

MR. MARTS: Yes.

MEMBER BROWN: To restore the system? Okay. You kept talking about cutsets. Where do those come in? I relate to all the other stuff. The plant transient that you do, and then the cutsets, who gives a rat's if you've got all this data that now tells you how the thing performs and you can say, okay, I can develop, because it's passed all the tests, it always generated trips or didn't. You can get a statistical idea of how reliable that software is.

Of course, there's a lot of stuff that's not mixed into this. I'm very familiar with that approach to testing operational software as well as the housekeeping stuff that has to run the whole operating system itself.

Where does the PRA come into this? This

looks like nice kept stuff to see if it breaks, the make them and break them type approach to doing this?

MR. CHU: In the PRA, they model, they develop a --

MEMBER BROWN: But that's not in this thing. This is test data. The PRA is not in the LOCS thing. The PRA is separate, a separate analysis, right?

MR. CHU: Yes. But it identifies the scenarios or the test cases that need to be run. That is the PRA --

MEMBER BROWN: But that's of the overall ATR plant design, right, or the reactor design, or the reactor, or thermohydraulic setup, or the transients that you did or what have you, valves failing, this not operating, a pump stopping, et cetera. Is that where the PRA came into this? So all the PRA was used for was to develop then the cases that you ran against the software?

MR. CHU: Right.

MEMBER BROWN: Okay. All right. Now --

MR. CHU: Right.

MEMBER BROWN: Okay. Now, can I ask one other question since I'm, again, not a Bayesian guy?

Just between this, this looks like real life. And when we discussed the Bayesian Belief Network routine, that almost sounded like an abstract, pluck this stuff out of the ether and evaluate and analyze, but there's no real connection to the real world. It's just this. And, you know, in other words, you're analyzing and developing models based on what you think the thing looks like.

MR. CHU: Yeah, I kind of --

MEMBER BROWN: They're divorced from real data.

MR. CHU: The VDM model is much more abstract, while --

MEMBER BROWN: Okay. You answered my question. We don't need, I just wanted to make sure I understood the difference. You had one question from Myron who made a comment a minute ago about how you thought the CPU or whatever you called it, the processing unit, slows down with time.

And I recognize that. In our little commercial PC world, as you build up all kinds of garbage and things can interfere, it's an interrupted rhythm system. You never know what all types of stuff is going to come in and keep it going.

But in a dedicated system, or you've got a dedicated one set of applications, one set of routines you always go through, I wouldn't imagine that your system would slow down and give you really inconsistent processing time.

MR. CHU: That is just --

MR. HECHT: I wasn't thinking permanent slowdown. Sometimes you get a transient load, for whatever reason, that you may not have anticipated. But real time systems aren't always hard real time.

MEMBER BROWN: Yeah. I tested 15 different protection systems, and time responses, and everything else and never experienced, in over 22 years, and never experienced any processing slow downs. We had variability depending on when you picked up a sample. But you never had any functional, and I was trying to relate that experience to your comment, because I'm not familiar, you know --

MR. HECHT: Okay, I'll --

MEMBER BROWN: -- with the commercial world.

MR. MARTS: On our particular hardware, since it's not a protective system, it can be, if an operator calls up a separate screen that has a lot of

data for that particular --

MEMBER BROWN: Okay. So the operator can influence the processing.

MR. MARTS: Yes.

MEMBER BROWN: Because that didn't happen in my, it just spit out data. And we had a --

MR. MARTS: Yeah, and so --

MEMBER BROWN: -- system that did that.

MR. MARTS: Myron's suggestion --

MEMBER BROWN: I got it.

MR. MARTS: -- is valid for our particular --

MEMBER BROWN: I got it. Thank you very much. That's --

MR. MARTS: -- application.

MEMBER BROWN: I'm finished now. Thank you, John.

CHAIRMAN STETKAR: Thank you. Anything else for the folks up front? If not, what I'm going to do is, because we've had several presentations by the staff in Talk Crafters, I'm going to ask for public comments at the moment to see if we have any comments relating to what we've heard to this point in our meeting.

First of all, I'll ask anybody in the room have any comments? If not, we have the bridge line open. And I hear somebody coughing out there. So I know the bridge line is open. Is there any member of the public on the bridge line who'd like to make any comments from what we've covered thus far?

MR. ENZINNA: Yes, sir.

CHAIRMAN STETKAR: Okay. Identify yourself please.

MR. ENZINNA: I am Bob Enzinna at AREVA.

CHAIRMAN STETKAR: Okay.

MR. ENZINNA: And you spell that E-N-Z-I-N-N-A. I just want to say for the record that we have done several PRA studies, digital I&C systems. We have customers around the world that have our systems, including one in the U.S. at an operating plant. And I wanted to say -- there's a lot of background noise.

MEMBER BLEY: Not here, we hear you fine.

CHAIRMAN STETKAR: Not here. We hear you fine.

MR. ENZINNA: Okay. I want to say that, just because the I&C system is complex, you know, doesn't mean that methodology for quantifying the reliability has to be complex. And I say that

because, in the PRA, the model of the I&C is resolved at the functional level of the actuated equipment, you know, the valves, for example, that you guys have been talking about. It fails to open, it fails to close, it's very -- and so you can calculate the I&C contribution to that failure probability.

But in honesty, that probability isn't particularly important. I mean, being able to precisely quantify that probability isn't particularly important. Because the PRA's not sensitive to that. What the PRA is sensitive to is identifying the dependencies.

CHAIRMAN STETKAR: Identifying what?

MR. ENZINNA: The dependencies, the digital systems are multi-function devices. Because you've got CPUs, you've got IO modules that are multiple channels.

A typical system that we provide for a protection system has 30 different computers in it, divided by function, by diversity, by high division. And so what will drive the PRA result is the assumptions that are made about the dependencies and the common cause failure.

And to understand that, what you need to

study is the failure mode taxonomy. And hand-in-hand with that are the common cause failure defenses that are built into the system.

So it's not enough just to look at preventing the defects. You have to look at features in the system that prevent failure triggers, features to prevent propagation between different divisions, and computers and redundancies.

And so if you don't understand the taxonomy of the failures and the common cause failure defenses, but you're very specific to the system and the vendor, then the tendency is to be too conservative. And you end up with hypothetical failure modes like all the computers in the plant fail. And those kind of conservatisms will drive the result and aren't productive for anybody.

CHAIRMAN STETKAR: Thank you.

MR. ENZINNA: -- I have to say.

CHAIRMAN STETKAR: Great. Thank you very, very much. Is there anyone else out there who has any comments to make?

(No audible response)

CHAIRMAN STETKAR: If not, we'll re-close the bridge line. You're still welcome to listen in.

We're here for the duration.

What I'd like to do now, Ming, unfortunately I'm going to take executive privilege here. I've looked through the presentation on the taxonomy, kind of interesting. But I do want to make sure we have enough time for EPRI. So we are going to take a break now until 3:25 and come back with EPRI's presentation.

(Whereupon, the above-entitled matter went off the record at 3:12 p.m. and resumed at 3:27 p.m.)

CHAIRMAN STETKAR: Let's come back in session. I shorted EPRI on now 11 minutes of their time, I don't want to short them anymore so let's hear from EPRI. Ray, I don't know whether you or --

MR. TOROK: Very good, yes.

CHAIRMAN STETKAR: There you go.

MR. TOROK: I'm going to start out here. My name is Ray Torok, I'm form EPRI. And for starters I want to thank you guys for letting us come back to talk to you and for giving us a lot of time on the agenda. I know how tough it is to get time on your agenda.

So we're back this time to really pick up where we left off last time we were here, in September

of last year.

With me here I got, what I call the project team. These are the principle investigators on most of the work, on maybe all the work we're going to talk about today.

So I got Bruce Geddes here and Dave Blanchard. And of course with them here there is someone here to answer the tough questions.

So we're going to be talking about four areas here listed here. And I'll talk about each of them briefly I guess. Let me move on.

All of these things have something to do with failure modes and digital, and now looking at this I've introduced a new term here, digital failure mode. What in the world is a digital failure mode, right?

But we want to update you on where we're going and what we've done and a number of areas related to that. We talked about software failures and whether or not software really fails and all that. And that's certainly an ongoing discussion.

And for our purposes we've used the term software failure, we understand that the software really does exactly what the design tells it to do.

For us the digital failure is a little different in that we treat the digital system as hardware and software together. And the digital failure to us means a failure of that system that is systematical deterministic.

So because a deterministic systematic failure can come certainly from a software bug, but it can also come from a problem in the architecture, the hardware architecture of the system. So we tried to include it all.

We also often use the term misbehavior or unintended behavior. Because for us a failure, a software failure or digital failure includes those things. And in fact those are some of the most interesting ones to go after as opposed to the kind where something actually did fail.

So our topics today are, the first one there, digital failure modes. And it's, let's see, we'll extend the conversation from what we talked about last September, where we got into it in terms of a hazard analysis discussion, and a number of questions came up regarding the way we treat failure modes and so on and we basically ran out of time before we got to the end.

There was questions about what we looked at in terms of taxonomy of failure modes and mechanisms for digital components and sub-components at low levels. So Bruce is going to take up that discussion.

And obviously we're going to talk about modeling in PRA. And Dave of course is our, if I got the term right, I'm not sure I know how to use this, but he's our big number tricks guy for PRA. So he'll tell you what we've been doing there.

And that's something we've been working on for many years. This isn't just the last couple years. I think Dave's been working with us on this for what, ten years now or thereabouts, doing various kinds of analysis and scoping analysis early on. And we maybe in a sense did this backwards.

We looked at tying PRA to hot-button issues of the day to understand what we could in terms of risk insights. And we learned a lot.

We thought about how you can deal with digital systems in PRA, what kinds of risk insights you can generate. And after we did all that we came back and put together a methodology that is intended to be applicable for utility engineers.

And that is the report that was sent to you recently, 1025278. And Dave is going to be focusing on that.

In terms of the next the thing, techniques for failure prevention mitigation, that's really about an ongoing project we have where the primary focus is on susceptibility evaluation for digital system failures, including common-cause failure. And so we're talking about susceptibility and ways to deal with potential failures. So that's what that one=s about.

And then, as I said, last time here we talked about hazard analysis because that was a document we had just published and so, and that was the latest and greatest.

Now coming out of that, our advisors told us, this is all well and fine but we need to go do some demonstrations to show that this method really does what we think it does and that sort of thing.

So we do have a demonstration project in play right now with Arizona public service at the Palo Verde Plant to apply to a real upgrade that they're working on. And we'll talk about that.

That's an ongoing project right now. We

don't have a lot in the way of lessons learned, so there we'll mostly give you a status on what we're doing and how we're applying the hazard analysis methods that we talked about last time we were here.

Now a theme throughout this that I think is pretty important is we want to show you that we really are applying the principles of mechanisms modes and effects consistently throughout. For failure modes, for PRA, for hazard analysis, the while thing.

And this gets into that discussion of levels of interest that's come up today and then we talked about last time and so on. So expect to see more on that.

Now let's see, moving right along. Okay, so our so-called problem statement goes back to SECY 93-087 where they're talking about digital failures, including common-cause, you know, that result in unacceptable behaviors or loss of critical systems functions.

And there's been a lot done since then, since 1993. And we want to emphasize that.

We feel that we have a much improved understanding of digital system failure modes and ways you can protect against them. I think it's, one way

to characterize 90-087 is that it's more or less a black box approach to handling digital systems.

At the time there was a lot awareness that software can do all kinds of crazy things and we need to be really careful with it. And I think was what reflected out knowledge at the time.

Now since then we've come a long way. As I said, we understand failure modes and mechanisms better and we'll talk more about those.

We've also spent a fair amount of time looking at application of PRA to assess risk insights and so on and identify potential vulnerabilities. And we've shown, I think, where it can be very useful. That's all good stuff.

And of course you heard about hazard analysis last time where we used that to identify potential vulnerabilities and talked about ways to address them.

Now I wanted to say that our perspective on all this, our EPRI perspective let's say, is a bit different from what you've heard about earlier today in that our audience, our customers, are typically utility engineers. And when they come to us it's with a problem that relates to some real life issues that

they have going on.

So for example, when some utility engineers in with stories like, hey, we put in a digital feedwater system last year, it worked great for awhile and then it burped and tripped the plant and now everybody's upset. And we went backed and looked and discovered that it had a failure mode that we didn't pick out when we did the failure modes and effects analysis before we put this in, help us find a better way to do this.

And that's what drove us into this whole hazard analysis arena. And sure enough, we discovered along the way that there probably are better ways to do hazard analysis that can see things that traditional detailed FMEA can't see.

And as part of that in fact, Dave did some PRA analysis, on a real system, and called attention to certain potential multiple failure cases that bubble to the top in PRA and say, hey, you really need to look at these. And sure enough, it was one of those that happened in the real plant, it wasn't something that the FMEA could see.

So we see benefit. And I think we've demonstrated benefit in these things.

Now I think we're at the point, and we're sort of trying to make the case or the point now where we understand the failure modes and how to apply them at the correct level of interest and so on so that we can get beyond the discussion of, what are the failure modes, and get more into the discussion of, what is it we should be doing about them. And in that sense we would be talking applying the knowledge we gained and so on in real upgrades.

And of course, as I said, from the EPRI perspective that's more or less does a better job of answering the questions that we get from our utility members.

Like hey, we're putting this digital stuff into the plant now, we have to because our old analog equipment is worn out, we can't get parts for it anymore and we have to do something. And oh, by the way, we have to update our PRA to reflect that, help us do that now with the tools we have now. So that's more the kind of focus we've had.

As it stands now, a lot of work is ongoing still by the industry and the utilities to update their processes to doing these things. And then we're supporting with guidance, like what we're going to

talk about today, and later on, you know, tech transfer mechanisms for framing and industry workshops. And that's our thing, that's what we do.

Let's see. So yes, I think that gets us to really the first topic here which is the digital system failure modes to update. And at this point I'll turn it over to Bruce Geddes whose our principle investigator in that area.

MR. GEDDES: Yes, thank you. Good afternoon. The key points in this failure modes discussion, I'm sorry, we're going to cover key points, a little bit of history, levels of interest. There was some of that discussion this morning, we'll take another look at that.

Various methods that are in the EPRI hazard analysis guideline, we'll touch on that very briefly. And then we'll discuss an example with a functional FMEA as a top-down method, not a bottom-up, not the traditional design FMEA, but you'll see guide words and tricky phrases in there that have been pulled out and are of some interest.

And then last year, we ran out of time, but during a break, Mr. Bley, I think you brought up the taxonomy of failure modes from the back of the

appendix in the EPRI guideline?

MEMBER BLEY: It's likely.

MR. GEDDES: I think you caught us during a break and you expressed a lot of interest in that so we have a couple slides on that in here.

MEMBER BLEY: Okay.

MR. GEDDES: And then some conclusions from this presentation. So again, we want to extend the discussion, like Ray mentioned from the 2013 presentation, and we want to touch again on failure mechanisms, modes and effects at various levels of interest, top-down, bottom-up.

We want to make the point that our failure mode treatment is consistent with PRA principles. Dave and I will probably have a little interplay on that in this presentation. We also want to get the appropriate level of interest.

For some people a bottom-up, you know, approach is of interest to them. People who design, for example, digital platform components controllers, IO modules, they're in the game of selling reliable equipment. So they're going to take a bottom-up approach.

A team of detailed FMEAs that get down to

the board level and the component piece part level. But that's not necessarily of interest, perhaps, in the PRA. So we're targeting different levels of interest and it's important to take that point of view.

Of course ultimately what we're trying to assess is protection against undesired effects at the higher levels. All the discussion about, is the valve closing on demand or opening on demand or is it spuriously misbehaving. That's the, maybe the appropriate level of interest in some contexts.

So to bring out the historical perspective, you all wrote a letter back in 2008, digital I&C may introduce new failure modes that are not well understood. We think we've come a long way since then.

We having taken a look at NUREG 492, and I think this quote has been used a couple times today. Failure mechanisms produce failure modes which in turn have effects on plant system operation. That's the key.

So we discussed this work. The EPRI report is 3002000509. We brought this last year. We started down the path of presenting its results to

this Subcommittee, and we want to extend that again on this visit to talk about how it provides a framework for identifying mechanisms, modes and effects at the appropriate levels of interest.

So I think you've seen this slide before, it's sort of a hierarchy of functional and physical representations of the plant. At the top you've got plant functions like make steam and plant systems that do those things, main turbine, main generator feedwater.

In a plant system we can break that down into a collection of components like pumps and valves. And then we influence those plant components, or control those plant components, with digital I&C technology.

So we might have a digital feedwater system or a feed pump turbine speed control system in the plant. And then of course a digital system is made up of digital components like controllers, communication modules, item modules.

You can see the list. And then down inside those boxes we've got CPUs, A/D converters, D/A converters, RAM, ROM and then software.

So that 2008 letter focused on issues like

task crash and task hang. And we feel like that letter was focused down at the device level where the software is resident in a given component.

But where's the effect of interest if the task crashes in a digital controller, what happens to the pumps and valves that are being influenced by that controller? So that's one of our research questions and we feel like this work has helped us, you know, identify where that effective interest should be.

But the effect, of course, is a function of failure modes that, and hazards, and hazards also include misbehaviors, not just hard, functional failures. But also misbehaviors due to perhaps software design defects.

And then how do we manage the hazard.

MR. HECHT: Excuse me, Bruce?

MR. GEDDES: Yes.

MR. HECHT: Isn't a misbehavior just an incorrect result?

MR. GEDDES: Yes.

CHAIRMAN STETKAR: Myron, get closer to the microphone so that it picks it up.

MR. HECHT: Isn't an incorrect fail -- I mean isn't a misbehavior just an incorrect result?

MR. GEDDES: Yes, that's one way to put it.

MR. BLANCHARD: Well I think we can extend that. Sometimes it's designed in behavior of the plant that you didn't expect that's adverse to safety. Or adverse to generation.

It might not be a failure or misbehavior at all, but it's not the result you wanted.

MR. HECHT: Well --

MR. BLANCHARD: It's the way the plant system was designed.

MR. TOROK: Yes, to expand on that. There have been cases where all the components and sub-components did exactly what they designed to do, but at high level the system did a wrong thing because of interactions and what have you.

And as a response, typically, a response to unanticipated conditions, right? As opposed to something broke.

MR. HECHT: Well that's the same thing, isn't it?

PARTICIPANT: Right.

MR. TOROK: And the reason we got into that discussion was because if you look at traditional

hazard analysis methods, like FMEA, the first assumption is, this failed, that failed. And it turned out that it was very well suited for finding these kinds of misbehaviors were nothing really failed.

And some of the hazard analysis methods are really pretty good at that. The STPA systems theoretic process analysis, for example, is really pretty well suited to go after those kind of things. So that's why we started talking about it that way.

MR. GEDDES: But I think you're question is, what do we mean by misbehavior and that's essentially it. An unexpected or unanticipated result.

MR. TOROK: Or undesired behavior under abnormal conditions. Usually.

MR. HECHT: Okay.

MR. TOROK: System didn't do what the designer wanted it to do.

MR. HECHT: Okay, I guess the FMEA is a bottom-up analysis where you have whatever it is you have and then you consider one failure at a time. Some of the other things that you were talking about are things that you might call emergent behaviors.

When you integrate systems of systems.

MR. TOROK: Yes.

MR. HECHT: Which is, I guess, something else that one might need to do. But that's not a top-down, that's not a bottom-up analysis.

MR. GEDDES: Correct.

MR. HECHT: It's part of a hazard analysis, but it's not --

MR. GEDDES: Bigger. Yes, this guidance has six different methods. One of them is the traditional bottom-up design FMEA.

We're not suggesting that a bottom-up design FMEA can identify those misbehaviors. We're suggesting that maybe a combination of methods helps you identify those single point vulnerabilities that a design FMEA can do.

But there are other problems or issues. Like these misbehaviors that other methods go after. We're trying to cover the spectrum with this guidance. Did that answer your question?

MR. HECHT: Kind of. I guess it's a terminology issue and that can get rather emotional and we don't need to do that here.

MR. GEDDES: Okay. So the last point I

wanted to make, on this slide, is the fundamental questions. How do you manage the hazard?

If you can identify it, how do you mitigate or manage the hazard? And the example we like to use in discussions like this, consider a fuel handling machine.

If there are mechanical stops that limit the motion of the machine, then perhaps if the software misbehaves, the mechanical limits will still keep the fuel within a certain envelope. So maybe it doesn't matter, I'm over-simplifying the point, but sometimes it's other things outside the digital system that you can use to help manage the hazards that may be introduced by the digital system.

MR. TOROK: Or you could build, into the software, checks to see where the machine is and try to keep it in balance that way too. All right. So there are multiple ways to look at dealing with that particular hazard.

MR. GEDDES: Right.

MEMBER BLEY: Or like in a protection system where you got a hardware monitor that monitors the CPU that makes sure if it doesn't work, tells you downstream to do something else.

MR. TOROK: That's a really good defensive measure.

MR. GEDDES: Absolutely.

MR. TOROK: We'll get to that tomorrow morning I think.

MEMBER BLEY: And watchdog timers are great at that.

MR. TOROK: Yes.

MEMBER BLEY: Had to get that in.

MR. TOROK: We're with you.

MR. GEDDES: Any other questions or comments on this slide?

MR. HECHT: Yes, just one more. I'm sorry. When you say that the 2008 ACRS letter focused there, and then point down at the bottom, why wouldn't it necessarily have focused at higher levels as well? Because aren't those digital components also running software?

In other words, a computer can consist of multiple, a main processor and the some co-processors that are doing things. Like a ethernet board or --

MR. GEDDES: Sure. Sure, that software can be spread across multiple devices. We're only showing one particular device in this picture.

MR. TOROK: And all the blue boxes have software in them, that's what you're saying, right?

MR. GEDDES: Yes.

MR. HECHT: Okay, so the crash, hang and stop could also be there?

MR. GEDDES: Yes.

MR. TOROK: Yes.

MR. HECHT: Okay. Thank you.

MR. GEDDES: There is another point of view. We show the software where it's actually physically stored in this construct. But others would argue that software is maybe a model of the overall system.

We've had some advisors suggest that software should cut across this entire hierarchy because that's what it does. It influences components and systems much higher up.

So we talk about a task that crashes, that to us means something is going on inside a digital box. So it manifests itself a certain way.

So here are the six different methods that are discussed in the EPRI guidance. The first one is functional FMEA. We learned about this method through one of the advisors who had been schooled in this

method. And she gave us some really valuable input so we included and we learned a few things about it.

Design FMEA is the bottom-up, Myron, that you just described. David is our guru on top-down suing fault tree analysis.

HAZOP is something we picked up. We worked with some Rolls-Royce folks who done a lot of work with HAZOP.

And then STPA, we talked about last year. That's the MIT method. We brought Dr. Thomas with us from MIT and we spoke to that at length at our last session.

And purpose graph is something that we picked up from some research at Georgia Tech.

Today we want to talk about the functional FMEA method. So back to this system or levels of interest. This particular example is the same high pressure cooling injection example that we talked about last year when we talked about STPA. Again, that was the MIT method.

So today we're taking that same example and driving through what we learned about the functional top-down method for FMEA. And it's Example 4-1 in this EPRI report. If you want to go back and

take a look at your leisure.

So the plant system of interest is high pressure cooling injection. The plant components are the turbine and the pump and the valves.

Then the digital system is in this blue box at the bottom right, what we're calling the HPCI/RCIC flow control system. And we're modeling that system using this method just as one lump box.

Functionally it opens and closes that governor valve based on some sensor inputs. That's all it really does from a purely functional point of view.

And you notice we have failure effects at the top that are derived from failure modes and that restriction for failure mechanisms or causes in the digital system that can lead to undesirable failure effects. It's sort of a backwards search from the traditional design FMEA point of view.

So in the EPRI report there's a work example using this functional FMEA method. And I drew out two particular columns in this table, this is, you know, published in the reports, Table 4-1. And using these guide words, the functional FMEA method puts these guide words to use to help you identify

particular potential failure modes.

Now we've obscured the basic function, which is in the first column here, but the basic function is high pressure injection. Underneath that is a process. We have, a turbine pump provides required coolant flow. And then we have a requirement statement.

Again I apologize, it's a little obscured, but there are certain functional and performance requirements, like provide 5,000 gpm at a certain pressure. And then using these guide words, what can go wrong?

Well a no function means no coolant flow. And you go off to the right, what is the effect? Loss of reactor inventory. And then what can cause the problem? Now we're getting into causes.

These are not necessarily failures of the digital equipment, but how can the digital equipment fail or misbehave in a manner that results in no coolant flow? And so we found some interesting results.

And this method also has you consider methods for identifying and detecting and mitigating the causes of component failures or system failures

that can lead to loss of function or partial function or over function and so forth.

MR. TOROK: This goes back to that issue, mechanisms, modes and effects, right? We're going the other way now. Failure mode and you figure now failure effects because they're related to that failure mode.

MR. GEDDES: Well we're starting with failure effects --

MR. TOROK: Right.

MR. GEDDES: -- getting to the potential failure mode and what it causes.

MR. HECHT: I see that.

MR. GEDDES: Right.

MR. TOROK: Sorry.

MR. GEDDES: This is top-down so it's backwards.

MR. HECHT: So where did you, you came up with those, the effects are basically what you're worried about, right?

MR. GEDDES: Right.

MR. HECHT: Those are the items of concern. So you have to have come up with those from someplace, right?

MR. GEDDES: Yes. Dave, can you speak --

MR. HECHT: Do you have them?

MR. GEDDES: -- to that, the function of process map?

MR. BLANCHARD: I can speak to it, but first I'll speak to it from a PRA perspective.

MR. GEDDES: All right.

MR. BLANCHARD: We have a variety of safety functions that are like the model in the PRA. Generally we display those in the form of an event tree.

And the top events of the event tree are functions that are important in responding to a transient or accident. The activity control, reactor pressure control, primary coolant assistant inventory control, removal of heat from the reactor through secondary cooling and those types of things.

From those very high level functions we can break those down into the individual systems. The frontline systems that support those functions, reactor inventory control, as an example, in a BWR might be the feedwater system or HPCI or RCIC. You know the two safety-related systems that might respond to a transient.

And then having identified the function of HPCI, with respect to safety, we can then move to this functional FMEA to identify the processes and the various potential failure modes of HPCI and their potential causes of failure mechanisms.

So we, you know, just beginning from a safety perspective we can start with a PRA in the high level functions that support all the different accident sequences in a PRA.

MR. HECHT: So you have what you're calling failure modes for HPCI at a fairly high level of interest. Is that what you're calling the effects in this example here or, you know, there's still the failure modes at the high level, right?

You said you were going from effects to causes to failure modes, right? You were doing it backwards, so --

MR. BLANCHARD: Effects to failure modes to causes.

MR. HECHT: To causes, okay, I'm sorry. So are you, and you've also pointed out that an effect at a higher level is cause at an even higher level. So are you just saying that you're doing an FMEA at, with blocks at very high levels rather than doing them

at the lower level with components?

MR. GEDDES: Well in this particular example we chose this as our level of interest. You can apply this method at any level, okay.

So in this case we're going after, well let me back up. This HPCI/RCIC flow control system we used as a running example all through the guideline. We wanted to examine what can we learn with a functional FMEA if we modeled the flow control system as the target.

We did the same example with a bottom-up, from the gory details down inside the box all the way back out, on the governor and the positioner components that make up the flow control system.

They did some analysis with fault trees, we did the analysis with MIT researchers using the STPA so we could compare and contrast the results of each method against the same basic example. So that's what we chose this particular case.

The failure effect would be loss of injection, among other failure effects, and what are the failure modes and the causes that can lead to those failure modes? That was our, just where we settled on the level of interest for the purpose of

comparing and contrasting the results of the methods.

MR. HECHT: Is this just the same as doing the higher level FMEA or doing a FMEA at the higher level of interest or is it something else?

MR. GEDDES: You could do an FMEA at a higher level of interest, but it's going to be more from the bottom up.

If we were to take this flow control system and break it into its constituent components, in fact we do have a work example that does just that, but we end up working our way from the failure mechanisms of the digital components up to the failure modes that effect the plant components. And ultimately the effects on whether or not we have inject or spurious actuation.

MEMBER BLEY: Myron is really starting at the other end but with FMEA you start with the low level and you say what happens if this fails.

MR. HECHT: Right.

MEMBER BLEY: With this one they're starting up with the things you care about saying, how could this fail and then working your way down from functions to --

MR. HECHT: And then I asked the question,

how do you know what you're worried about? And then we seem to --

MR. TOROK: Go to the PRA guys and ask them.

MR. GEDDES: Because guide works --

MR. BLANCHARD: That's one example of it you=re interested in plant response from an accident and transient standpoint, you can begin with the structure of the event trees in PRA to start asking what you're worried about.

MR. GEDDES: Another way to look at it might be the top events.

MR. BLANCHARD: The top events of the fault trees that makeup the accident sequences in the pyramid. Is it reactively --

MR. HECHT: Okay, well --

MR. BLANCHARD: -- comprehensive place to start.

MR. HECHT: -- stop asking questions because all of a sudden it sounds to me like it's a fault tree.

MR. TOROK: In effect here the effect you don't like is HPCI doesn't do what it's supposed to do.

MR. GEDDES: Well no. I would add that we're looking at causes which may or may not be failures. That's the difference.

You can have misbehaviors, you can identify misbehaviors that can lead to an undesired effect in the absence of any hard failures.

This method gets to it's casual. Now necessarily constrained by the problem by of faults and failures. That's what's different.

A design FMEA makes you postulate failures, or failure mechanisms to be more specific. So by definition, the design FMEA, the bottom-up method doesn't get you to potential misbehaviors perhaps due to software design defects. That's what's different here.

MR. HECHT: Okay, well if I can just ask one last question and then I think I'll stop. In military programs what we start, let's do something called a preliminary hazards list.

And so that tells you what you worry about at the highest level. And my question, the question always is, when you start out with a PHL, is it complete?

And so I guess that's the question I'm

trying to get to here. How do you know that your list of effects or what you're worried about is complete?

MR. GEDDES: This method comes after that step. Somebody has to identify your PHL or your top events or what have you.

This method, once those top events or first preliminary hazards are identified, then this helps you systematically analyze the system at the appropriate level of interest. This method by itself doesn't help you make that list.

MR. BLANCHARD: Right. And what we have in the hazard analysis report is from both a safety and a generation standpoint for a generating plant.

What candidate, example, high level functions you might want to start with. You need to pull those from PRA, we can pull those from assessments that have been done for generation under AP-913 for nuclear power plants.

And so there's several tables in the report that says at the very highest level here's what you're worried about, PWRs and BWRs from both a safety and generation standpoint. So you don't have to start off with the fault trees, there's some candidates --

MR. GEDDES: Or a blank sheet of paper.

MR. BLANCHARD: Right.

MR. GEDDES: But that set come from experience.

MR. BLANCHARD: Right.

MR. GEDDES: Okay. That's fair enough.

MR. BLANCHARD: So did we get there?

MR. HECHT: I think so. So you have a list of, you have a standard list that you're starting off with so that's based on experience, so that's good or best practice and that, yes. That's better than everybody coming up with their own list for the first time using this method.

MR. BLANCHARD: Right.

MR. GEDDES: Okay, so any more questions or comments on this functional FMEA? This is the last slide on this particular method.

MEMBER BLEY: So on the slide before you had all the, or two slides ago, you had all the methods laid out. Having gone through and played with these, we have X's in this document, are the X's equal?

MR. GEDDES: You know --

MEMBER BLEY: If I do the Levinson thing do I get the same answers that the integrated view of

design as I do if I do a fault tree?

MR. GEDDES: That's a great question. We struggled with this. We tried to express which methods would be more preferably for different situations.

We tried to use a matrix approach, we tried to score them on a scale of one to five, negative five to positive five, you know. What are the strengths and weaknesses and limitations of each method.

And the best we could do is an abstraction. There's actually a whole section in the report devoted to that problem and we asked Nancy, how would you compare STPA to FMEA to fault tree.

MEMBER BLEY: Well I can guess.

MR. GEDDES: But to her credit she said, look, there's no, the fact that it's an ongoing research question at MIT, how do you rack up what each method contributes to, you know, solving the problem. And so we took a shot.

But at her workshops on STPA there are people who come asking that question. And I've offered papers. But I don't know what our answer is any better than anyone else's. The best we could do

is abstract it out.

MEMBER BLEY: Just a, I don't know if you ever saw it, but some years ago, Alan Swain, the guy who wrote the HRA manual years ago, did a report for the Germans.

It's a nice little report where he looked at, well I forget, eight or nine HRA methods and laid them all out. And then in the end he had the various originators of those methods write a couple pages about, you know, how could they solve different kind of problems and the like.

And at first when you look at it it seems disingenuous, but every guy thought the method that he or she had evolved could solve all the problems and the other ones had very severe restrictions. And I finally decided that the, what was really going on was if it was a method I developed I could always adapt it to solve any problem.

And I wouldn't adapt your method because I didn't trust it to start with, you know. We've got a bit of that back here.

MR. GEDDES: Now I would say this --

MEMBER BLEY: But it's nice you've played with them all.

MR. GEDDES: Well this guideline is written for EPRI members, I&C engineers, reliability engineers, PRA engineers at the plants. And my personal belief is that people will pick up the method that they're most comfortable with.

Most I&C engineers have it burned in to do a design FMEA. They'll specify in a purchase order to a system integrator or an equipment supplier, I want a design FMEA. Well why do you want that? Well, it's because it's what we always do.

And then sometimes they review the results and they get really good insights and sometimes, you know, sometimes it goes in the MOD package and it gets forgotten. So we're trying to further that, you know.

If you use a design FMEA, we wrote a procedure on how to do a design FMEA for people who need a procedure on that, and then what to do with the results. Done just put it in a MOD package and file it away, sometimes the results are indicative of a problem that might be impairing in the system, then you need to tell somebody.

MEMBER BLEY: I think you missed a column that might be important to people doing that. And the column, and maybe it's what you mean by Integrated

View of Plant Design.

But if you want to see the importance of different failure modes, these are the some characteristic safety or risk or something else. Some of these methods can give you that kind of an order ranking of things that are important and other ones just give you a list.

MR. GEDDES: Right.

MEMBER BLEY: And I don't get that from this table. And it seems to me that would be helpful to people trying to pick something if it would let them know what they get out of it.

MR. TOROK: Another thing that we seem to see is, in the very simple example, it didn't seem to make much difference which method you used you got to the same point. In the more complex examples it turned out differently.

For example, in the PRA the PRA could see vulnerabilities that FMEA couldn't. You know, so there's --

MEMBER BLEY: If you've got ten components you can look at that FMEA and kind of put it all together. If you've got a hundred you start not to and if you've got a thousand you don't got a prayer.

MR. TOROK: It vary. But the top-down methods then become good at helping you focus on what you care about.

MEMBER BLEY: And a column that would help see that would be useful.

MR. GEDDES: Well we didn't include any slides on, there's a whole section with figures that go to that problem.

MEMBER BLEY: If you read the report you'll be all right?

MR. GEDDES: Yes, Section 3.3.

MEMBER BLEY: Okay. You know what people do? They look at the figures in the tables and then pick little pieces.

CHAIRMAN STETKAR: And they read words. Some of this stuff that I stumbled over is in the guidance. There's a lot of stuff that says you don't need to think about these things if you don't think they're credible.

MEMBER BLEY: And that's a free pass too.

CHAIRMAN STETKAR: That's a free pass, especially if you don't want to really think. It's, well they said I don't, I don't think it's credible, I don't think I need to think about.

MR. TOROK: Different methods do that differently though. And we got corrected on that one with STPA, right?

CHAIRMAN STETKAR: Right.

MR. TOROK: They said, you keep all that stuff in till the very end.

CHAIRMAN STETKAR: Well but --

MR. TOROK: You know, which was really good because it held you find especially these misbehaviors that didn't involve failures.

CHAIRMAN STETKAR: I'm reading guidance for the functional failure modes guidance. It says, it's not necessary to identify potential failure modes for all six guide words if one or more guide words is not applicable or not credible.

MR. TOROK: All right.

CHAIRMAN STETKAR: You know, well to me okay, I don't think an unintended function of shutting off high pressure injection is credible because I can't think of how something ought to do that so I'm not even going to go look for it.

MR. TOROK: You're right. Not credible is kind of a trap.

CHAIRMAN STETKAR: Not credible is a big

trap.

MR. TOROK: Yes.

CHAIRMAN STETKAR: Because my not credible, my dad had heart surgery and a three percent chance of dying, to him, was incredible. I'm not going to die. So it's a --

MEMBER BLEY: That's a pretty good bet.

CHAIRMAN STETKAR: It's a pretty good bet, but it's credible. So, you know, you need to be careful because people will, as Dennis said, people will look at the words and tailor them to the minimum amount that they feel is necessary to accomplish --

MR. TOROK: Yes, you're right.

CHAIRMAN STETKAR: -- compliance with what they feel is the guidance. So keeping all of those and forcing everybody to think about all of them is probably a good thing.

MR. TOROK: The longer you keep them in the better problem, yes, that's right. Maybe we didn't say that loud enough in the report.

MR. GEDDES: Any other questions or comments on functional FMEA?

Okay, switching gears, now we're at the bottom-up traditional design, what we call a design

FMEA. This is in another section of the report, it's got a whole procedure and work examples to itself.

And this particular worksheet, design bottom-up worksheet on the left hand side is the same HPCI/RCIC flow control system. But this time we're evaluating the positioner that moves the governor valve in response to the governor controller. The positioner is a digital box and the controller, the governor controller is another digital box.

And so we're looking at certain failure modes and failure mechanisms that can lead to those modes. Now these are hard failures, right.

And in response to EPRI member interest, we developed a taxonomy, what we call taxonomy sheets for a various kinds of devices. And this is Appendix B, I think it is, Ray, in the guideline.

MR. TOROK: Yes, Appendix B. It says right there.

MR. GEDDES: So here we have a sheet, on the right hand side, for what we call a Type 1 controller.

We did a little bit of research. We're not claiming that the taxonomy is complete or correct, it's presented as a method for constructing

taxonomies. I think it was the AREVA gentleman that called in and said, these taxonomies need to be platform specific, different vendors need to adapt.

But it gives you a framework that you can use.

So here we have a controller. The positioner happens to be equivalent to this Type 1 controller. It's got a CPU, RAM, ROM, internal data structures, a clock, a watchdog timer.

And so in this taxonomy sheet there's a couple of interesting things going on. What are the failure modes that this type of controller can experience? We hired a grad student to help us, you know, dig out some of this information.

And then what are the mechanisms? So if you have a controller lockup, a controller can result from a CPU halt or a CPU crash.

Now these sound like some of the things that were in the ACRS letter from 2008. But also what's interesting are, what defensive measures can be employed to help reduce the likelihood or prevent a CPU halt or a CPU crash altogether?

In some cases defensive measures are very strong, in other cases, um, not so much. But here's

just a structure that can be used to prepare taxonomy.

And then using the taxonomy you can port that information, as long as it's valid, into a design FMEA worksheet as an A, this was only meant to be an A, it's not meant to be the definitive list, so that users of this EPRI guide who are interested in a bottom-up design FMEA worksheet, can follow the procedure, use the taxonomy to inform the analysis and get on with life.

Again, one of the targets that the EPRI members were asking for is, we have operating experiences shows that we missed the failure mode, can you at least help us go after that problem? Even if they just do a design FMEA worksheet.

Which is not trivial. I don't mean to say that it's just, but if they focus on this method, here's some more perhaps complete in a more systematic way to approach the problem.

MR. HECHT: I guess in the defensive measures it says, see CPU device, taxonomy sheet B-1a and what does that say?

MR. GEDDES: Right. Well that's a great segue because that's the next slide.

MR. HECHT: Oh.

MR. GEDDES: Okay.

MEMBER BLEY: And we do have the report.

MR. HECHT: Yes.

MR. GEDDES: Right. So if we have the digital component, which is Sheet B-4a, on the left hand side, we break that down to, what is a CPU? We have a short description of what a CPU is, or could be, and then how can it fail and what defensive measures might be available to, you know, limit or reduce the likelihood of those failure mechanisms?

So you see, you have CPU halt is a failure mode of a CPU chip that transports across, becomes a failure mechanism, in controller and then a controller becomes the failure mode to, you know, something that's controlled, and you work your way up.

Now we set out with a noble lofty goal of trying to build as a complete taxonomy as we could to go all the way out to plant components, or typical plant components in a way. But we, you know, we ended up running out of time and we stopped with about, I don't know, six or seven sheets.

MR. TOROK: Something like that.

MR. GEDDES: So it's interesting that the AREVA gentleman, it almost sounded like he as reading

this taxonomy because he discussed it exactly the way it's constructed here. And it sounds like maybe they went a step further and built a taxonomy for TELEPERM, I don't know, but that sounds interesting to me.

MR. TOROK: But the intent was that this would be helpful to the utility engineers looking at these gadgets and maybe talking with their suppliers about what kinds of defensive measures were involved and the things they were buying, that sort of thing.

MR. GEDDES: Right. And a lot of these defensive measures are really just good practice among people who design robust, you know, digital I&C platform components. So it's an aid for a utility engineer who might be assessing different products to see which products might be better suited for, you know, certain applications.

Any questions or comments on this slide? Just a taste.

MEMBER BLEY: Is there any, as you said you were time limited, is there any intent to try to go further with this taxonomy?

MR. TOROK: At this point we don't have that in the plan. It probably will depend on what kind of feedback we get from utility engineers looking

at this thing. It's too early I think.

MEMBER BLEY: Are you getting any feedback at all yet?

MR. TOROK: Well not a whole lot.

MEMBER BLEY: Okay.

MR. TOROK: Not a whole lot. And you know, we're working on this demonstration project right now --

MEMBER BLEY: Okay.

MR. TOROK: -- and we're learning, well you'll hear more about it, but the idea is we want to learn about two things.

One is, does the methodology work like we thought, we were hoping it would. And the other is, how difficult is it to communicate this stuff, especially for novel methods and get people to do it, you know. As Bruce said, they want to gravitate to what they know.

MR. GEDDES: So one question that comes up is, what does this have to do with PRA, task crash, task hang, controller lockup?

I would submit that people who design the digital components or purchase them, that are interested in reliability at the component level or

device level, play this game.

I've seen a platform vendor to go into their shops. I do audits and support assessments and that sort of thing. I see FMEAs down at this level. It's very interesting that some of this information kind of gleam from that experience.

But I'll throw it to Dave, why would a PRA engineer be interested in this?

MR. BLANCHARD: All right, let's back up one slide. First of all, the functional FMEA, if I add one of those, I'd use it to help build the top-level structure of the functions in my accident sequences.

And eventually I would get down to individual components that I have modeled in the PRA. Such as in this case, on the left side of this slide we have the governor or maybe we have the governor valve itself.

Right there is probably where I would end modeling my PRA. Where the governor valve does not open and control steam flow to the turbine. Or maybe the governor doesn't, you know, send the signal to, or position the valve correctly.

The remainder of this slide, what it

contains, are different ways you can get to that failure mode that I've modeled in my PRA.

And what Bruce has done here is listed a bunch of ways to defend against that particular failure mode. And he's even gone so far as to say some of them are pretty strong and some of them are not so strong.

I can use these defensive measures, if they're available, to start screening out the different failure mechanisms that might lead to the failure mode that I'm interested in for the governor or the governor valve and limit the set of failure mechanisms that might lead to that.

With that limited set of failure mechanisms, now I can perhaps use that as input to deciding how likely that failure mode is and even come up with a failure probability of the governor or governor valve.

So what you're going to see when we get to the PRA presentation is a discussion of the context of the digital system in the plant itself. And that, you know, in that context will talk about the components that the digital systems controls or actuates, in this case the governor valve.

And we'll talk about defensive measures and they're principle purpose is going to be assets in coming up with a likelihood that those digital misbehaviors may cause the failure modes of the components that I have modeled in the PRA for the mechanical and electrical systems.

MR. GEDDES: So in summary, we feel like we do have a framework that for understanding and assessing digital failure modes, we feel like this treatment is consistent with PRA principles. It's important to consider these failure modes at the appropriate level of interest.

Functional FMEA applies guide words from a top-down point of view. A bottom-up FMEA, deep inside the guts of the box, might take advantage of a taxonomy. That could be employed.

And it is useful to understand these things in assessing compaction against undesired effects at the high levels.

Work remains to be done. We do see, you know, some evidence that utilities are bringing these methods into their procedures.

And of course, tech transfer activities, you'll see a presentation on the Palo Verde

demonstration project, is it tomorrow or --

MR. TOROK: Tomorrow or, yes tomorrow morning. And there is something other training courses, computer-based training modules and so on we have that are related to these topics. And there is talk, anyway, of doing industry workshops and what not. So we'll see.

MR. GEDDES: Okay.

MR. TOROK: But there's definitely a need for more tech transfer.

MR. GEDDES: Okay, that's all I got on failure modes.

MR. TOROK: There you go. Oh, here. So any other questions, do you want us to move on or do you want to take a break or?

CHAIRMAN STETKAR: I interpret silence as move on as quickly as possible.

MR. TOROK: Okay. We can do that.

MR. GEDDES: Okay.

MR. TOROK: So the next topic, PRA. This is a report that came along in 2012. Dave's our principle investigator and there you go.

And I think this was sent to you some several weeks ago. Now I can't think.

MR. BLANCHARD: All right, Modeling Digital I&C in PRA. EPRI published a guideline on how to model digital I&C in PRA. I'll go over that at least at a high level as a part of this presentation. To begin with some key points, high level principles that we included in the guideline, that are emphasized in the guideline.

I want to at least reference several research projects that preceded development of the guideline that were input for development of the guideline where we applied the PRA to some specific applications.

Modeling basis. We're going to talk about just what is it that we're trying to model and a little bit about high level. How we're trying to model it.

Then we'll get into the guideline itself, an overview of the modeling process. And as we go through that process we'll point to some lessons that we learned, either as, you know, part of developing the guideline or some of these applications.

How to determine the sensitivity of the PRA results to the I&C that you're modeling and then the role that defense-in-depth and diversity plays in

determining the effect the I&C has on your PRA and safety. And then we'll finish this in conclusions.

First the key points. Modeling Digital I&C in PRA, used via collaborative effort with both people who understand the digital I&C system design and the PRA experts. And that might be obvious to some folks here.

There are PRA folks who like to grab a system notebook in the P&ID and go off in a corner and do a bat the envelop FMEA and develop his fault trees for this PRA. And for a large digital upgrade, that might not be so easy.

And he's definitely going to need to introduce himself to the I&C folks in order to be able to build a PRA for a digital system to include in his PRA. The digital systems that they're building today are capable of doing lots of things.

Some of which the PRA folks may not anticipate but will be interested in. There are a lot of things the digital systems do that you may not be interested in incorporating in the PRA given the functions and systems that are incorporated in the PRA.

At the same time there is credit for the

mechanical and electrical equipment that are modeled in the PRA that the I&C folks probably don't know about. And it might be a good idea that they did, given that they're installing this digital system.

So this collaboration is intended to encourage the, you know, discussions between the I&C folks and PRA folks with respect to not only how the digital system works, but how the PRA folks are accrediting it from a safety analysis standpoint.

MEMBER BLEY: You know, I didn't really want to interrupt you but I kind of do. It seems to me you might save yourself some arguments with some of us if you showed, it's Figure 2-1 I think, it's your Slide Number 8, before you went into some of the details that are coming up in a couple slides. You know, the flow chart of what we're trying to do.

MR. BLANCHARD: Do you want to --

MEMBER BLEY: Because I think when you get to this stuff, we might get diverted from your overall depth. I think that's a very helpful, it just seems to me you might avoid some questions if you started there and then backed up. If you don't want to it's okay, you can go back the other way and see how it works.

MR. BLANCHARD: I'm conjugating on that.

CHAIRMAN STETKAR: For two weeks you've been choreographing this thing.

MEMBER BLEY: On this report this is the first picture he has.

MR. BLANCHARD: We've gone back and forth on this very issue over the last --

MEMBER BLEY: Well go ahead the way you lined it up. It's fine.

MR. BLANCHARD: All right.

CHAIRMAN STETKAR: Well hold that thought for this slide or two perhaps.

MEMBER BLEY: But you might want to jump to this one, depending on what people have to say to you.

MR. TOROK: Right. Yes, and that figure shows that some steps are team efforts and others the, you know, PRA guy has the lead and the others the I&C guy has it.

MEMBER BLEY: And it qualitatively shows some of the big picture things you're looking at as well.

MR. HECHT: Dave, I did want to point out, on the previous slide I think it was, or is it, the

slide you've shown before --

PARTICIPANT: Next one coming.

MR. HECHT: No, I'm sorry.

MR. BLANCHARD: This one?

MR. HECHT: Okay, yes. And it says, software is different, behaves deterministically, doesn't wear out.

Well we just had a presentation before you guys came on where they had, where they experienced, in their test, failure to basically initiate a trip which was not reproducible.

I don't think that you can say that in any kind of a reasonably complex system, which is basically any software system that does anything useful, that it behaves deterministically. At least all the time and that's one of the problems we have.

I mean yes it's true that software is written, but when it's, but it runs in a sequential machine and it runs in time and things get interrupted and --

MR. BLANCHARD: And in their particular instance perhaps they land in some unexpected conditions where it behaves just as it was designed to do --

MR. HECHT: Well I wouldn't say it wasn't --

MR. BLANCHARD: -- but that is also unacceptable.

MR. HECHT: I wouldn't say as it was designed to do as, you know, the instructions were executed as the instructions were written. Not necessarily as they were designed to do.

And the point is is that software, in execution, is not always deterministic. And that's why we're concerned about it.

MR. TOROK: Did that example really show that it wasn't deterministic though? They don't know what --

MR. HECHT: It was.

MR. TOROK: -- what happened there.

MR. HECHT: Sure it was. It was a timing problem. And it was a timing problem that happened sometimes, it didn't happen others. And they showed other examples of that and that timing window.

MR. BLANCHARD: And the timing issue was the unexpected condition. And what we're trying to model, probabilistically here, is the fact there are possible defects in the software and you need a

triggering condition to have the effects of that defect manifest themself in what we're trying, what we modeled in the PRA, the combination of those two.

The fact that there's a defect, and we may not know what that defect is, but the triggering conditions are probabilistic. And that's really what we're modeling in that.

MR. HECHT: The triggering conditions can be both external in the environment, they can be internal in the operating platform.

MR. BLANCHARD: Sure. And we don't argue with that.

MR. HECHT: Okay, so then in that case, how can you say the results will be reached deterministically?

MR. BLANCHARD: Well I guess I don't claim that it does most of the time.

MR. TOROK: Okay. We're in agreement that --

MR. HECHT: Which determines that it behaves deterministically most of the time.

MR. TOROK: Which is very close to one. Right?

MR. HECHT: I wouldn't say it's very, well

yes it is very close to one, but we're worried about when it's not. Because if it was deterministic then we could prove it.

CHAIRMAN STETKAR: Myron?

MR. TOROK: Yes.

CHAIRMAN STETKAR: Sorry, we don't, this is back to HRA. Under certain conditions people will do what they're expected to do. Sometimes they won=t.

I don't care why they don't. Maybe they had a stroke that day, maybe they drank too much coffee, doesn't make any difference. It's if we can define the input conditions and think carefully how the system works. I don't care why it didn't do that.

MR. HECHT: Yes.

CHAIRMAN STETKAR: I don't care why I didn't do, maybe you do, I don't. I care about trying to evaluate the likelihood given the set of input conditions that you, what are the potential outputs.

MR. HECHT: Agreed, but that does --

CHAIRMAN STETKAR: I don't care whether it came from inside or whether it came from outside.

MR. HECHT: Agreed. But everything that you said is consistent with the notion that you don't always know why things happen, which means that the

determinism --

CHAIRMAN STETKAR: Right.

MR. HECHT: -- is may not, may not be the right word.

CHAIRMAN STETKAR: So there's some likelihood, give what you believe is a perfectly defined set of input conditions, that you still won't get the expected output. But we ought to be able to quantify that given what we know about how things work.

It's not as likely as getting, if you have a perturbed set of input conditions in an unexpected output conditions because you understand that, gee, under that perturbation the input conditions the software will close the valve. I didn't expect it to close the valve.

MR. HECHT: Well I just wanted to point out --

CHAIRMAN STETKAR: It's 100 percent of the time it will do that.

MR. HECHT: I just wanted --

CHAIRMAN STETKAR: Not a hundred percent.

MR. HECHT: Yes, okay.

CHAIRMAN STETKAR: It will 99.99 percent

of the time because sometimes it fails internally and didn't do what you had expected it to do, which was close the valve.

MR. HECHT: Well just as a human being with the same inputs, with that normal inputs, might respond some ways, in some conditions, if he didn't have enough sleep the night before, he or she is going to respond differently than if she did.

CHAIRMAN STETKAR: Sure.

MR. HECHT: And that's also part of the equation. Which is why or part of the situation where, which is why one loses that deterministic.

MR. TOROK: Okay, so at some point you're going to take, let's say the probability of that and it's non-deterministic behavior, and add that in with the other behaviors you don't like and figure out what the overall misbehavior probability is, right?

MEMBER BLEY: At least. The way I interpret what he has up here is once I get into executing the software, it goes through those steps. But the whole system has things associated with it that can affect the timing, such that you enter it at different spots or at different times. And that's what he's talking about. Is the adverse condition.

So --

MR. HECHT: Well I'm saying that even within a processor, because a CPU --

MEMBER BLEY: Because it's a system, yes.

MR. HECHT: System.

MEMBER BLEY: That's right, I agree with that.

MR. HECHT: Okay.

MEMBER BLEY: And all it's saying is we shouldn't spend our effort trying to worry about code executing step by step and doing it differently, but we ought to worry about the system doing it differently. I think that's what you're saying.

MR. BLANCHARD: Yes. I'm trying to say, and Research this morning said the same thing, we believe we can treat software misbehaviors, I'll call them, probabilistically in PRA. Even though it is intended or designed to operate systematically or deterministically.

Another couple of principles that are throughout the guideline is concept to context and defensive measures. And we kind of talked about this in Bruce's presentation.

Context is the role that the digital

system plays in the integrated plant design as a whole. What does actuate and control in terms of a mechanical and electrical systems.

And that information, and the roles that the mechanical and electrical systems play, are a key input into the functions that you model with a digital I&C or the digital I&C and the level of detail that you need to put into the model.

And then defensive measures. These are design practices and features used by the designer to prevent or mitigate or cope with digital system and component should they occur.

And those then are input to determining the likelihood that a digital component or a digital system will fail. So it beats coming up with so called failure probability for the given components on the digital system.

Some insights that we got out of developing the guideline, as well as some of the application we performed leading up to the guidelines development, once again having the context and defensive measures, is that you can design the digital system such that the PRA is insensitive to some of misbehaviors of the digital system. And you do that

by focusing on the defense-in-depth and diversity of the mechanical and electrical systems that the I&C actuates or controls.

If you can reflect the defense-in-depth and diversity that's already built into mechanical and electrical systems into the digital I&C system itself then the misbehaviors of the I&C system will not be all that significant with respect to the results of your PRA.

And having implemented your digital system such that it reflects the defense-in-depth and diversity, the context of the digital system in the plant design as a whole, the reliability of the digital system can be shown not to effect the result of the PRA over broad ranges of assumed failure probabilities.

You only need to come up with a digital system that is as reliable as maybe a comparable analog system that you might replacing. And later in the presentation we might be able to show some examples to that.

MR. HECHT: Is another way of saying that, is if you knew all the bad things that the digital system could do, and you had external measures that

your defense-in-depth measure contained those effects, that that's the reason for the top statements insensitive to its misbehaviors?

MR. BLANCHARD: That's close. And if you know all the bad behaviors of the mechanical and electrical systems that you want to avoid, that then you can be reflective in the I&C to avoid the misbehaviors in the I&C that may be the difference. That make sense?

MR. HECHT: Is that whether it's digital or analog?

MR. BLANCHARD: Yes. That applies either way. Yes.

In the developing the guideline we actually performed quite a number of applications of the PRA, attempting to apply the PRA to specific digital issues that were important at the time we were reviewing this work.

Very early in the process of determining how to use PRA in examining digital I&C, defense-in-depth and diversity analyses were a hot topic. In coming up with a risk informed approach to doing defense-in-depth and diversity, was one of the methods that we developed and was published in an EPRI report.

In the 2006 to 2008 timeframe the NRC and NEI formed task working groups to examine key issues associated with a licensing of digital I&C. Among them were the defense-in-depth and diversity, human factors and PRA.

There was a task working group built around using PRA to model digital I&C. One of the applications that we recognized that we could use PRA for was to examine the risk and benefits of the automated diverse actuation system that would be proposed with digital I&C ISG2.

And so an analysis of automated diverse actuation systems was performed, the risk and benefits identified. And we had ten plants volunteer for that.

So we had five BWRs. BWR 2, 3, 4, 5 and 6 and five PWRs volunteer their PWR for that. A two loop Westinghouse plant, a four loop Westinghouse plant, two combustion engineering plants and a BMW plant. So there was, you know, a fairly broad application of the PRA to a spectrum of plant designs.

Throughout that application of the PRA, to the issues we took a look at, we were doing quite a number of sensitivity studies. Not only on individual plant systems determining the effect misbehaviors the

I&C could have on the reliability of those systems, but also on individual accident sequences that finally culminated in an analysis.

And a full scope level 1 PRA for the Westinghouse plant were we took a look at what level of diversity did we need in the I&C for the various plant systems for that four loop Westinghouse plant. How reliable did the digital systems need to be and what level of common-cause failure could we have between the various mitigating systems in terms of the digital I&C. And that was also published in an EPRI report.

All of these applications eventually led up to developing a couple of guidelines. One was estimating the failure probabilities for digital systems or actually a probability of misbehavior of those systems.

This report examined five different methods of coming up with failure probabilities for digital components in digital systems that eventually evolved into kind of a blended method where we examined the digital system design, looked for defensive measures for various failure mechanisms that might lead to digital component or digital system

failures. And then either use, use one or two methods to come up with failure probability for those digital components.

Either statistical testing or a review of operating experience. And so that's published in an EPRI report.

And then finally we got the modeling digital I&C in PRA itself. And that's the subject of this particular presentation.

Just a couple other additional points. The guideline begins with an answer, a couple of questions. Just exactly what are we trying to model and how are we trying to model it?

What we're trying to model, in terms of digital systems are sensor signal processors, communications devoting logic.

And the guideline strongly emphasizes, that's not a whole lot different than what we model today in terms of the analog I&C. We're just modeling different component types. You know, things that have processors.

And a reason for emphasizing that is there are PRA folks out there who do model analog I&C systems in some detail and they're comfortable with

doing that. And our emphasis in the guideline was, you know, you're really doing much the same thing when you model digital I&C.

How are we trying to model it? What's different in the digital I&C is the software. And what we have here is a diagram that appears in a lot of the EPRI reports.

It begins with an initiating event, has multiple mitigating systems in responding to that initiating event. And maybe an operator action that actuates the system, some of the systems are automatic, some are backed up by diverse actuation systems.

But during this initiating event, which may be a loss of feedwater, the mitigating systems, which maybe aux feed water in feed and bleed systems, if they both fail we end up with a situation we have inadequate for our cooling.

Now the fairly common and understood how we go about modeling the mechanical and electrical equipment that support this, the digital I&C, it being systematic in the way the software responds, we model the common-cause failures between the trains or divisions of the I&C a little bit differently.

MEMBER BLEY: This is a good point to inject a couple of questions or just comments.

MR. BLANCHARD: Yes.

MEMBER BLEY: One is in your report you get a lot of space to think about common-cause. At least to me the two things that are most worrisome about digital I&C are, one, common-cause things. Especially if you got a box that controls a lot of different stuff.

And the other is the issue that is really mush easier in analog, and that is if something goes wrong in the analog system, you can get, instead of just does it fail to do this, you can get things going in opposite directions and funny things. But it's easy to look at what causes that. And it's usually very limited in scope.

Inside a digital system, if it starts generating wrong output, it seems a much more open problem. And I don't think I saw you talk much about that.

MR. BLANCHARD: I think in the guideline, or maybe we didn't give it enough text, but from an accident sequence perspective, I know we've presented this in some of the industry meetings that we've had,

we don't really think there are new accident sequences that are developed with that type of a situation.

If you were to take a look at a functional event tree, as an example, there's reactivity control, reactor pressure control, there's secondary heat removal, there's reactor, those are all still going to be important functions to consider. And the same mechanical and electrical systems will support them.

So I don't think there's --

MEMBER BLEY: I think you're probably, well I'm not sure.

MR. BLANCHARD: But --

MEMBER BLEY: I think you're probably right, but the likelihood of them could change.

MR. BLANCHARD: Right. The distribution and the risk will change.

MEMBER BLEY: And it's like back to the human factors analogy. It's the errors of commission thing.

MR. BLANCHARD: Right. Right.

CHAIRMAN STETKAR: And your report does not spend enough time and effort to point people at this. That's his statement.

MR. BLANCHARD: Okay.

CHAIRMAN STETKAR: I look at this analogously to, this part of it, not so much because people haven't really struggled. That's for the person to my left not withstanding with this error of commission.

On the other hand, people have struggled with this issue when they do fire analysis.

MEMBER BLEY: Yes.

MR. BLANCHARD: Yes.

CHAIRMAN STETKAR: Multiple spurious operations.

MR. BLANCHARD: That's right.

CHAIRMAN STETKAR: So when I do a fire analysis of a room that contains a bunch of cabinets full of stuff. Stuff might be digital, it might be analog, it might be manual knife switches, it doesn't make any difference, I look at what can the fire do. And the fire can cause a valve to open spuriously or it can cause the valve to close spuriously.

Now maybe it can't cause the valve to open spuriously because of something else. Maybe there's something else in another room that there's an interlock that prevents that from happening. If there isn't, it can't.

So I look at the back-end of stuff of what can be caused by this fire. In the same sense of looking at the output of a digital protection control system, what can it do? Can it cause that valve to open or close, yes it can. It can cause the valve to open or close, okay, it can.

Now most, there are snippets of that notion in the report, in the front-end.

MEMBER BLEY: Yes.

CHAIRMAN STETKAR: But it very quickly devolves into, how do I determine that the digital system does not do what I wanted it to do in the context of the way that I built my internal event PRA.

MR. BLANCHARD: Yes.

CHAIRMAN STETKAR: It does not trip the reactor or it does not initiate safeguards actuation. And in the fire analyses we've learned that there may be strange combination of signals that put the plant on the trajectory that you never even thought about in your internal event PRA.

How many internal event PRAs have you modeled that have containment bypass LOCAs through the letdown system? It isn't very modeled.

MR. BLANCHARD: In every PWR that I have

worked on has that --

CHAIRMAN STETKAR: Okay, but most people don't. Okay, you and I model it but most people don't.

But the fire analyses can put you on that trajectory and it might not be something that's even in the construct of your logic model.

MR. BLANCHARD: Yes.

CHAIRMAN STETKAR: Now I've stumbled across it when I've done fire analysis for other logic models. Said, well you haven't even modeled that and yet it can happen.

MEMBER BLEY: I think that example you two agreed on also points out an important thing. In the argument that there aren't any new scenarios, if you've really been thorough that might be true.

I'm still not absolutely convinced, but for every PRA you did, or you did, I can go out and find a whole bunch of others that don't have that one.

CHAIRMAN STETKAR: Right.

MEMBER BLEY: So there are scenarios they didn't do. So if the general guidance doesn't warn them to think of this, it's not helping them as it should.

MR. BLANCHARD: I'm beginning to think we should have started with the diagram because this --

MEMBER BLEY: This isn't where I thought it would have been a problem, but.

MR. BLANCHARD: This very issue is addressed in the first step.

CHAIRMAN STETKAR: It's addressed in the first two steps, but once you get down into the more detailed guidance, it sort of disappears.

PARTICIPANT: Where it should continue.

CHAIRMAN STETKAR: Where it should continue.

MR. BLANCHARD: All right. But your point about the fire PRAs is well taken too because they are more complete at the system modeling level with respect to being able to incorporate unexpected effects from --

CHAIRMAN STETKAR: Exactly, because it's that thought. They've been forced into that thought --

MR. BLANCHARD: Right.

CHAIRMAN STETKAR: -- by saying, thou shalt consider the effects of multiple --

MEMBER BLEY: But only recent --

CHAIRMAN STETKAR: -- fire and multiple spurious operations.

MR. BLANCHARD: All right.

MR. TOROK: That's a really interesting point too because tomorrow we're going to talk about this other project we're working on. Mostly common cayuse failure stuff, and this multiple spurious actuation is one of the issues that everybody is struggling with right now.

MR. GEDDES: As an I&C person, to me modeling is one problem, but what do you do about it is to me the most interesting problem. How can you mitigate it, how can you reduce its likelihood --

MEMBER BLEY: Well that's where I didn't quite agree with John when he says, I don't care why it happened. I'd like to be able to fix it too.

CHAIRMAN STETKAR: Well --

MR. TOROK: Right. So sometimes --

CHAIRMAN STETKAR: But at one level if it's so unlikely --

MEMBER BLEY: That means it's not where I'll spend my money.

CHAIRMAN STETKAR: -- in another words, that is not where I'm going to spend my money. I mean

that's the whole point. If I try to understand every single way that something can happen, I spent a lot of effort, I probably spent a lot of effort in areas where I might not need to.

MR. GEDDES: Yes.

CHAIRMAN STETKAR: If I want to make everything perfect, that would be fine. But, you know, this is a risk informed type of process.

MR. GEDDES: Functional allocations in controllers or sensitive controllers is a very interesting problem. And it goes right to, I think, what you're discussing.

MR. TOROK: And which is enough.

CHAIRMAN STETKAR: I looked at this. The first one I every looked at was 23 years ago. And I found a really neat behavior.

This happened to be on integrated control and protection system. And it actively was designed to shutoff high pressure injection under some conditions, you know.

And darn I tried to get the likelihood of those conditions to be high enough where it showed up and I couldn't. You know, but it was designed to do that. You know, whether the people who designed it

thought about those likelihoods --

MEMBER BLEY: Not the purpose of another one.

CHAIRMAN STETKAR: No, it was designed on purpose.

MEMBER BLEY: Okay.

CHAIRMAN STETKAR: Under certain conditions it shutoff high pressure injection. Because it knew that it didn't need it and you'd overload the diesels if you had high pressure and low pressure injection running. For example.

It's a particular plant design, particular plant system. They designed it that way. But there that sounds like a really bad thing to do. And it seemed to me like a really bad thing to do.

But I couldn't force, try as I might, couldn't force the frequency of those scenarios to be high enough where then I started to look into defensive mechanisms. Despite it sounded like something that's absurd.

MR. TOROK: That's a really good example of this kind of thing you go after with this STPA hazard analysis. Were you say, under what conditions would a designed-in behavior be wrong, right? And do

I have adequate protection against that somehow.

MEMBER BLEY: Well when we had that session, I mean that was a very systematic elaborate way to do something. I think I good PRA guy is always doing, thinking about those very issues and cataloging them. I thought most examples we saw somebody could have worked out without all of that overhead.

MR. GEDDES: That's what Dave said. Why are we doing all that.

CHAIRMAN STETKAR: He's the guy that's got let down line failures in his models.

MEMBER BLEY: Go ahead.

MR. BLANCHARD: Well let me finish with this slide and then we'll move onto the diagram you wanted to start with.

We emphasize in the guideline that you got to treat software common-cause failure differently than you do common-cause failure in mechanical and electrical equipment.

If you have a actuation system for one of your mitigating systems, each division gets the same input. If you do have a failure, software failure in one division, it's very highly likely that actuation of the other division won't happen either.

And so your beta factors, your common-cause beta factors, are going to be very high. And PRA folks aren't used to modeling that.

And also this comment you made about if you have software that controls a lot of different things, that creates the prospect that you may have common-cause failure across systems --

MEMBER BLEY: Yes, which is really unusual.

MR. BLANCHARD: -- and there is tremendous resistance -- yes, it's tremendous resistance on the part of PRA folks now to model that.

And then if it happens that the information needed to automatically actuate a system also influences the information the operator is getting, or his normal controls, it influences those.

A common-cause failure can affect the ability of the operator to take his action. And then sometimes there are similarities between the software, between instrumentation and control that can cause an initiating event in some of the mitigating systems that you credit in the PRA.

And so the guideline emphasizes, you need to consider the potential for common-cause failure of

other digital system in a variety of different places that we may not be used to in the mechanical or electrical system.

MEMBER BLEY: Now the real reason I wanted you to go to this one first --

MR. BLANCHARD: Okay.

MEMBER BLEY: -- was I thought my colleague Charlie Brown over there would really like Steps 1 and 2 on this diagram and what they're saying you do before you do any PRA.

MR. BLANCHARD: Okay. Well the --

MEMBER BLEY: Just wanted to make sure.

MEMBER BROWN: I saw that, I'll re-look at it at after you said something.

MEMBER BLEY: All right, okay.

MEMBER BROWN: It's the top-down approach for designing system as opposed to figuring out how to make the carburetor and the fuel injection system and --

MR. GEDDES: It's system engineering.

MEMBER BROWN: Yes, In other words I want the car to run, how do I make sure the pieces all fit together.

MR. GEDDES: Cover the basic functions.

MEMBER BROWN: Right.

MR. BLANCHARD: Well the guideline is a nine-step process and --

MEMBER BROWN: However, I would think you left one thing out.

MR. BLANCHARD: Yes.

MEMBER BROWN: Actually four things out.

MR. BLANCHARD: Okay.

MEMBER BROWN: Those are the, define the architecture in terms of the fundamental principles of I&C reliability of independence, redundancy, deterministic behavior, diversity defense in-depth and simplicity. As well as control of access from external resources.

MEMBER BLEY: That's right, don't forget, Charlie.

MEMBER BROWN: Those are all, I don't forget that. And those are parts of that. And so you've got to have a set of standards when you talk about an I&C architecture and that's not emphasized anywhere.

MR. BLANCHARD: That's correct, that's not --

MR. GEDDES: But this report is not about

how to design an I&C system.

MEMBER BROWN: That's not the point. It says, define I&C architecture. You still need, when you talk PRA and trying to eliminate problems in your design, go back to your earlier charts, those get wrapped up in principles.

Like when you talked about software being deterministic, Myron argued with you. Software doesn't have to be deterministic, it doesn't have to be, if it's an interrupt driven system, it's not deterministic.

The key is repeatable and predictable. And when it's not you have to have, what's your defensive measure, something's not happening the processor doesn't do it in a predictable and repeatable manner.

You can work your butt off trying to get something in other defensive measurement but there's no, you need something bounding it. That's your, I forgotten what, one of the other slides, the watchdog timer or some hardware alternative, mitigating, whatever you want to call it, that's independent of the main function, the main processes that you're dealing with.

You got the top level thought process captured and that's what you want to see in the architecture. So I don't know, I just threw that in from a thought process.

You don't have principles and, well defining it a lot, seeing some of the system design, they got an architecture that sucks. Not very independent.

And they argue they don't, their software is perfect. It never breaks. And I can protect it with check sums and cyclic redundancy checks and all kinds of other good stuff. And those will always make sure I'm okay.

Or dual core RAM. Which is no more than a transformer that takes garbage in and puts garbage out. Just like a transformer will put garbage in, you get garbage out.

That's a simplistic thought process of it but it's kind of, anyway, I'll stop right now. Now that Dennis left.

CHAIRMAN STETKAR: Yes, he'll be back.

PARTICIPANT: Oh, and he's the one interested in --

MEMBER BROWN: Well I wanted to get that

in.

PARTICIPANT: Oh, you're interested.

MEMBER BROWN: Because I have to leave a little bit early, that's way.

MEMBER SCHULTZ: And you will find on our record that those principles are always inserted on the record anytime we talk about I&C architecture.

CHAIRMAN STETKAR: Yes.

MR. GEDDES: Really?

MEMBER SCHULTZ: So it might as well be right here.

MEMBER BROWN: Well that's why I mentioned earlier, when you were talking, in your introductory part, and you were talking about the stops on the governor, the turbine valve or whatever it was you were talking about --

MEMBER SCHULTZ: I truly meant that seriously.

MEMBER BROWN: -- and I said that's kind like a watchdog timer for the boundary condition on the CPUs don't operate properly.

CHAIRMAN STETKAR: But, Charlie, in some sense they're working backwards in, you know. And it kind of resonate with what Bruce said, that if you get

this situation where the software has a high likelihood of shutting off high pressure injection during conditions when you don't want it to shut it off, you can backtrack and say well, there is something in the design that caused that. I mean that's the approach they're taking.

MEMBER BROWN: Yes.

CHAIRMAN STETKAR: Okay.

MEMBER BROWN: That's not inconsistent with that I've said. Which I will keep saying as Steve points out.

MR. GEDDES: Well one thing that we've learned along the way, is that hazard analysis is great, but it can also serve a very good purpose to help assess requirements, completeness and correctness.

Most I&C designers come at it from a functional point of view. What do you want the car to do? And they have a sunny day mentality.

You know, you show the Google car driving itself, it's a sunny day, there's no traffic, right? Well it's a rainy day and something goes wrong and the brakes are worn out and so that hazard analysis helps you force a more complete and correct, I'm not going

to say we're going to guarantee a complete and correct set of requirements, but everything hinges on requirements in systems engineering.

So it turns out Nancy Leveson and John Thomas and others, set out to solve that problem first and then discovered that hazard analysis could also be used in arrears to see if there were already residual hazards in a system.

So that's my soap box on requirements. But to me defining I&C architecture is just one element of a larger problem of systems engineering requirements definition and all that goes into that.

MEMBER BROWN: Yes, I maintain those come down right underneath the architecture. You got to have an architecture, if you want to have system requirements, you got to have an architecture from within which to derive those requirements.

MR. GEDDES: It's iterative.

MEMBER BROWN: So that's the top level, very top level of what you need. And it also gives you a picture of what hazards you may encounter.

MR. TOROK: And the architecture can furnish defensive measures lots of times.

MEMBER BROWN: Absolutely.

MR. TOROK: So they need to be, yes, calculated.

MEMBER BROWN: Well they lead you to defensive measures.

MR. TOROK: Yes. Where are we, Dave?

MR. BLANCHARD: All right, we're at the diagram Dennis wanted to start with.

CHAIRMAN STETKAR: Dennis, I'll mumble along --

MR. BLANCHARD: All right. This is a nine step process in the EPRI guideline and it explicitly highlights responsibilities, lead responsibilities, for the PRA folks, as well as the I&C folks. And also identifies where they need to collaborate in order to proceed to develop a model for the I&C in the PRA.

And throughout this you're going to hear a lot of discussion about both context and defensive measures and the role they play in developing --

MEMBER SCHULTZ: So can we just talk about that for a minute --

MR. BLANCHARD: Yes.

MEMBER SCHULTZ: -- Dave, because when you presented defensive measures before, one element that you focused on was the digital system reliability need

only be similar to that of a comparable analog system to manage risk adequately.

And I think that's a decent statement but I, in the design of digital systems, I'm expecting that the designer is most likely to go beyond --

MR. BLANCHARD: Yes.

MEMBER SCHULTZ: -- what it is for the --

MR. BLANCHARD: Oh, absolutely.

MEMBER SCHULTZ: -- what the design is for the analog system. And what's why we're here and talking about all of this. So I'm wanting to hear more about the defensive measures and the context of the digital I&C.

MR. BLANCHARD: You also need --

MEMBER SCHULTZ: From what you stated previously.

MR. BLANCHARD: And you also need to take that statement as being in conjunction with the context statement that was made. Which was, pay attention to the defensive and depth and diversity between the mechanical and electrical components --

MEMBER SCHULTZ: Yes.

MR. BLANCHARD: -- that the I&C controls. And if you do both of those then, you know, the level

of the reliability that you need in order to manage your plant safely is similar to what you probably turn out in experience in your analog I&C.

Yes, I absolutely agree. You probably can expect better performance --

MEMBER SCHULTZ: Yes.

MR. BLANCHARD: -- under the analog system.

MEMBER SCHULTZ: Well better performance, but there's also, as we've been talking here, there's also the opportunity to also incorporate issues that you don't have with the analog system.

MR. BLANCHARD: Right. But to manage the plant safely, you want to have that higher bar to go over. This needs to be similar to what we currently have in the analog systems.

And I think that's a big story, you know. We don't have to guarantee that the digital I&C system is as, you know, much more reliable than any other I&C system.

MR. GEDDES: I think in practice, in particular, in control systems like turbine control and feedwater control, most I&C designers go after the problem, single point vulnerabilities. Were digital

is more properly designed and properly implemented.

Digital systems should be more robust than an analog system that, in some ways, is vulnerable to things that it can't handle.

MEMBER BROWN: It all depends on what you define as robust. I mean the digital systems are much less likely to drift or go outside the bounds of the design parameters within which you design them then analog systems are.

Very much fewer things to be effected by the temperature and humidity and things like that if it's properly designed. Whereas the analogs, pots wear out. Digital settings don't wear out.

MR. GEDDES: In a lot of cases a single failure will trip the plants when a well-designed digital system should be less susceptible to single failure.

MR. BLANCHARD: All right, moving on to the diagram. Step 1, the first step in the process is for the PRA folks and the I&C folks to get together and to introduce each other to first the digital I&C design and then to the functions and systems that are modeled in the PRA.

And the purpose of this is for, not just

for the PRA folks to have a better understanding of the different functions of the I&C system, but to also, you know, identify what portions of the I&C system are most important to modeling in the PRA.

So the architecture of the PRA is going to include process interface, system automation, supervisory controls. And the PRA folks may not be interested in all of that.

And at the same time there will be functions that the PRA folks are interested in seeing how it interfaces with the I&C system that the I&C folks might not know about.

And so at this stage of the process what we're going to be dong is identifying the mechanical and electrical components that are modeled in the PRA and the I&C folks and the PRA folks are going to be deciding what portions of the I&C system, you know, effect the behavior of those particular components modeled with it.

CHAIRMAN STETKAR: The only question there again, Dave, is that it's all written from the context of that distinct construct you have there in terms of the stuff that you built the PRA --

MR. BLANCHARD: Right.

CHAIRMAN STETKAR: -- to do. Rather than things that the I&C system could do to you.

MR. BLANCHARD: That's --

CHAIRMAN STETKAR: Which may involve non-safely related systems that haven't been modeled, excessive steam flow, those kinds of things.

And as I read the guidance, it's all structured in terms of, how do you think about this not accomplishing the functions that you modeled in your PRA not accomplishing those functions.

MR. BLANCHARD: There is a completeness question that needs to be answered by the PRA folks when they find out the kinds of things that the I&C is capable of doing.

CHAIRMAN STETKAR: Yes, but my point is that the guidance ought to stress --

MR. BLANCHARD: Doesn't emphasize --

CHAIRMAN STETKAR: -- the PRA folks, and I've talked to PRA folks who don't think that way. It's, I have this model and it is do not trip the plant, that's all I care, you know, does it not trip the plant. And the I&C folks who might also not necessarily think that way is, what can it do bad to me?

MR. BLANCHARD: That's right. And a simple example of what you're talking about is a valve that's, has to open may not have the fail to remain open.

CHAIRMAN STETKAR: Right, failure mode in the PRA because people didn't, a good example, steam relief valves. People don't look at, you know, as long as they open it's okay.

MR. BLANCHARD: Right.

CHAIRMAN STETKAR: As long as one out of 12 open you're okay. Supposed 12 out 12 open, that's not so good.

But people typically don't model that. On the other hand, if something in here could cause that, one ought to be looking for that type of behavior. Couldn't you?

MR. BLANCHARD: And you're right. There's not a lot of detail on the kind of conversation that the I&C folks and PRA folks should have at this point.

And I agree, there should be an emphasis on, okay, you modeled the steam relief valves from a failed open standpoint, somebody should be asking you the question, all right, now that this digital system controls the position of those steam relief valves,

should we be worried about them opening when they shouldn't.

CHAIRMAN STETKAR: Correct.

MR. BLANCHARD: And that kind of detail isn't in the guideline.

CHAIRMAN STETKAR: Right. I mean, you know, detail, detail, it's just the sensitivity to that type of thinking.

MEMBER SCHULTZ: I think you set up here the very proper way in which to create a value proposition. But in order for it to really deliver value, you have to describe in more detail the robustness of that conversation and the openness of the conversation in order to allow all the participants to gain flow value from it.

Because I can, you know, picturing it you can picture it being a discussion between PRA and I&C designers and they'd be complimenting each other and nothing would change. And the combination of effects that you want to see happen would not.

And so some more guidance associated with how that deliberation should go would be very useful.

MR. GEDDES: I think the first step is, can they even understand each other.

MEMBER SCHULTZ: Well that, yes. But I think that this process is leading it to that understanding, if in fact a dialogue happens. And more information about the intent of the dialogue is delivered as guidance.

MR. BLANCHARD: All right. At least at the end of Step 1 we know the components that the PRA folks care about and we've identified the interface with the I&C system. And the next step then is to talk a little bit about failure modes.

Those components in the PRA, in order for things adverse to safety to happen, have to fail in a certain way. And dialogue with the I&C folks about whether or not the I&C can cause those particular failure modes, or as we just discussed, are the new failure modes that the PRA folks have to consider, given the behaviors of the I&C that the I&C folks can identify. Now that dialogue has to happen at this point.

What we're going to do at this particular step is translate the failure modes that are or should be modeled in the PRA into misbehaviors of the instrumentation and control system, you know, that we'll have to be concerned about.

And we have a table here that just gives a small example of taking the component in a plant system and then converting that to the way the I&C system has to behave in order to get to that particular component failure mode.

And then we can get down into failure mechanisms. But again, the PRA models failure modes and not failure mechanisms. So the PRA would stop at the, say the protective action.

If there's no protective action there needed and then perhaps continue the model in I&C system from that particular top event to the I&C system.

Now there's going to be situations in which it's not certain, you know, just how the I&C system will behave. What its misbehavior might be with respect to a particular component in this failure mode.

And in that situation the guideline recommends simply, for the PRA folks to simply assume that the failure mode that they're concerned about in the PRA, or should have in their PRA, can in fact happen and continue to process from that point on.

And then later on there will be a

sensitivity study in this analysis to decide what parts of the I&C system, what behaviors, are most important for the PRA and that particular failure mode, which we're not sure about, can happen with the I&C, shows up as being important, we make a decision at that point whether or not to pursue whether that failure mode can actually occur for the I&C or whether to continue with the assumption that we'll just assume that it occurs and see its impact on applications down the road.

Step 3 of the process begins to involve identifying the potential for common-cause failure coming from the I&C in ways that we didn't traditionally evaluate in PRA when we had the analog systems.

And what, you know, for the hardware part of the I&C system, think modeling the digital I&C is very similar to the way we would for hardware and mechanical and electrical components that the I&C controls. If it's a different component type and failure mode, you may not model common-cause failure.

Different manufacturer in different systems with different, and operating conditions and/or environments and maintenance practices. It's

likely we wouldn't model the common-cause failure of the hardware of the I&C.

But software is different. What we would do with the software is break the software apart of the digital I&C component or system down into its operating system application software and communications and look for specific defensive measures that are particularly effective in addressing the potential for common-cause failure.

The operating system, as an example, may appear in all, throughout the digital system in all sorts of different components. And if it, defensive measures against operating systems failures include cyclic operation, allowing fewer interrupts, having the operating system be completely transparent to plant conditions.

It operates the same way during normal operation as it would during a LOCA or a transient. It continues to perform its function regardless of what's going on in the plant.

What the guideline recommends is that if you're missing any one of these three in the operating system or a portion of the digital I&C system, then that portion of the I&C system is a candidate for

common-cause failure with other parts in the I&C system that are also missing for that particular defensive measure.

Now there are other defensive measures that you can have besides these. But these are particularly important.

MR. HECHT: With regard to the third option that you have the transparent to plant conditions, I would have assumed that most of real-time kernels, whatever you want to call them, are in --

MR. GEDDES: Yes.

MR. HECHT: -- fact transparent.

MR. GEDDES: That's the reason why would want to use a real time kernel.

MR. HECHT: I guess are there any counter-examples?

MR. GEDDES: Yes.

MR. HECHT: There are, yes.

MR. GEDDES: I don't want to go into it, but people aren't, all right a plant trip is a great educational experience.

MR. HECHT: I just also wanted to say that when I talk about lack of complete determinism in

software systems, with respect to having redundant operating systems or other things at that level, what I call the infrastructure, you gain something by having parallelism.

Because something that might cause one instance of, or one copy of an operating system to crash because of a particular sequence of events, that sequence of events may have happened differently in another copy so that it evolved.

And in fact if we look at cloud computing or virtual machines and all that stuff, all this, you know, how we get our movies off of Netflix, those people depend on that.

MR. GEDDES: I think we'll talk about that tomorrow. Not Netflix, but --

MR. TOROK: Well there's more, you'll have more opportunity to talk about that tomorrow too.

MR. GEDDES: Yes.

MR. BLANCHARD: All right, the application software, functional diversity and signal diversity are particularly useful in, you know, reducing the potential for common-cause failure in the application software.

However, the application software is

sometimes unique to a particular system and you may not be able to completely eliminate the potential for common-cause failure in the application software. And we'll talk a little bit more about how PRA can handle design errors and functional specification errors.

But at any rate, the guidelines suggest those high level defensive measures. And if you're absent any of these for these particular parts of the digital system, then it recommends then strongly three candidates for incorporating common-cause failure.

MEMBER BLEY: Now I think right here, Charlie would jump on your few interrupts and say we really want deterministic behavior and no interrupts if we can have that.

MEMBER BROWN: That's right.

MEMBER BLEY: And if you have any you really got to be careful in design and therefore careful in analysis to make sure you pick up all of the potential impacts and such that --

MR. TOROK: Right. Everything here is an extension of what Charlie was bringing up.

MEMBER BLEY: It was. There's a couple of his points that I'm not sure we brought into this yet. And at least an awareness that is important. The

last one is one we added recently and it's, but I forget --

CHAIRMAN STETKAR: Simplicity.

MEMBER BLEY: No, no. It's keeping people out of control of access.

CHAIRMAN STETKAR: Oh, oh, control of access.

MEMBER BLEY: And if that's not really solid, we've opened up a whole new world of possibilities of what goes wrong here. And at the simplest level that means, where everything is hooked to somewhere else, if you don't have a hardware diode blocking communications, you don't know what could be going on.

And if we don't think about that when we model these things, I mean, with any luck that's going to be fixed and we aren't going to see any of those. And so we won't have a problem with --

CHAIRMAN STETKAR: Do it in the design.

MEMBER BLEY: -- do it in the design. But if it's not in the design, it almost calls for a caveat on one=s analysis saying, if somebody breaks through this, everything I've got here is mush.

And the other one, and it's kind of up

here, it's, I mean we look for independence electrically, but looking for independence on communication on data strings.

And I don't know, I think it's implied. I think you have here, I'm not sure it's called out directly, and it's something that people aren't geared to think about, maybe they don't. If you got words in there I've kind of missed them if they're in there.

They might even be in the catalogue in the back. But that's more failure modes of smaller pieces where you wouldn't have that problem. Sorry for the interruption.

MR. BLANCHARD: I think that particular issue is probably more in the hazard analysis report than it is in the modeling.

MEMBER BLEY: Well it is, but if it makes it through and it's in the system, you got to model it like a form of dependency across the pieces that are communicating with a data string.

MR. BLANCHARD: Right.

MEMBER BLEY: Because they can bring corruption with them and cause lockups and other problems. So you can pick it up in the modeling if you're thinking about it.

MR. BLANCHARD: Right.

MEMBER SCHULTZ: And it needs to be in that dialogue in Steps 1 and 2.

MR. TOROK: Well I think you do have that effectively in your next slide coming up.

MEMBER BLEY: Is it?

MR. TOROK: Well in the next, the TCF slide. It does it too.

MEMBER BLEY: I mean it might be obvious to you guys, but to the guy out in the plant who hasn't thought about this a lot, it might not, it might be too subtle --

MR. TOROK: Maybe the way the linkages are between different things, they want to be in there.

MEMBER BLEY: Yes.

MR. BLANCHARD: All right, the fourth step in the process is for the PRA folks to take the information that's been generated thus far and build a high level representation of the digital system into this PRA.

And this is where this block diagram comes in showing all the different places that the I&C can have an effect. Both at the division level as well as common-cause within individual mitigating systems,

across mitigating systems.

And if it's identified and is possible to, you know, move things in the operator actions. And perhaps even between the I&C for the initiating event and some of the I&C systems.

And this is all at a high level at this point. We need to --

CHAIRMAN STETKAR: Dave?

MR. BLANCHARD: Yes.

CHAIRMAN STETKAR: No, no, no. This is perfect. I wanted to wait till this slide before I brought it up.

The nice little dotted box that says operator action and associated human systems interface. Back when I go into the more detailed guidance, in Section 4.1.4, there's a discussion and I'll just read this so it's on the record.

Main control room instrumentation systems are typically not modeled explicitly in the PRA.

MR. BLANCHARD: Right.

CHAIRMAN STETKAR: Parenthetically I agree with that and I'll continue now with the quote.

Adequate instrumentation is assessed in the human reliability analysis. This includes

implicit modeling of instrumentation dependencies in the HRA if there dependencies upon the initiating event, for example, power dependency. The diversity and redundancy of instrumentation is usually sufficient that its failure is an insignificant contributory to the HRA. And its reliability can be included in the HRA if this is not a case.

System-based EOPs often provide appropriate guidance, irrespective of the availability of specific instrumentation, further reducing the significance of modeling operator informational I&C in the performance of human reliability analysis.

What this tells me is, don't worry about, the HRA folks will take care of it. I submit that if my digital instrumentation control system causes all 12 of those valves to go open and simultaneously won't tell the operator that he's overcooling, we have a problem.

MR. BLANCHARD: And that's where we get into the simple EOPs because --

CHAIRMAN STETKAR: No, no, no. The operator doesn't know. He doesn't know that he's overcooling.

MR. BLANCHARD: He's --

CHAIRMAN STETKAR: He don't know.

MR. BLANCHARD: He's blowing down all the steam generator --

MR. IDRISSI: No, no, he don't know that. He doesn't have any of that indications because my digital system has made his great displays go black.

MR. BLANCHARD: Well going black is probably a good failure mode because he knows not to trust that, right? It's when they read normal that he's probably got a bigger problem.

But I've been in a plant where all the steam vents came open and he knows that that's what happened, okay. Now maybe --

MEMBER BLEY: Your plant had lots of instruments that weren't all hooked together in a digital system.

PARTICIPANT: He can hear it.

MR. BLANCHARD: No, he can feel it.

CHAIRMAN STETKAR: No, you can't.

MR. BLANCHARD: But I think there are several aspects here. You would definitely be into some more than EOPs at that point, which would, you know, provide some guidance. You know, maybe it wasn't completely written. Definitely wasn't written

for that --

CHAIRMAN STETKAR: Which is why the guys at H.B. Robinson didn't recognize the fact that they had loss coolant to their reactor coolant pumps which is why we've had fire. That's when people got focused over on other things despite the fact they've had system oriented procedures, and the instrumentation available, to tell them what was going on.

Just I can give you counter example after counter example.

MR. BLANCHARD: But then one additional argument is the Branch Technical Position 19 requires the set of independent display of controls to be normal.

CHAIRMAN STETKAR: Have you thought at all, my whole point is that this write up perpetuates the notion this human reliability analysis is not an integral part of the plant model. It's a don't worry, the HRA people will take care of this because you look at procedures, you look at Branch Technical Positions, you look at all of that wonderful stuff. It doesn't tell the people, now your PRA analysts and your I&C analysts to also think about how this stuff might effect the human. How it might just confuse the hell

out of the human.

MEMBER BLEY: I mean the good thing you had in the flow chart was you finally got it saying PRA guy, don't go off and try to do this by yourself. Work with the I&C guy.

And elsewhere we told people doing PRA not to go off without people who understand the systems and operations. But right here's a place we could remind them.

And we have HRA people, despite 20 years of telling them you can't do an HRA if you're not part of the integrated team, we still have people going off to do HRA without really understanding the event trees and the fault trees and the operations of the plant.

And I really agree with John on this one. It's an opportunity to say this ought to be an integrated development. And I&C and humans are so closely integrated, it belongs together.

CHAIRMAN STETKAR: And it might be true. That if indeed, under whatever conditions you've established here, that it makes the whole screen go blank and does not affect those other diverse, you know, you have a higher likelihood of people succeeding then if the screen was half black, you

know, if you will.

MR. BLANCHARD: Right.

CHAIRMAN STETKAR: But identifying conditions where it might make it half black might be important. Because they might have a high likelihood of getting confused.

MR. BLANCHARD: Right.

CHAIRMAN STETKAR: That's the only point that --

MR. BLANCHARD: Yes, that last sentence in that particular section is black and therefore you don't need to know that.

CHAIRMAN STETKAR: That's --

MR. BLANCHARD: I agree, there's some caveats there that are expressed in that section that I --

MEMBER SCHULTZ: The encouragement is for you to turn that around completely because you've got the arrows pointing into the right box, you just haven't elaborated about it.

CHAIRMAN STETKAR: The arrow is pointing to the right box, but when you final get down to where people are going to read it and say --

MEMBER SCHULTZ: Right.

CHAIRMAN STETKAR: -- oh, EPRI told me that I didn't need to think about this because --

MEMBER SCHULTZ: Health will take care of it.

CHAIRMAN STETKAR: -- he, as the HRA person, will think about it. Okay, I don't talk to him because --

MEMBER BLEY: Because he doesn't even know about these failure modes.

MEMBER SCHULTZ: The HRA won't take care of it unless he's talking to the other parties.

MEMBER BLEY: That's right.

MEMBER SCHULTZ: So you've got a great setup here and we just want to make sure it's utilized to its full extent.

MR. TOROK: That's a point well taken. I wish we had come to you guys two years ago and we could have gotten it right.

MEMBER SCHULTZ: Oh, it's not too late. It's not too late to get it right.

CHAIRMAN STETKAR: It is too late, they published this already.

MEMBER SCHULTZ: I understand.

MR. TOROK: That's okay, we --

MEMBER SCHULTZ: EPRI is a living organization --

MR. TOROK: Yes, we have a --

MEMBER BLEY: They'll talk to people, they can make sure this --

MR. TOROK: We have a list, it's okay.

MEMBER SCHULTZ: I know you're still doing your PRA training frequently so, for practitioners, that's great.

MR. BLANCHARD: All right, we've incorporated at a high level the effects of a digital I&C under the PRA and now we need to start generating some probabilities for potential misbehaviors that we believe are important that you can look from vendor operating experience, maybe international standards.

We have IEC-61226 here to quote. For an individual system which incorporates software developed in accordance with the highest quality criteria, a figure of the order of 10 minus 4, failure for demand may be an appropriate limit to place on the reliability that may be claimed.

And this is a sensitivity study that we're going to start with, and so our recommendation is, this is an appropriate value, assume we have high

quality digital systems and appropriate value to begin with, and do a number of sensitivity studies varying that parameter, common-cause beta factors in order to identify which parts of the digital system are important to the PRA or the operation that you're doing.

MEMBER BLEY: It's tied this to the I&C. Have you gone further and gone back to chase the pedigree on this?

MR. BLANCHARD: I'm --

MEMBER BLEY: Based on where --

MR. BLANCHARD: We're going to get back to a statement that we discussed earlier. And that was, if you pay attention to the defense and depth and diversity of the mechanical and electrical systems and you reflect that in your I&C, all you really need is a digital system that is reliable as a comparable analog system. And we know we can do better than that.

What this is getting, what this sensitivity study will be getting to is that the PRA may well be insensitive to the probability that you put on some of you digital components.

MEMBER BLEY: Well you're almost to that box in your flow chart.

MR. BLANCHARD: Right. Yes, that's the next step. Right. And if it's insensitive to it then perhaps using an I&C standard is adequate for the purpose of a particular application that you're doing.

CHAIRMAN STETKAR: Well but Dennis is asking, what's the basis for that number in the IEC standard. My basis is that I fly on airplanes a lot, the crash frequency ought to be zero. That's what it ought to be.

IEC for the number, I've looked at it, I can't find a genesis for that number other than it's a nice goal.

MR. TOROK: I think it's a --

MEMBER BLEY: Ten guys in a room wrote it down.

MR. TOROK: That's right. And it's based on process only too.

MEMBER BLEY: Well --

MR. TOROK: As opposed to design.

CHAIRMAN STETKAR: Yes.

MR. TOROK: But that's very different, well I don't know how different it is actually, from what the FAA version says, right? Where if you follow the process and all that they'll take your word, well

I shouldn't say it this way, but they will accept the claim that the failure probability is less than ten minus 9 per hour. I think that's the number they used. And there again, it's just the opinion of a bunch of experts.

CHAIRMAN STETKAR: And they ---

MR. TOROK: It's qualitative, right? Now I think, as part of Dave's word, you want to say, well, it's okay to have a qualitative number and an estimate because the results aren't sensitive to it.

MEMBER BLEY: Yes.

MR. TOROK: Because in part. Anyway, don't let me --

MEMBER BLEY: No.

MR. TOROK: -- understate that.

MEMBER BLEY: Well I mean, you did have a may, they had a may in their statement.

MR. TOROK: Yes.

MR. BLANCHARD: That's right. There is definitely uncertainty around that. And what we're going to do is find out how important that uncertainty is. All right?

And so the next step in the process is to do a sensitivity study on the model we've developed it

up to this point. And the way we're going to do this sensitivity study is we're going to take the failure probabilities for digital I&C, as you've modeled it, and raise those failure probabilities in order of magnitude, raise the common-cause beta factors.

Now the beta factors within a system of the software are already set to one because of the systematic, assuming systematic behavior of the software. But we have some common-cause factors in between systems, which perform different functions, maybe received different signals.

So we're going to raise the beta factor of those for this particular sensitivity study. And the idea here is to do a sensitivity study which in the end collectively shows the parts of the I&C system that you think the PRA or your application has low sensitivity to and collectively show that it really doesn't effect the decisions you're making for that application by varying the failure probabilities and beta factors.

CHAIRMAN STETKAR: You know, conceptually I understand the notion of this step. In practice I've seen people write these things in human reliability analysis. It's called scoping step.

In practice, human reliability analysis, I talk to every, every analyst I've ever spoken with said, that's kind of useless. You know, yes we can do that, but we always determine the thing is so sensitive that we need to do the detailed modeling anyway.

So the question is, do you actually expect to kick out much stuff off to the right as a result of this? In this practice.

MR. BLANCHARD: Yes.

CHAIRMAN STETKAR: You do? Okay. Now then, before you go on, I'll challenge you.

This now feeds back into my initial question that perhaps that might be true for failure to perform this specific functions that you've modeled in the PRA. It might not be true for it doing undesired things to you that you haven't thought about.

And my concern is, if you're kicking stuff out to the right chunks of the digital I&C system based on the fact that they're not important to achieving the functions that you've modeled, you might not go back and think about those things again. Unless you've considered all of those other failure

modes first.

MR. BLANCHARD: Yes. There is --

CHAIRMAN STETKAR: You know, that, my example of opening up all the steam valves or something like that.

MR. BLANCHARD: Right. We talked earlier about this completeness question --

CHAIRMAN STETKAR: Yes.

MR. BLANCHARD: -- and whether or not the PRA that you're starting with, in fact has --

CHAIRMAN STETKAR: If it indeed is complete, I agree with you.

MR. BLANCHARD: Right. And so we need to get into Steps 1 and 2. The question by the PRA folks, what haven't I modeled, what did I conveniently leave out --

CHAIRMAN STETKAR: This is the problem that a lot of the fire analyst people have run into. You know, you're aware of this that they kind of, my God Almighty, I have to put all of this stuff in the PRA because I never thought of it before.

MR. BLANCHARD: Well I thought of it but I knew it wasn't important, so --

CHAIRMAN STETKAR: But I knew it wasn't

important for starting HPCI or something like that.

MR. BLANCHARD: Yes.

CHAIRMAN STETKAR: You're right.

MR. BLANCHARD: Right, so we have to address that completeness question early in the process and then we'll get down here to the sensitivity study. And maybe we're still not a hundred percent complete, but we're a lot farther towards that goal.

CHAIRMAN STETKAR: Okay.

MR. BLANCHARD: Well, I do the sensitivity study and it's not for the purpose of limiting the work that the PRA folks have to do in modeling the digital I&C in more detail. It's really for the purpose of influencing the I&C design where we can practically do this.

Right now where we are, at least in the U.S., is that there are a number of plants considering doing upgrades to their protection systems and they're just in the process of developing those designs. And with an evaluation like this, we can identify, with a sensitivity study like this, where the design may actually influence safety, may actually influence the results of the PRA and where it doesn't.

And the question that I would expect to be asked, if you identify a portion of the I&C system as the PRA being sensitive to that, is the potential for core damage or the potential for a large early release to be sensitive to that. The natural and next question is, well what can I do about it?

Given that the I&C systems are currently being designed, we can now influence the designs with the PRA much in the way the new plants are designed, as they design their plants for their I&C systems. So that's the purpose of the sensitivity study.

CHAIRMAN STETKAR: And that's a good, I think that's a, and I didn't think about it from that perspective quite honestly. But again, I'll come back this completeness issue because I'll give you an example that we kind of stumbled on.

It doesn't have to with I&C necessarily, but it could. On one of the new designs where they did not have, I think this is on, well I interpret what's on the record and what's not on, where they did not include in their PRA, for example, a certain failure mode spurious opening of a certain set of valves that would drain their injection water supply. Put it in a place where it ought not to be.

Now all of the controls for those valves were part of the digital instrumentation. Under certain sets of conditions that the designers had built in, certain temperatures and things like that, those valves were supposed to open because that was an indication of needing to put water in Place A rather than Place B or Place B rather than Place A.

If you've thought about that, in terms of completeness of what the instrumentation control system can do to you, they hadn't. Because they hadn't included that failure mode in the PRA, therefore hadn't even challenged themselves.

MEMBER BLEY: They only thought about those valves under the case where you wanted the water there.

MR. BLANCHARD: Right.

CHAIRMAN STETKAR: Do they fail to open? So this comes back to the completeness stuff. And that can be important when you're starting to make decisions, even then, about designing your system.

Because if your system is somehow now vulnerable under certain conditions, to giving you a signal to open those valves, if you only got the single input signal or something like that, that could

be important information to feed back to the designers, you know, even in this context.

MR. TOROK: How are you going to make sure that doesn't happen, right? That's the question for the designer at that point.

CHAIRMAN STETKAR: Well first you have to, I mean --

MR. TOROK: You have to --

CHAIRMAN STETKAR: -- think about it.

MR. TOROK: That's the problem right. But then the next question is, what are you going to do?

MR. BLANCHARD: All right, so that's the purpose of the sensitivity study.

CHAIRMAN STETKAR: And, okay.

MR. BLANCHARD: And we've done the sensitivity study on a number of PRAs for individual systems and for entire accidents sequences, even on Level 1 internal events PRA.

And for each of these, which did, in the plants that we did the sensitivity studies on, the I&C was modeled in, the analog I&C was modeled in some detail. And we found that it, generally that I&C was not generally an important contributory to risk in their PRA for either individual systems or for the

accident sequences as a whole.

So what we want to do with the sensitivity study is help keep it that way. We want to continue to have the I&C not be significant for the general risk. And again, that gives us the opportunity to influence the design. Okay? All right.

MR. TOROK: We've got 18 minutes.

MR. BLANCHARD: Okay. Well we're on section --

All right, so now that we've done the sensitivity study we've classified portions of the I&C systems as being relatively safety significant or influences the PRA or the decision you're going to make for the application of the PRA. And we have a number of systems, portions of the digital I&C system, to which the PRA is not sensitive.

Now we go ahead and begin to complete the model and perhaps expand the model for the high sensitivity systems and assign data to the expanded model.

For the low, for the portions of the digital I&C systems to which the PRA or your application is not sensitive, the level of modeling detail may be very similar to what you used in your

sensitivity study. So you may be very close to where you need to be for modeling the low sensitivity portions of the I&C.

So the high sensitivity I&C system is, again, we're back to what kind of detail do you need in your PRA? And our guideline recommends, you know, very similar to the way we model analog I&C, sensors, signal processing, voting logic.

Once again, as you're modeling different types of components, components that have processors in them instead of components, such as contacts and relays.

And in this portion of the guideline we also note that maintenance errors, an unavailability to do maintenance, we should break that out and model that separately at this point in the modeling.

Now we have to assign data to the new portions of I&C that we've incorporated in the PRA. Again, for low sensitivity systems what you've done as part of the sensitivity study maybe sufficient in IEC standards or statistical testing, if you haven't had that available with the vendor, operating experience that the vendor beta is available.

For high sensitivity systems we now have

to go down to the component level of the assigned beta. And the guideline recommends one of two approaches for this. One is statistical custom and it's similar to what we heard this morning.

The second is it comes out of the estimating failure rates for high reliability digital systems. That EPRI report that we noted earlier in the presentation.

And it recommends assigning data to the components in the digital I&C system for the hardware as well as the software portion. In my presentation I'll focus on the software portion.

What's recommended in the guideline at this point is that you go down to the computing minute level, say the voting logic or the signal processing units, and break each of the computing units up into its, for the software up and through various parts.

The operating system, elementary functions, application specific software and begin to review each of these portions for common failure mechanisms that might be applicable to one of those particular parts of the digital system. And where you identify defensive measures, you assess their effectiveness in addressing problems, common problems

that could occur with respect to each of those portions of the software.

And as you find that defensive measures are available, you screen those mechanisms out. And in the end you will be left with a small set of failure mechanisms that most likely dominate the potential for misbehavers of the digital system.

You need to recognize that you're probably not going to be able to screen out all the potential sources of failure mechanisms. Among them are specification, functional specifications on the design errors.

And we expect --

MEMBER BLEY: I guess I would think some for which you have defensive measures, while they become less likely, aren't really less likely enough to remove. So maybe somehow you --

MR. BLANCHARD: Right, this is kind of a map --

MEMBER BLEY: Oh, okay.

MR. BLANCHARD: -- there's only --

MEMBER BLEY: Fine.

MR. BLANCHARD: Yes, there's only so far you can go with respect to eliminating all these

failure mechanisms. You're always going to be left with the unknown unknowns. The things you didn't think about, okay.

And we think those will likely be dominated by functional specification and design errors. Okay. And operating experience supports that. I think there is published information that also supports that.

MR. TOROK: Dave's talking about the OE that we looked at a few years ago that we talked with you guys about. We were looking at for it potential and actual common-cause failures --

CHAIRMAN STETKAR: That was still pretty limited and mostly for, you know, digital feedwater control systems and stuff like that.

MR. TOROK: It was digital safety and non-safety, but it was all we had.

CHAIRMAN STETKAR: The safety was pretty limited though, if my recollection serves.

MR. TOROK: That's right. There wasn't a lot there. But in a way it, how should I say it, it supported the work of others who said that on their investigations, it came down to functional specification errors most of the time.

CHAIRMAN STETKAR: Okay. One of the things here, Dave, and I have to count this, we don't have 1021077. And I tried to find it, I'm not going to pay $25,000 for it because I'm a poor farm boy trying to make a living in the free technological world, so I'm not sure what detailed guidance, you know, you've excerpted sort of high level snippets in this report --

MR. BLANCHARD: That's right.

CHAIRMAN STETKAR: -- so I'm not sure what details are in there, so I'll give you the benefit of the doubt.

On the other hand, there is no mention whatsoever in the report that we have, in the quantification area, about addressing uncertainties. Despite the fact that it says that there is a high level of uncertainty.

So I'm not sure whether the more detailed guidance in that other document addresses this issue of uncertainty or not.

MR. BLANCHARD: No, that --

MR. TOROK: I would have to say not.

MR. BLANCHARD: That other document doesn't address uncertainty and how to quantify it.

It doesn't either. Yes, that's definitely something that's missing from the guidance.

CHAIRMAN STETKAR: Because, especially if the actual, if the operational data experience are quite rare. In many cases you probably will have to revert to some sort of expert opinion, elicitation, whatever you want to call it.

At least even in a Bayesian sense as a basis for some sort of prior distribution which you can then update with whatever experience you do have available.

MR. TOROK: I agree.

CHAIRMAN STETKAR: And that, of necessity, introduces the notion of uncertainties.

MR. TOROK: Yes.

CHAIRMAN STETKAR: Again, not having that report I didn't know how much it addressed the --

MR. TOROK: It doesn't really get into that. But then the other question that we come back to is, how sensitive are the results --

CHAIRMAN STETKAR: Well but that's fine. But you can still look at those, if there's a five percent probability that the failure rate is two, I'm sorry, one, if it's two there's something wrong, but

if it's one, you might be willing to accept that. If there's very broad uncertainties.

MR. TOROK: Yes.

CHAIRMAN STETKAR: Given everything else.

MR. BLANCHARD: All right, with respect to the operating experience, in fact the industry does have some. Particularly with respect to the unknown unknowns. The designer errors and the functional specification error. And EDF has provided that information for this report. They have over 500 reactor operating --

CHAIRMAN STETKAR: They, of anybody in the world, they would have it. Maybe the Japanese might have some.

MR. BLANCHARD: And so what we did is we used that to estimate a failure probability for the functional specification and design error as a part of this report. And, you know, that data is also provided in the 1021077 report.

All right, having generated detailed logic models where we need them, and again, the detail only goes down to the computing unit level, assigned data to that based on the availability of defensive measures and their effectiveness. We now incorporate

that with PRA, regenerate the PRA results and repeat some of our sensitivity studies, identify what now dominates the risk associated with the PRA.

And the last step of the process is to present those results to not only the I&C folks, but members of the plant staff and providing them with the assumptions that the results of sensitivity training and also explaining to them what dominates the risk of the PRA in terms of the design features of the plant and the way it's operating.

And then have the plant staff come to the conclusion about both the classifications of the digital systems in terms of what's, and what is the, you know, safety significance of what it is and confirm some of the assumptions with PRA results.

Now coming to the conclusions, the guideline emphasis the model development ought to be a collaborative effort between the designers and the I&C personnel, the PRA analysts.

The level of detail needed in the model is dependent on the context of the I&C within the overall plant design. The importance of the systems that the I&C controls dictates the level of detail, even in the I&C system itself.

In developing probabilities of misbehavior of the I&C system and its components, you should consider a blend of diversity and defensive measures, which are available both within the I&C system and external of the I&C system to cope with such misbehavers.

And then software, for the most part, behaves deterministically. What we're trying to model in the PRA is the effects of encountering conditions for which the software wasn't designed and having its response being adverse for the functions that we're trying to accomplish. The safety functions we're trying to accomplish in modeling the PRA.

And the initial insights that we got out of our research on applications before we developed the guideline and also within the guideline, because we really think it's important to be modeling the digital systems in PRA now as they are designed before they are installed in order to have some influence on them.

And at the end of the presentation we have a number of references from which we drew our research and --

CHAIRMAN STETKAR: Ah, his name is

Yastrebenetsky.

MR. BLANCHARD: What?

MR. TOROK: Oh, now he wants to know how to pronounce this.

CHAIRMAN STETKAR: No, in the report, I've been looking for that paper, I don't know whether it's available, but I believe it's --

MEMBER SCHULTZ: There you have it.

CHAIRMAN STETKAR: No. I think in the EPRI it's Y-A-T-R-E --

MEMBER BLEY: Oh, it's spelled differently?

CHAIRMAN STETKAR: -- netsky.

MR. TOROK: We misspelled it?

CHAIRMAN STETKAR: Yes, I think --

MR. TOROK: I can't imagine.

CHAIRMAN STETKAR: -- because I was googling two nights ago trying to find that.

MR. TOROK: But that's right, the way it is there I think.

CHAIRMAN STETKAR: Well this may be right. I'll tell you, I couldn't find it any other way, so.

MR. TOROK: It's from an NPIC paper from a few years ago. And what he did was pretty similar to

what we did with the U.S. data.

CHAIRMAN STETKAR: Well because I couldn't find --

MR. TOROK: Yes.

CHAIRMAN STETKAR: -- because I couldn't find yours I was looking to see whether I could find his.

MR. TOROK: And he had pretty similar results by the way.

CHAIRMAN STETKAR: Did it?

MR. TOROK: In terms of software not dominating the problem. I wonder, I must have that paper somewhere.

CHAIRMAN STETKAR: Oh, you probably --

MEMBER BLEY: I think I do too.

CHAIRMAN STETKAR: You guys are really good in terms of timing.

MR. TOROK: That's why we're here for you. We could go on if you want.

CHAIRMAN STETKAR: I'm sure you could. As could we, but we won't.

MEMBER BLEY: I think it referred to a lot of IEC standards, which near as I can tell, we don't keep here when I look on the internal website.

MS. ANTONESCU: Yes, we do in the library.

MEMBER BLEY: The library. But I looked on the website where we have all the standards and I didn't see them there.

MR. SYDNOR: I don't think we have an agreement with IEC via the electronic.

MEMBER BLEY: Okay.

MR. SYDNOR: But we do have --

MEMBER BLEY: But we do have hard copies?

MR. SYDNOR: I don't think we have --

MS. ANTONESCU: Yes, you know, you're right.

MEMBER BLEY: Okay. Okay. Yes, I mean they're not as expensive as some other people's reports.

CHAIRMAN STETKAR: Poor farm boy trying to make a living out here in the big world. Thanks. And for my own, again, this is subcommittee meetings so we're allowed to make individual comments.

There are lot of things that, about this approach that I like a lot. I think that, you know, you've heard my comments about completeness and thinking about it, but I think this approach make a lot of sense. In my own personal opinion, you might

have other opinions from other's but --

MR. TOROK: Could we get you to write that down? Just kidding.

MEMBER SCHULTZ: It's on the record.

CHAIRMAN STETKAR: It's on the public record. You do with it what you will. And it's only one opinion of a member of a small, a decreasing subcommittee.

With that, do any of the members have another questions or comments for EPRI? If not --

MEMBER BLEY: Just at the end of the day I thank everybody for really good discussions.

CHAIRMAN STETKAR: Let me do one more administrative thing, make sure we get the line open again because --

MEMBER BLEY: Oh, yes. The bridge open.

CHAIRMAN STETKAR: It is open, thank you, Theron. First, is there anybody in the room whose anything they'd like to add or make any comments?

If there is anyone out there on the bridge line, do me a favor and just say hello or something so I know you're out there and we confirm that it's open?

PARTICIPANT: Hello.

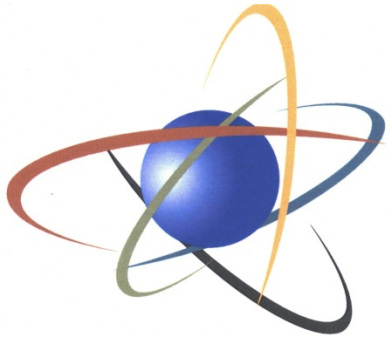
CHAIRMAN STETKAR: Thank you very much.

Okay, that being confirmed, is there anyone who would like to make any comments regarding the presentations that we've heard from EPRI? Hearing silence I will assume that is a negative.

And as Dennis mentioned I would, I like to thank everybody. I think that today's presentations were really, really useful. I know we had to skip a couple of the shorter ones and I apologize for that. It's a full day.

And we will see everybody else in the morning, as far as I know. And with that, we are recessed until tomorrow morning.

(Whereupon, the above-entitled matter went off the record at 6:01 p.m.)



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

NRC & EPRI DIGITAL SYSTEM RESEARCH

Digital System PRA Methods, Failure Modes and Hazard Analysis

Joint Digital Instrumentation and Control Systems and Reliability and PRA Subcommittee Meeting
November 18-19, 2014

Kevin Coyne and Russell Sydnor

Office of Nuclear Regulatory Research
(301-251-7586, kevin.coyne@nrc.gov)
(301-251-7405, russell.sydnor@nrc.gov)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Purpose

- To present status and results of NRC Digital System research activities of interest to the ACRS
- To discuss and obtain insights from ACRS members on the results and direction of Digital System Regulatory Research
- To support presentation of related Industry (EPRI) research status and results
- No letter is requested

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Background

June 7, 2011– ACRS Digital I&C Systems Subcommittee Meeting

- **NRC Staff presented overview on quantitative software reliability methods, plans to implement BBN and STM methods**
- **ACRS Feedback:**
  - **Achieving an appropriate balance between system complexity and PRA modeling.**
  - **Understanding of digital system failure modes (with regards to completeness of PRA context and dependencies)**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Background

September 19, 2013 – ACRS Digital I&C Systems Subcommittee Meeting

- **NRC Staff presented research results - Digital System Failure Modes and Hazard Analysis**
- **ERPI presented their research work on Hazard Analysis and related topics**
- **ACRS Feedback:**
  - **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.**
  - **Staff agreed to provide ACRS a briefing by both DE and DRA staff to address concerns.**

Relationship Between RES Activities - Objectives

- All RES digital I&C Activities are covered by the FY2010 – FY2014 Digital System Research Plan
- Research Objectives:
  - ALL: Understand digital system behavior
  - RES/DE: Develop staff position and review guidance to support deterministic safety reviews and licensing of digital systems
  - RES/DRA: Develop methods and associated guidance for including digital systems (HW and SW) in nuclear plant PRAs

Relationship Between RES Activities – Reliability Analysis

- **Role of Qualitative Reliability Analysis**
  - **RES/DE: Directly supports staff assessment of digital systems**
  - **RES/DRA: Provides modeling insights**
- **Role of Quantitative Reliability Analysis**
  - **RES/DE: Not used to support a "reasonable assurance" finding, but can provide insights**
  - **RES/DRA: Ultimate objective of method development activities. However, the practicality and usefulness of proposed methods is still being evaluated**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Relationship Between RES Activities – Failure Modes

- **Failure Modes**
  - **Provide insights into the behavior of a digital system**
  - **Insights are dependent upon scope, analysis boundaries, and level of detail considered in analysis (e.g., function, system, train, component, subcomponent)**
  - **RES/DE: Supports FMEA/Hazard Analysis, system design reviews**
  - **RES/DRA: Characterizes basic events in PRA model**

Relationship Between RES Activities – Failure Modes

- **Failure mechanisms produce failure modes which in turn have failure effects on the system (NUREG-0492)**
- **As the level of analysis becomes more detailed:**
  - **Failure mechanisms become failure modes at the next level**
  - **Failure modes become failure effects at the next level**

Level of Detail	Failure		
	Mechanism	**Mode**	**Effect**
Train	Valve Fails to Open	No Flow	
Component (Valve)	Stem Binding	Valve Fails to Open	No Flow
Subcomponent (Stem)	Corrosion of Stem	Stem Binding	Valve Fails to Open

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Relationship Between RES Activities – Failure Modes

- **For PRA, need to model digital system at a level of detail that:**
  - **Captures function and/or system failure effects**
  - **Can adequately represents potential dependencies**
  - **Can support parameter estimation**
- **For deterministic licensing applications, need to consider level of detail that supports reviews, for example:**
  - **to determine that digital system design meets single failure requirements**
  - **to determine that digital system design meets independence requirements**
- **PRA modeling will generally require less detail than deterministic licensing applications**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Today's presentations

- **RES/DRA – Digital System PRA research topics**
  - **Ming Li**
  - **Louis Chu and Athi Varuttamaseni (BNL)**
  - **Tim Kaser and George Marts (INL)**
  - **Dr. Hyun Gook Kang (KAIST) and Dr. Seung Jun Lee (KAERI)**
- **EPRI - Digital System PRA, Failure Modes, Failure Prevention & Mitigation, and Hazard Analysis**
  - **Ray Torok, Dave Blanchard, Bruce Geddes**
- **RES/DE - Failure Modes in Digital Systems**
  - **Mauricio Gutierrez and Ming Li**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Key Messages

- **RES/DE and RES/DRA digital system research is complimentary and aligned,**
- **Related NRC and Industry research is complimentary and aligned,**
- **RES/DE, RES/DRA and EPRI agree on basic digital system behavior concepts**
  - **Use, intent and focus sometimes drives differing objectives**

Overview of Digital I&C PRA Research Activities

ACRS Meeting
Rockville, MD
November 18-19, 2014

Ming Li
Probabilistic Risk Assessment Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research
(301-251-7627, ming.li@nrc.gov)

Digital I&C Research Plan (ML082470722)

- 3.1.6: Digital System PRA
  - Objective: Identify and/or develop methods, analytical tools, and regulatory guidance for:
    - Including digital system models into nuclear power plant (NPP) PRAs
    - Incorporating digital systems into NRC's risk-informed licensing and oversight activities
  - Research areas:
    - Failure modes identification and failure effects determination
    - Hardware components failure data
    - CCF modeling and parameter estimation
    - Uncertainty modeling
    - Self-diagnostics, reconfiguration, and surveillance modeling

Interface with RES/DE Activities

- 3.1.5: Analytical Assessment of DI&C Systems
  - Identify and analyze digital system failure modes
  - Discuss the feasibility of applying failure mode analysis to assess the safety impact of digital systems
- 3.4.5: Operating Experience Analysis
  - Analyze operating experience (OpE) of digital systems to identify credible failure modes
  - Use the knowledge derived from this analysis to improve the efficiency and effectiveness of regulatory reviews.

Probabilistic Modeling of Digital Systems

- Hardware reliability can be modeled
- Software fails due to “triggered” faults
  - Faults are design errors
    - Deterministic
  - Condition to trigger
    - Probabilistic
- Reasonable to model software failure probabilistically

software failure is defined as the triggering of a defect of the software, which results in, or contributes to, the host (digital) system failing to accomplish its intended function or initiating an unwanted action.

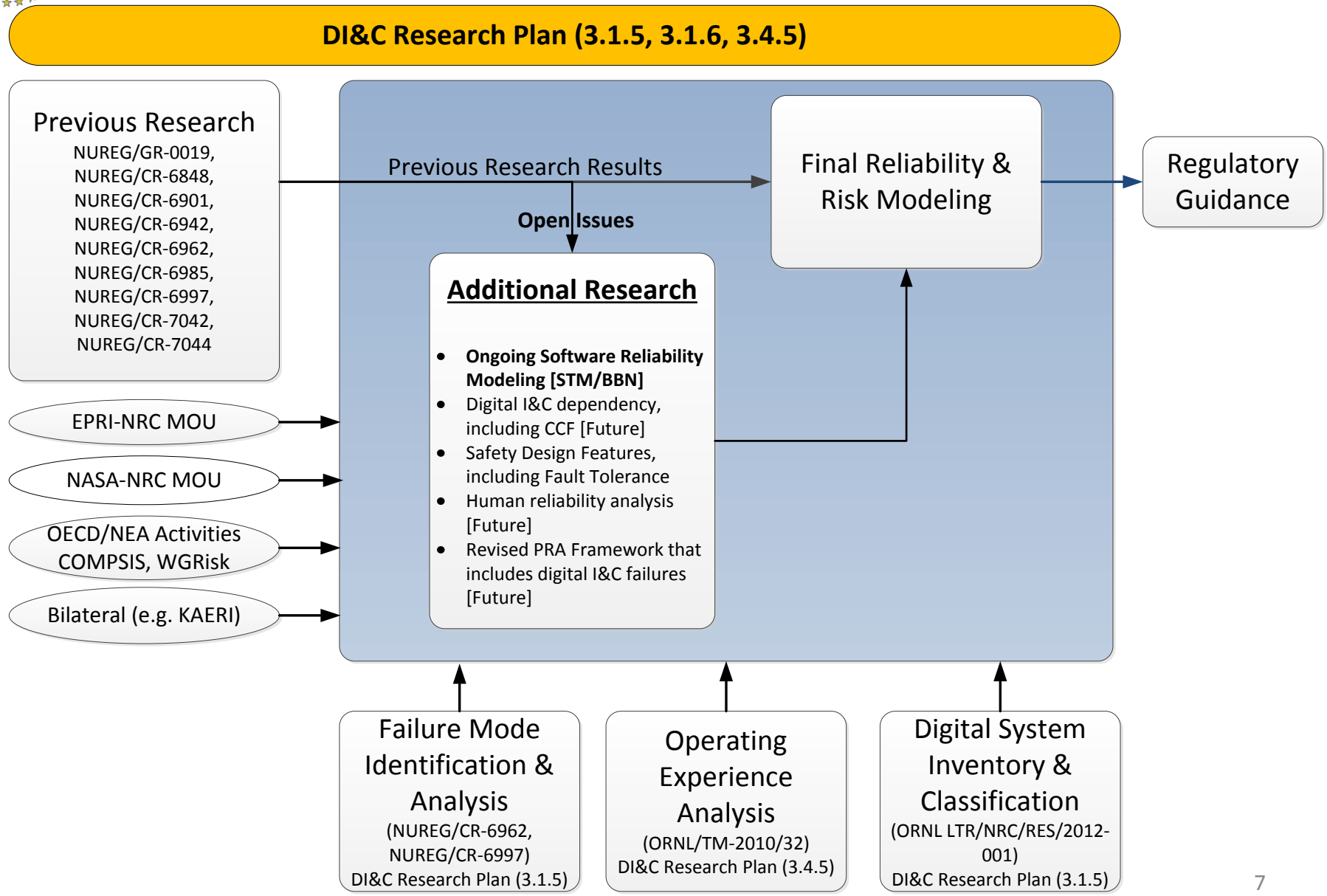
Challenges

- Software failure is a function of software defect content and software use
- Software defects generally include design errors
  - We don’t have a lot experiences of design errors
    - Significant system design variability
    - Appropriate level of detail
    - Data availability

Key Objectives

- Staff believes that modeling digital system in PRA is possible
- However, need to determine if
  - It is practical, and
  - Useful

Overview


DI&C Research Plan (3.1.5, 3.1.6, 3.4.5)
Previous Research
NUREG/GR-0019,
NUREG/CR-6848,
NUREG/CR-6901,
NUREG/CR-6942,
NUREG/CR-6962,
NUREG/CR-6985,
NUREG/CR-6997,
NUREG/CR-7042,
NUREG/CR-7044
Previous Research Results
Open Issues
Additional Research
Ongoing Software Reliability Modeling [STM/BBN]
Digital I&C dependency, including CCF [Future]
Safety Design Features, including Fault Tolerance
Human reliability analysis [Future]
Revised PRA Framework that includes digital I&C failures [Future]
Final Reliability & Risk Modeling
Regulatory Guidance
EPRI-NRC MOU
NASA-NRC MOU
OECD/NEA Activities COMPSIS, WGRisk
Bilateral (e.g. KAERI)
Failure Mode Identification & Analysis
(NUREG/CR-6962, NUREG/CR-6997)
DI&C Research Plan (3.1.5)
Operating Experience Analysis
(ORNL/TM-2010/32)
DI&C Research Plan (3.4.5)
Digital System Inventory & Classification
(ORNL LTR/NRC/RES/2012-001)
DI&C Research Plan (3.1.5)

Previous Research on Hardware/System Reliability Modeling

- Ohio State University/ASCA/University of Virginia – Dynamic reliability modeling methods applied to a DFWCS (NUREG/CR-6901 [2006], NUREG/CR-6942 [2007], NUREG/CR-6985 [2009])
- BNL – Traditional reliability modeling methods applied to a DFWCS (NUREG/CR-6962 [2008], NUREG/CR-6997 [2009])

Previous Research on Software Reliability Modeling

- UMD-OSU Metrics Based Studies (NUREG/GR-0019, NUREG/CR-6848, NUREG/CR-7042)
  - Ranked metrics with respect to estimating software reliability
  - From metrics to # of residual defects in the software
  - Estimate failure probability using finite state machine simulation and operational profile
- BNL Studies (NUREG/CR-7044 and ongoing)
  - Expert panel on software reliability
  - Ranked software reliability models and chose two for further study
    - Bayesian Belief Network (BBN)
    - Statistical Testing Method (STM)

International Activities

- OECD
  - Digital I&C – NEA/CSNI
  - Failure mode taxonomy
  - COMPuter-based System Important to Safety project (COMPSIS)
- Bilateral
  - South Korea (KAERI/KAIST)

Ongoing Research on Software Reliability

- Statistical Testing Method (STM)
  - Test software in a PRA context
    - Uses PRA to define the operational profile
    - Generates test cases via the operational profile based thermal hydraulic simulation
    - Integrated hardware/software testing environment
- BBN
  - Characterize software attributes that can affect reliability
  - Estimate the number of fault in the software
  - Estimate reliability

Path Forward

- Publish STM results in a NUREG/CR report
- Complete BBN research and publish results in a NUREG/CR report
- Update digital I&C research plan to reflect next phase of work

Insights and Results on Quantitative Software Reliability Method

ACRS Meeting
Rockville, MD
November 18-19, 2014

Ming Li
Probabilistic Risk Assessment Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research
(301-251-7627, ming.li@nrc.gov)

Tsong-Lun Chu
Brookhaven National Laboratory
(631-344-2389, Chu@bnl.gov)

Outlines

- Objectives
- Software reliability quantification methods
- Selection criteria
- Evaluation and candidate methods selection
- The example system
- Applications of candidate methods to the example system

Objectives

- Evaluate software reliability methods against a set of selection criteria and select two candidates method for further study
  - Obtain insights of candidate methods' feasibility, practicality, and usefulness of including digital I&C systems into PRAs
- Select an example system for application
- Develop approaches to apply candidate methods to the example system

List of Software Reliability Methods

- Software Reliability Growth Model (SRGM)
- Bayesian Belief Network (BBN)
- Test-based (black-box)
- Test-based (white-box)
- Frestimate
- Metrics-based
- Standard-based: IEC Safety Integrity Level (SIL)

Selection Criteria

1. Method description
2. Reasonable assumptions
3. Consideration of operating conditions
4. Consideration of life cycle quality
5. Use of data
6. Addressing uncertainty
7. Verification and validation
8. Demonstrating high reliability
9. Software CCF
10. Data availability

Evaluation Results

	1	2	3	4	5	6	7	8	9	10
SRGM	Y	M	N	N	Y	Y	Y	N	N	N
BBN	**Y**	**M**	**N**	**Y**	**Y**	**Y**	**M**	**M**	**N**	**M**
Test-based (black-box)	**Y**	**M**	**M**	**N**	**Y**	**Y**	**M**	**M**	**N**	**Y**
Test-based (white-box)	Y	M	M	N	Y	Y	N	M	N	Y
Frestimate	N	M	N	Y	Y	N	M	N	N	M
Metrics-based	Y	M	M	N	Y	Y	M	M	N	Y
Standard-based	Y	N	N	Y	N	N	N	N	N	N

- Y: YES, method conceptually meets the characteristic and its implementation is deemed practical
- M: MAYBE, method may conceptually meet the characteristic and/or its implementation may not be practical
- N: NO, method does not conceptually meet the characteristic

Example System

- Advanced Testing Reactor (ATR)
  - In pile tube (IPT)
- Loop Operating Control System (LOCS) functions
  - Control used to control the loop parameters specified by experiment requirements
  - Detect abnormal conditions in the IPT and its supporting systems to initiate mitigating actions
- LOCS is not a safety system
  - Does have demand function similar to safety system
  - Availability of information
  - Availability of actual hardware and software

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Development of a Bayesian Belief Network Model for Quantifying Software Failure Probability

Advisory Committee on Reactor Safeguards
Joint Digital Instrumentation and Control Systems Subcommittee and PRA Subcommittee Meeting

November 18 - 19, 2014

Tsong-Lun Chu
Varuttamaseni, Athi
Brookhaven National Laboratory
(631-344-2389, Chu@bnl.gov)

Hyun Gook Kang
Korea Advanced Institute of Science and Technology
(hyungook@kaist.ac.kr)

Seung Jun Lee
Korea Atomic Energy Research Institute
(sjlee@kaeri.re.kr)

BROOKHAVEN
NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Outline of Presentation

- Objectives and Background
- Development of a BBN model for estimating software failure probability
- Issues and limitations of the BBN method
- Treatment of uncertainty
- Project Status

BROOKHAVEN
NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Objectives

- Development of a BBN model for quantifying the probability of software failure of safety-critical systems, taking into consideration of the quality in the software development process.
- Application of the model to an example system to obtain a prior distribution for the probability of software failure, such that it can be further updated using the data from statistical testing of the system.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Bayesian Belief Network Models

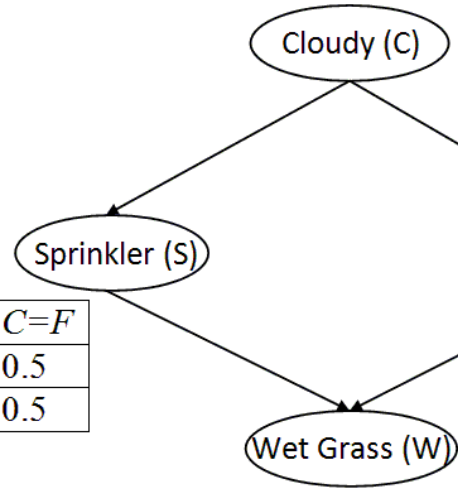
- A Bayesian Belief Network (BBN) is a probabilistic graphical model depicting a set of random variables and their conditional independencies via a directed acyclic graph.
- A basic assumption for BBN is that a node is conditionally independent of its non-descendent nodes, given its parent nodes. In addition, the root nodes are independent.
- For a BBN, the joint distribution of all variables $\{V_i\}$ is

$$P(V_1, V_2, \cdots, V_n) = \prod_{i=1}^{n} P(V_i \mid parents(V_i)).$$

- The conditional probabilities (Node Probability Tables) can be estimated using data, if available, and expert elicitation.
- Bayesian inference is performed by updating the above equation using the acquired evidence; there exists a spectrum of software tools for the inference.
- Before specific evidence is applied, a BBN model is generic.

An Example Bayesian Belief Network Model

$P(C=T)$	0.5
$P(C=F)$	0.5



	$C=T$	$C=F$
$P(S=T)$	0.1	0.5
$P(S=F)$	0.9	0.5

	$C=T$	$C=F$
$P(R=T)$	0.8	0.2
$P(R=F)$	0.2	0.8

	$S=T, R=T$	$S=T, R=F$	$S=F, R=T$	$S=F, R=F$
$P(W=T)$	0.99	0.9	0.9	0.0
$P(W=F)$	0.01	0.1	0.1	1.0

Reference: Murphy, K., "A Brief Introduction to Graphical Models and Bayesian Networks," 1998.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Applications of BBN Method to Software Reliability

- Some researchers consider that the application to software (SW) reliability is promising.
  - Johnson[2000] did not fully develop his model.
  - Littlewood [2000] suggested that BBN be used, and later further explored the use of BBN.
  - Gran [2000] developed a BBN model that used expert elicitation to directly estimate software failure probability.
  - Eom [2009] adopted the approach first developed by Fenton [2007] for estimating the number of faults remaining in a software program.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Approach for Developing the BBN Model for a Safety-Critical Software

- Consideration of 5 software development phases in which faults may be introduced and detected.
  - Software Requirements (SR)
  - Software Design (SD)
  - Software Implementation
  - Software Testing
  - System Installation and Check out

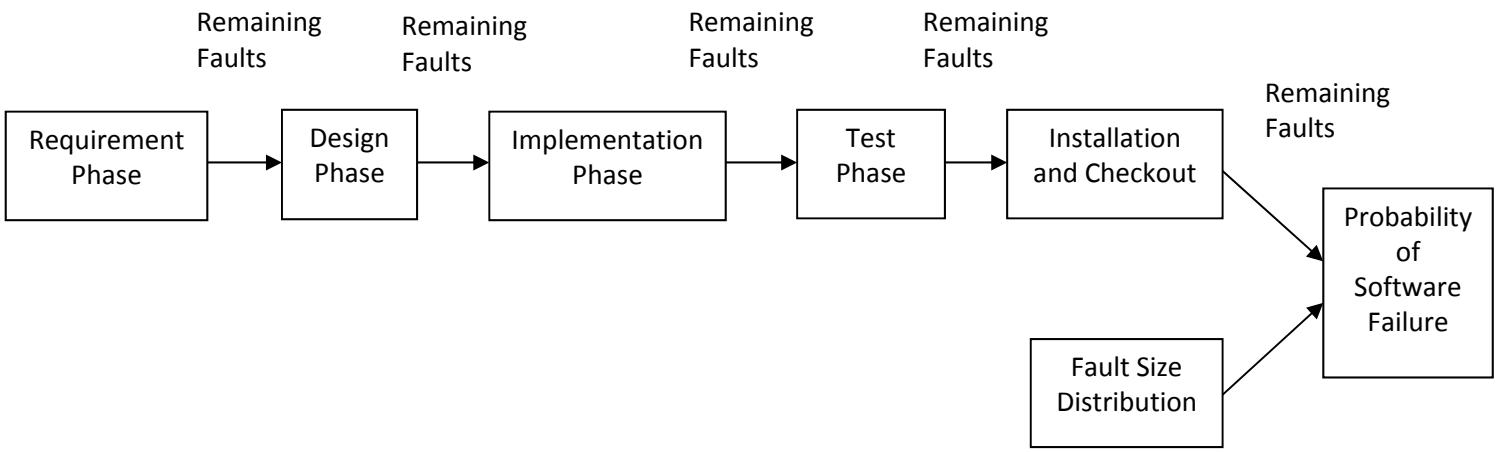
BROOKHAVEN
NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Approach for Developing the BBN Model for a Safety-Critical Software

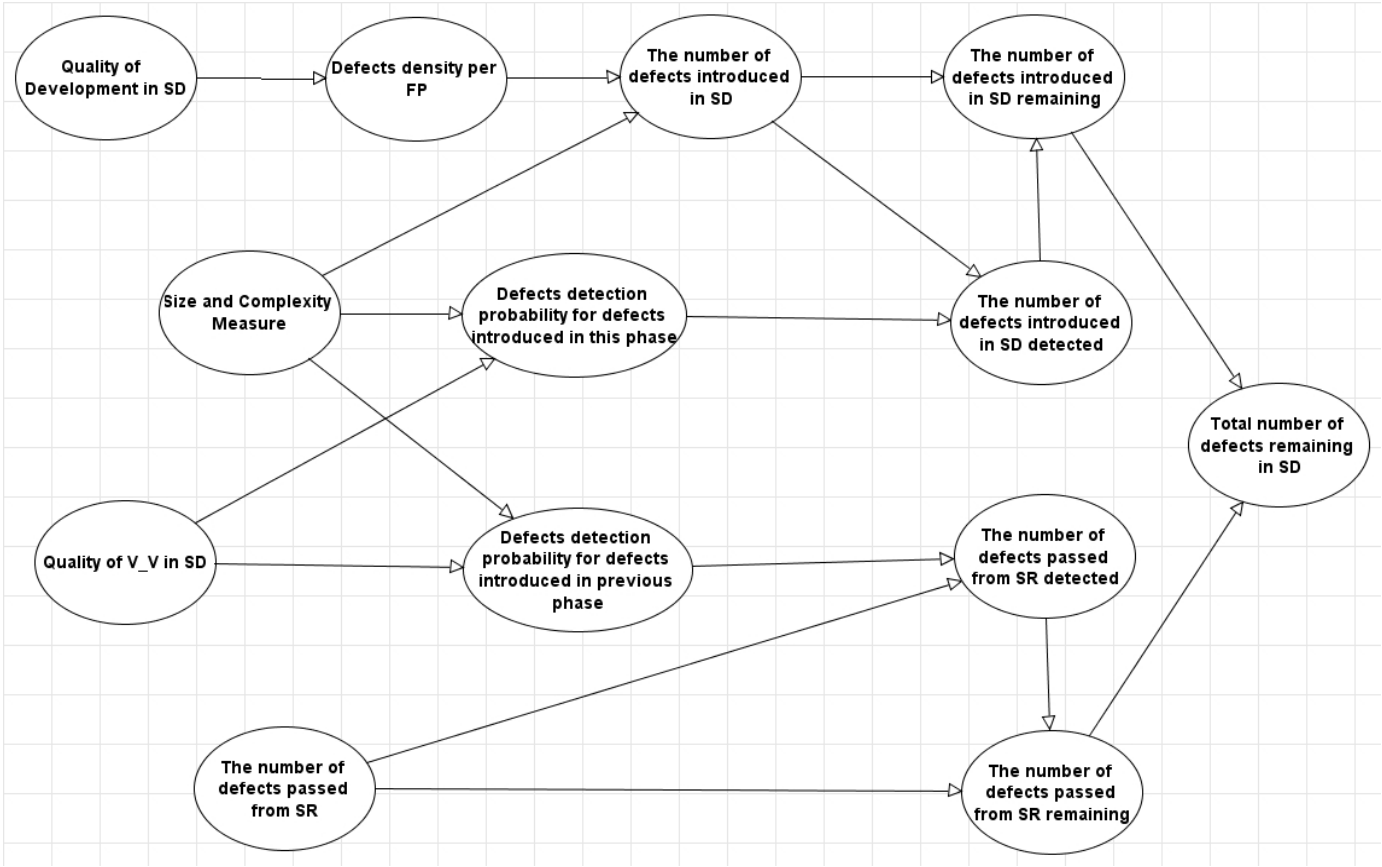
- Development of attributes and associated activities for assessing the quality of software development and verification and validation (V&V) for each phase.
- Assumption that the quality of development and V&V affect the defect density and defect detection probability, respectively.
- Use of expert elicitations in assessing the structure of the BBN model (completed) and estimating the parameters (node probability tables) of the model (on-going).
- Use of specific experts to assess the quality of software development and V&V for the Loop Operating and Control System of the Advanced Test Reactor (to be done in the future).
- Use of a fault size distribution to convert the number of faults (after installation and checkout at the plant) to software failure probability.

High Level Structure of a BBN Model for Quantifying Software Failure Probability
Figure 1



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

A Simplified BBN Model for the Design Phase – Figure 2

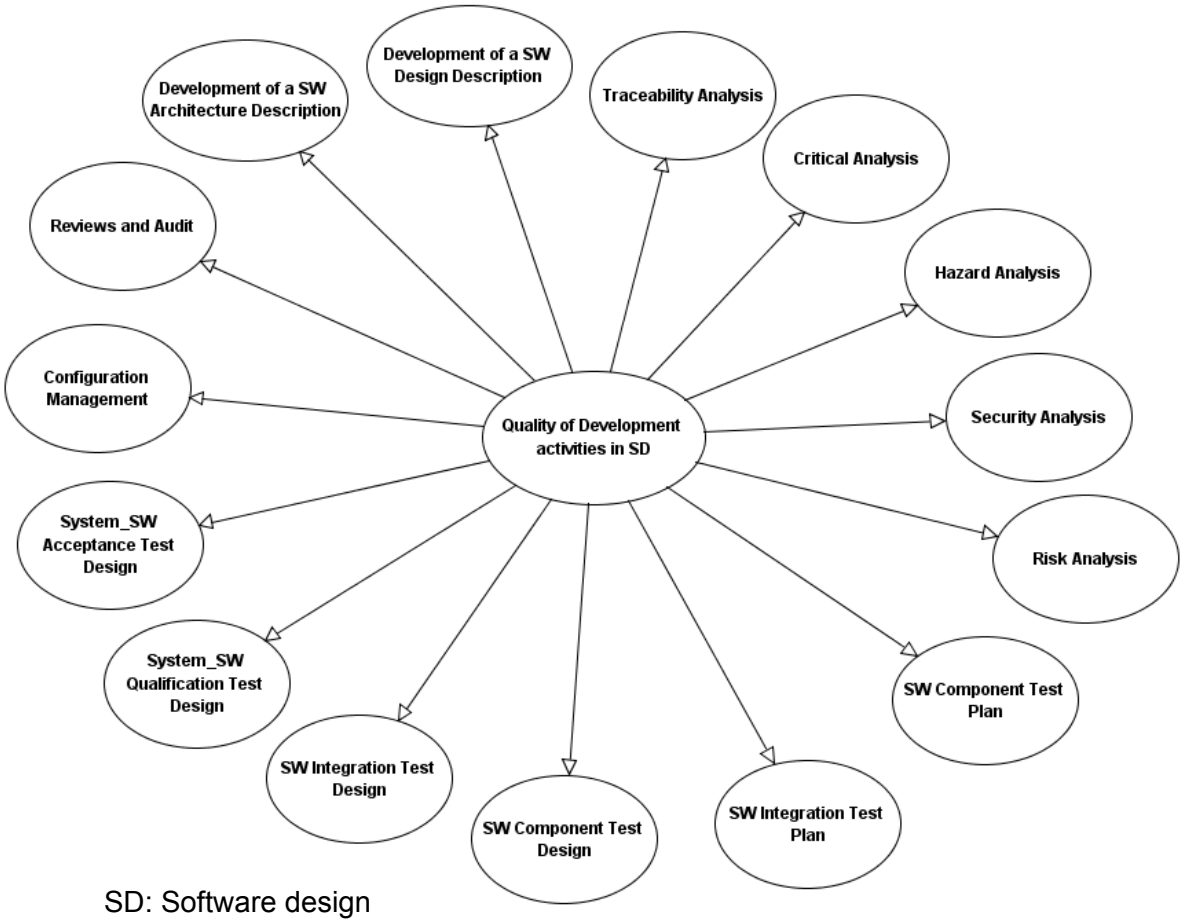


SD: Software design
FP: Function point
SR: Software requirement

BROOKHAVEN NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Detailed Model for the Development Quality Node of the Design Phase – Figure 3



SD: Software design

BROOKHAVEN NATIONAL LABORATORY

Identification of Attributes and Associated Activities for Software Development and V&V

- Review of guidance on software development to identify attributes and associated activities. For example:
  - IEEE Standard 1012 on V&V
  - NUREG-0800, Chapter 7, Branch Technical Position (BTP) HICB-14.
  - NUREG/CR-6101 on software reliability
  - IEC 60880 on Category A functions and associated equipments
  - Avionic standard DO-178C
- An attribute is modeled as a node representing the quality in carrying out the associated activities. For example, an attribute of the design phase is “Development of a Software Architecture Description”, and its associated activities are listed and described in detail.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Assessing the Quality of Software Development and V&V Activities Using BBN

- When evaluating a specific software program, experts familiar with the development of the program are used in determining the quality of the attributes on a High, Medium, and Low basis.
- The attribute nodes are “aggregated” into an overall quality of the development activities modeled as a node with three states (High, Medium, and Low). They are modeled as indicator nodes of the overall quality nodes.
  - That is, if an attribute node is a strong indicator of the overall quality, then given the overall quality is High the probability that the attribute node is High is high. The strength of an indicator will be estimated by expert elicitation.

BROOKHAVEN
NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Quality of Development and V&V Determine the Defect Density and Defect Detection Probability

- It is assumed that a high development quality would lead to a low defect density.
- It is assumed that a high V&V quality would lead to high defect detection probability. Two separate probabilities are used, one for the defects in the current phase and one for the defects passed from the earlier phases.
- Quantification of the qualitative relationship will be done by eliciting experts in software development, management, and V&V.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Expert Elicitations

1. Evaluation of the BBN structure and associated assumptions (e.g., conditional independence).
2. Estimation of generic parameters for safety-critical software.
   - Importance of attributes to overall quality of development and V&V
   - Defect density per function point, given overall quality of development
   - Defect detection probability, given overall V&V quality
3. Application to the LOCS software
   - Assessment of the quality of the attributes
   - Collection of evidence on the number of defects detected during software development

BROOKHAVEN
NATIONAL LABORATORY

Expert Elicitation on BBN Structure

- Thirteen international experts on software development, management, and V&V.
- Summary of Questions
  - Dose the model structure adequately captures the causal relationships?
  - Is the conditional independence assumption satisfied?
  - Is function point a suitable measure on size and complexity?
  - Is the use of High, Medium, and Low states adequate? Are they clearly defined?
- Diverse opinions were provided by the experts.
- The comments from the experts were addressed to the extent possible in the current BBN model.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Summary of Expert Elicitation (BBN Structure)

- Accepted Experts' Recommendations
  - Use of separate detection probabilities for faults of the current phase and faults passed from the previous phase.
  - The number of function points (complexity) also affects defect detection probability.

BROOKHAVEN NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Summary of Expert Elicitation (BBN Structure)

- Other Experts' Comments
  - A majority of the experts agree that there are causal relationships among some of the attribute nodes.
  - Most experts feel that development and V&V quality influences each other and hence are dependent on each other.
  - Several experts felt that our current definition of attribute states is not systematic and that it is not clear what a high state is. Some experts are not confident that just doing one extra activity will be enough to sufficiently distinguish the quality from "Medium".
  - Some experts are concerned that not many organizations are using FP to measure their software.
  - Several experts are uncomfortable with the idea of indicator nodes. They feel that it does not make sense to ask about knowing the development and V&V quality nodes without knowing the quality of the corresponding activities.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Estimation of Software Failure Probability – Conversion of Number of Faults to a Failure Probability

- Fault Size Distribution (FSD) is the conversion factor. That is,
  Software failure probability = Number of faults * FSD.

- The "size" represents the probability that a fault would be triggered and the distribution represents the variability of the probability among the faults [Littlewood 1980 and Delic 1995].

- It is equivalent to the Fault Exposure Ratio that is used in converting the number of faults to a failure *rate* commonly assumed in software reliability growth models, e.g., IEEE Std 1633 [IEEE 2008]. That is,
  Software failure rate = Number of faults * FER.

BROOKHAVEN NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Estimation of Software Failure Probability – Conversion of Number of Faults to a Failure Probability (Continued)

- Its use is similar to the conversion of Failure Likelihood Index (FLI) to a human error probability (HEP) [Chu 1994]. That is, Logarithm(HEP) = A + B(FLI), where parameters A and B are estimated by "calibration".
  In the case of software failure probability, the number of faults is a physically more meaningful index.

- Fault Size Distribution should be estimated from experience with similar software-development projects of the same vendor [Delic 1995]. In our study, this should be done for the safety-critical software.

- Due to lack of data on the number of faults and failure probability of safety-critical software. Some kind of calibration may have to be used instead (e.g., assuming the failure probability of a safety-critical software meets a reliability goal and back calculate the fault size distribution).

BROOKHAVEN
NATIONAL LABORATORY

Treatment of Uncertainty

- The BBN model is applicable to all safety-critical software. Its parameters represent variability among the safety-critical software. Once estimated, they do not change with evidence collected from the specific software program being evaluated.
- Elicitation of experts opinion will be used to estimate these parameters (ongoing). The estimates from the experts have variability that represents state-of-knowledge uncertainty. Two ways of treating the state-of-knowledge uncertainties (pre-processing and post-processing):

1. Aggregating (e.g., averaging) the estimates from different experts and using the results in the BBN model.
2. Using the set of estimates from an expert in the BBN model and aggregating the end results (i.e., failure probability).

- When applying the model to evaluate a specific software program (i.e., the LOCS software), specific experts are asked to assess the quality of the attributes in the form of either a hard or soft evidence. The state-of-knowledge-uncertainty can be treated in the two ways described above.
- After applying the specific evidence, the model becomes a model specific to the software program.
- Two software programs having exactly the same quality scores will have exactly the same failure probability distribution.

Issues and Limitations of the BBN Model

- Qualitative causal relationships have to be converted to quantitative relationship without adequate data.
  - High software development quality should lead to low defect density.
  - High V&V quality should lead to high defect detection probability.
  - Small number of faults should lead to low failure probability.
- It is difficult to demonstrate that the only dependency between every pair of nodes is through the BBN structure. For example, an attribute in one phase often provides input to attributes in the same phase and later phases. In the design phase, software architecture design and software design may well be inter-related. The dependence is considered weak and ignored.
- Complexity of the model makes it difficult to solve. The large number of attributes makes it a challenge to use a converging configuration (computational demand due to state explosion) which is more consistent with the actual causal-relationship. A diverging configuration (Figure 3) is used instead.
- "Ranked nodes" are used to model the attributes nodes' relationship to their parent nodes. The use includes calculations internal to AgenaRisk using a truncated normal distribution and assignment of variances subjectively.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Project Status

- A BBN model has been developed with the experts' comments on the model structure addressed.
- A second expert elicitation on estimating BBN parameters is on-going. The results of the elicitation will be used to complete the BBN model for safety-critical systems.
- A third expert elicitation will use specific experts of the LOCS to estimate its probability of failure to generate a trip signal.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

References

- [Chu 1994] T-L. Chu, Z. Musicki, P. Kohut, et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry Unit-1: Analysis of Core Damage Frequencies from Internal Events During Mid-Loop Operations", NUREG/CR-6144, Volume 2, June 1994.
- [Delic 1997] Delic, K.A., Mazzanti, F., and Strigini, L., "Formalizing Engineering Judgment on Software Dependability via Belief Networks," Sixth IFIP International Working Conference on Dependable Computing for Critical Applications, "Can We Rely on Computers?" Garmisch-Partenkirchen, Germany, IEEE Computer Society Press, pp. 291-305, 1997.
- [Eom 2009] Eom, H-S., et.al., "Reliability Assessment of a Safety-Critical Software by Using Generalized Bayesian Nets," ," *6th ANS Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-Machine Interfaces Technologies (NPIC&HMIT 2009)*, Knoxville, Tennessee, April 5-9, 2009.
- [Gran 2000] Gran, B.A., and Dahll, G., "Estimating Dependability of Programmable Systems Using Bayesian Belief Nets," OECD Halden Reactor Project, HWR-627, May 2000.
- [IEEE 2008] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Recommended Practice on Software Reliability," IEEE Standard 1633-2008, March 27, 2008.
- [Johnson 2000] Johnson, G., and Yu, X., "Conceptual Software Reliability Prediction Models for Nuclear Power Plant Safety Systems," Lawrence Livermore National Laboratory, UCRL-ID-138577, April 3, 2000.
- [Littlewood 2000] Littlewood, B., and Strigini, L., "Software Reliability and Dependability: A Roadmap," International Conference on Software Engineering, Proceedings of the Conference on The Future of Software Engineering, Limerick, Ireland, June 2000.

BROOKHAVEN
NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Backup slides

BROOKHAVEN NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Example System - LOCS of ATR

- The Advanced Test Reactor (ATR) Loop Distributed Control System (DCS) software is a commercial software developed and provided by Metso Automation Max Controls, Inc. in compliance with ASME NQA-1 (Nuclear Quality Assurance).
- The following information are available to BNL regarding the LOCS development.
  - The V&V report of the most recent LOCS upgrade.
  - The software quality assurance plan of the Loop Operation Control System (LOCS) upgrade and the review activities of the software development cycle.
  - A Configuration Management Plan that contains some information about the software development activities.
  - Some details of a previous upgrade project of the LOCS and definition of the phases in the software development cycle.
  - Specification for the distributed control system (DCS) used in loop 2A.
  - Technical and function requirements for loop 2A LOCS.
  - Test plans for loop equipment and integrated system.
- Experts familiar with the development of the LOCS software are essential to the application of the BBN model.

Definition of the States of Attribute Nodes

- High: In addition to satisfactorily carrying out the required activities, additional activities were performed that are expected to significantly improve the quality of the work, and enhance software reliability.
- Medium: All required (or equivalent) activities were satisfactorily carried out.
- Low: Some of the required activities were not carried out satisfactorily.
- Other rules were specified. For example, if both the development and V&V teams *independently* performed traceability analysis, then both teams are given a High.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

How the NPT of a Ranked Node Is Determined – An Example

- A ranked node *B* (with 3 states) with its parent node *A* (also with 5 states) is denoted as *B* ⟸ *A*.
- Assuming one sample point is taken from each interval, then if A has 5 states and B has 3 states, within AgenaRisk, the 3 states are represented by 3 values representing the mid-point of the 3 equally spaced intervals between 0 and 1 (0-1/3,1/3-2/3,2/3-1), that is, 1/6, ½, and 5/6. Similarly, the 5 states are represented by mid-points of the intervals (0-1/5,1/5-2/5,2/5-3/5,3/5-4/5,4/5-1).
- The node probability table of *B* given *A* is calculated using a truncated (at 0 and 1) normal distribution (TNormal) whose mean is equal to its parent node (as a random variable) and variance is subjectively assigned. This is denoted by

  B = TNormal (*A*,*variance*).
- For example, assuming the variance is 10, the NPT elements are calculated as (assuming one sample point is taken from each interval):

  P(b1I a1) = P(TNormal(1/10,10) <1/3), P(1/3<TNormal(1/10,10) <2/3), P(TNormal(1/10,10) >2/3)
  P(b1I a2) = P(TNormal(3/10,10) <1/3), P(1/3<TNormal(3/10,10) <2/3), P(TNormal(3/10,10) >2/3)
  P(b1I a3) = P(TNormal(5/10,10) <1/3), P(1/3<TNormal(5/10,10) <2/3), P(TNormal(5/10,10) >2/3)
  P(b1I a4) = P(TNormal(7/10,10) <1/3), P(1/3<TNormal(7/10,10) <2/3), P(TNormal(7/10,10) >2/3)
  P(b1I a5) = P(TNormal(9/10,10) <1/3), P(1/3<TNormal(9/10,10) <2/3), P(TNormal(9/10,10) >2/3)

- Given the NPT, the relationship between the two nodes are completely defined.

BROOKHAVEN NATIONAL LABORATORY

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

List of Experts for the First Elicitation

Organizations	Experts
NRC	Stattel, Richard
Joongbu University, Korea	Son, Han Seong
KAIST, Korea	Baik, Jongmoon
KEPCO E&C, Korea	Baek, Seung Min
Doosan Heavy Industry, Korea	Koo, Seo Ryong
Idaho National Laboratory	Marts, George
Queen Mary University of London	Fenton, Norman
NASA	Vorndran, Kenneth
NASA	Costello, Kenneth
NUV Technology	Yang, Steve
Raytheon Company	Peterson, Jon
Raytheon Company	Gullo, Lou
SoftRel	Neufelder, Ann Marie

BROOKHAVEN
NATIONAL LABORATORY

DEVELOPMENT OF A STATISTICAL TESTING APPROACH FOR QUANTIFYING SOFTWARE RELIABILITY AND ITS APPLICATION TO AN EXAMPLE SYSTEM

Advisory Committee on Reactor Safeguards
Joint Digital Instrumentation and Control Systems Subcommittee and
PRA Subcommittee Meeting

November 18-19, 2014

Tsong-Lun Chu
Athi Varuttamaseni
Brookhaven National Laboratory
(631 344-2389, chu@bnl.gov)

Timothy Kaser
George Marts
Idaho National Laboratory
(208 526-9025, timothy.kaser@inl.gov)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Outline of Presentation

- Overview of statistical testing method (STM)
- Loop Operating Control System (LOCS) system description
- Advanced Test Reactor(ATR) PRA model
- RELAP5 model of Loop2A
- Cutset grouping and Probabilistic Failure Models
- Test case generation
- Evaluation of test results
- Reproducibility of test results
- Estimate of software failure probability
- Challenges and limitations of STM

BROOKHAVEN NATIONAL LABORATORY

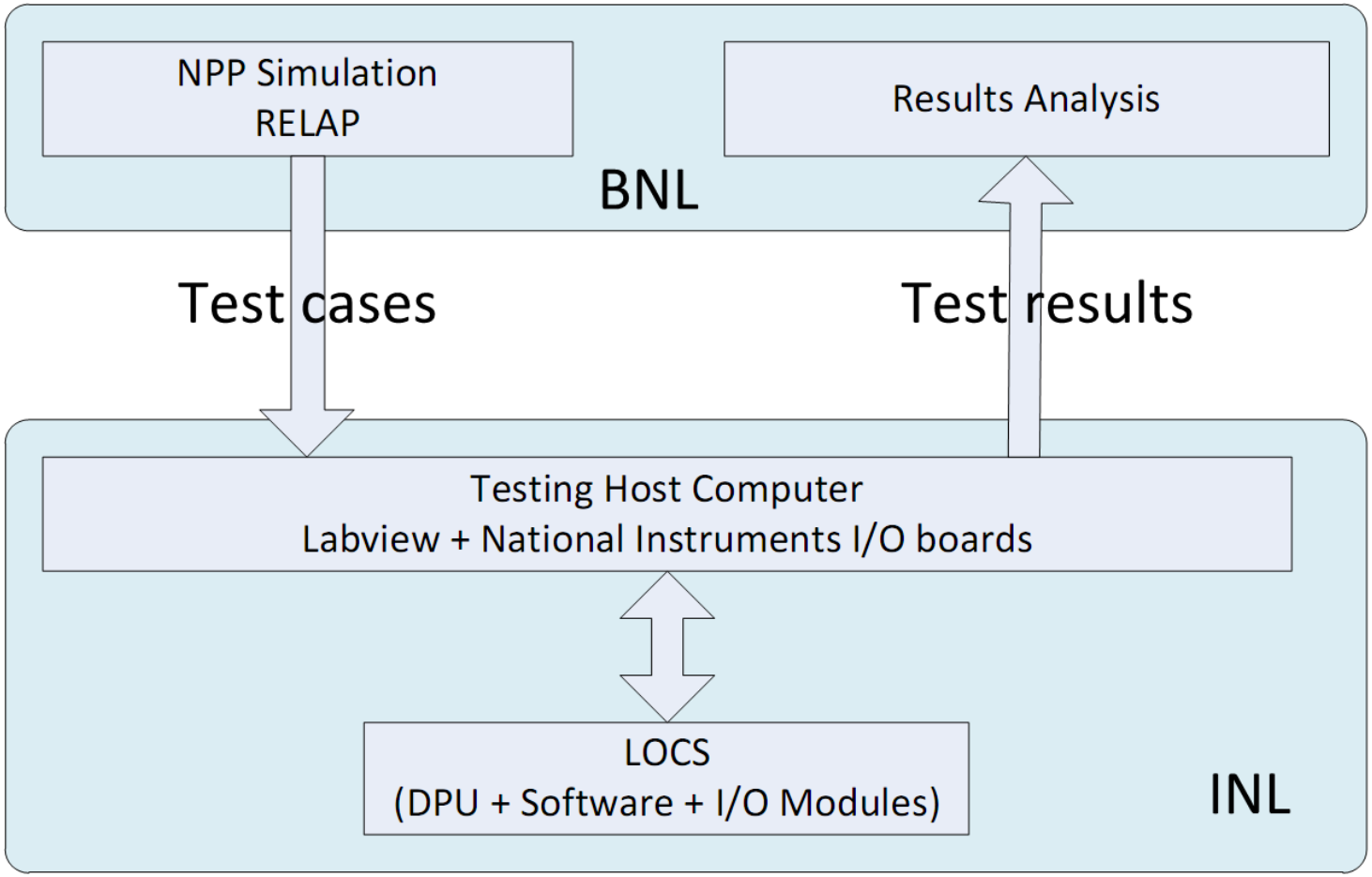
INL Idaho National Laboratory

The Statistical Testing Method (STM)

- Goal: Estimate the probability of failure on demand (PFD) (i.e., failure to trip) of LOCS protection function.
- Key steps:
  1. Develop failure effect groups to model the (qualitative) failure effects of PRA cutsets.
  2. For each failure effect group, construct a probabilistic failure model to represent the (quantitative) effect of the failure effect group on the system.
  3. Sample from the cutsets and sample from its associated probabilistic failure model(s) and simulate the failure effects using thermal-hydraulic (T/H) model to define the operational profile for the software.
  4. Test software using test cases that follow operational profile
  5. Estimate PFD from the result.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Statistical Testing Workflow Between BNL and INL



BROOKHAVEN NATIONAL LABORATORY

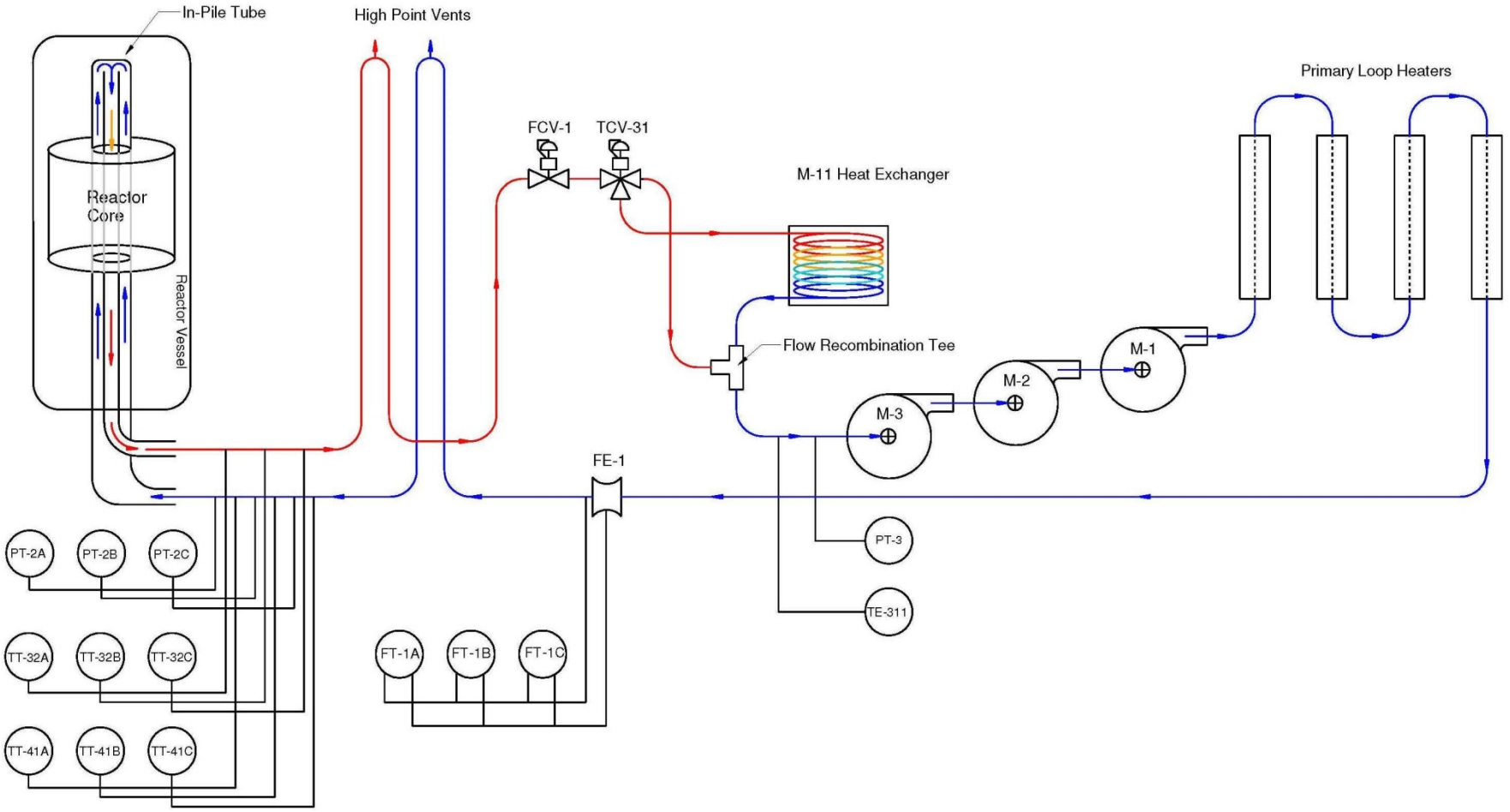
INL Idaho National Laboratory

Pressurized Water Loop 2A

- Pressurized water loop 2A is a facility within ATR that can provide pressurized water at prototypical PWR conditions independent of the ATR primary system to support irradiation of materials. Failure of the Loop 2A piping or control system can cause an increase in the ATR power.
- The Loop 2A digital control system is interfaced with the ATR Plant Protection System (PPS) to cause a reactor trip. The primary purpose is for experiment protection, however this function also provides defense in depth to the ATR PPS.
- Loop 2A control system consists of a Metso Automation maxDNA Distributed Control System (DCS), along with transmitters, interface equipment, and power systems that allow the DCS to control and collect data for pressure, temperature, and flow within Loop 2A.
- Loop 2A control system (LOCS) provides experiment protection and experiment control functions. There is no separate system for control and experiment protection.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

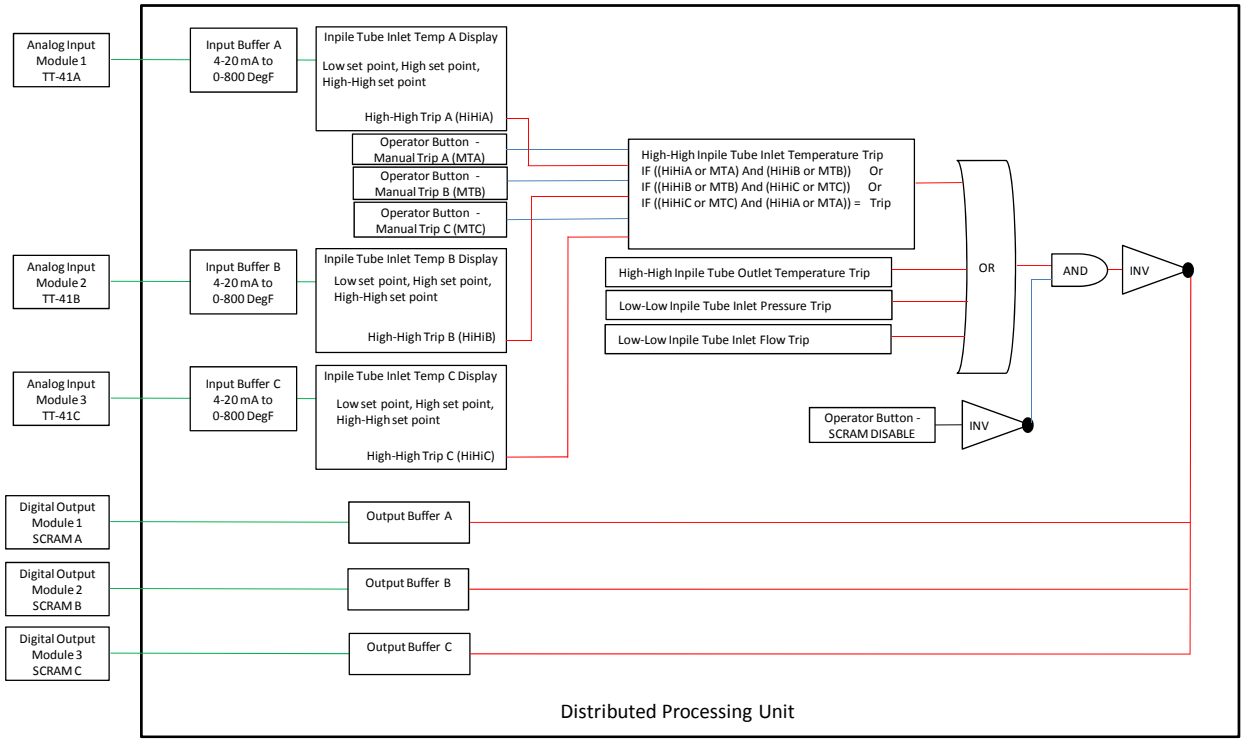
Loop 2A Simplified P&ID



BROOKHAVEN NATIONAL LABORATORY

INL Idaho National Laboratory

Loop 2A LOCS
Typical Safety Relevant I/O



HiHi – Out above the High-High set point (SP)
MT – manual trip (channel out-of-service)
OB – Operator Button (Off/On)

Inv – Inverter (0 to 1, 1 to 0)

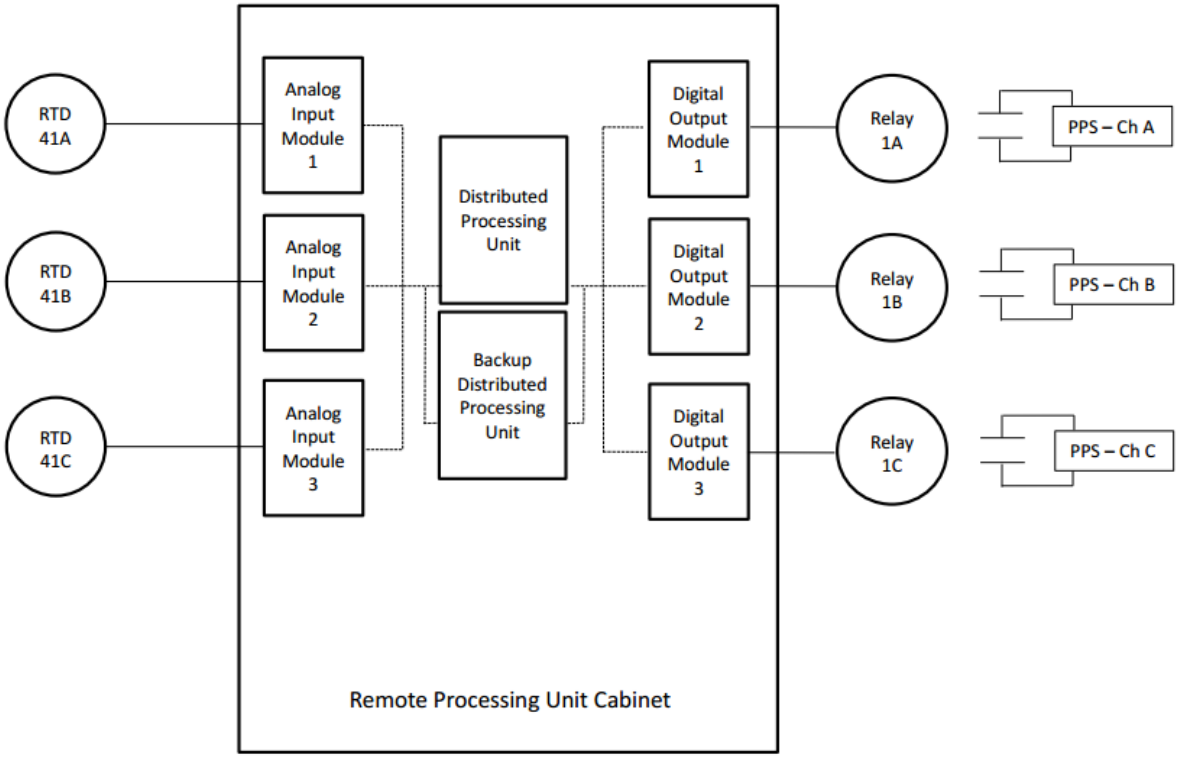
SP – Set point

Conditions that can initiate scram are

1. Low IPT inlet flow
2. Low IPT inlet pressure
3. High IPT inlet temperature
4. High IPT outlet temperature

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Major Loop 2A
LOCS Components for Trip Function



RTD – Resistance Thermal Detector
PPS – Plant Protection System

- 3 sensors, trip on 2/3
- Each sensor connected to 1 analog input module (AIM)
- One AIM for each of the three (A/B/C) channels
- 3 digital output modules (DOMs), trip on 2/3 relays de-energized
- 1 distributed processing unit (DPU) pair in remote processing unit (RPU) cabinet

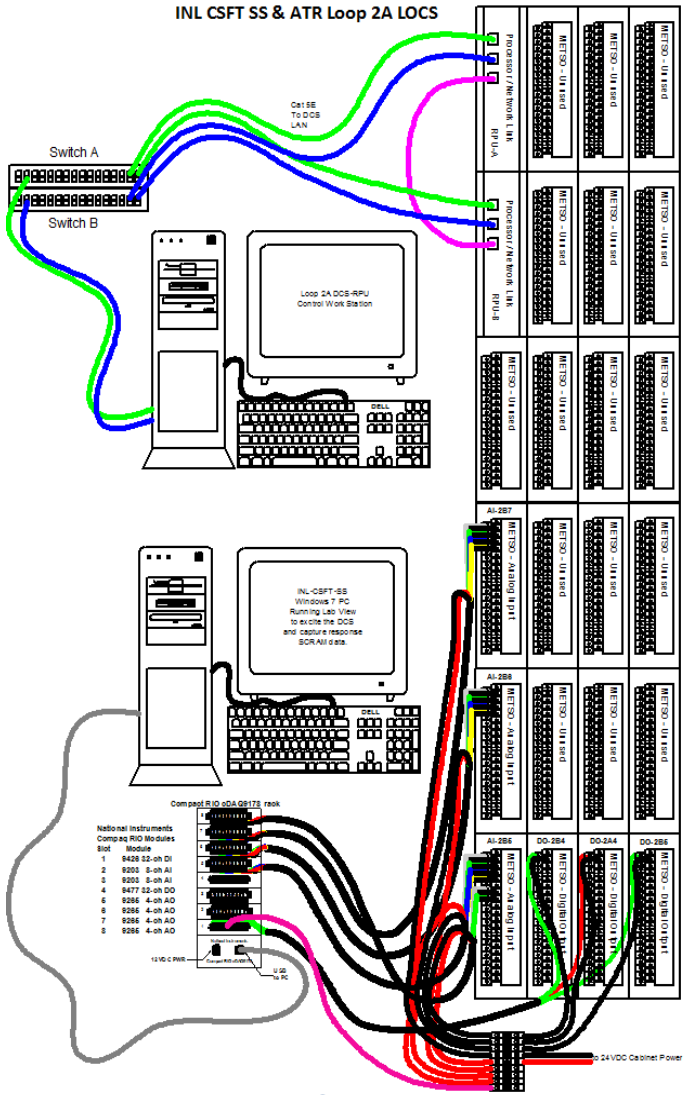
BROOKHAVEN NATIONAL LABORATORY

INL Idaho National Laboratory

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Loop 2A LOCS Test Bed

- Actual testing was conducted using a mockup digital control system with identical DCS components and software typical of the ATR installation.
- Loop 2A digital control system can be configured to simulate each analog or digital input. This functionality is not used on the actual system.
- Loop 2A digital control system software for the STS was changed to use the inputs provided by CSFT-SS and to simulate the values of the remaining inputs. This was done to maintain the processor loading of the actual Loop 2A digital control system. Simulated signals were kept at nominal non-alarming values.

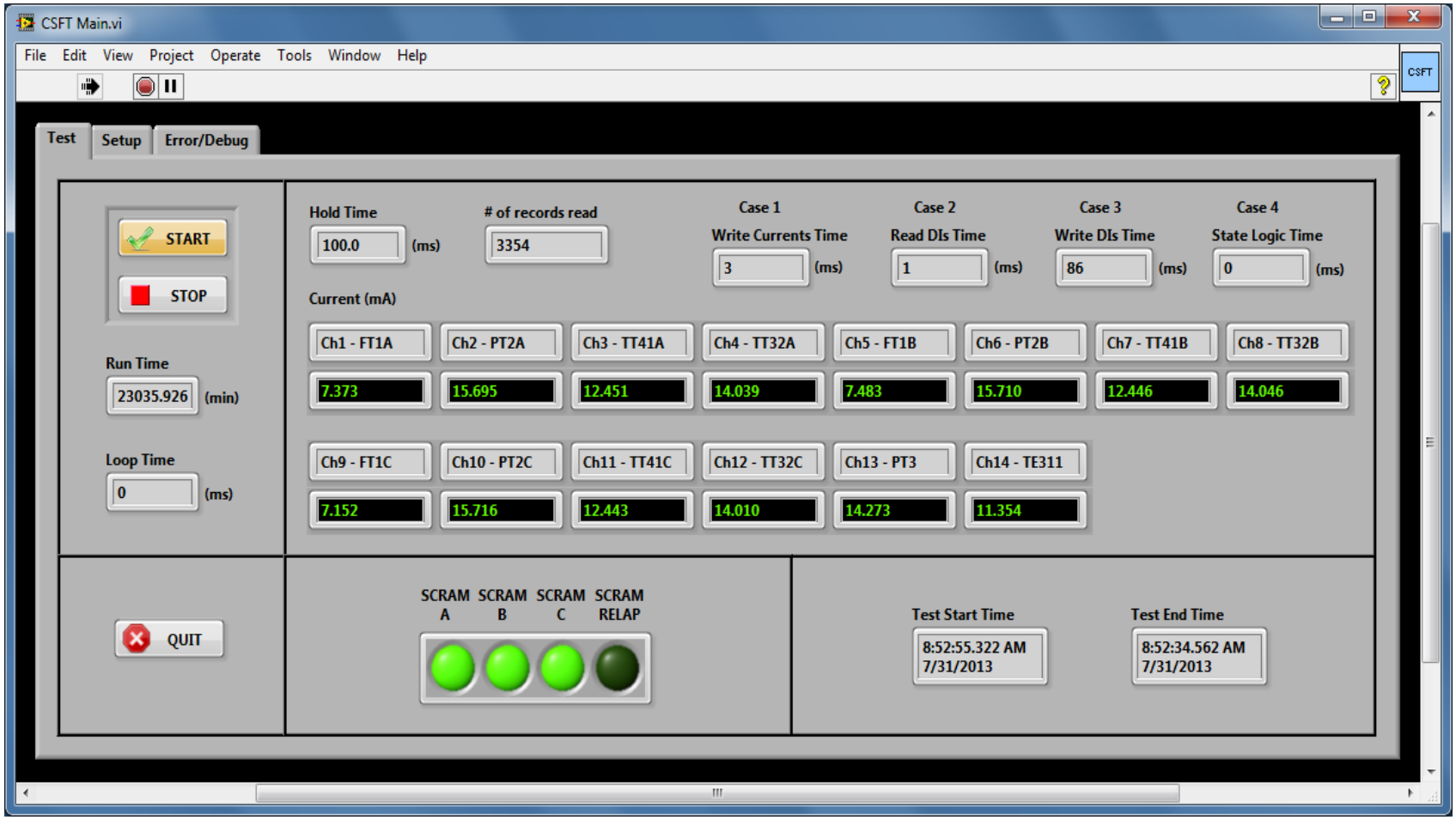


BROOKHAVEN NATIONAL LABORATORY

INL Idaho National Laboratory

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Test Bed Software Development



BROOKHAVEN NATIONAL LABORATORY

INL Idaho National Laboratory

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Test Bed Limitations/Recommendations

- Test case input values were loaded into memory as electrical values in order to improve system throughput. RELAP5 output is normally produced in engineering units.
- Windows does not directly support real time execution
- To prevent apparent timing issues the signal simulation and monitoring cycle time should be adjusted.
- Develop two analytical methods that address both fixed cycle time control systems and variable cycle time control systems.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ATR PRA Model

- Model description for loop 2A is provided here; other loops are similar.
- Two different fault trees are used to model the control and protection functions of Loop 2A separately.
- Reactivity insertion events from experiment loops are broken into three groups:
  1. Loss of pressure control
  2. Loss of temperature control
  3. Loss of flow control
- "Loss of control" includes LOCS component failures and non LOCS-related events such as plugging and pipe break.
- Three systems that can generate trip signal:
  1. LOCS
  2. Plant protection system (PPS)
  3. Manual scram / Slow insertion
- PRA considers time from steady state to needing a trip signal to determine if an actuation system is credited.
- Slow insertion involves rotating drum, half of which is coated with neutron absorber. We assume that slow insertion cannot mitigate events where the threshold is exceeded within 3 minutes.

Examples of Modifications to PRA Model

- Use three branches in core damage event tree
  - Identify where LOCS is credited in PRA
- Add analog output modules, sensors, and DPUs as components that can cause initiating event
- Adjust initiating event fault tree so that only one analog input module is credited.
- Add digital output modules to “failure to trip” fault tree

Reactivity Insertion Events Associated with Loop 2A

- Frequency of reactivity insertion events associated with loop 2A: 0.97 /year (system's reliability criterion: <1 /year).
- Includes LOCS components failure and non-LOCS events such as pipe clogging.
- Consider only first 200 cutsets (these make up ~99% of total loop 2A reactivity insertion frequency).

Failure Cause	% Contribution
Failure of Secondary Loop Components	90
Failure of Primary Loop Pumps	4.6
LOCS Components	3.5
Primary Loop Plugging	3.0
Other	2.4

Note: The % contributions don't add up to 100% since some cutsets contain multiple events.

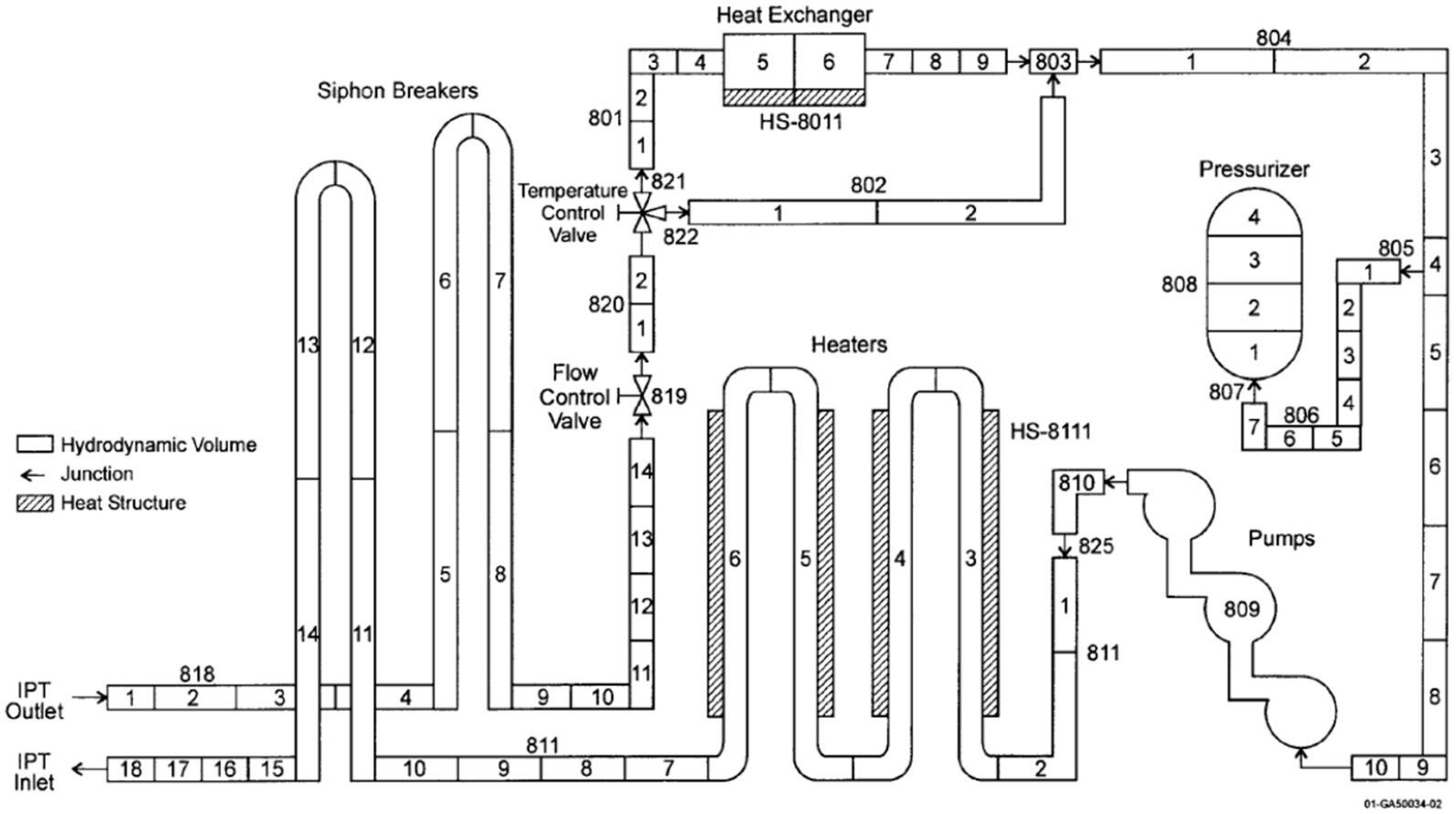
Risk Informed Considerations

- Total core damage frequency (CDF) ~ $3*10^{-6}$ /year
- Probability of LOCS hardware failure ~ $7*10^{-3}$
- Contribution of LOCS hardware failure to total CDF ~ $3*10^{-13}$/year

- ➢ Reliability goal of LOCS software failure ~ $7*10^{-3}$ should be acceptable (assuming software failure probability is the same as hardware failure probability).
- ➢ Test showing $\leq$ 1 failure in 10,000 cases is more than sufficient.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RELAP5 Model



BROOKHAVEN NATIONAL LABORATORY

INL Idaho National Laboratory

Probabilistic Failure Models for PRA Failure Events

- Issues:
  1. Not all necessary control systems and components are modeled.
  2. PRA model describes failure at high level (e.g., pipe break). Need details (e.g., break size, break location) for RELAP5 model.
- Solution:
  1. Group failure effects according to how they affect the systems. This leads to 13 groups each with a probabilistic failure model.
  2. Introduce random parameters into the probabilistic failure models. These are assumed to be uniformly distributed in an interval. Endpoint of the intervals are determined from engineering judgment (e.g., valve closing time of a temperature control valve).
- Assumption: All initiating events will have been detected by operator within 30 minutes → upper limit on simulation time
- Cutsets can belong to one or more failure effect groups (e.g., loss of power to LOCS belongs multiple groups)
- Group assignments are partially automated (based on the basic events).

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Probabilistic Failure Models

No.	Group	Variable
1	Loss of HX Cooling	Time at which heat-transfer coefficient reaches zero. [s]
2	Pump Failure	Multiplication constant to the time variable for pump coastdown curve
3	Pump Failure	Time for pump to reach complete stop [s]
4,5,6	Pipe Plugging	Flow Area [ft^2]
7,8	Pipe Break	Break size [ft^2]
9	Loss of Flow Ctrl (Up)	CV-240 (Flow controller input)
10	Loss of Flow Ctrl (Down)	CV-24 (Flow controller output)
11	Loss of Heater Ctrl (Up)	CV-1 (Line heater controller input)
12	Loss of Heater Ctrl (Down)	CV-4 (Line heater controller output)
13	Loss of TCV Ctrl	Time for valve TCV-3-1 to be fully closed. [s]

RELAP5 Test Case Generation

- Relap5 input decks are automatically generated.
  - ❖ Master file contains one section for each of the 13 failure models
  - ❖ During deck generation, different sections are copied from the master file, depending on group membership of the cutset
  - ❖ Random parameters are sampled from the uniform distribution

- 10,000 cases total, broken into 4 groups to be run in parallel on 4 PCs.
- Fortran script extracts relevant information from restart file
- Script used to add noise to the Relap5 parameters to simulate sensor noise. Noise magnitude derived from sensor accuracy.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Evaluations of Results

- The trip time window is the interval in which a trip signal should be generated. It is determined by considering
  1. hysteresis reset time windows,
  2. worst/latest and best/earliest time when a record is read or written,
  3. Since LOCS cycle is 0.3 s, trip condition for one or two records may not be read
- Assume constant 0.3 s cycle time for LOCS
- Test computer has a cycle time of 0.1 s

Channel Description	Trip Condition	Hysteresis Window
IPT inlet flow	$\leq$ 25 gpm	1 gpm
IPT inlet pressure	$\leq$ 1800 psig	5 psig
IPT inlet temperature	$\geq$ 510 ^{o}F	2 ^{o}F
IPT outlet temperature	$\geq$ 570 ^{o}F	2 ^{o}F

Channel Response Time

- Specification for channel response time

Channel	Response Time [s]
IPT inlet flow	1.13
IPT coolant temperature	1.13
IPT inlet pressure	0.78

- Assume that threshold is exceeded for three consecutive records (1 LOCS cycle)
- This criterion cannot give lower bound for trip record (trip lasting one record has 1/3 chance of being read by LOCS)

Timing Considerations

- RELAP5
  - RELAP5 output time step is 0.1 seconds
- LOCS
  - LOCS cycle time ~ 0.3 seconds
- Test Bed
  - Not synchronized with LOCS cycle time
  - Conversion of RELAP data introduces uncertainties in parameter values

Expected trip time delay could be as long as 0.4 seconds
(does not account for uncertainties in parameter conversion)

Evaluation Results (1)

Using Expected Trip Window criterion:

Delayed Trips

Delay (s)	Number of Cases
(0,0.5]	26
(0.5,1.0]	0
(1.0,1.5]	1
(1.5,∞)	0
Total	27

Early Trips

Delay (s)	Number of Cases
(-∞,-5)	0
[-5,-4)	3
[-4,-3)	4
[-3,-2)	16
[-2,-1)	19
[-1,0)	922
Total	964

- Hardware noise and channel accuracy may explain the early and delay trips
- The largest delay measured was 1.2s. However, using the channel response time criterion, this case is not a delay.

Potential Signal Processing Issues

- RELAP5 simulates Loop 2A thermo hydraulic parameters and outputs as test cases in digital format.
- BNL adds white noises to these test cases.
- Test computer reads test cases inputs and converts them into analog signals.
- LOCS receives analog signals and converts them to digital values and feed them to LOCS software.
- The preceding two steps can introduce delays and/or channel noises.

Evaluation Results (2)

Interesting anomalies:

- 44 cases have trips lasting one record [LOCS cycle is about 3 records so we expect a trip to last at least 2 records.]
- 398 cases where the three output channels didn't trip at the same time [DPU outputs trip status to all three digital output modules (DOMs) so the DOM outputs should match.]
- Initial test runs showed one failure to trip in 10,000 cases. However, this failure cannot be reproduced and was not considered to be an actual failure.

Reproducibility of Results

Case	Actual Trip Record	Number of Cases	Expected Trip Window
LI_5472 (pipe break)	4	7	[2, 417]
	5	1	
	409	2	
LO_9360 (failure of analog input module 1A3)	3348	13	[3354, 3381]
	3349	3	
	3360	1	
	3363	3	
RF_316 (failure of secondary loop pump)	17737	1	[11735, 11741]
	17738	99	
RF_9075 (plugging of flow element FE-4-2)	7679	15	[7664, 7679]
	7680	5	
RF_PT_LO_FO_HO_TV_9696 (loss of power to 4.16 kV commercial bus A)	54	15	[39, 71]
	69	1	
	70	3	
	73	1	

Due to noise and variation in when LOCS reads the input, results are not expected to be identical

Software Probability of Failure on Demand (PFD)

- Assume prior PFD has Beta distribution: $f(\theta) = \frac{(1-\theta)^{b-1}\theta^{a-1}}{B(a,b)}$
- After performing *n* tests with *x* failures, the posterior distribution has mean $\frac{a+x}{a+b+x}$.
- Consider 0 failure in 10,000 tests (and uniform prior so a = b = 1): mean of posterior PFD = $\frac{1}{10002} \cong 1 * 10^{-4}$

Limitations and Challenges of Applying STM

- Results depends on accuracy of test configuration, PRA model, and thermal-hydraulics (T/H) model (RELAP5 model).
  - Use of dummy values for signals that are not important
  - Non-minimal cutsets may impose new challenges to the software
  - T/H model may not contain all relevant control functions that can affect loop response
- Difficult to distinguish hardware from software failure. Did transient hardware failure cause observed delays?
- Timing of failures and effect of initial condition were not considered: all basic events in PRA assumed to happen simultaneously, initial condition = full power steady state → Can vary timing and initial condition in simulation in future applications.
- Did not consider events that are not be in PRA (e.g., fire and seismic induced events) → Can add such events into simulation in future applications.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Summary

- We demonstrated the STM on the LOCS (subject to realism of modeling)
  - Linked PRA context to operational profile
  - Generate test cases from RELAP simulation
  - Demonstrated feasibility of integrated hardware/software testing
  - Identify possible improvements to testing configuration to address test bed limitations
- The approach can be applied to real RPS and ESFAS

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Backup Slides

BROOKHAVEN NATIONAL LABORATORY

INL Idaho National Laboratory

Grouping of Failure Effects (1)

#	Group	Description	Effect of Failure (for modes leading to trip demand)	Modeling in RELAP5
1	RFW130	Loss of heat-exchanger cooling	The heat exchanger is unable to remove heat from loop 2A, leading to rise in the loop temperature.	Decrease the heat transfer coefficient at the heat exchanger to zero over a variable time.
2	gPump	Primary pump failure – Trip	Forced circulation in loop 2A ends.	Shift (in time) the coastdown curve by a variable multiplicative constant.
3		Primary pump failure – Seizure	Forced circulation in loop 2A ends.	Linearly reduce pump speed to zero over a variable period.
4	gFlow	Plugging – flow element 1	Flow area at flow element 1 decreases, leading to reduced flow rate in loop 2A.	Reduce flow area at flow element 1 by a variable amount.
5		Plugging – flow element 2	Flow area at flow element 2 decreases, leading to reduced flow rate in loop 2A.	Reduce flow area at flow element 2 by a variable amount.
6		Plugging – strainer 145	Flow area at strainer-145 decreases, leading to reduced flow rate in loop 2A.	Reduce flow area at strainer-145 by a variable amount.
7	gPipe	Pipe break – IPT Inlet	Volume and flow rate of loop 2A coolant decrease.	Introduce a pipe break of a variable size at the IPT inlet.
8		Pipe break – IPT Outlet	Volume and flow rate of loop 2A coolant decrease.	Introduce a pipe break of a variable size at the IPT outlet.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Grouping of Failure Effects (2)

#	Group	Description	Effect of Failure (for modes leading to trip demand)	Modeling in RELAP5
9	gFctrlI	Flow control components failure (sensors and analog input module)	Loss of ability to increase loop flow rate in response to transients resulting in flow rate reduction.	Reduce flow rate by a variable amount by adjusting input to the flow controller by a variable amount.
10	gFctrlO	Flow control components failure (DPU and analog output module)	Loss of ability to increase loop flow rate in response to transients resulting in flow rate reduction	Reduce flow rate by a variable amount by adjusting output from the flow controller by a variable amount.
11	gTctrlHI	Temperature control components (line heater) failure (sensor and analog input module)	Loss of ability to decrease coolant temperature via line heater output reduction in response to transients resulting in temperature increase.	Increase coolant temperature by increasing line heater output by a variable amount by adjusting input to the controller (CV-1).
12	gTctrlHO	Temperature control components (line heater) failure (DPU and analog output module)	Loss of ability to decrease coolant temperature via line heater output reduction in response to transients resulting in temperature increase.	Increase coolant temperature by increasing line heater output by a variable amount by adjusting output from the controller (CV-4).
13	gTctrlV	Temperature control components (TCV-3-1) failure	Loss of ability to decrease coolant temperature via increasing flow to heat exchanger in response to transients resulting in temperature increase.	Increase coolant temperature by fully closing TCV-3-1 over a variable period.

WGRisk DIGREL
Failure Mode Taxonomy

ACRS Meeting
Rockville, MD
November 18-19, 2014

Ming Li
Probabilistic Risk Assessment Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research
(301-251-7627, ming.li@nrc.gov)

Outlines

- Background
- Approach
- Failure mode taxonomy
- Failure mode taxonomy application
- Failure mode taxonomy validation

Background

- IECD/NEA/CSNI/WGRisk DIGREL WG
  - France, Sweden, USA, Finland, South Korea, Japan, Germany, the Netherlands, Czech Republic
- Develop a taxonomy of failure modes of digital components for the purposes of probabilistic risk analysis (PRA)

A failure modes taxonomy is a framework of describing, classifying and identifying failure modes associated with a system

General Approach

- Develop failure mode taxonomy requirements
- Summarize existing failure modes
- Develop an example system
- Develop a failure mode taxonomy that can be used to describe and classify failure modes
- Apply the failure mode taxonomy to a Nordic application
- Validate the failure mode taxonomy against the taxonomy requirements

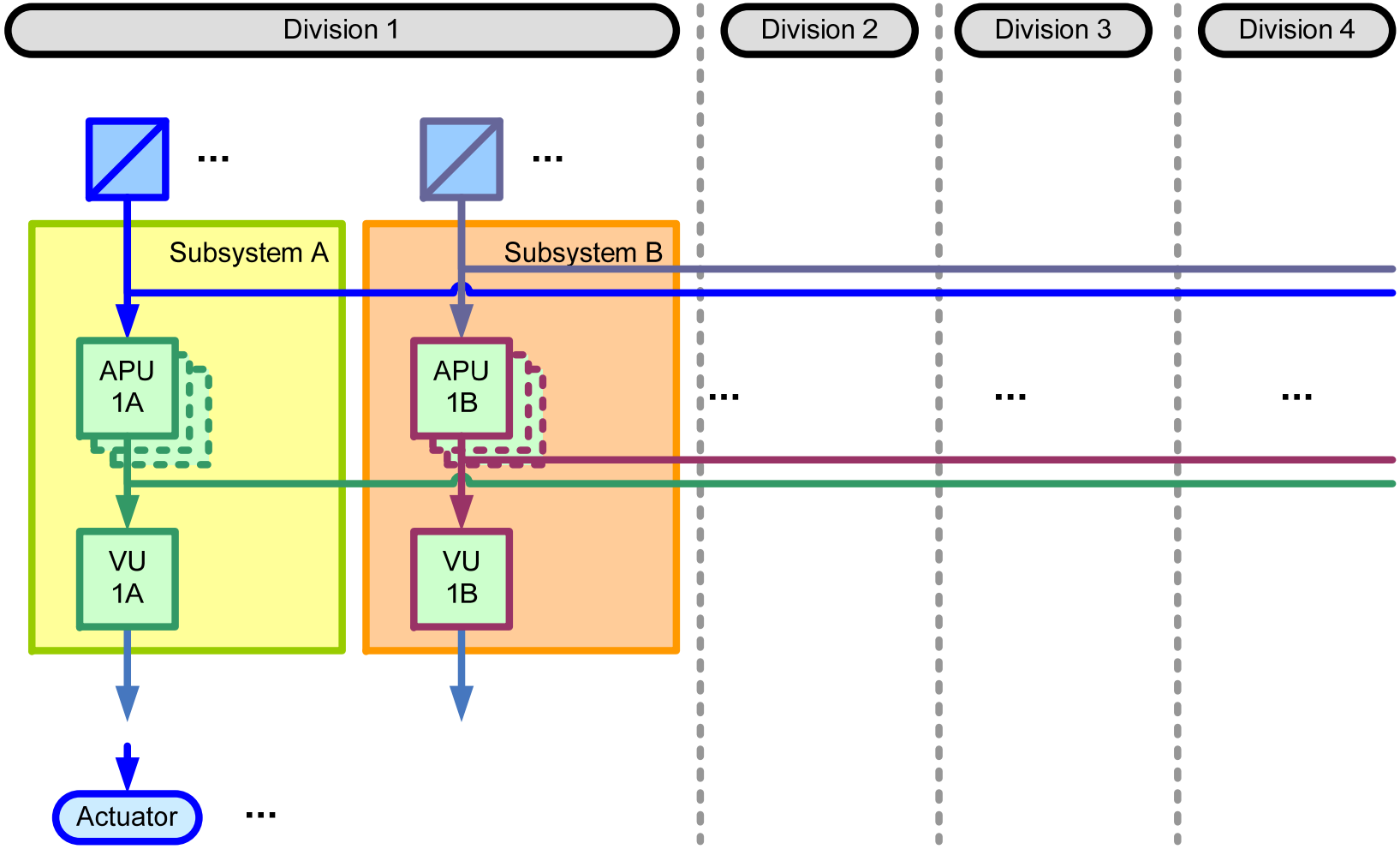
Failure Mode Taxonomy Requirements

Criterion 1:	Be defined unambiguously
Criterion 2:	Form a complete/exhaustive set
Criterion 3:	Be organized hierarchically
Criterion 4:	Be mutually exclusive
Criterion 5:	Data to support the taxonomy should be available now or in the future
Criterion 6:	There should be analogy between failure modes of different components
Criterion 7:	At the very least, the lowest level of the taxonomy should be sufficient to pinpoint existing dependencies of importance to PRA modelling
Criterion 8:	Should support PRA practice, and fulfil PRA requirements/conditions
Criterion 9:	Should capture defensive measures against fault propagation (detection, isolation and correction) and other essential design features of digital I&C

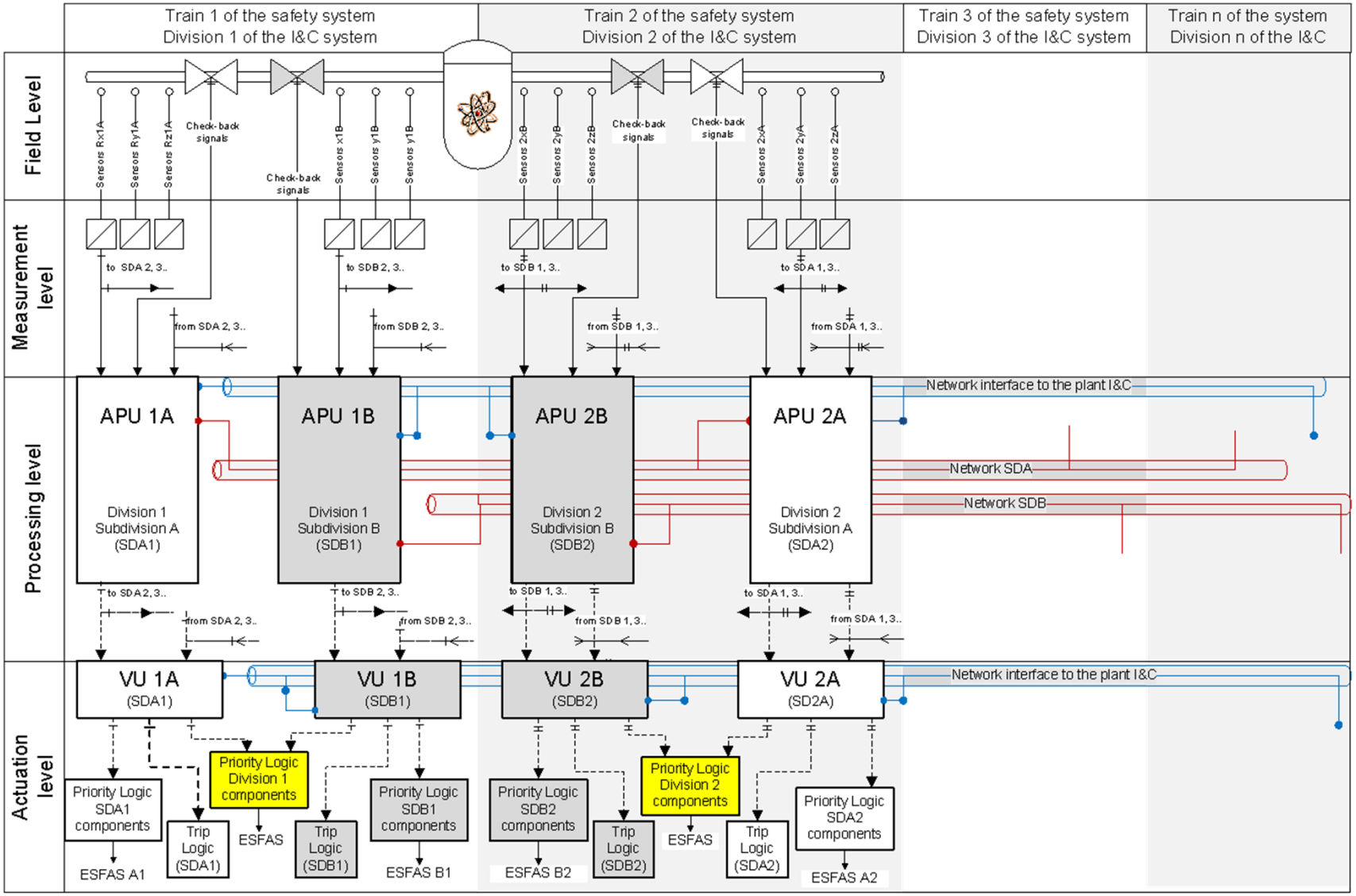
Summary of Collected Failure Modes

- BNL (Brookhaven National Laboratory)
- CNSC (Canadian Nuclear Safety Commission)
- EDF (Electricity of France)
- IRSN (Institut de Radioprotection et de Surete Nucleaire)
- JNES (Japan Nuclear Energy Safety Organization)
- KAERI (Korean Atomic Energy Research Institute)
- NRG (Nuclear Research and Consultancy Group)
- NKS (Nordic Nuclear Energy Research); summarising input from three Nordic utilities
- OSU (Ohio State University)
- RELKO Ltd (Engineering and Consulting Services)

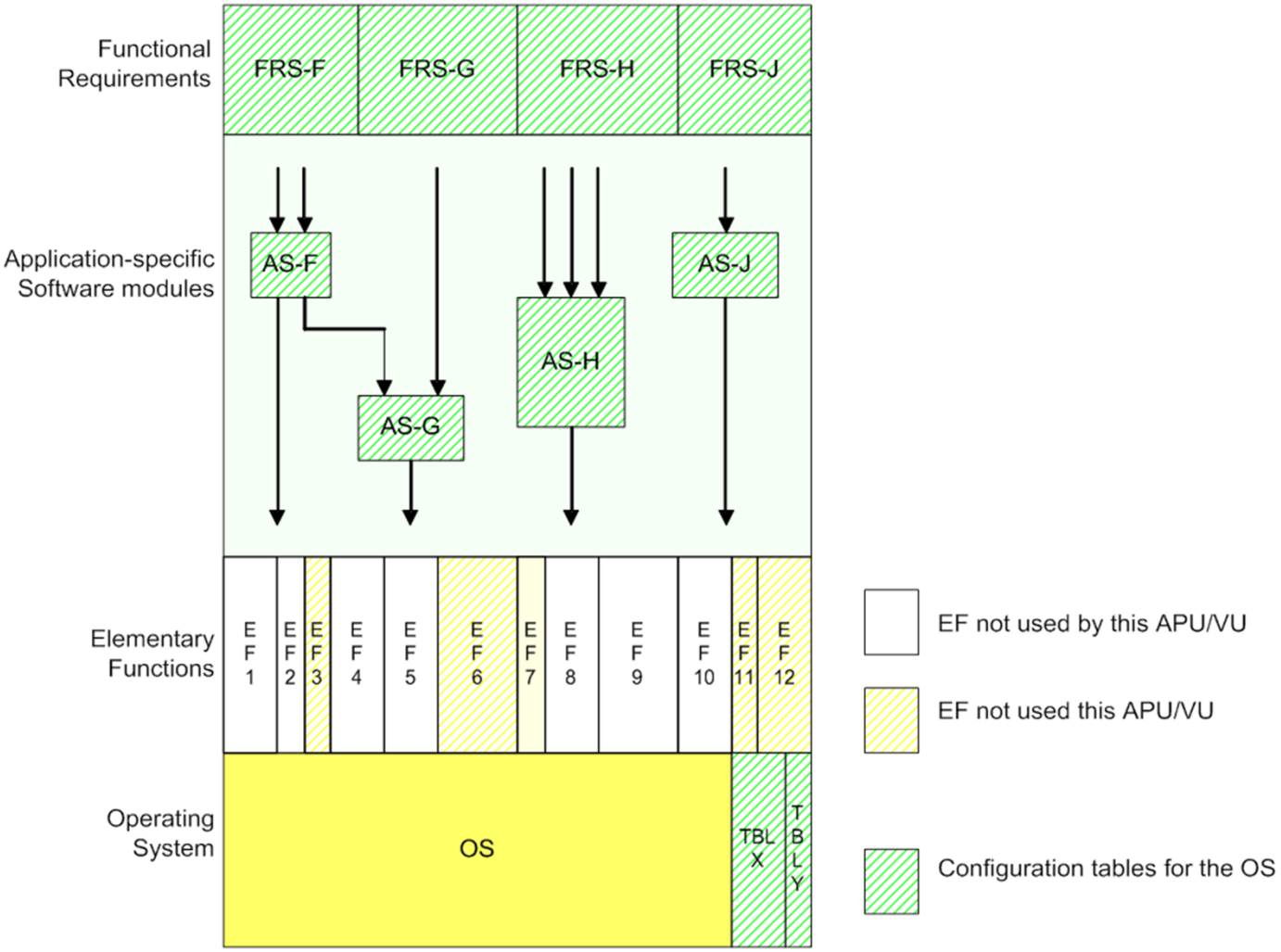
Example System – Architecture



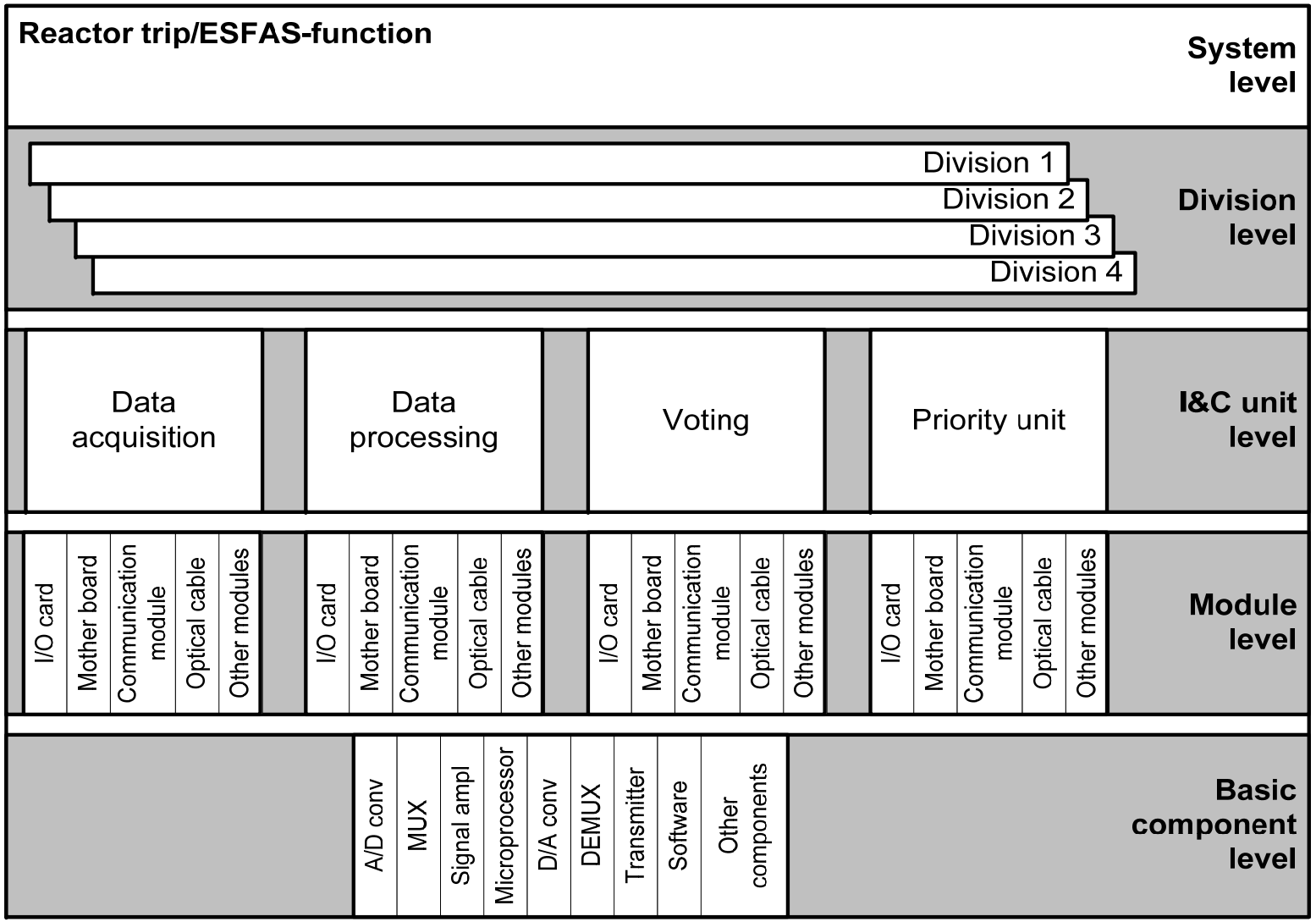
Example System – Hardware



Example System - Software



Failure Mode Taxonomy – Fault Location



Failure Mode Taxonomy
System/Division Level

- Failure to actuate the function (including late actuation),
- Spurious actuation

Failure Mode Taxonomy
Unit/Module/Basic Component Level

- Location
- Failure Effect
  - Fatal: ordered/haphazard failures
  - Non-fatal: plausible/non-plausible behaviors
- Uncovering situation
  - Online detection
    - Revealed by demand
    - Revealed by spurious actuation
  - Offline detection

Validation

Criterion	Description	Evaluation
Criterion 1	Be defined unambiguously	Met
Criterion 2	Form a complete / exhaustive set	Met
Criterion 3	Be organized hierarchically	Met
Criterion 4	Be mutually exclusive	Met
Criterion 5	Data to support the taxonomy should be available now or in the future	Open
Criterion 6	There should be analogy between failure modes of different components	Met
Criterion 7	At the very least, the lowest level of the taxonomy should be sufficient to pinpoint existing dependencies of importance to PRA modelling	Open
Criterion 8	Should support PRA practice, and fulfil PRA requirements/conditions	Open
Criterion 9	Should capture defensive measures against fault propagation (detection, isolation and correction) and other essential design features of digital I&C	Not Met

Status

- Final report is being reviewed by OECD/NEA/CSNI
- Expect approval to publish from CSNI in December 2014

EPRI | 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

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

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

Bruce Geddes
Southern Engineering Services

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

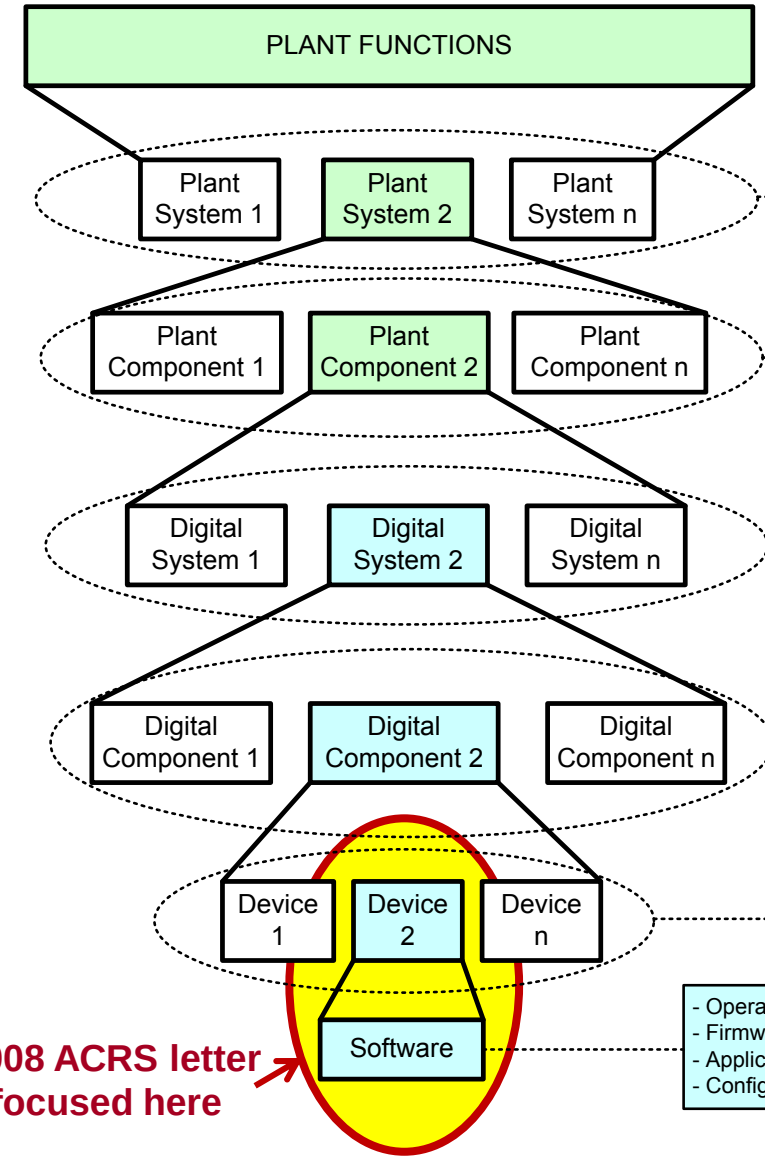
Digital System Failure Modes / Misbehaviors
Key Points

- 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

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"

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



- Main Turbine
- Main Generator
- Feedwater
- Rod Control
- Reactor Coolant
- Turbine Bypass
- Switchyard
- Electrical
- Plant Computer
- Reactor Protection
- Eng. Safety Features

- Pumps
- Valves
- Vessels
- Compressors
- Breakers
- Switchgear
- Xformers
- Heaters
- Pipes
- Ducts
- Air Handlers

- S/G Level
- FPT Speed
- Main Turbine EHC
- NSSS Controls
- Plant Computer
- Reactor Trip
- ESFAS

- Controllers
- Comm Modules
- I/O Modules
- Indicators
- Power Supplies
- Workstations
- Servers
- Sensors
- Actuators

- CPU
- A/D
- D/A
- RAM
- ROM
- Watchdog
- Parts

- Operating System
- Firmware
- Applications
- Configuration Data

Where is the "effect" of interest?

Where is the hazard managed?

Where is the failure mode/ hazard of interest?

2008 ACRS letter focused here

Plant Functions, Systems & Components

Digital Systems, Components & Devices

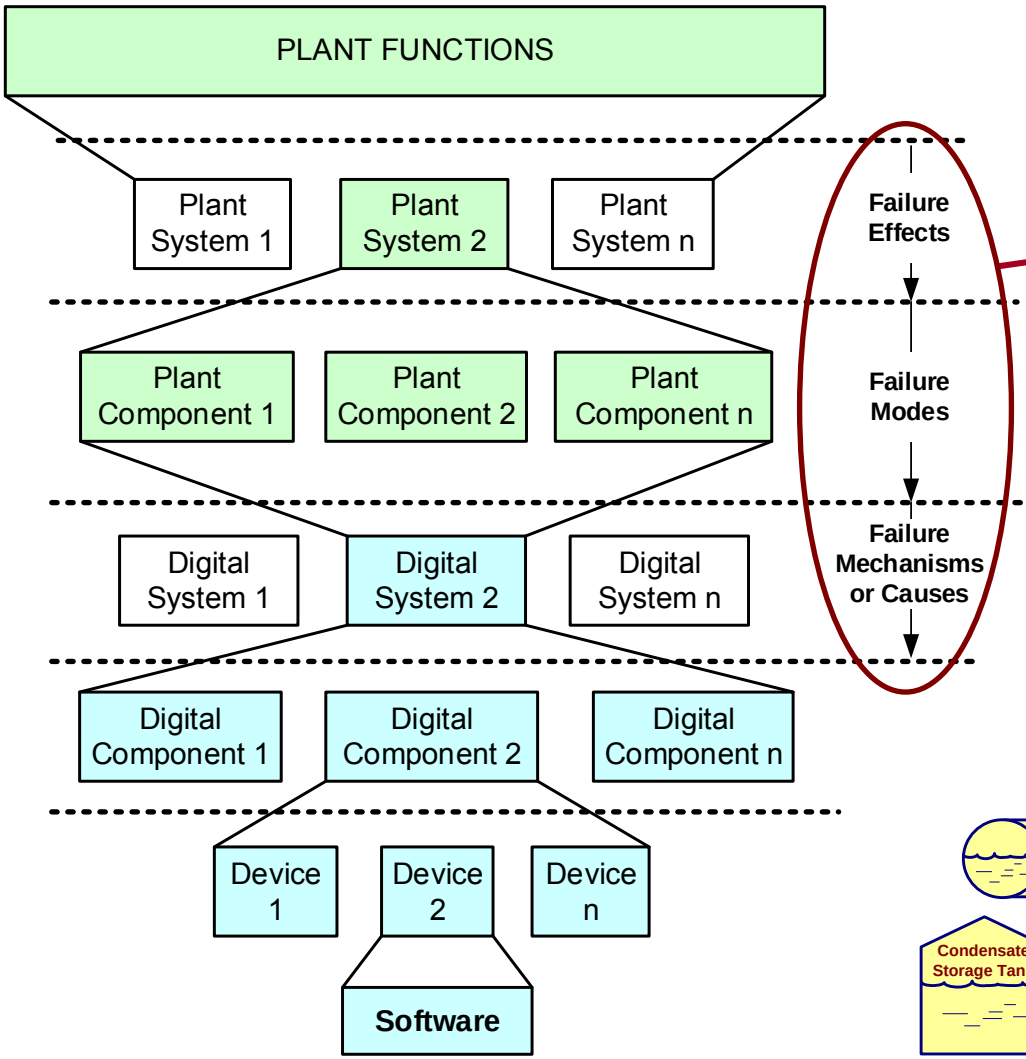
EPRI ELECTRIC POWER RESEARCH INSTITUTE

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

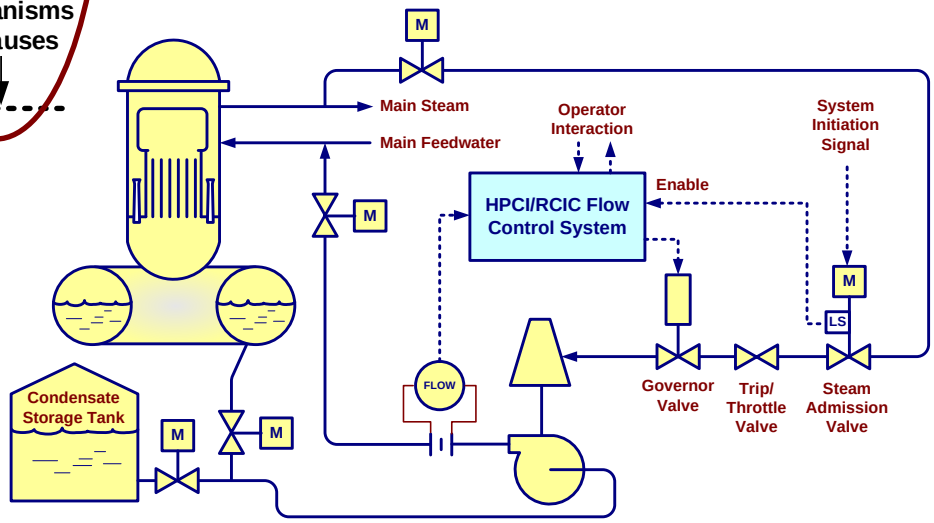
Six Methods Investigated	'Top-Down' or 'Bottom-Up'	Strengths		
		Identifies Hazards Beyond Faults/Failures	Integrated View of Plant Design	Mature, Well Documented
Functional FMEA (Failure Modes & Effects Analysis)	Top Down		X	X
Design FMEA	Bottom Up			X
Top-Down using FTA (Fault Tree Analysis)	Top Down		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

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



EPRI 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	Requirement	Potential Failure Mode	Potential Effect(s) of Failure	Possible Cause(s)/ Mechanism of Failure	Current/Detect Method: Prevention	Current/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, leading to core damage		1. [illegible] V&V 2. [illegible]S PM 3. Turbine PM	1. ESFAS Test 2. System Flow Test	Evaluate flow control modes
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. Turbine 4. Setpoint 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	
				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	
				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?

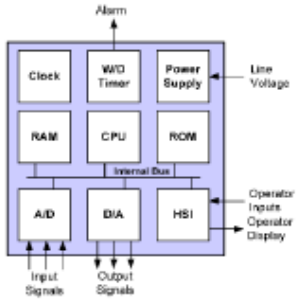
EPRI 3002000509 Appendix B: Taxonomy of Failure Modes, Failure Mechanisms & Defensive Measures

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.

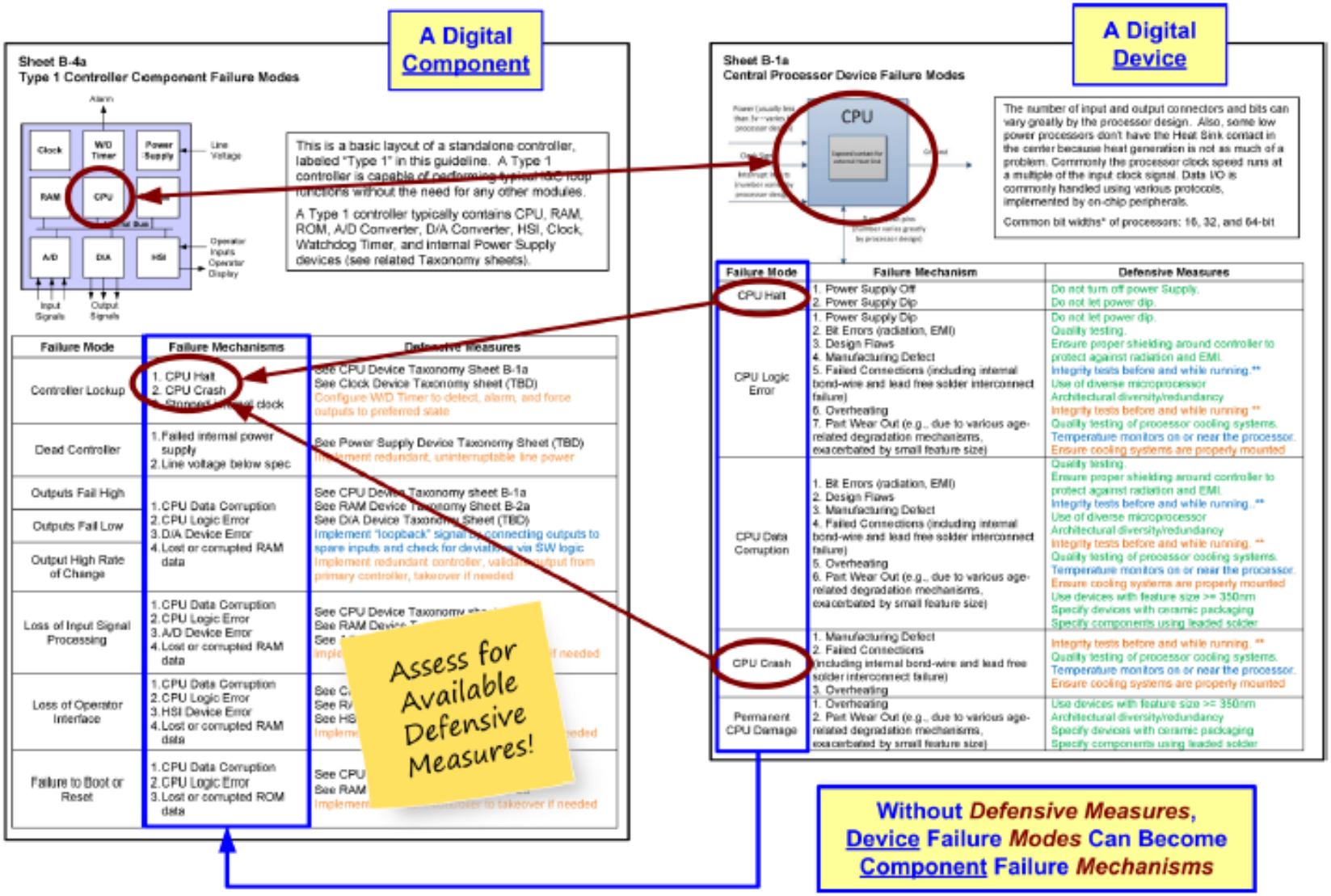
A Type 1 controller typically contains CPU, RAM, ROM, A/D Converter, D/A Converter, HSI, Clock, Watchdog Timer, and internal Power Supply devices (see related Taxonomy sheets).

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

EPRI ELECTRIC POWER RESEARCH INSTITUTE

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



EPRI 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)

Together…Shaping the Future of Electricity

EPRI | 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

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.

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.

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

Modeling Basis Reflects Lessons Learned

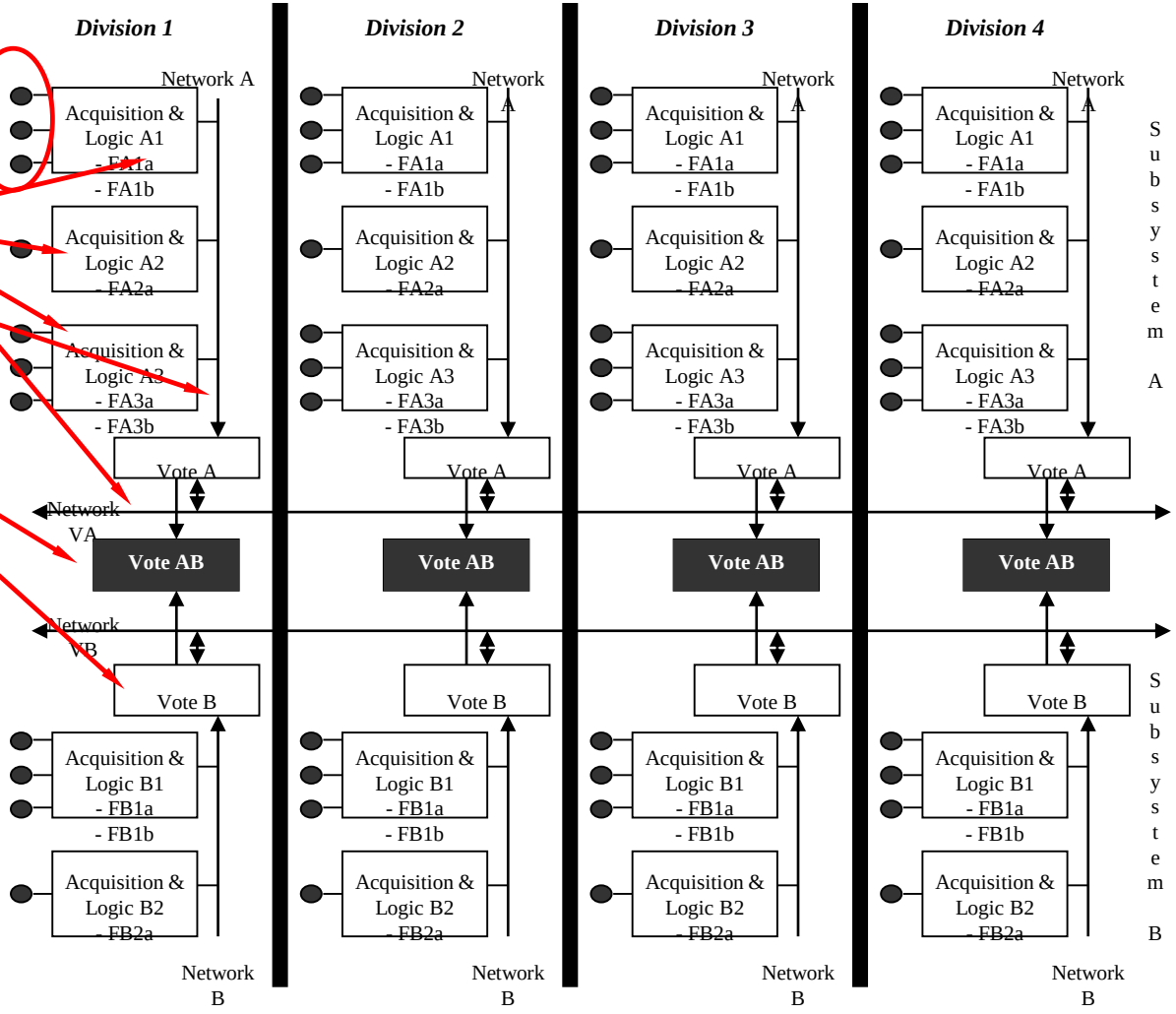
What are we trying to model?

Sensors

Signal processing

Communication

Voting



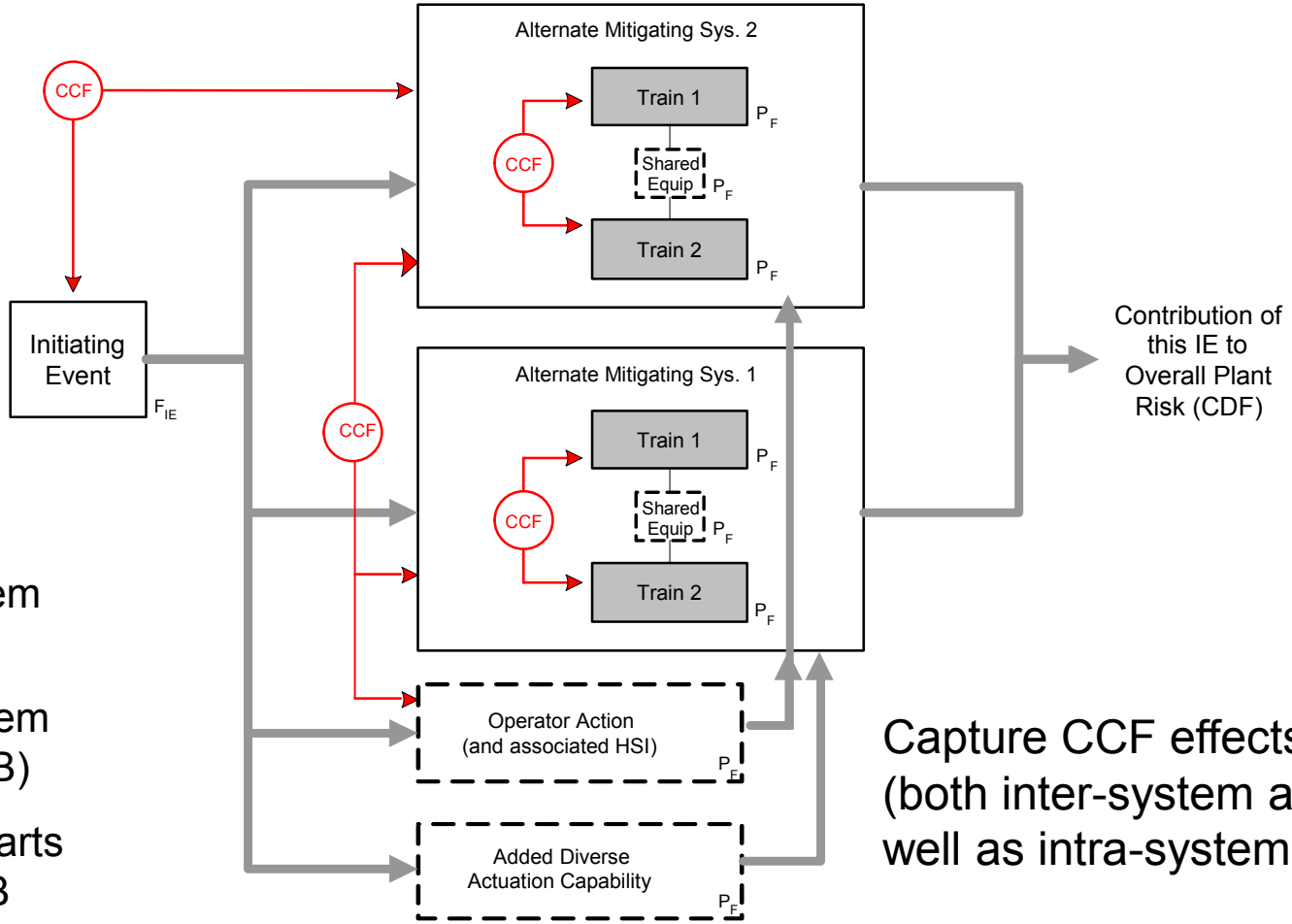
Functionally similar to analog I&C.

Modeling components having

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

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Modeling Basis Reflects Lessons Learned
How are we trying to model it?



Example

Initiating event-
loss of feedwater

1st mitigating system
AFW

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

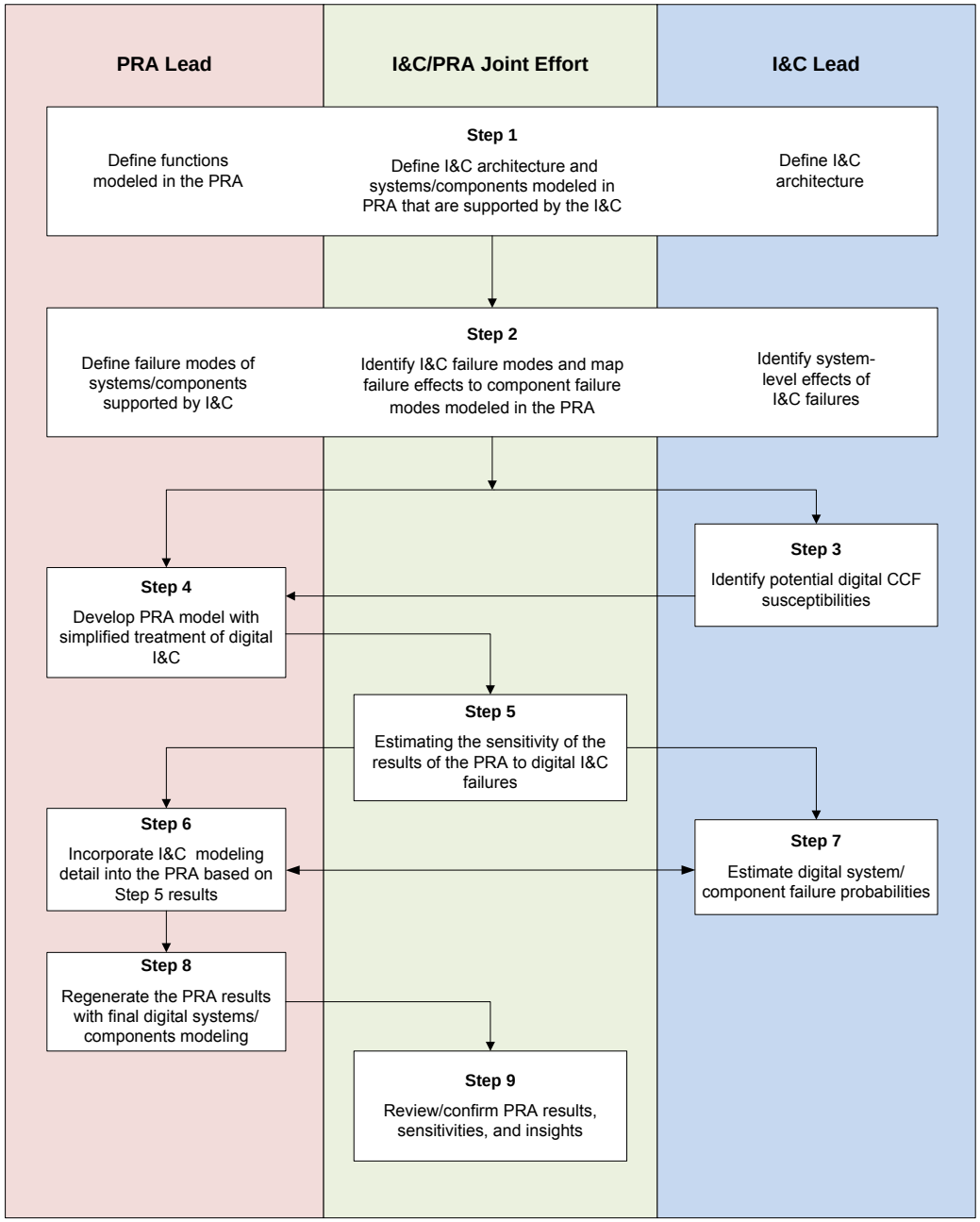
Operator action starts
AFW, initiates F&B

Diverse actuation
AMSAC

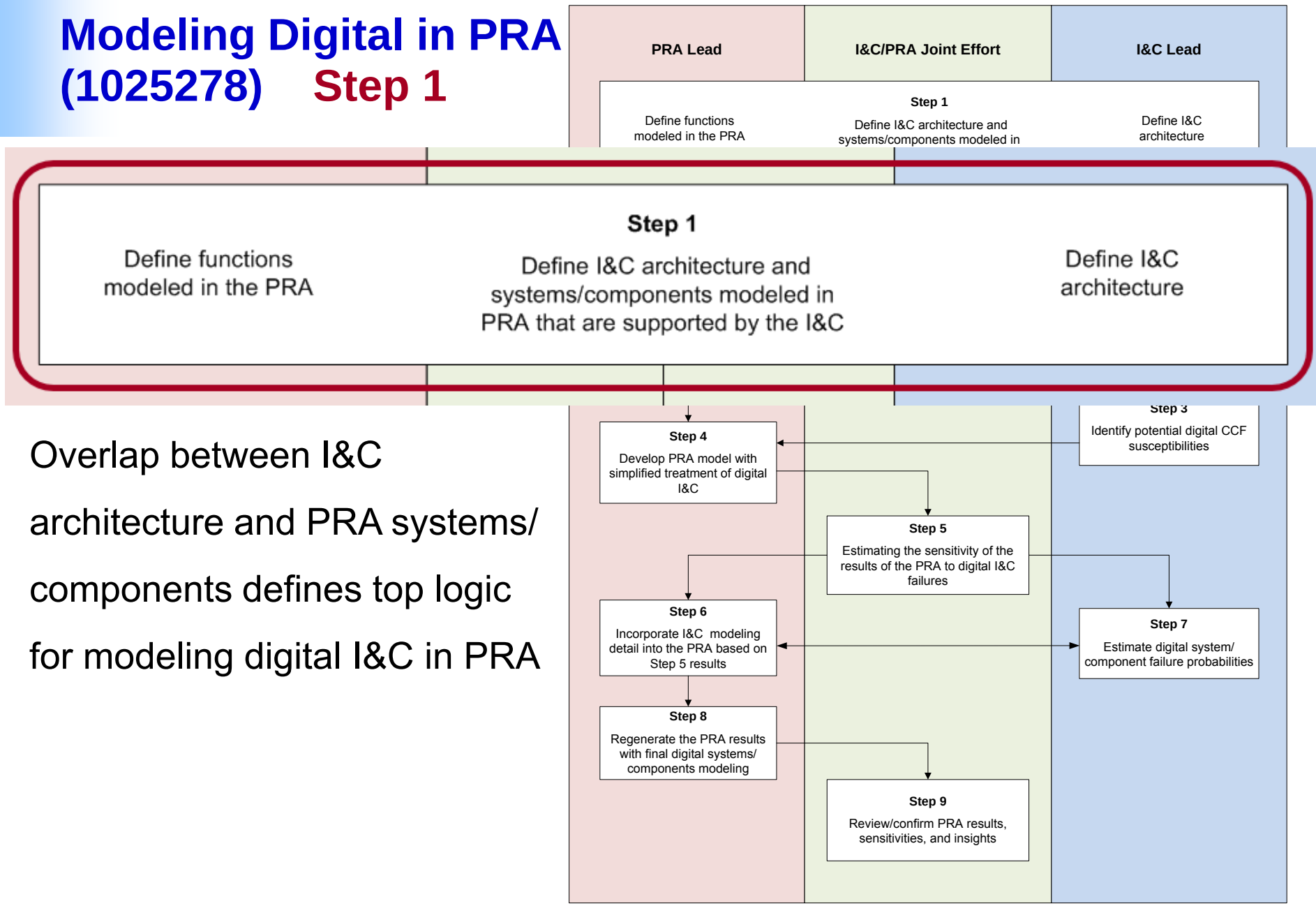
Capture CCF effects (both inter-system as well as intra-system)

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



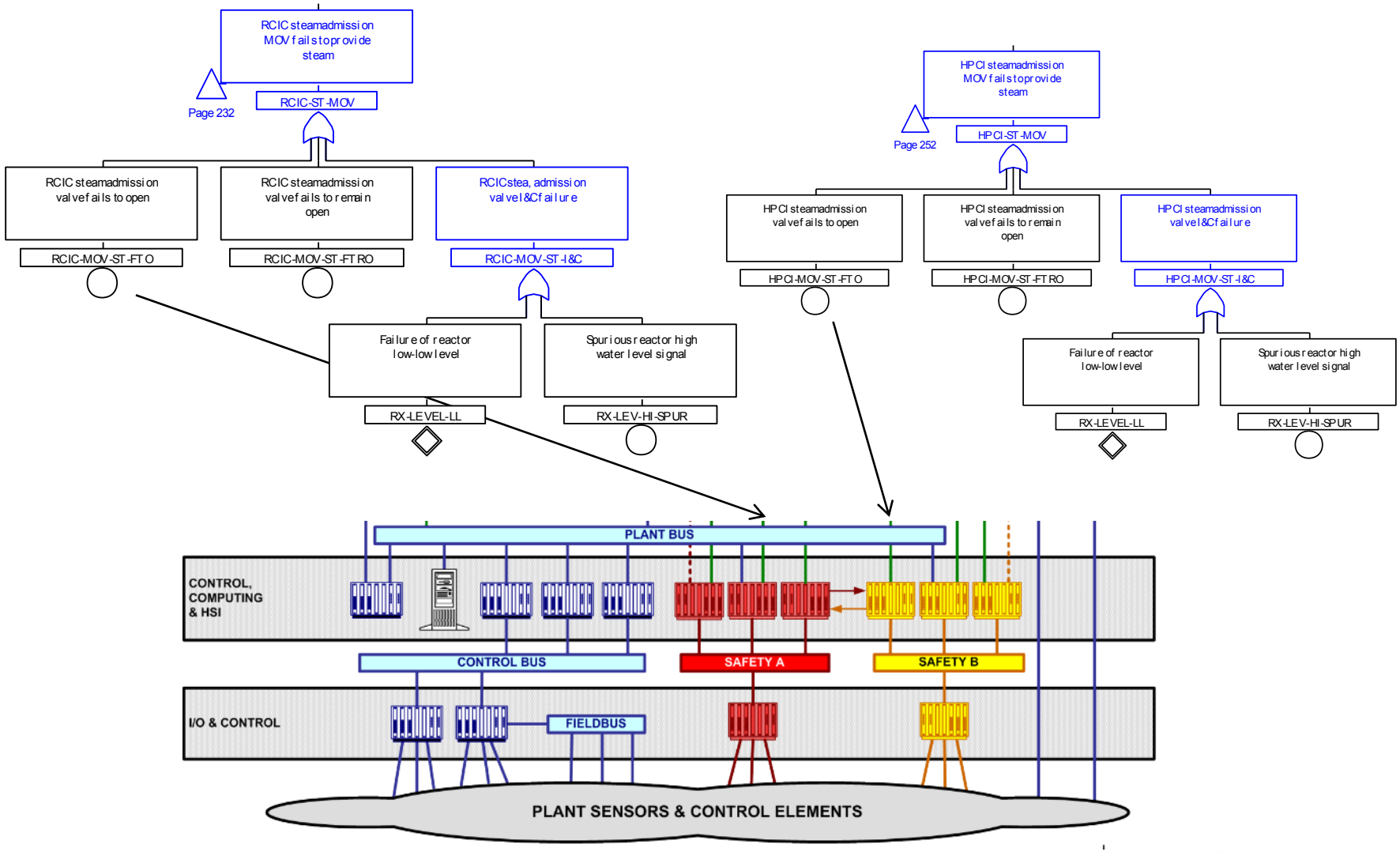
Modeling Digital in PRA (1025278) Step 1



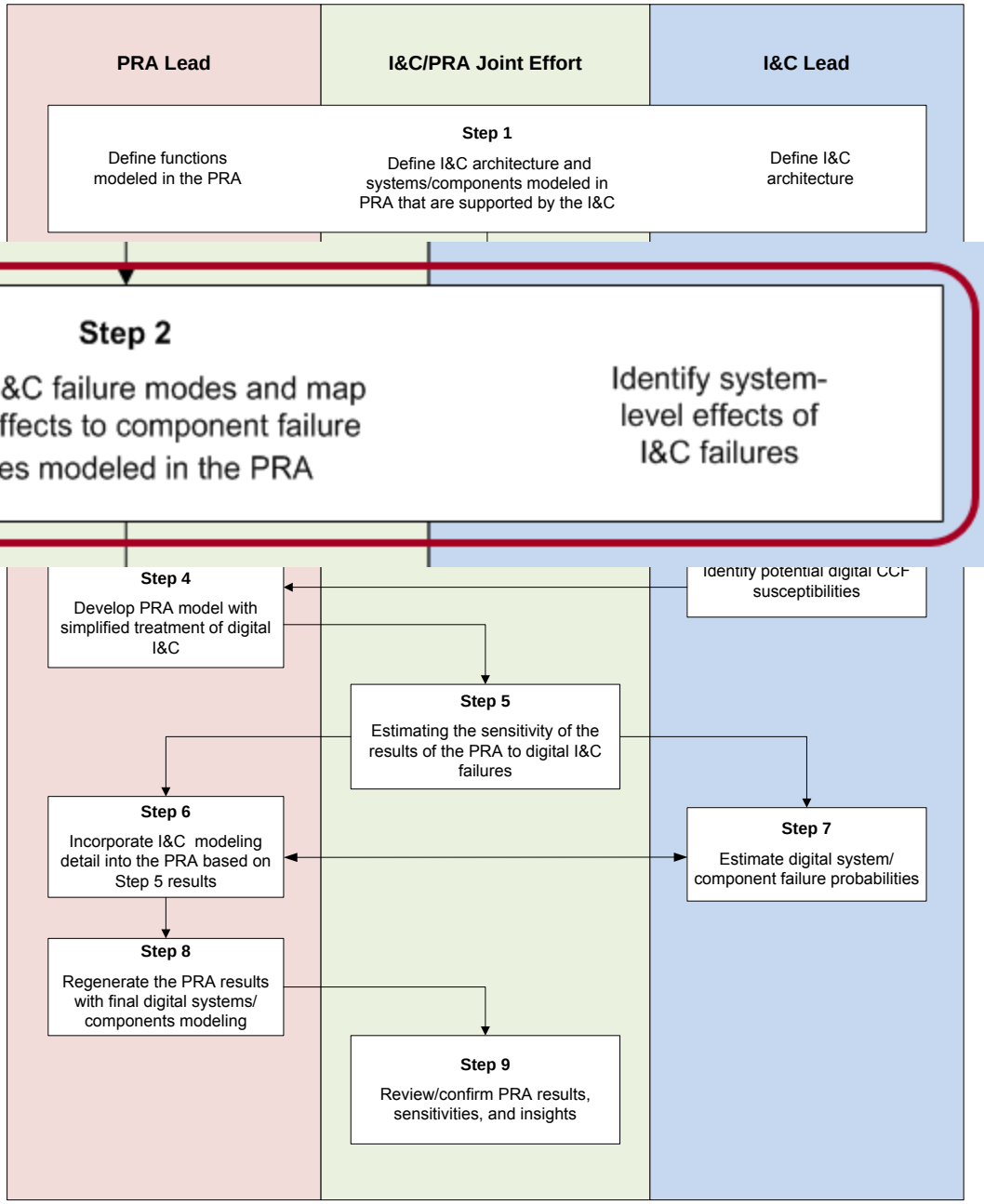
Overlap between I&C architecture and PRA systems/ components defines top logic for modeling digital I&C in PRA

Modeling Digital I&C in PRA

Step 1 – Interface between I&C and PRA components



Modeling Digital in PRA (1025278) Step 2



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

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

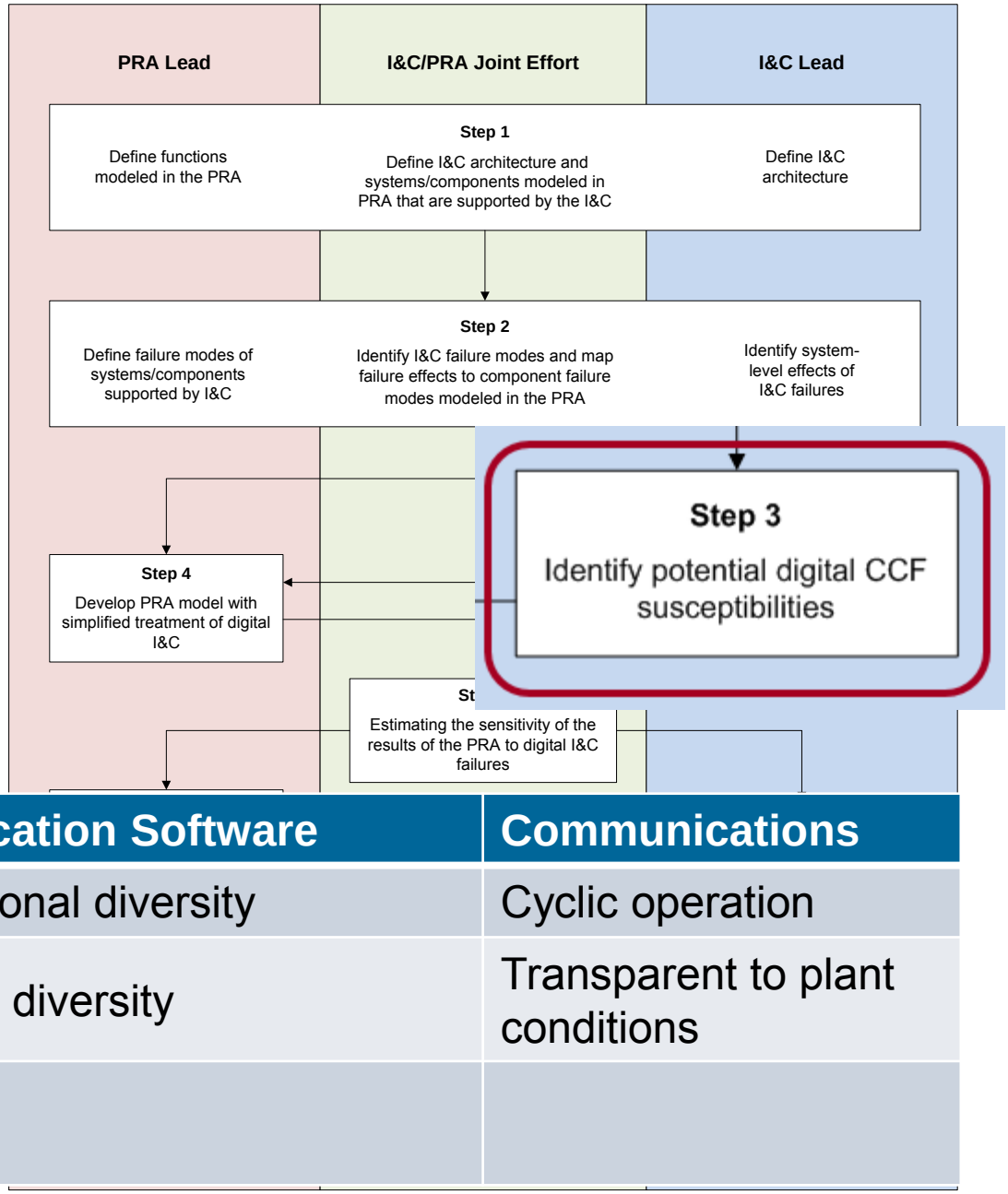
I&C System Failure Mechanism	I&C System Failure Mode	I&C System Failure Effect (on plant systems)
Output of 1 instead of 0	Protective action when none is warranted	Spurious operation of (pump, valve,...)
Output of 0 instead of 1	No protective action when needed	Failure of component to operate (pump FTS,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

controls.

Modeling Digital in PRA (1025278) Step 3

Preventive measures for CCF

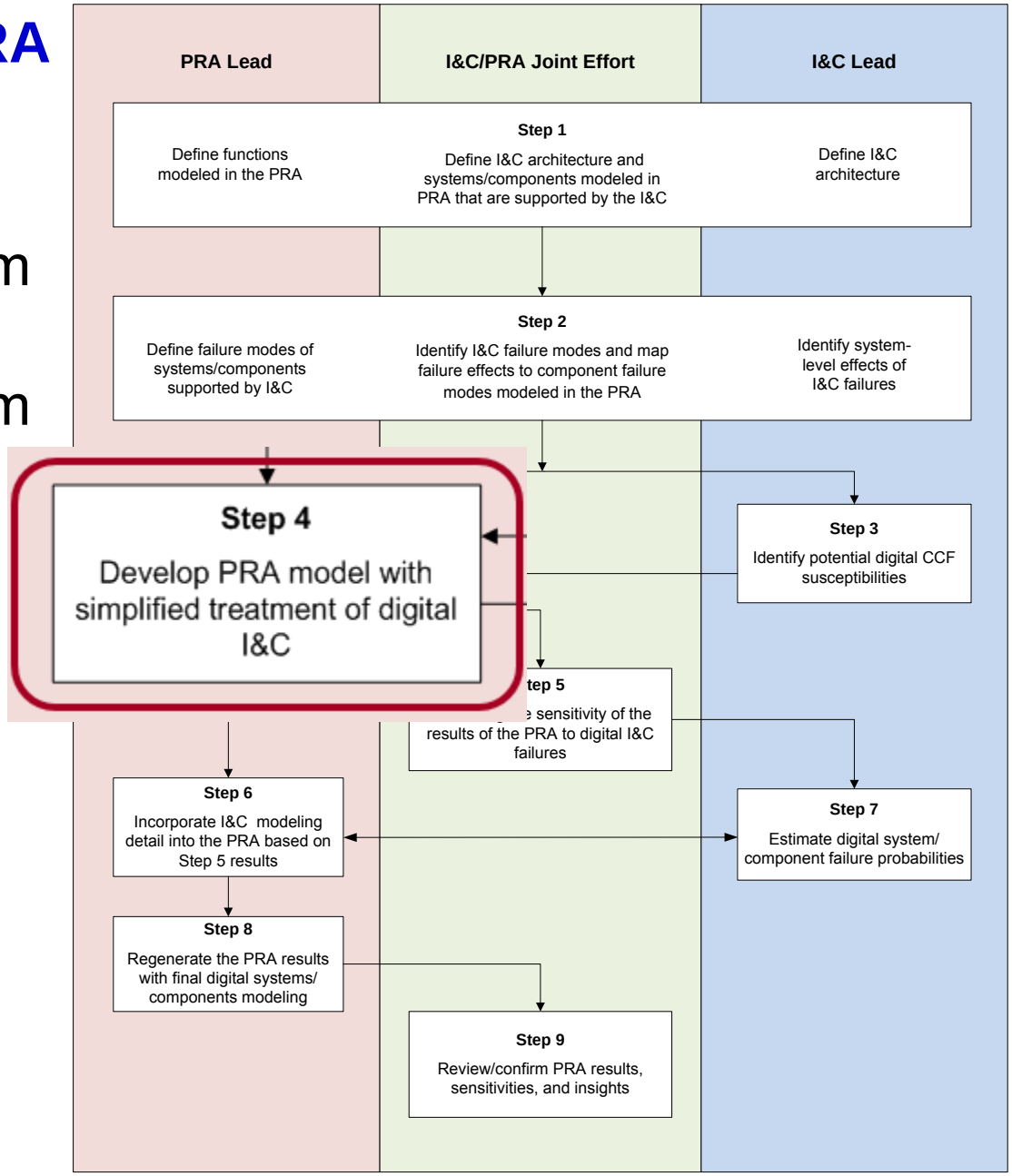
- Hardware – Different:
  - Component type / failure mode
  - Manufacturer
  - System (different operating conditions, environment)
  - Maintenance practices
- Software defensive measures:



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

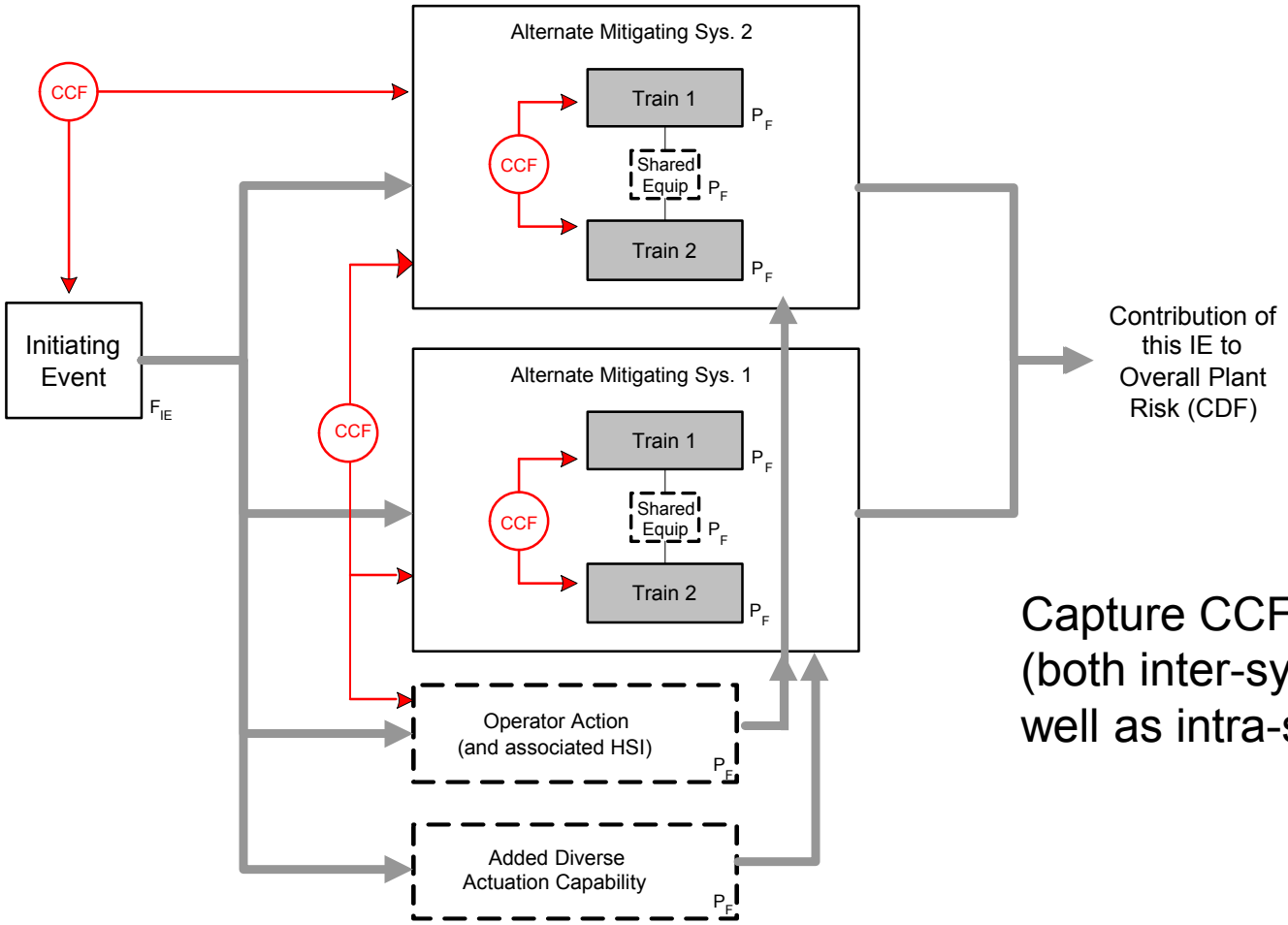
Modeling Digital in PRA (1025278) Step 4

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



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)

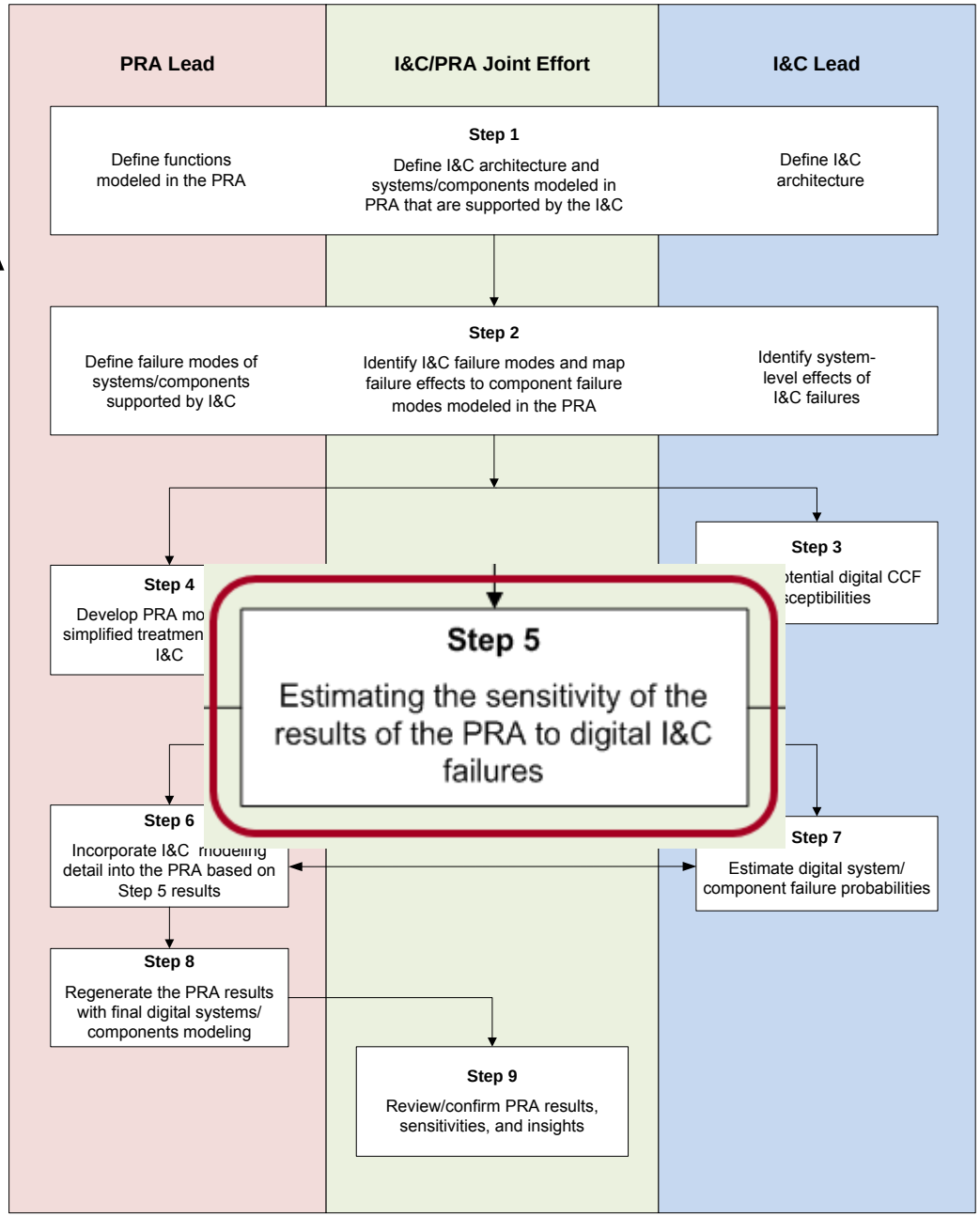
Modeling Digital I&C in PRA
Step 4 – Parameter Estimates

- 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

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



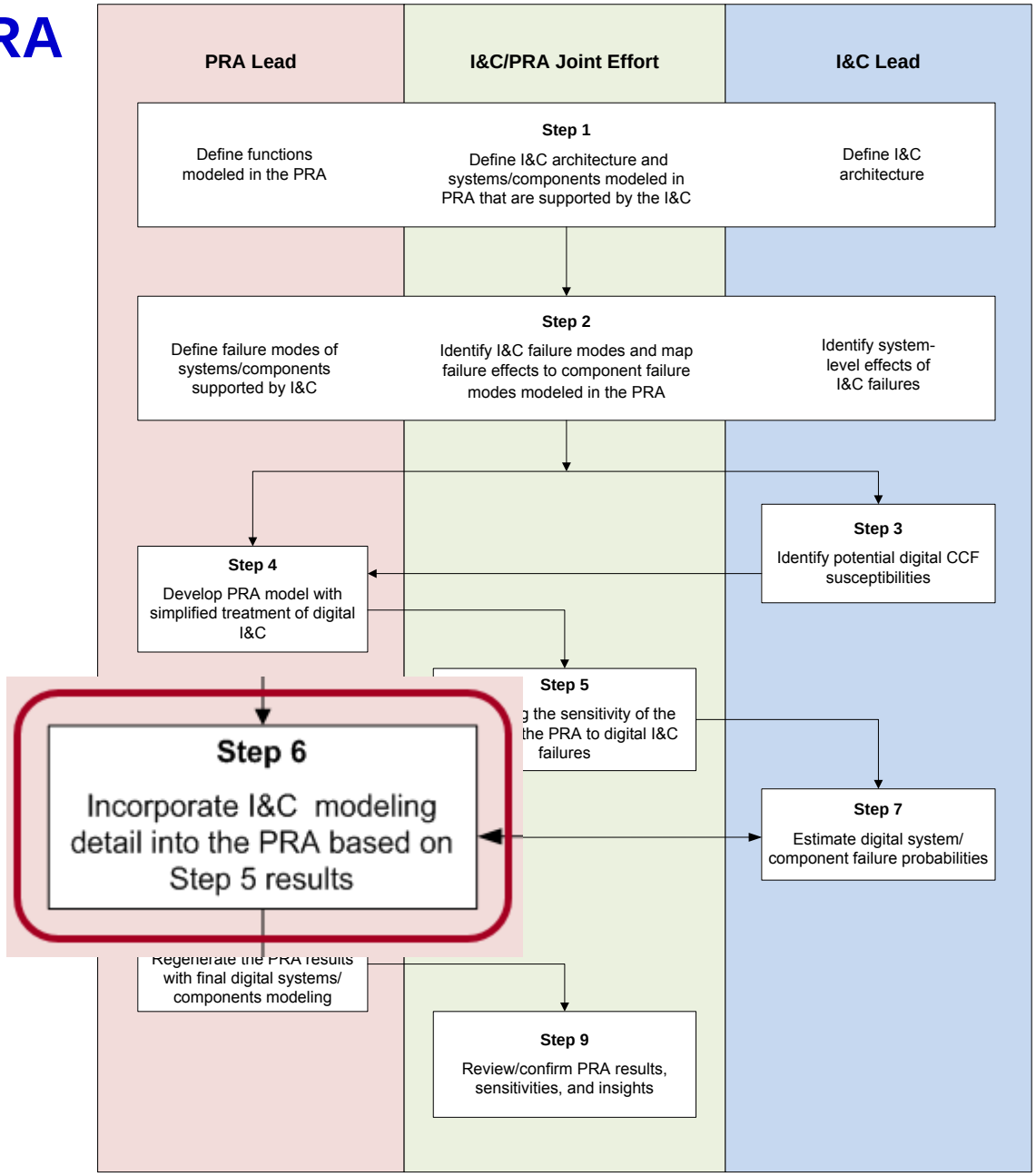
Modeling Digital I&C in PRA
Step 5 – Sensitivity Study

- 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

    We want to keep it that way
  - In upgrading I&C in the current generation of plants, we have the opportunity to incorporate risk insights into the design before the plant is modified – just like the new plants

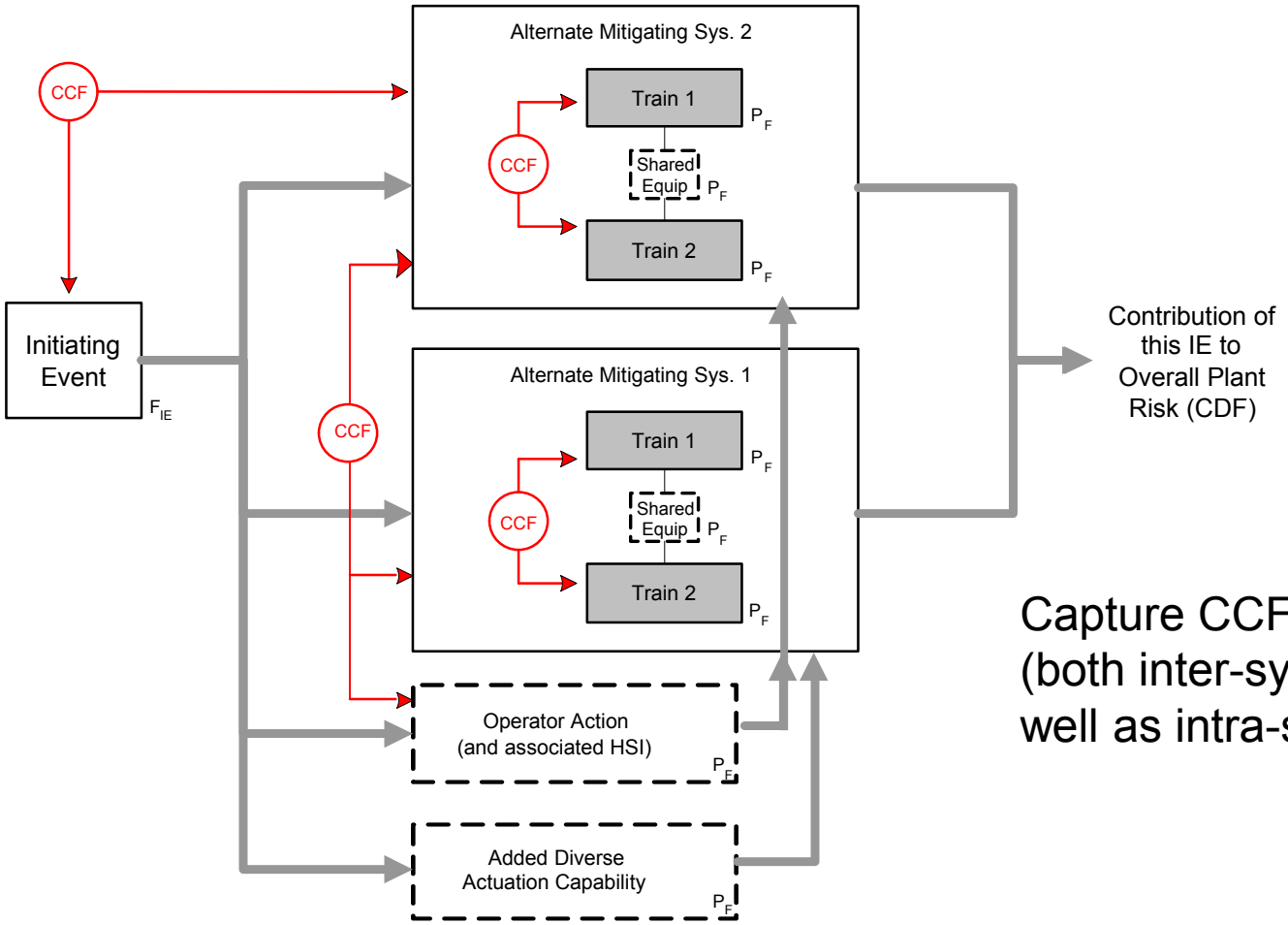
Modeling Digital in PRA (1025278) Step 6

Different levels of detail for low and high sensitivity systems



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)

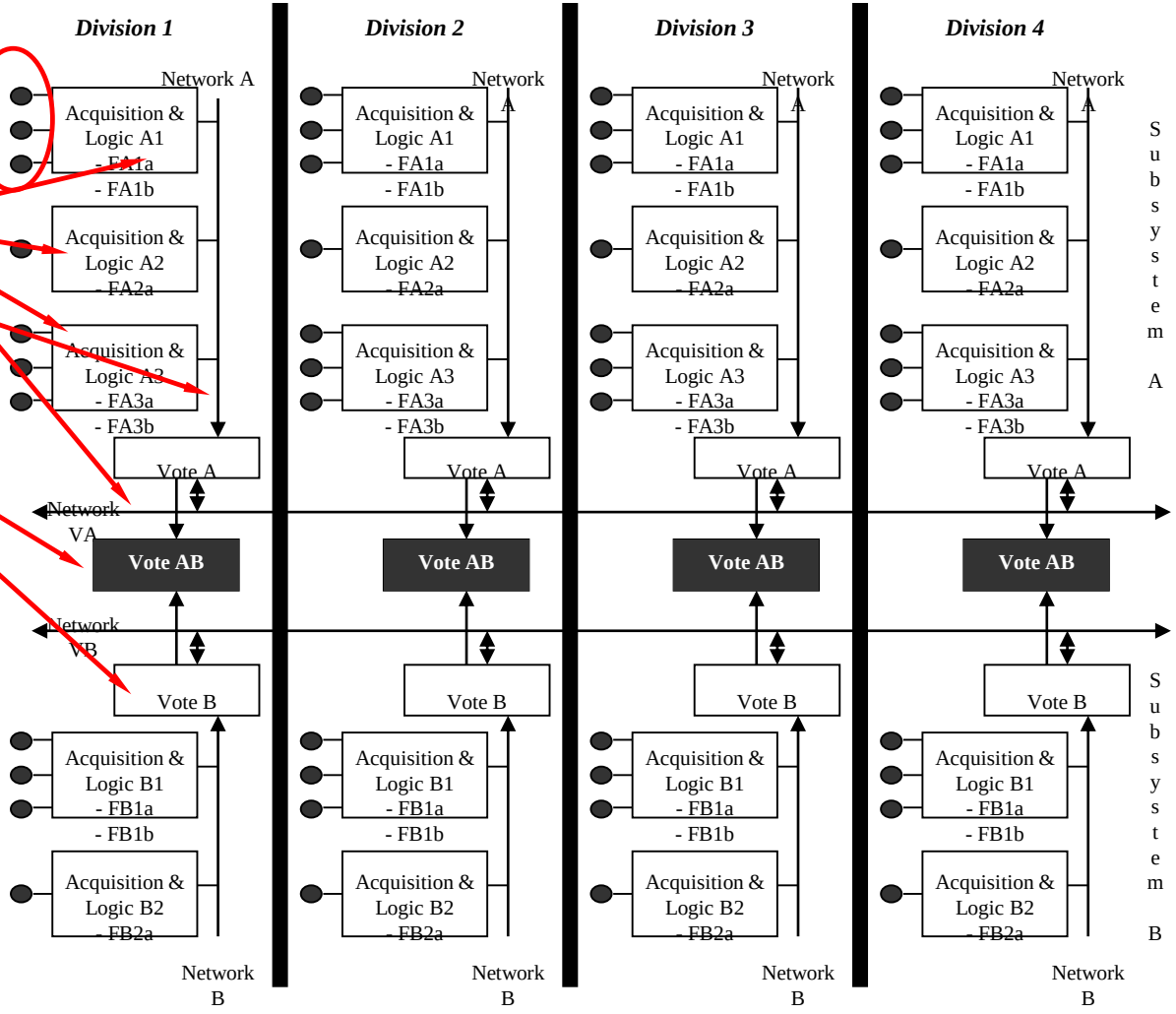
Modeling Digital I&C in PRA

Step 6 – Level of Modeling Detail for High Sensitivity Systems

Hardware
- Sensors
- Signal processing
- Communication
- Voting

Components, their failure modes and effects

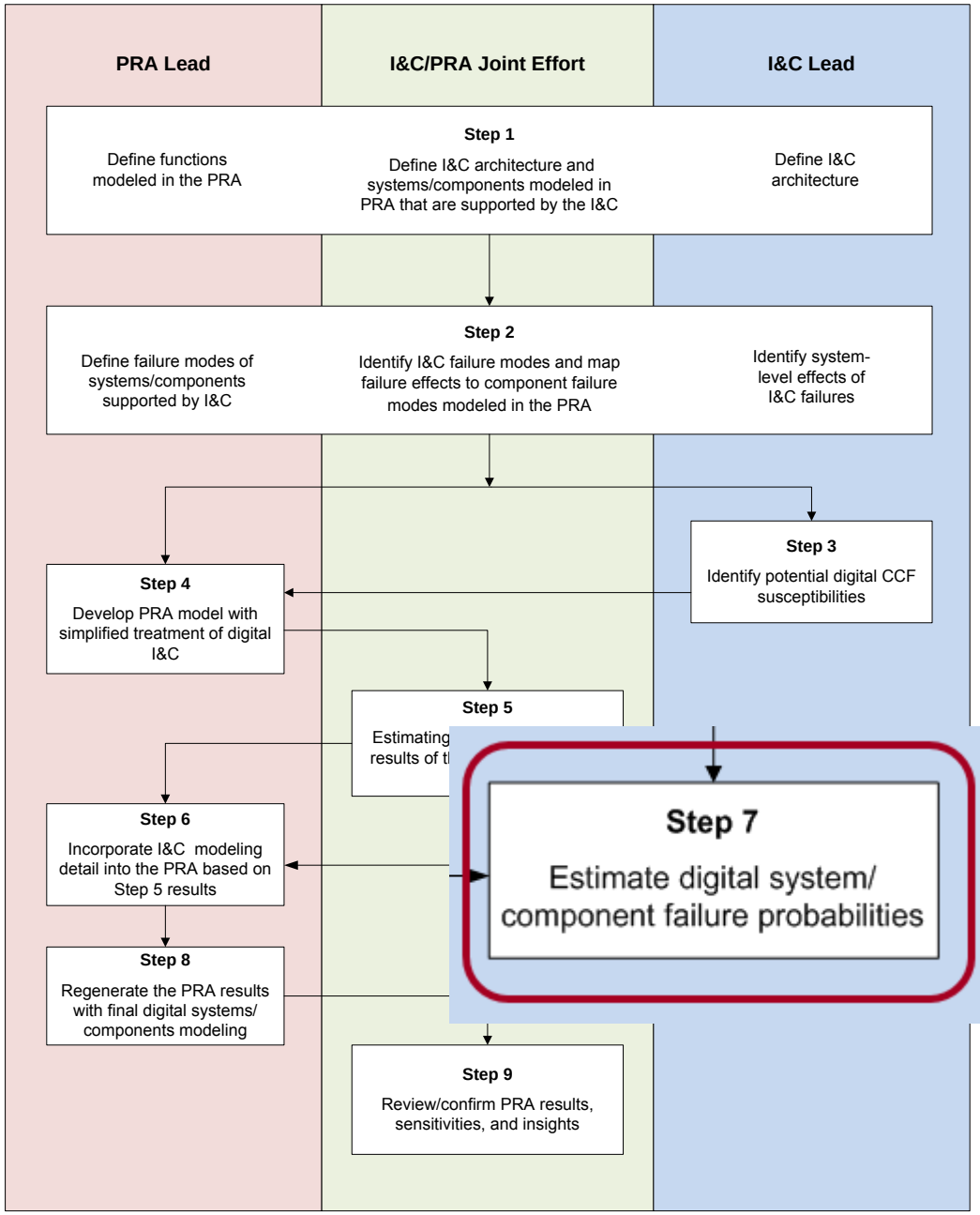
Note: Unavailabilty and maintenance errors modeled separately



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital in PRA (1025278) Step 7

Different parameter estimates for low and high sensitivity systems



EPRI 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

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

Modeling Digital I&C in PRA

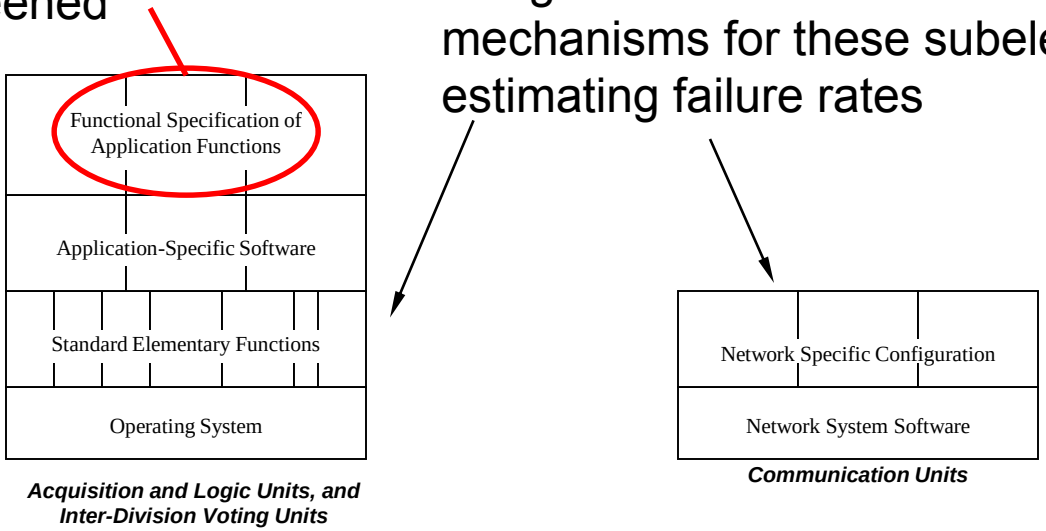
Parameter Estimates for High Sensitivity Systems (Software)

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

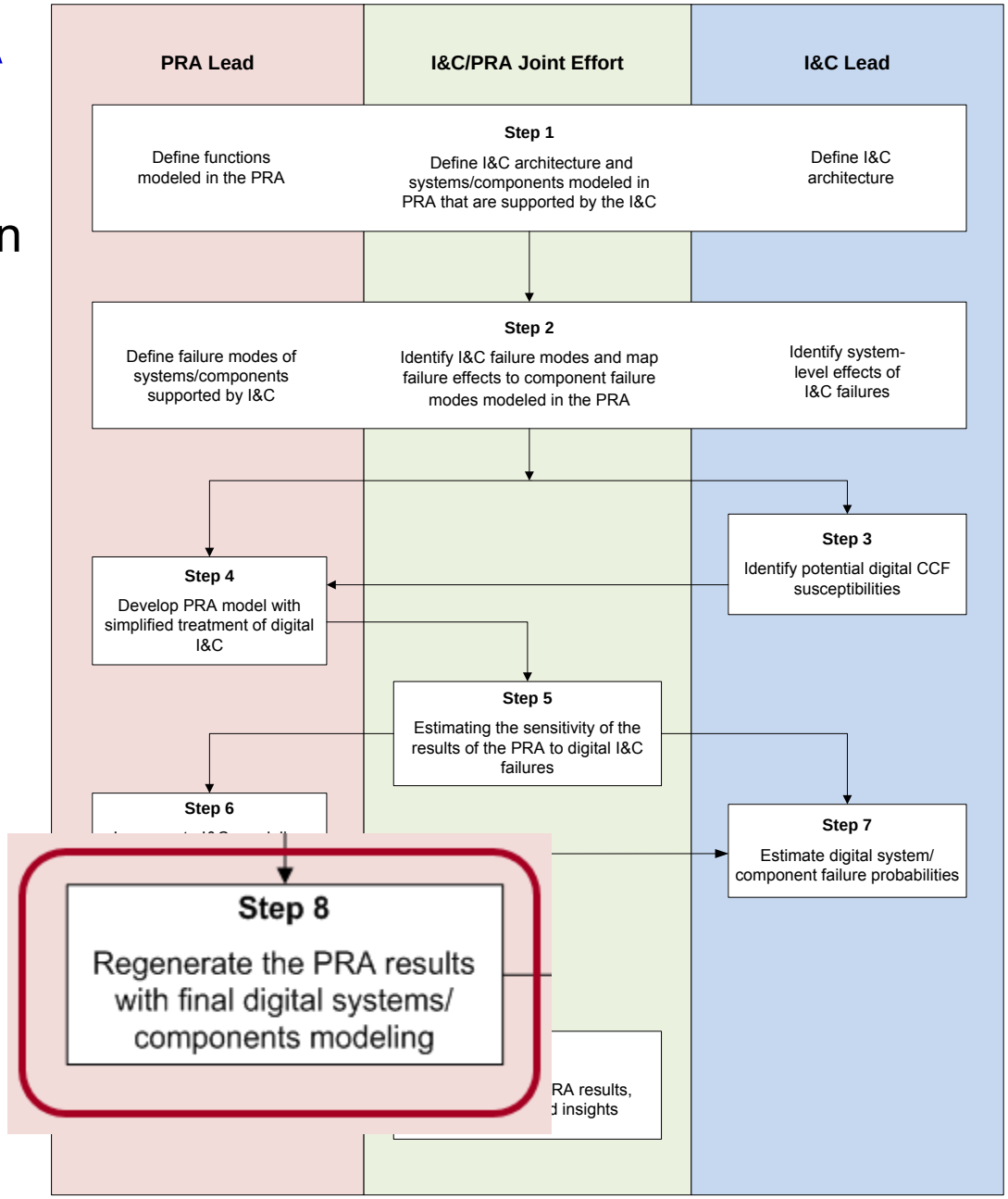
Modeling Digital I&C in PRA
Quantification of Residual Failure Modes

- 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

Modeling Digital in PRA (1025278) Step 8

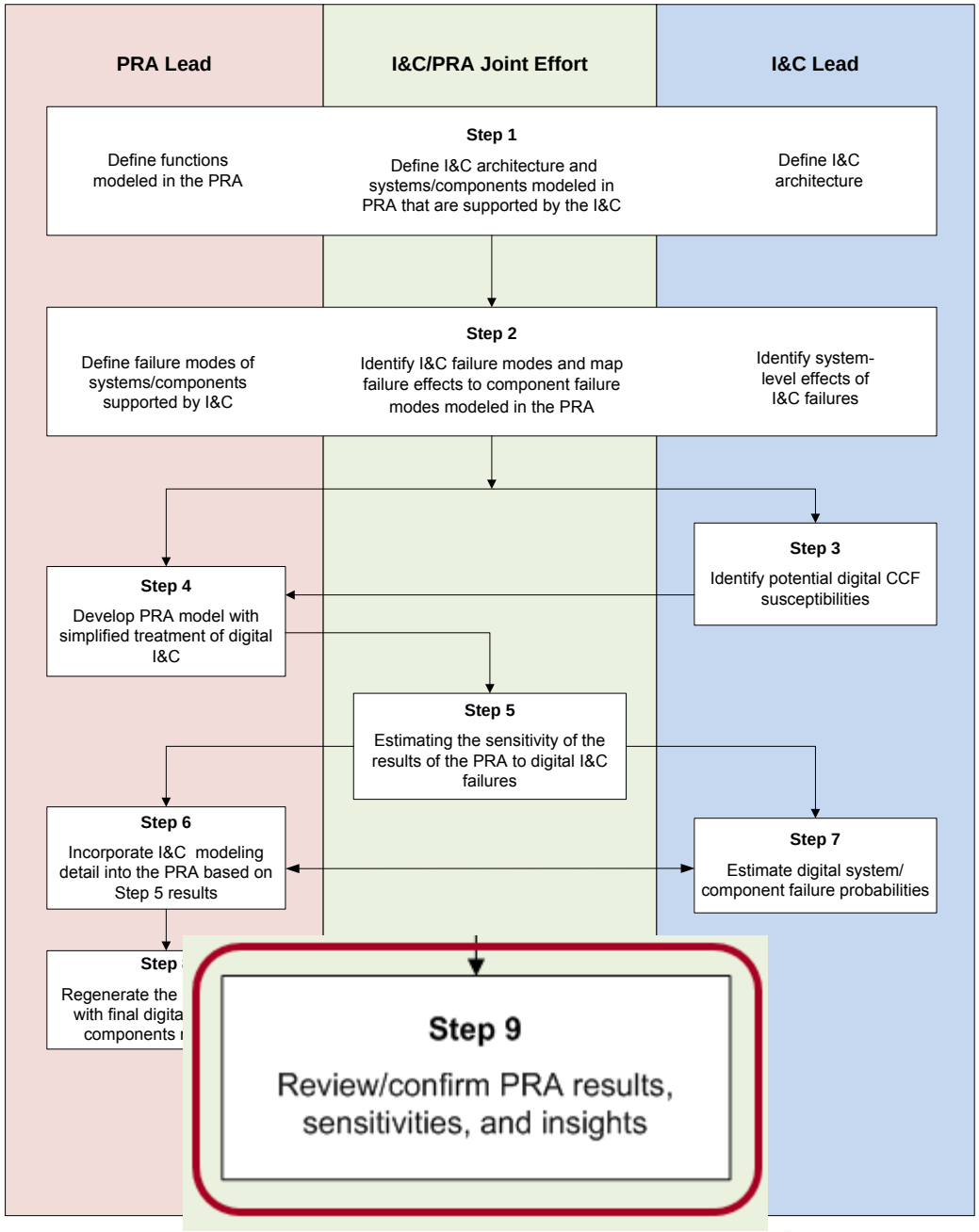
Accident sequence quantification

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



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



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

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

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.

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.

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.

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity

EPRI | 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

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

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

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

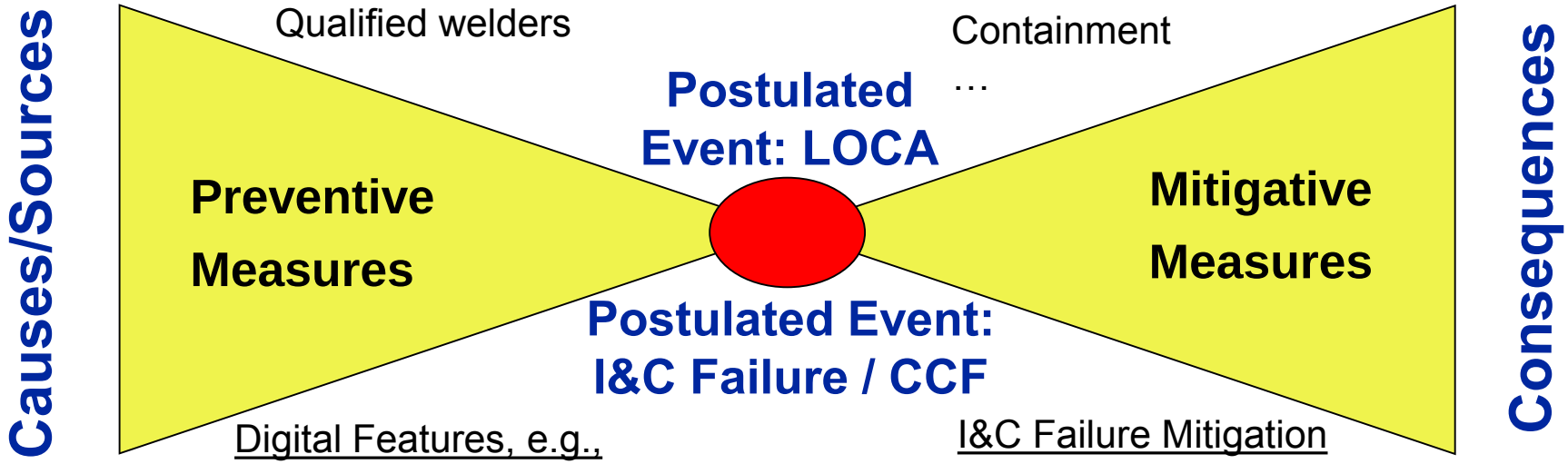
EPRI Project on Digital Failure Susceptibility Key Terms

- *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

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

Approach / Concepts
Prevention and Mitigation



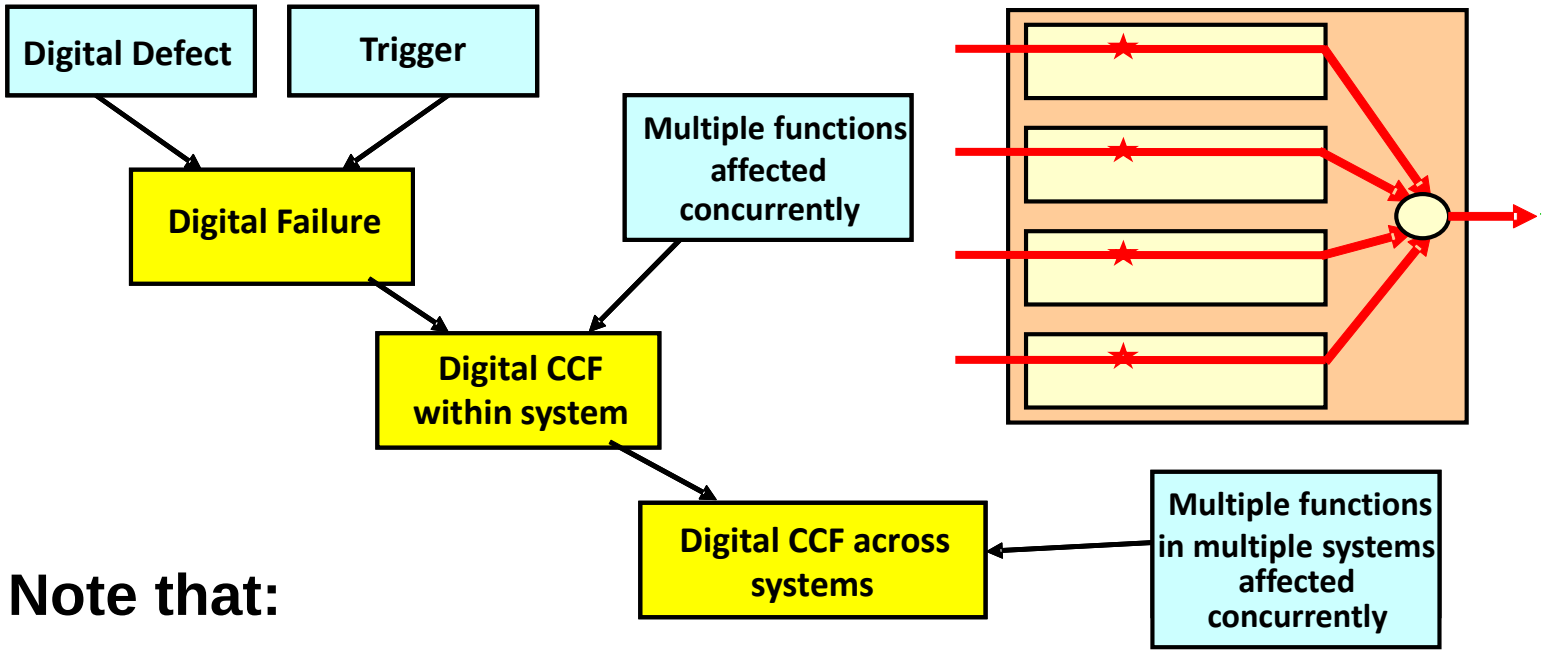
Piping Attributes, e.g.,
- Qualified materials
- ASME code
- Inspections
- Qualified welders

Piping Failure Mitigation
- Isolation valves
- Emergency core cooling
- Low pressure safety injection
- Containment
- …

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
- …

Approach / Concepts
Defects and Triggers



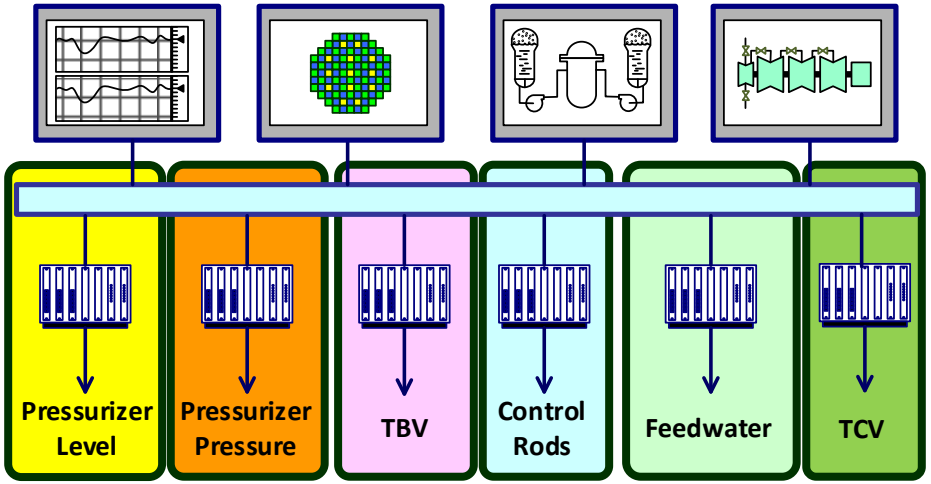
Note that:

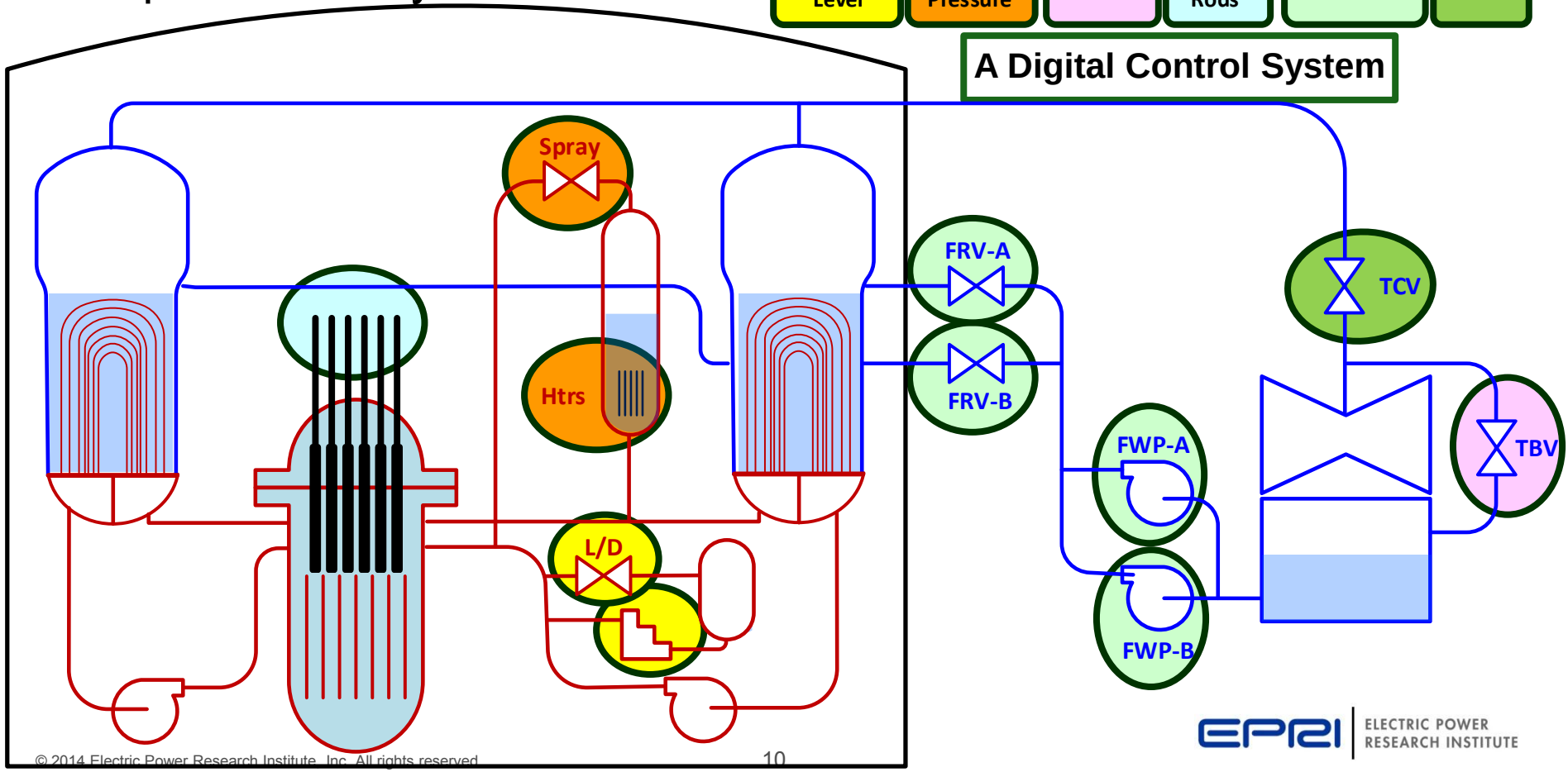
- Not all digital defects/failures can become CCFs
- Not all digital failures are safety-significant
- Defect-free software is neither expected nor needed
- Eliminating defects and triggers reduces likelihood of failure / CCF

Failure/CCF susceptibility evaluation looks for design measures and practices that reduce the likelihood of defects and triggers

Approach / Concepts
Common-Cause Failure Contexts

Failures and misbehaviors could affect single or multiple components or systems

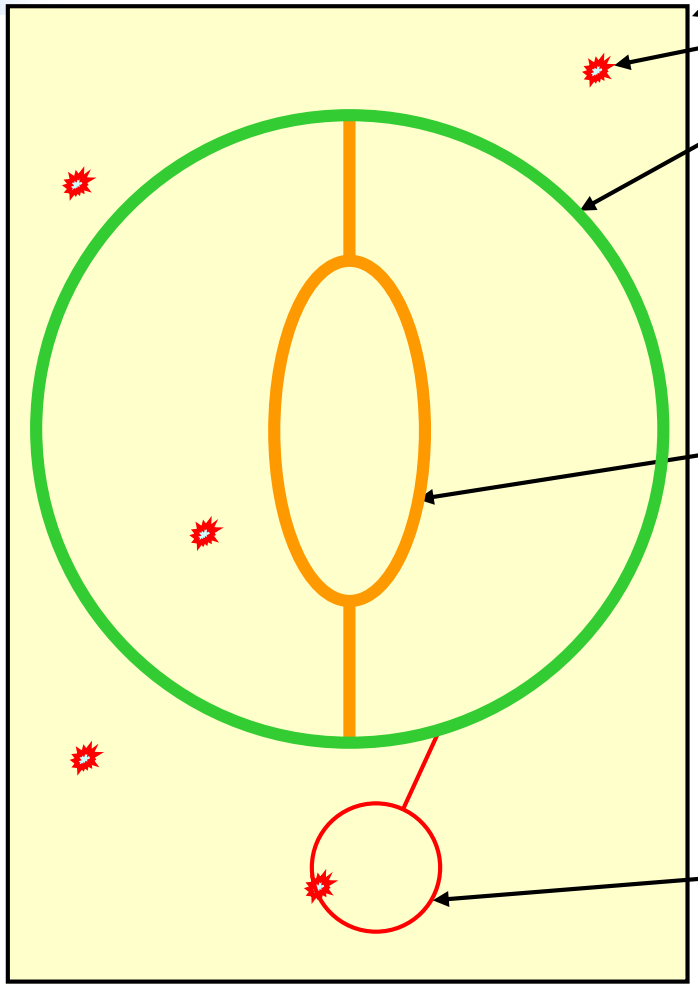




EPRI ELECTRIC POWER RESEARCH INSTITUTE

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

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

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

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

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

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

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

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

EPRI | 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

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

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

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

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)

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

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)

Palo Verde Exciter Hazard Analysis

9. Hazard Analysis Acceptance, Documentation and Maintenance
   - To be determined

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

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity

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 1-130

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

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.)

EPRI | 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

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

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

Bruce Geddes
Southern Engineering Services

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

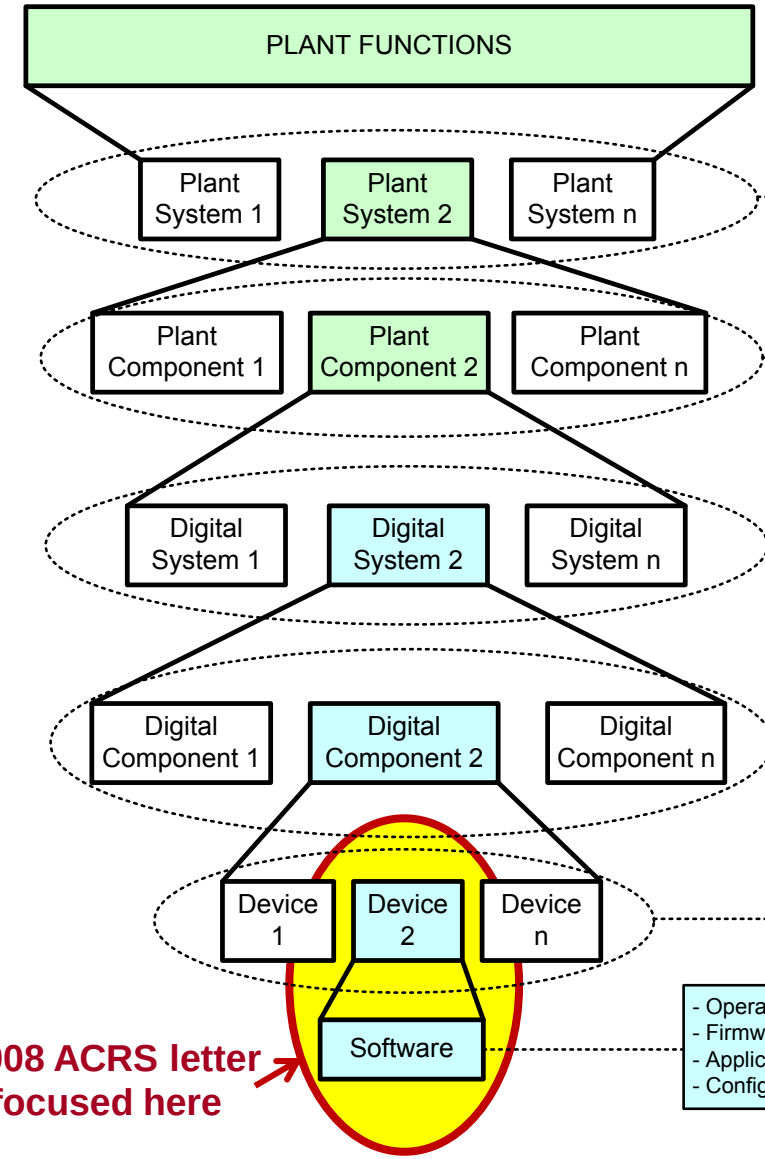
Digital System Failure Modes / Misbehaviors
Key Points

- 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

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"

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



- Main Turbine
- Main Generator
- Feedwater
- Rod Control
- Reactor Coolant
- Turbine Bypass
- Switchyard
- Electrical
- Plant Computer
- Reactor Protection
- Eng. Safety Features

- Pumps
- Valves
- Vessels
- Compressors
- Breakers
- Switchgear
- Xformers
- Heaters
- Pipes
- Ducts
- Air Handlers

- S/G Level
- FPT Speed
- Main Turbine EHC
- NSSS Controls
- Plant Computer
- Reactor Trip
- ESFAS

- Controllers
- Comm Modules
- I/O Modules
- Indicators
- Power Supplies
- Workstations
- Servers
- Sensors
- Actuators

- CPU
- A/D
- D/A
- RAM
- ROM
- Watchdog
- Parts

- Operating System
- Firmware
- Applications
- Configuration Data

Where is the "effect" of interest?

Where is the hazard managed?

Where is the failure mode/ hazard of interest?

2008 ACRS letter focused here

Plant Functions, Systems & Components

Digital Systems, Components & Devices

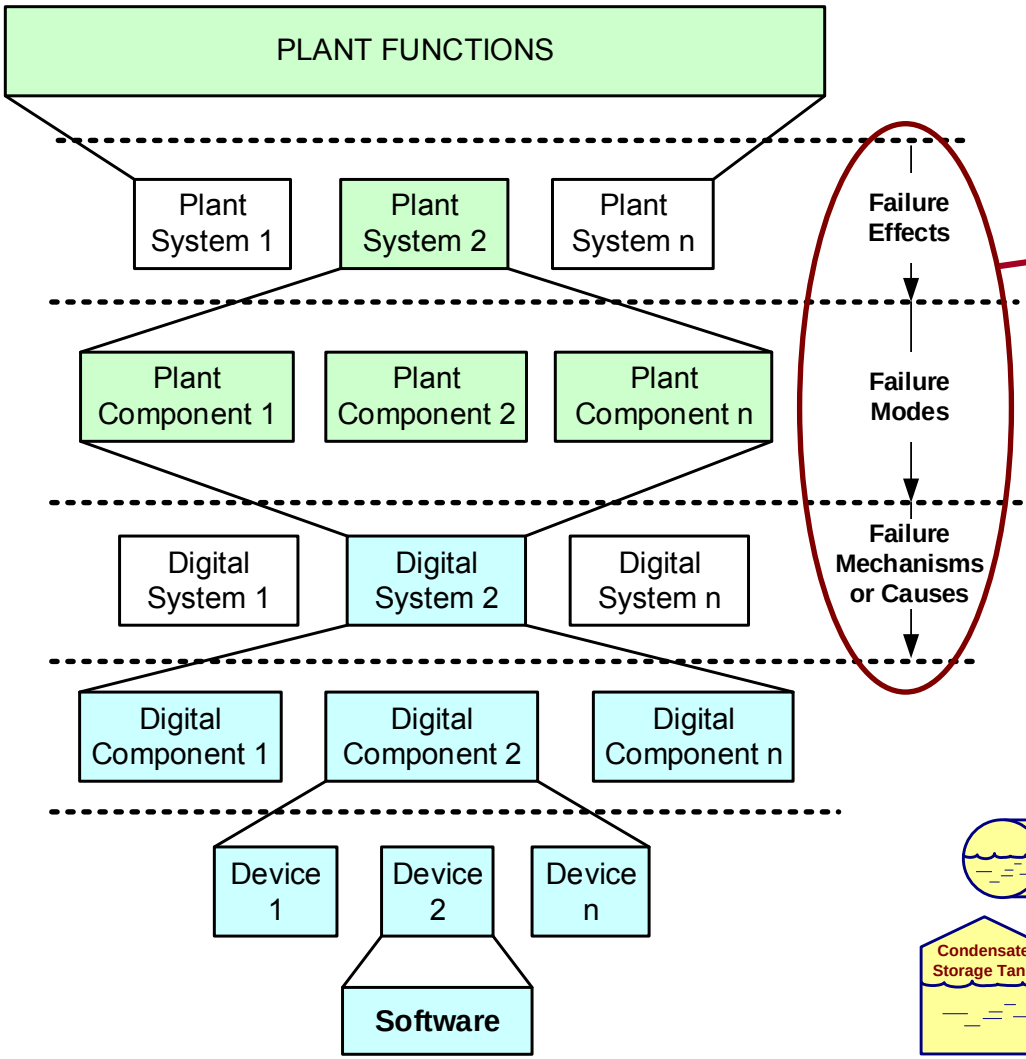
EPRI ELECTRIC POWER RESEARCH INSTITUTE

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

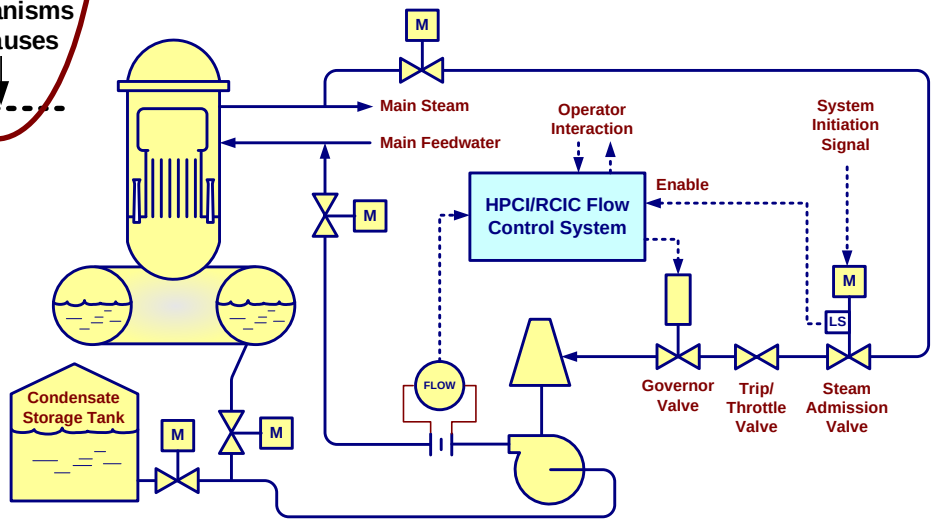
Six Methods Investigated	'Top-Down' or 'Bottom-Up'	Strengths		
		Identifies Hazards Beyond Faults/Failures	Integrated View of Plant Design	Mature, Well Documented
Functional FMEA (Failure Modes & Effects Analysis)	Top Down		X	X
Design FMEA	Bottom Up			X
Top-Down using FTA (Fault Tree Analysis)	Top Down		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

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



EPRI 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	Requirement	Potential Failure Mode	Potential Effect(s) of Failure	Possible Cause(s)/ Mechanism of Failure	Current/Detect Method: Prevention	Current/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, leading to core damage		1. [illegible] V&V 2. [illegible]S PM 3. Turbine PM	1. ESFAS Test 2. System Flow Test	Evaluate flow control modes
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. Turbine 4. Setpoint 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	
				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	
				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?

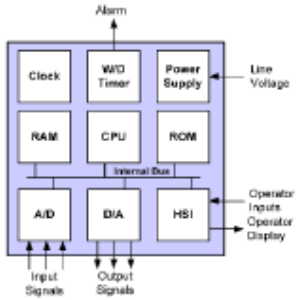
EPRI 3002000509 Appendix B: Taxonomy of Failure Modes, Failure Mechanisms & Defensive Measures

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.

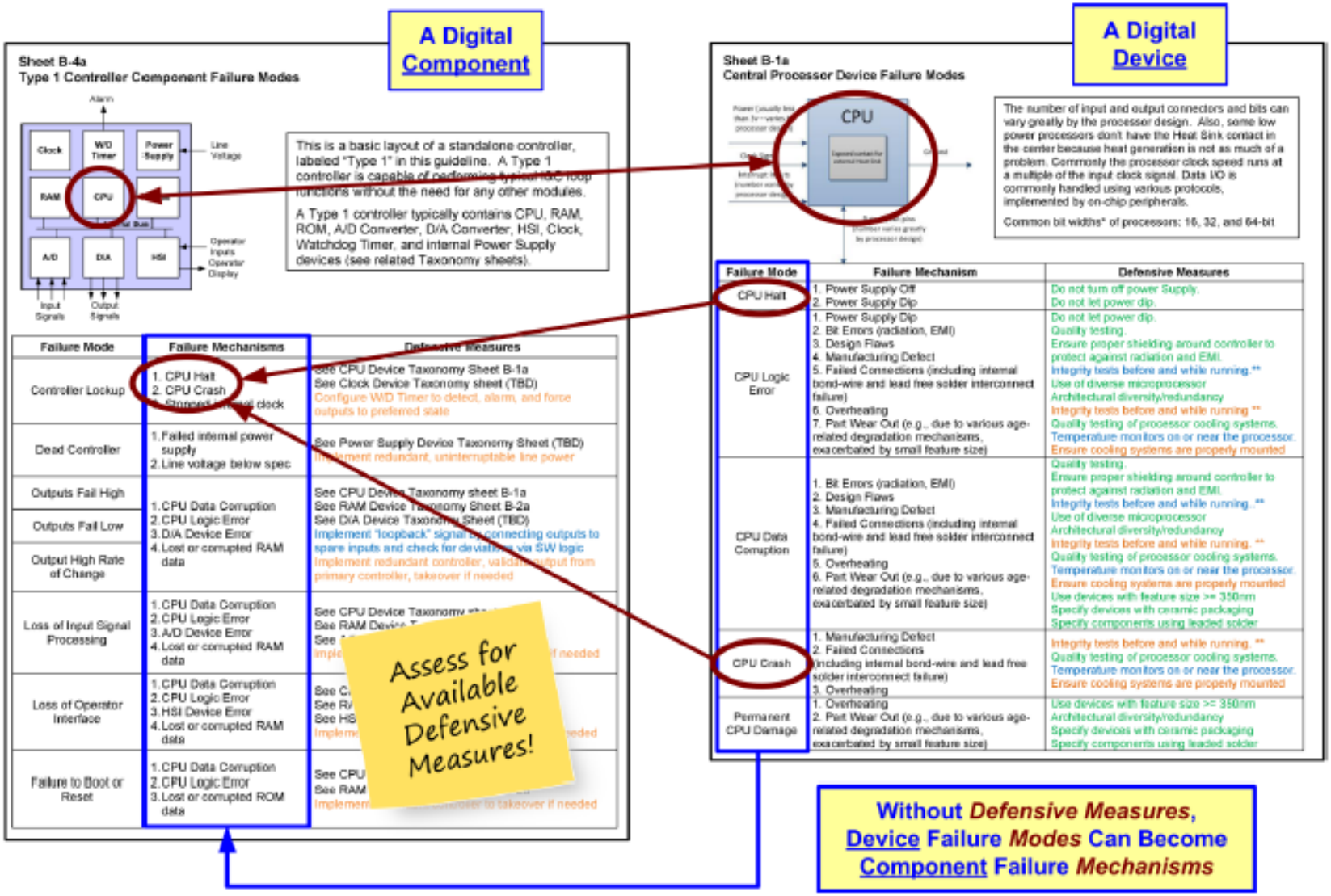
A Type 1 controller typically contains CPU, RAM, ROM, A/D Converter, D/A Converter, HSI, Clock, Watchdog Timer, and internal Power Supply devices (see related Taxonomy sheets).

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

EPRI ELECTRIC POWER RESEARCH INSTITUTE

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



EPRI 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)

Together…Shaping the Future of Electricity

EPRI | 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

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.

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.

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

Modeling Basis Reflects Lessons Learned

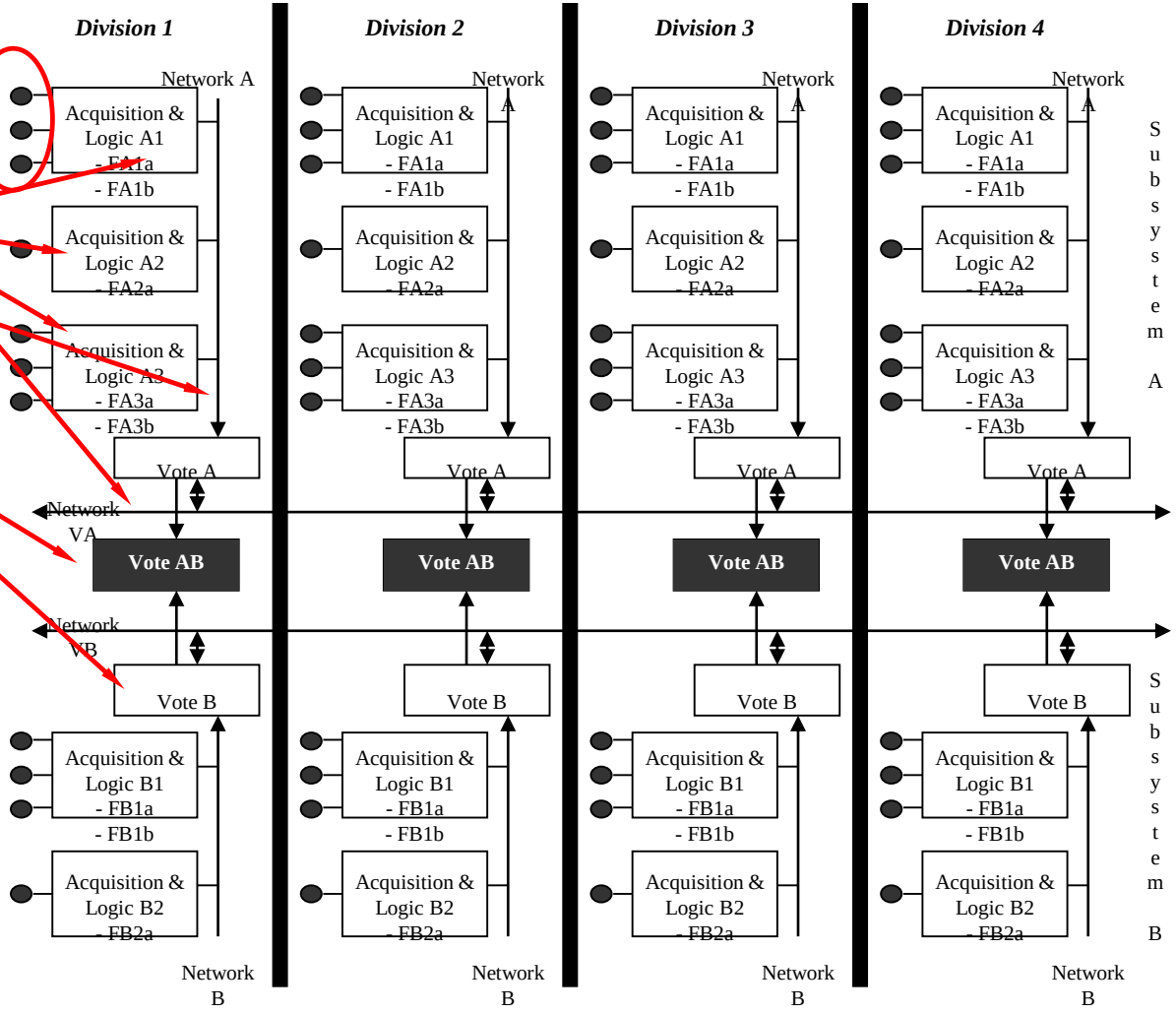
What are we trying to model?

Sensors

Signal processing

Communication

Voting



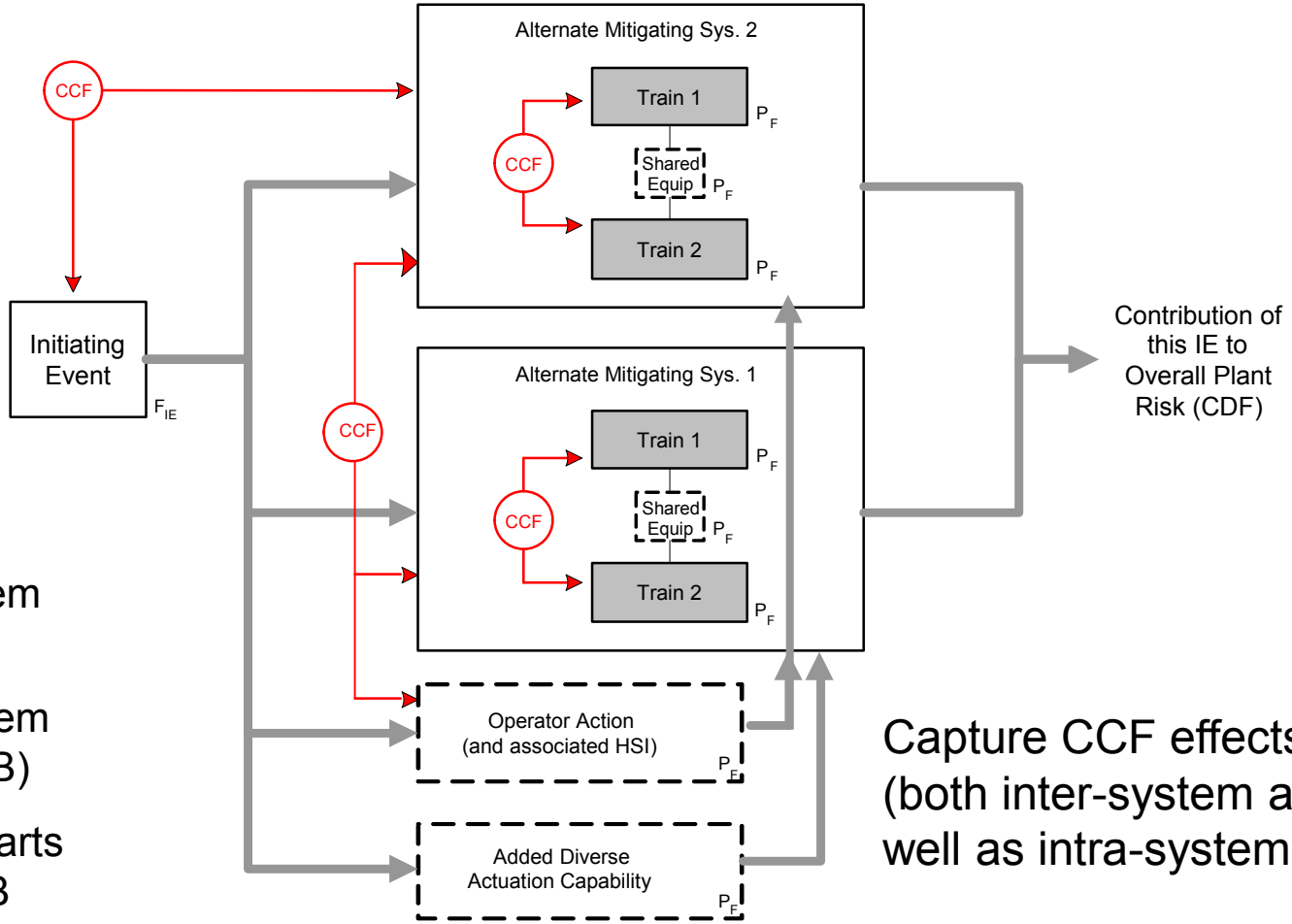
Functionally similar to analog I&C.

Modeling components having

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

EPRI ELECTRIC POWER RESEARCH INSTITUTE

Modeling Basis Reflects Lessons Learned
How are we trying to model it?



Example

Initiating event-
loss of feedwater

1st mitigating system
AFW

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

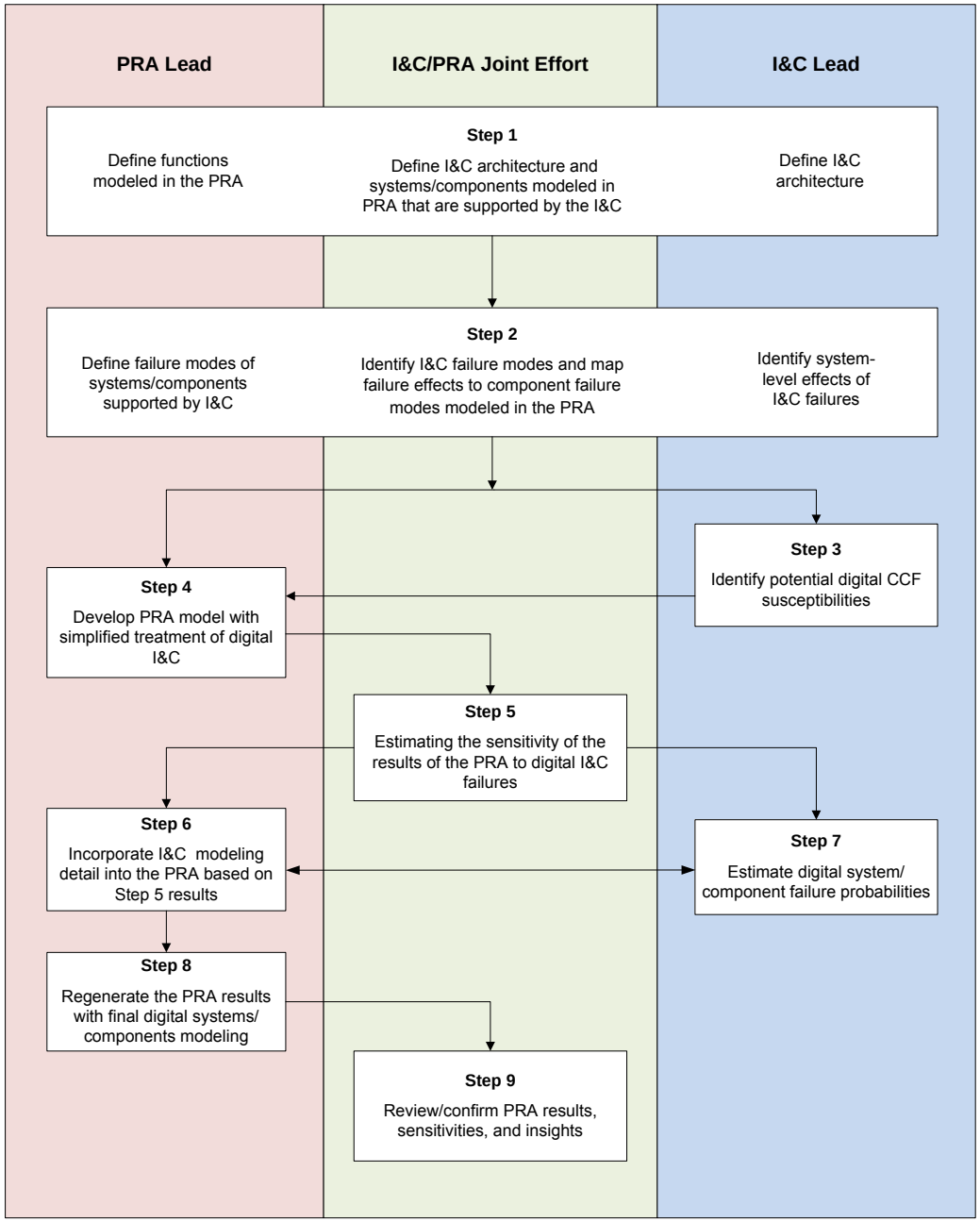
Operator action starts
AFW, initiates F&B

Diverse actuation
AMSAC

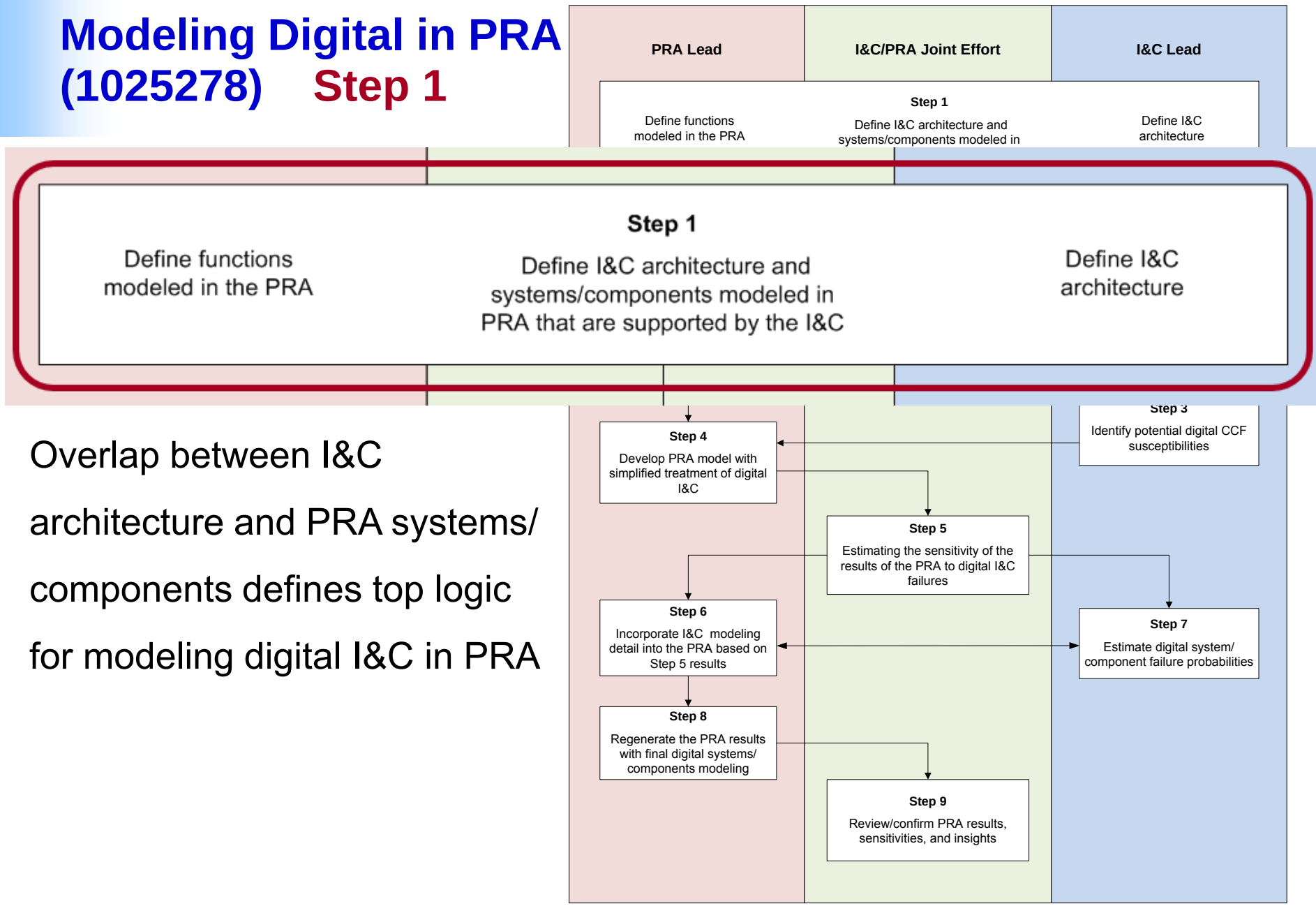
Capture CCF effects (both inter-system as well as intra-system)

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



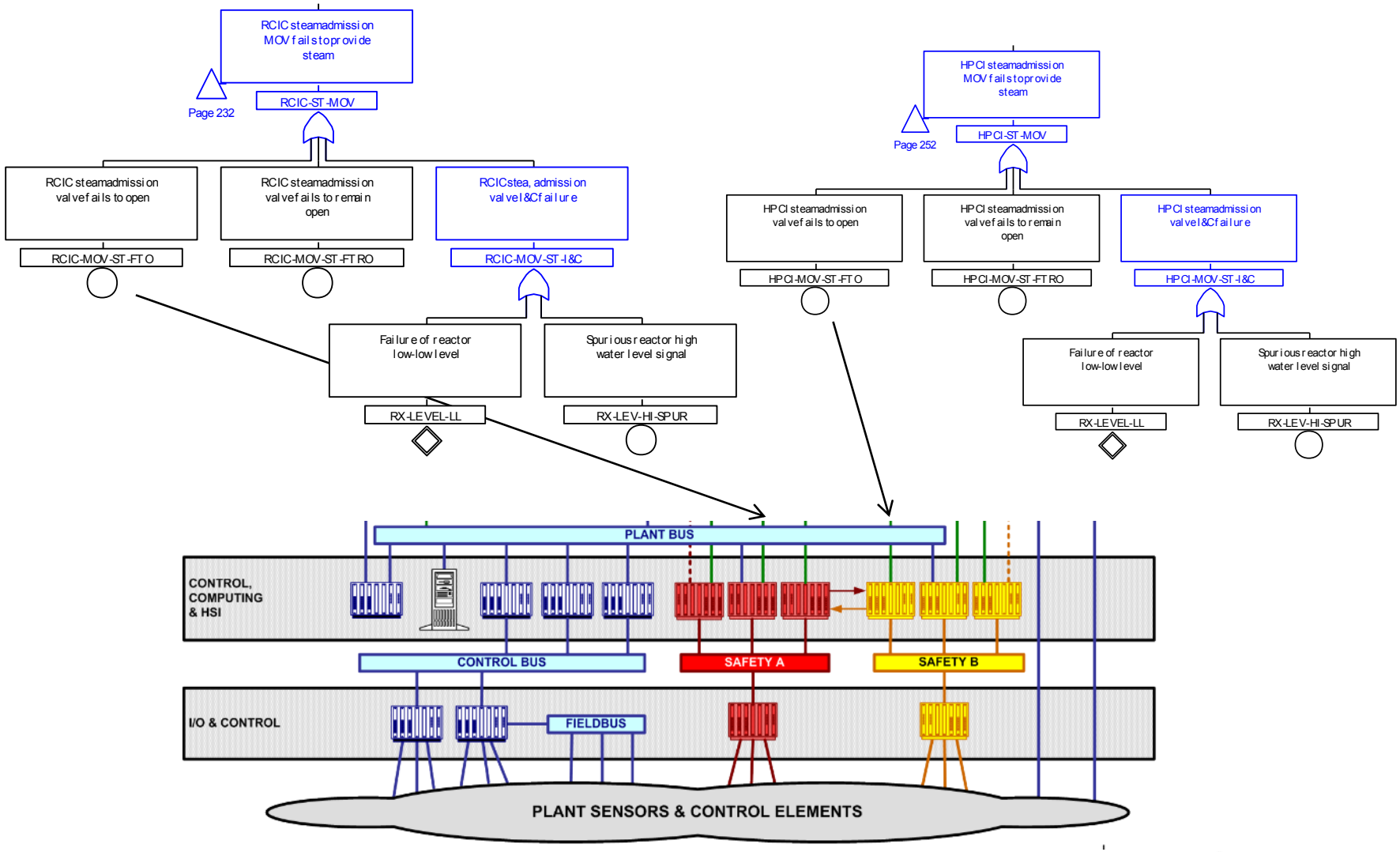
Modeling Digital in PRA (1025278) Step 1



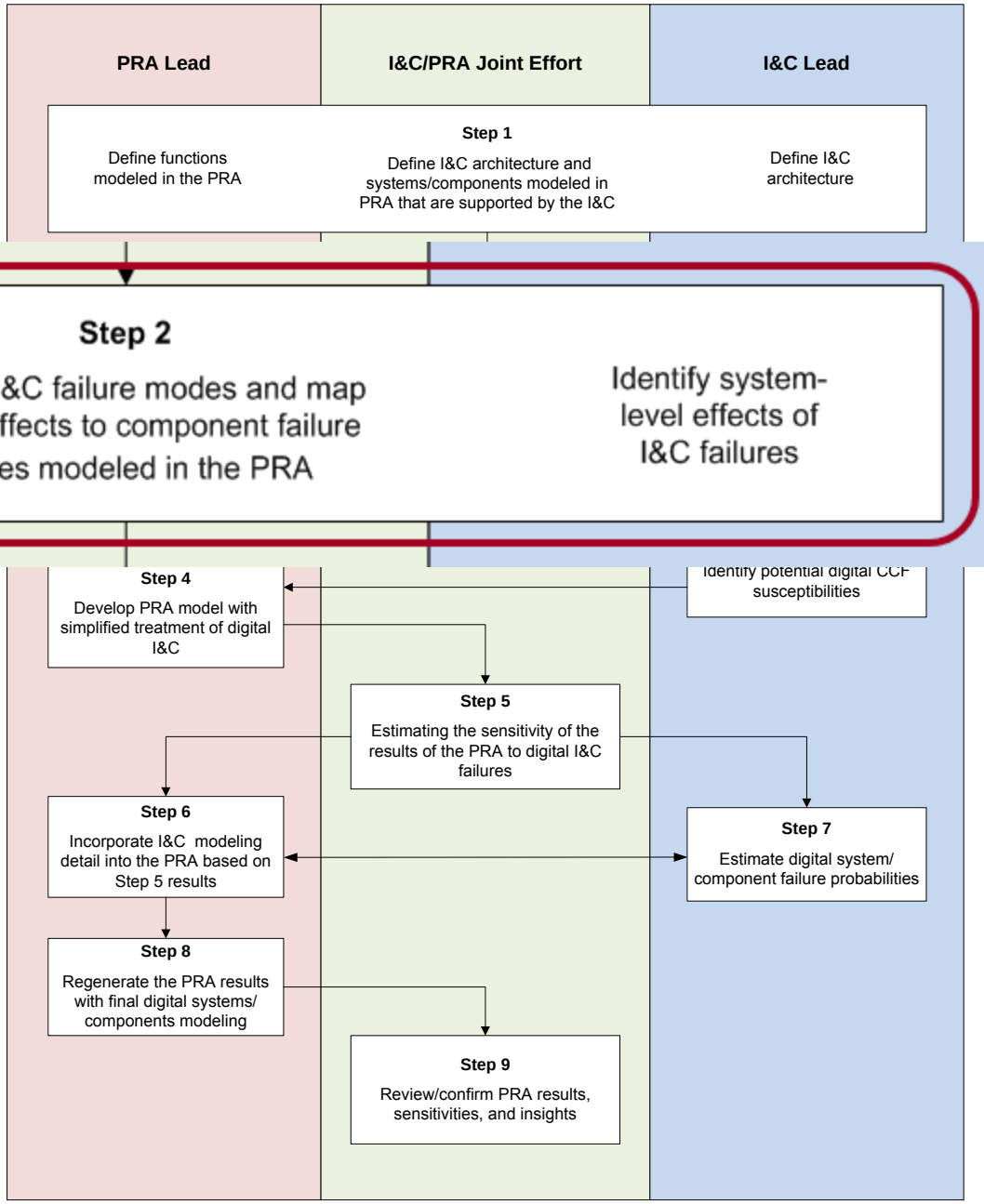
Overlap between I&C architecture and PRA systems/ components defines top logic for modeling digital I&C in PRA

Modeling Digital I&C in PRA

Step 1 – Interface between I&C and PRA components



Modeling Digital in PRA (1025278) Step 2



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

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

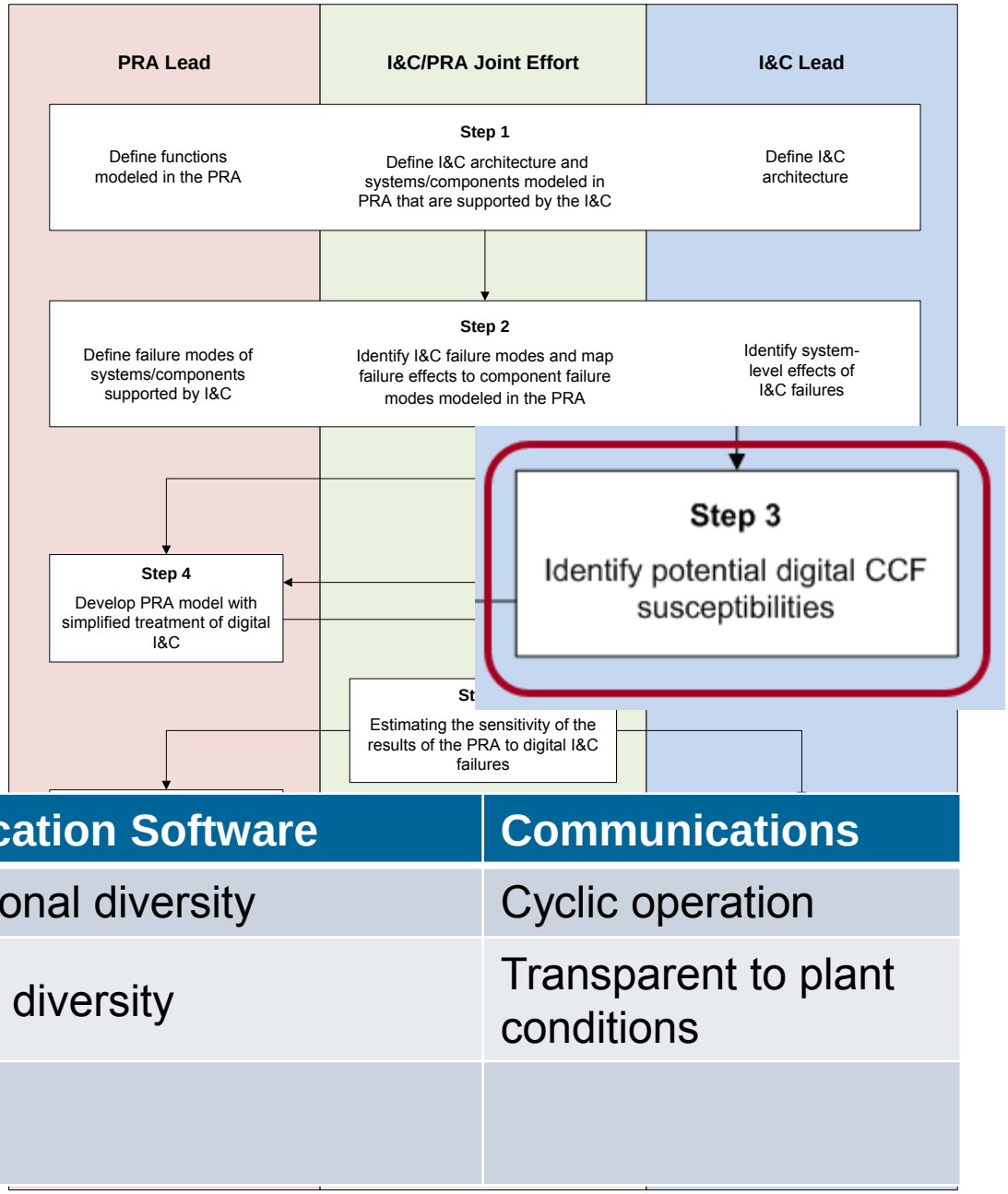
I&C System Failure Mechanism	I&C System Failure Mode	I&C System Failure Effect (on plant systems)
Output of 1 instead of 0	Protective action when none is warranted	Spurious operation of (pump, valve,...)
Output of 0 instead of 1	No protective action when needed	Failure of component to operate (pump FTS,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

controls.

Modeling Digital in PRA (1025278) Step 3

Preventive measures for CCF

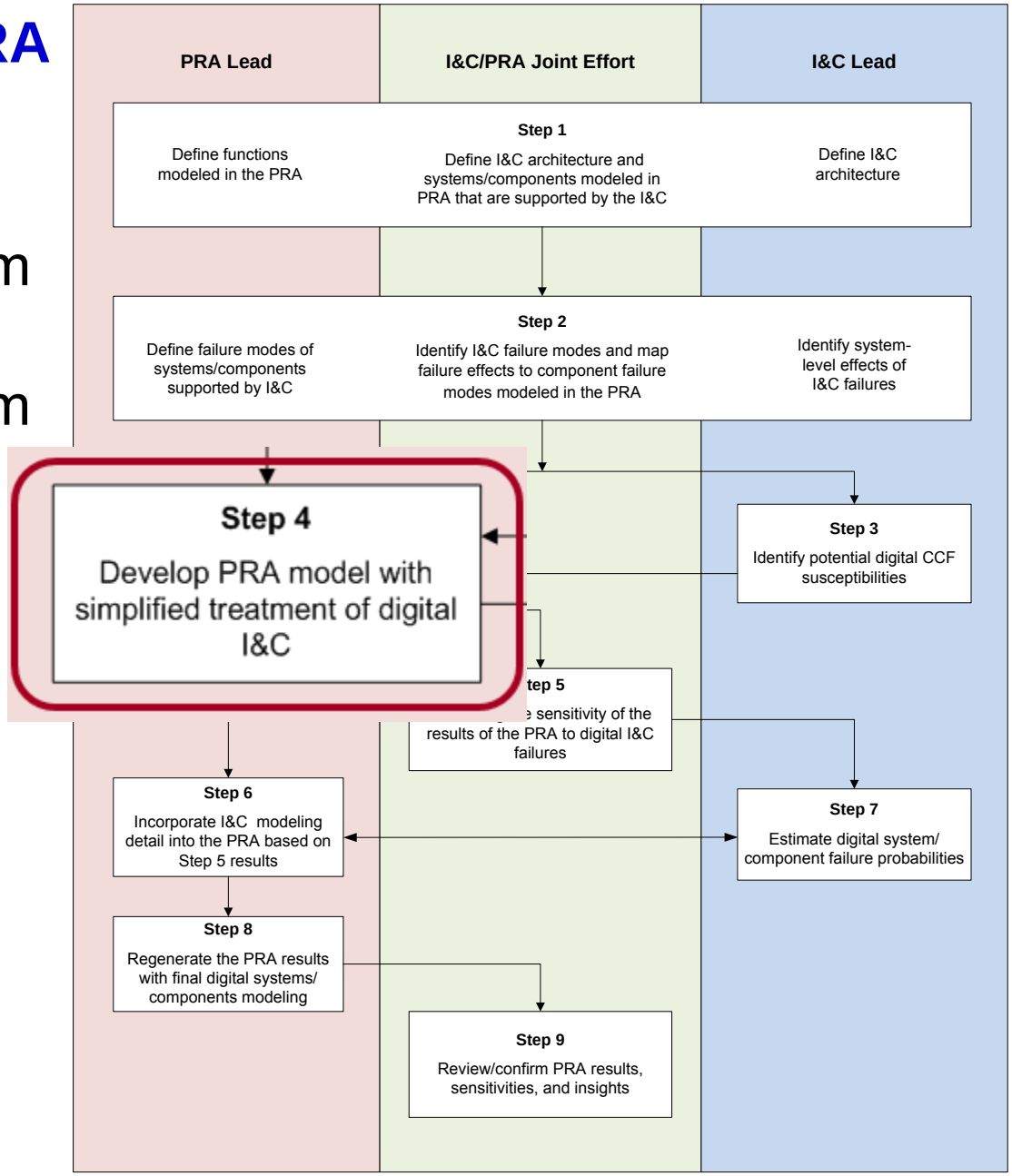
- Hardware – Different:
  - Component type / failure mode
  - Manufacturer
  - System (different operating conditions, environment)
  - Maintenance practices
- Software defensive measures:



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

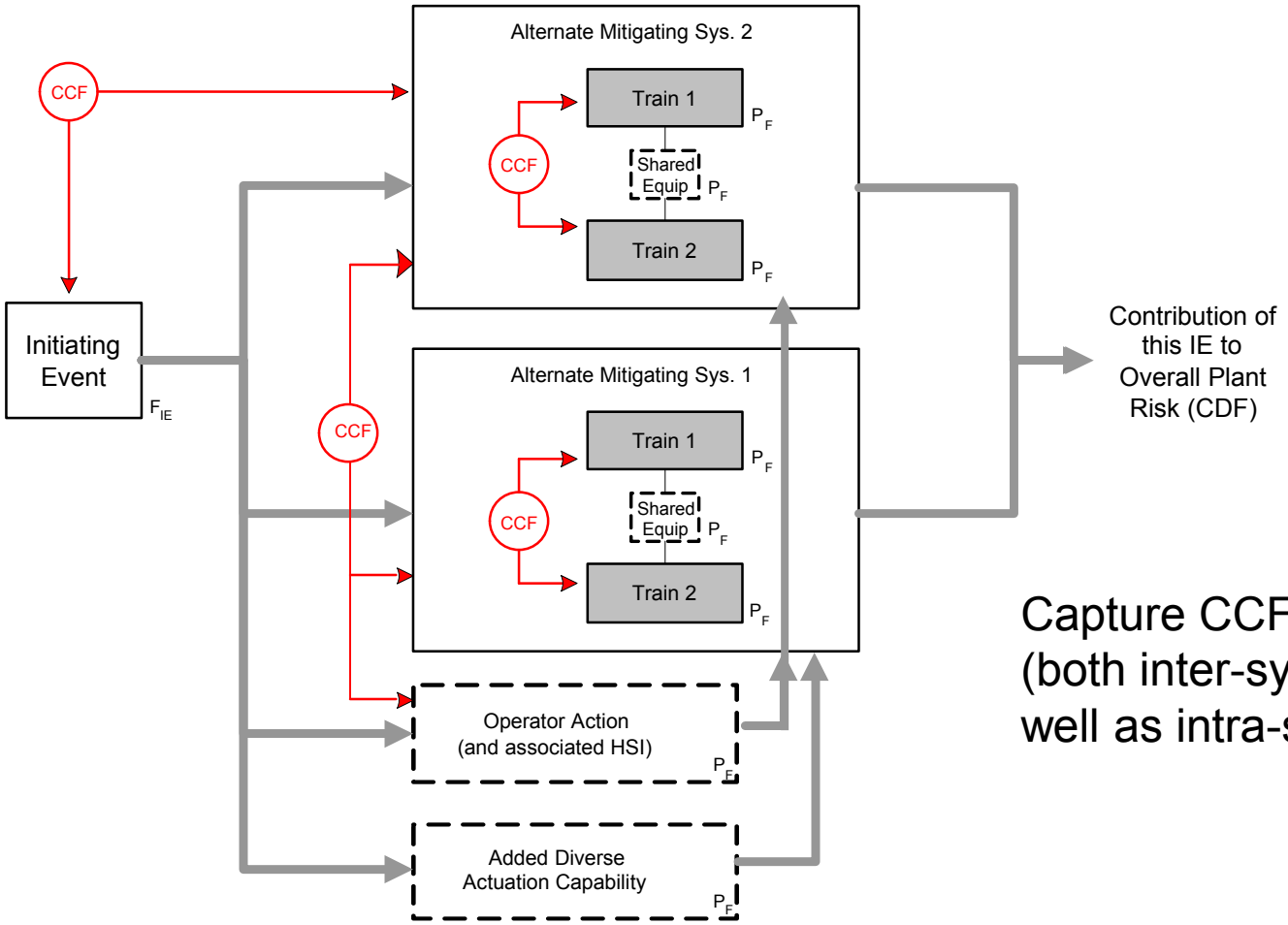
Modeling Digital in PRA (1025278) Step 4

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



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)

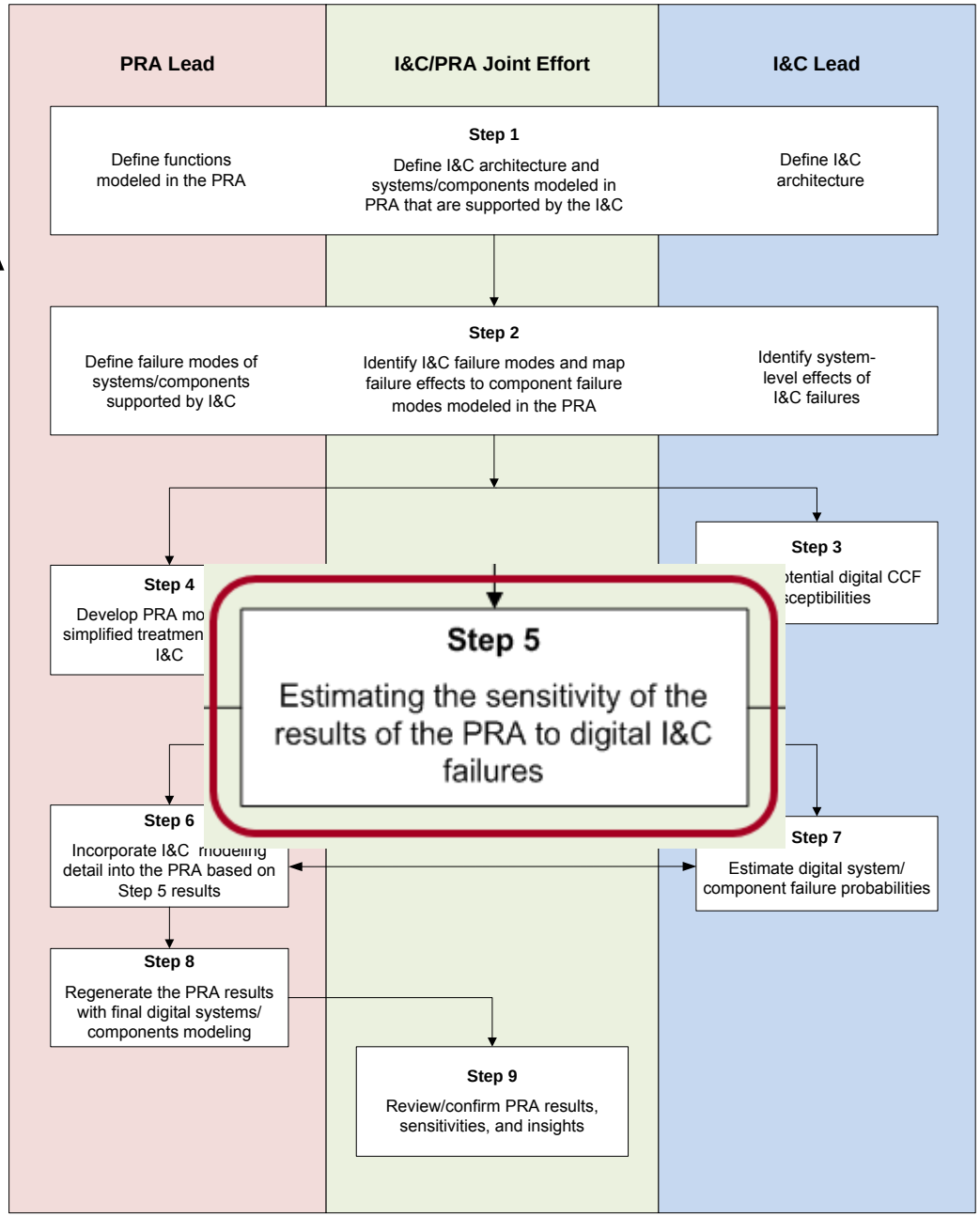
Modeling Digital I&C in PRA
Step 4 – Parameter Estimates

- 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

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



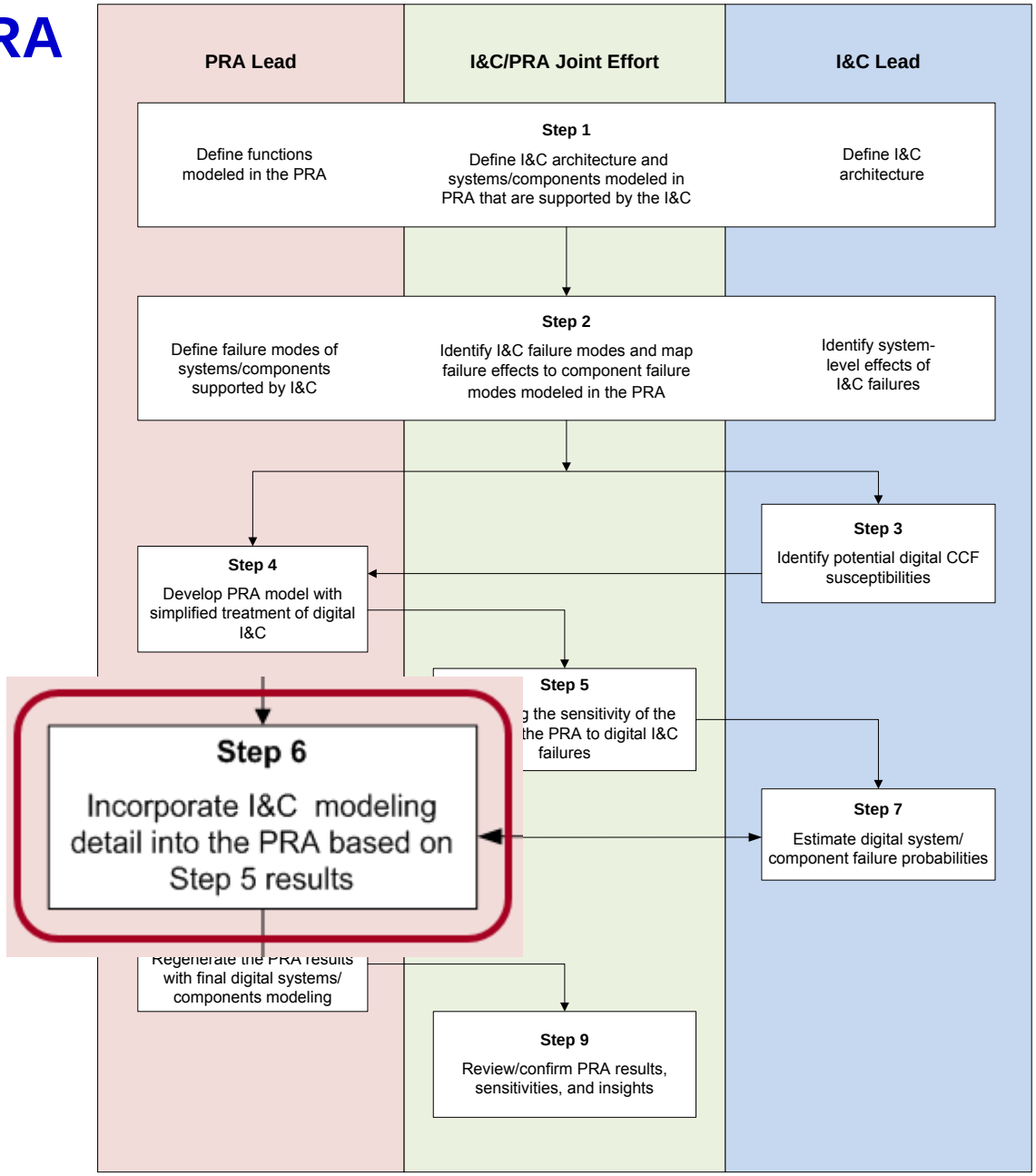
Modeling Digital I&C in PRA
Step 5 – Sensitivity Study

- 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

    We want to keep it that way
  - In upgrading I&C in the current generation of plants, we have the opportunity to incorporate risk insights into the design before the plant is modified – just like the new plants

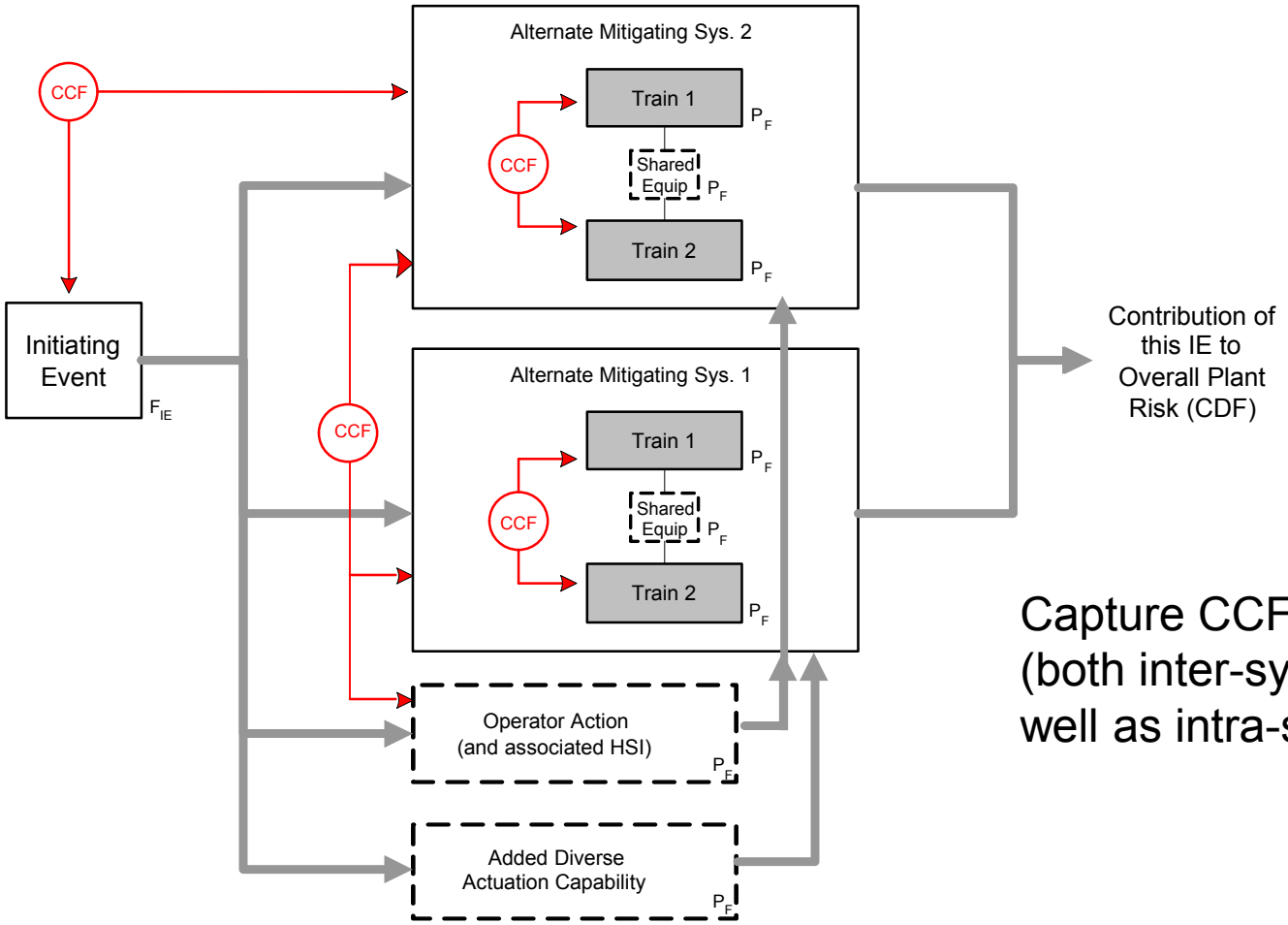
Modeling Digital in PRA (1025278) Step 6

Different levels of detail for low and high sensitivity systems



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)

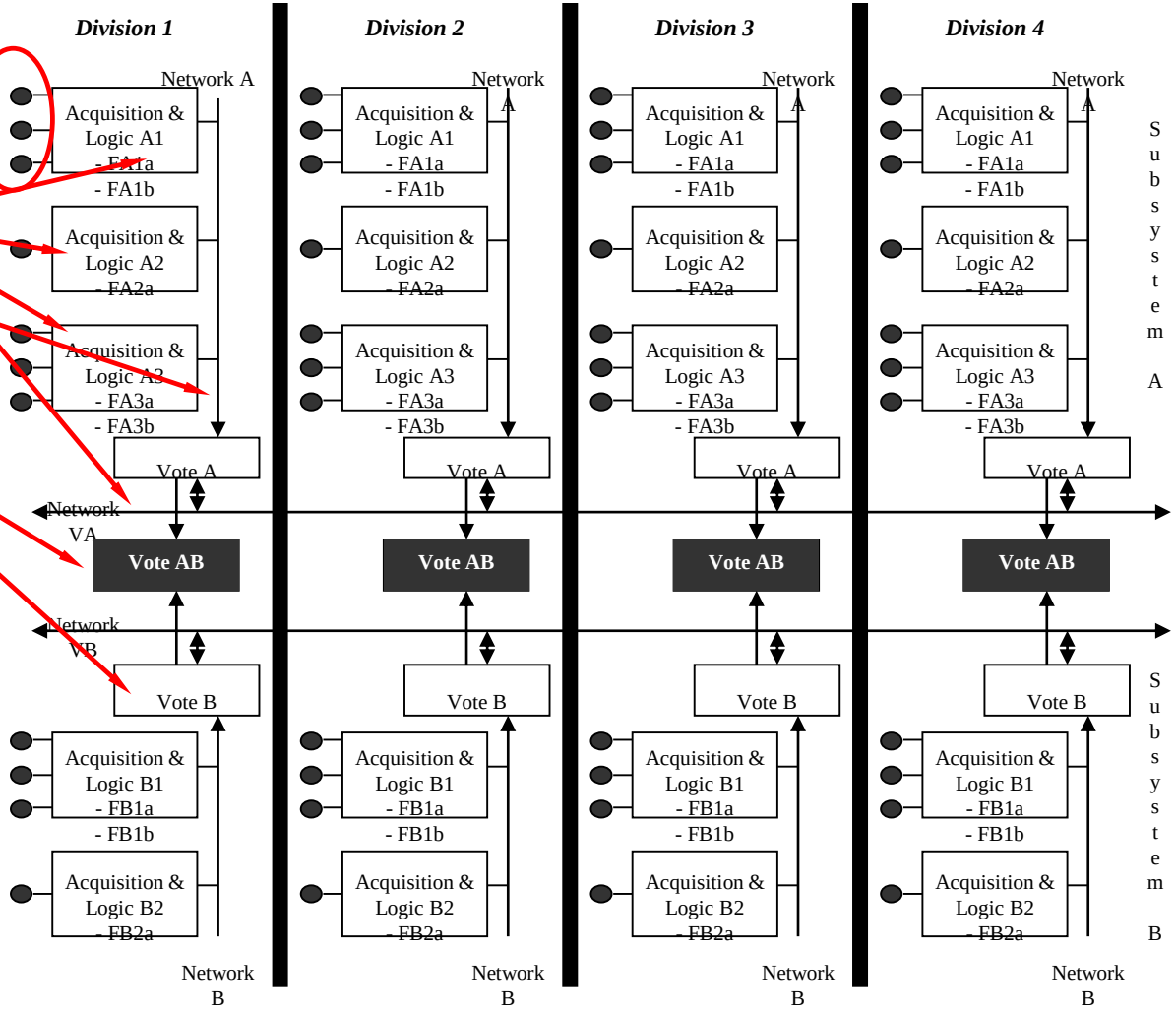
Modeling Digital I&C in PRA

Step 6 – Level of Modeling Detail for High Sensitivity Systems

Hardware
- Sensors
- Signal processing
- Communication
- Voting

Components, their failure modes and effects

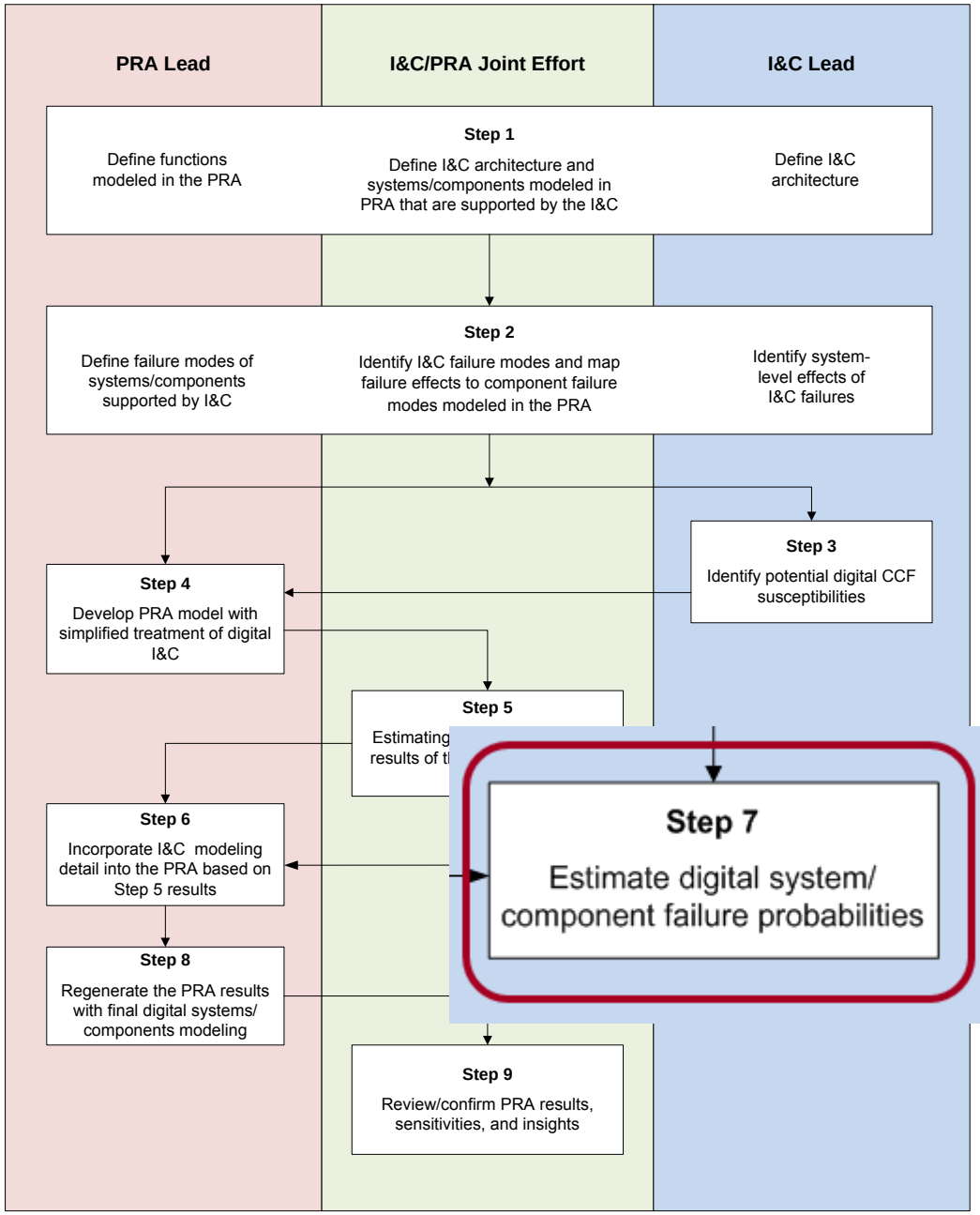
Note: Unavailabilty and maintenance errors modeled separately



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Modeling Digital in PRA (1025278) Step 7

Different parameter estimates for low and high sensitivity systems



EPRI 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

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

Modeling Digital I&C in PRA

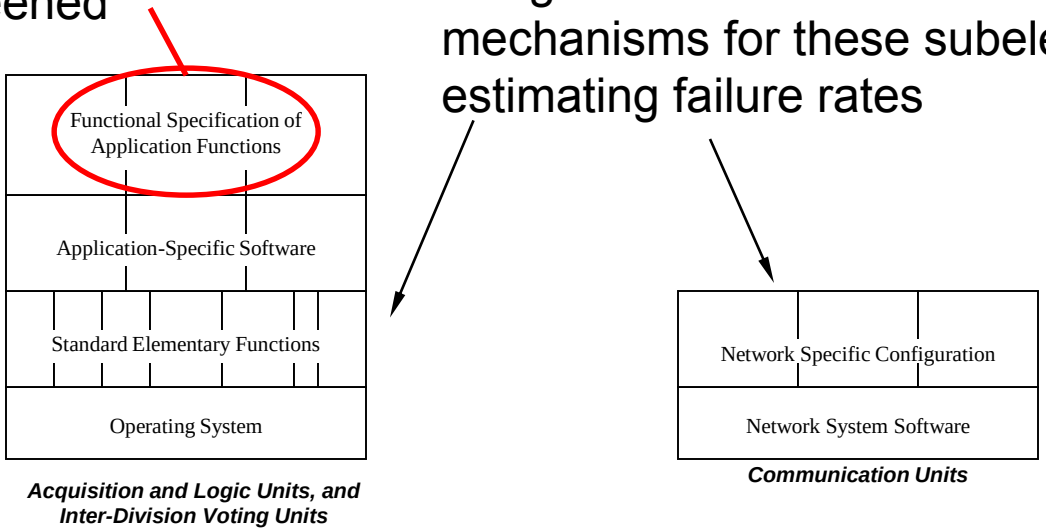
Parameter Estimates for High Sensitivity Systems (Software)

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

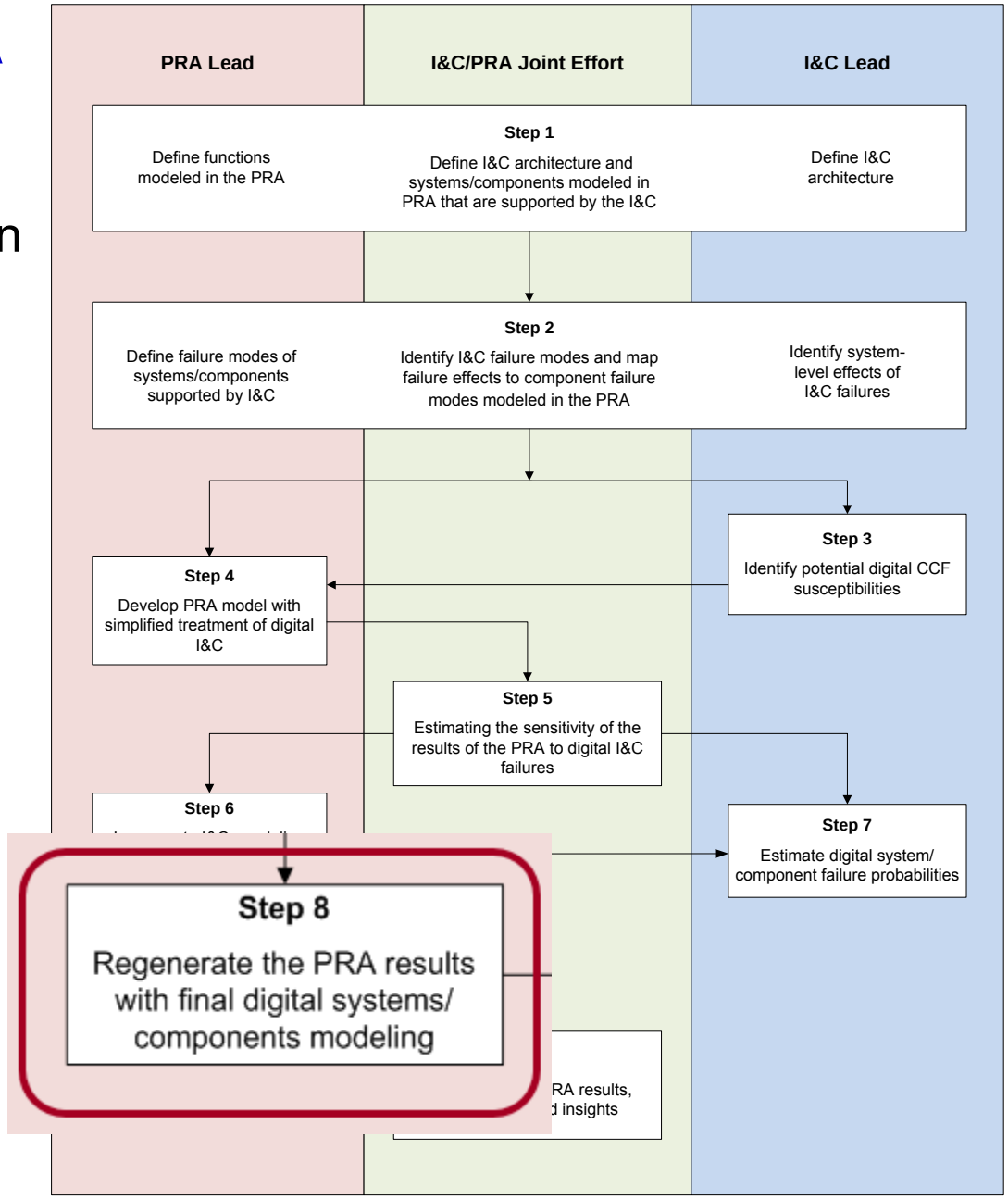
Modeling Digital I&C in PRA
Quantification of Residual Failure Modes

- 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

Modeling Digital in PRA (1025278) Step 8

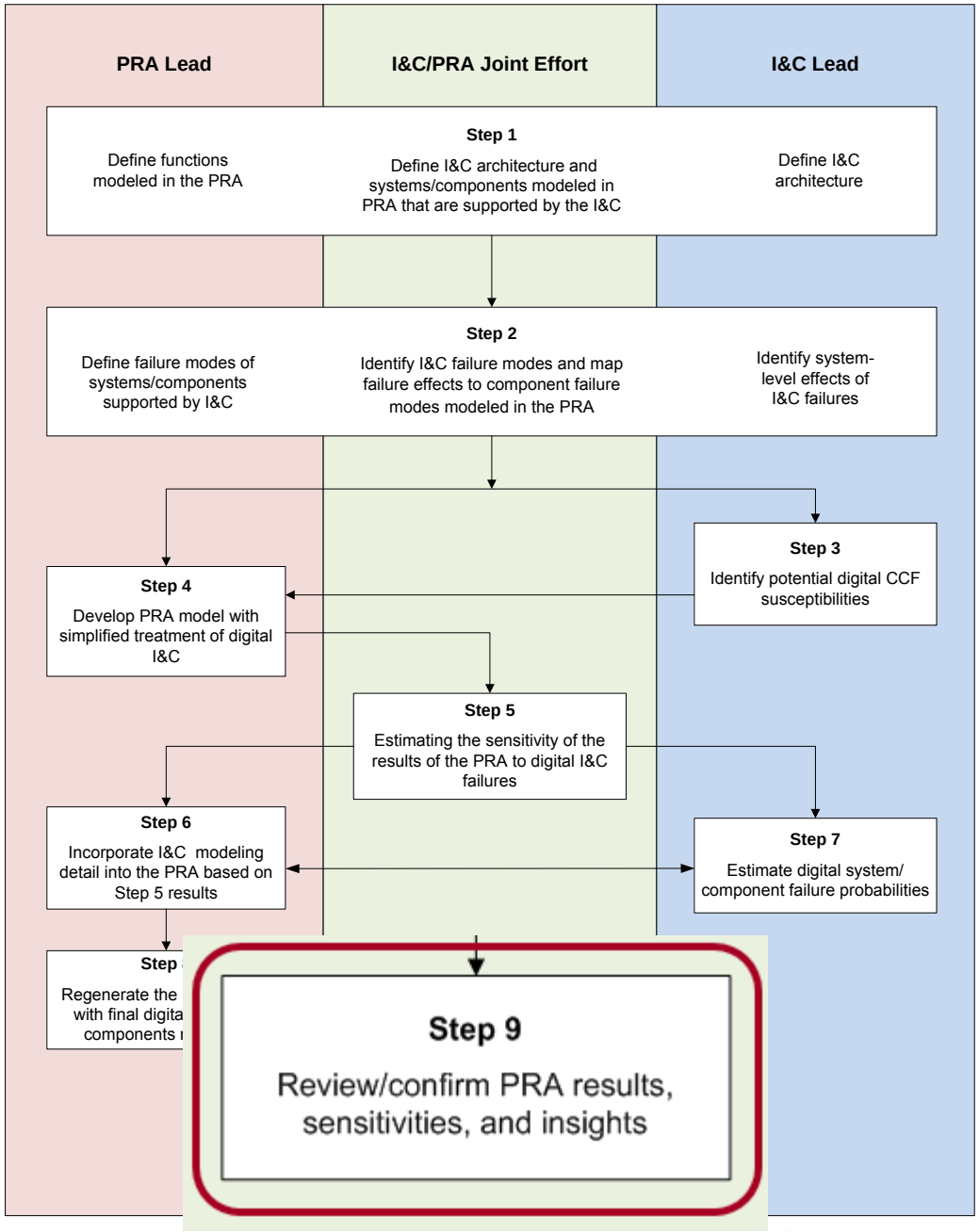
Accident sequence quantification

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



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



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

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

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.

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.

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.

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity

EPRI | 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

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

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

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

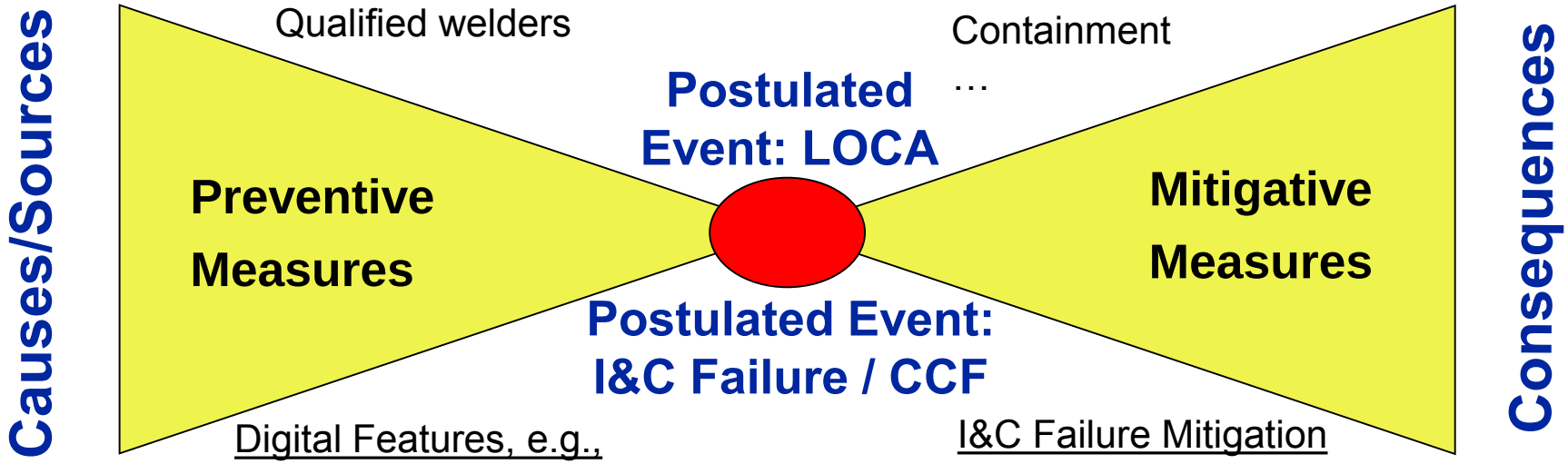
EPRI Project on Digital Failure Susceptibility Key Terms

- *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

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

Approach / Concepts
Prevention and Mitigation



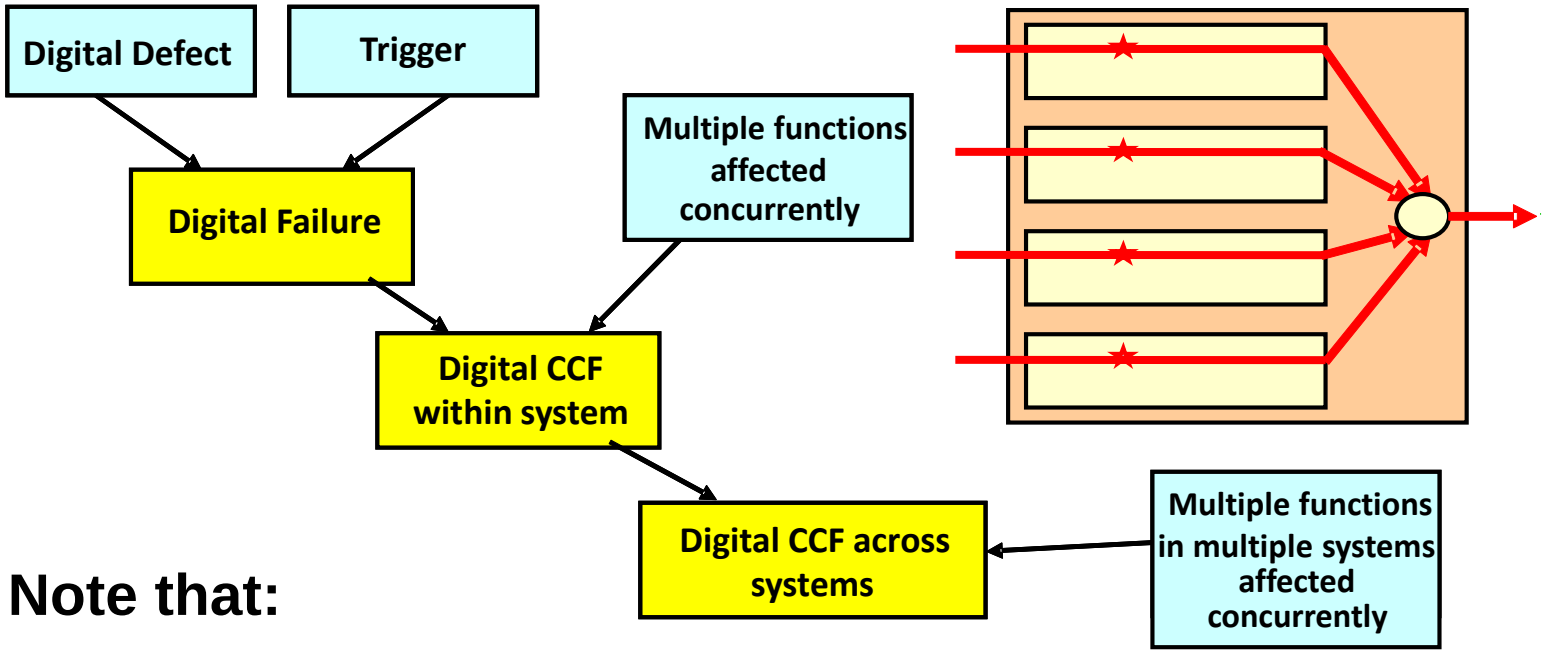
Piping Attributes, e.g.,
- Qualified materials
- ASME code
- Inspections
- Qualified welders

Piping Failure Mitigation
- Isolation valves
- Emergency core cooling
- Low pressure safety injection
- Containment
- …

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
- …

Approach / Concepts
Defects and Triggers



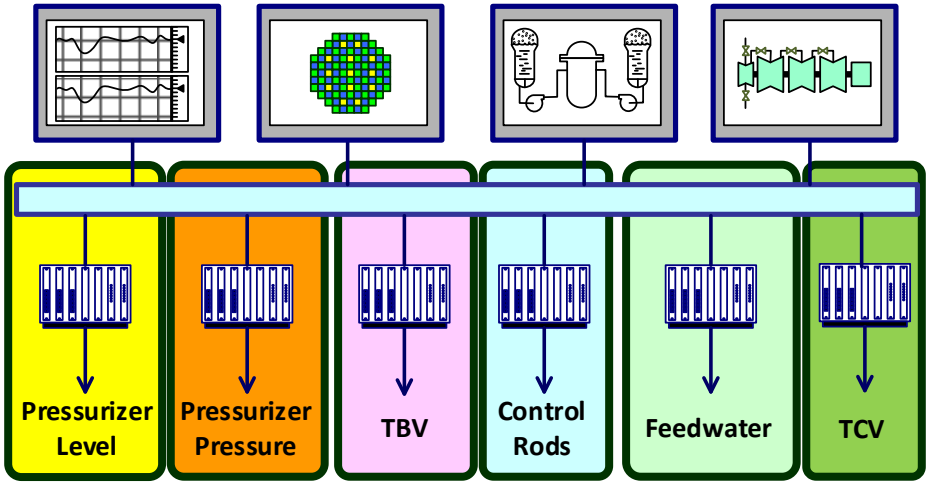
Note that:

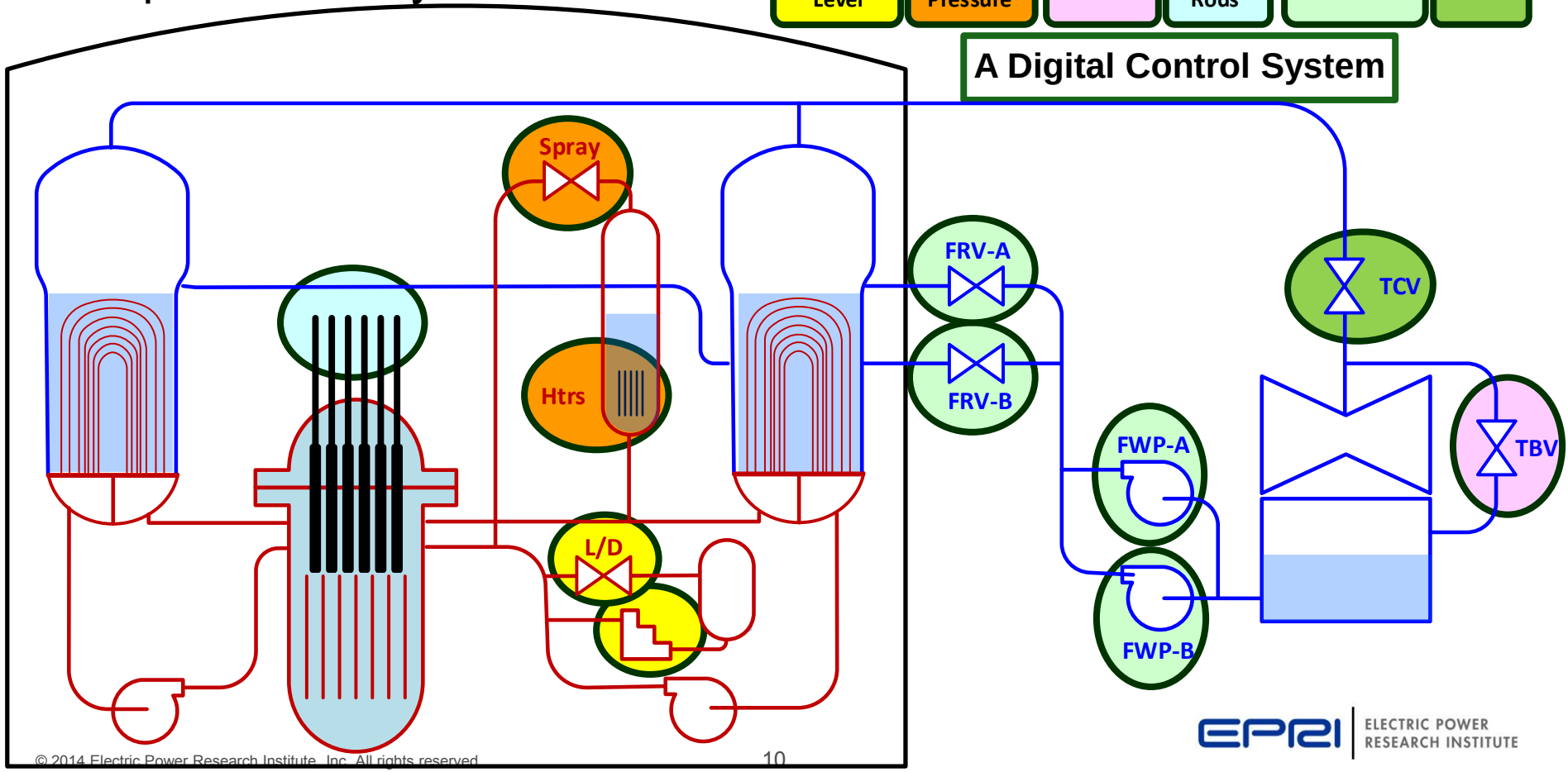
- Not all digital defects/failures can become CCFs
- Not all digital failures are safety-significant
- Defect-free software is neither expected nor needed
- Eliminating defects and triggers reduces likelihood of failure / CCF

Failure/CCF susceptibility evaluation looks for design measures and practices that reduce the likelihood of defects and triggers

Approach / Concepts
Common-Cause Failure Contexts

Failures and misbehaviors could affect single or multiple components or systems

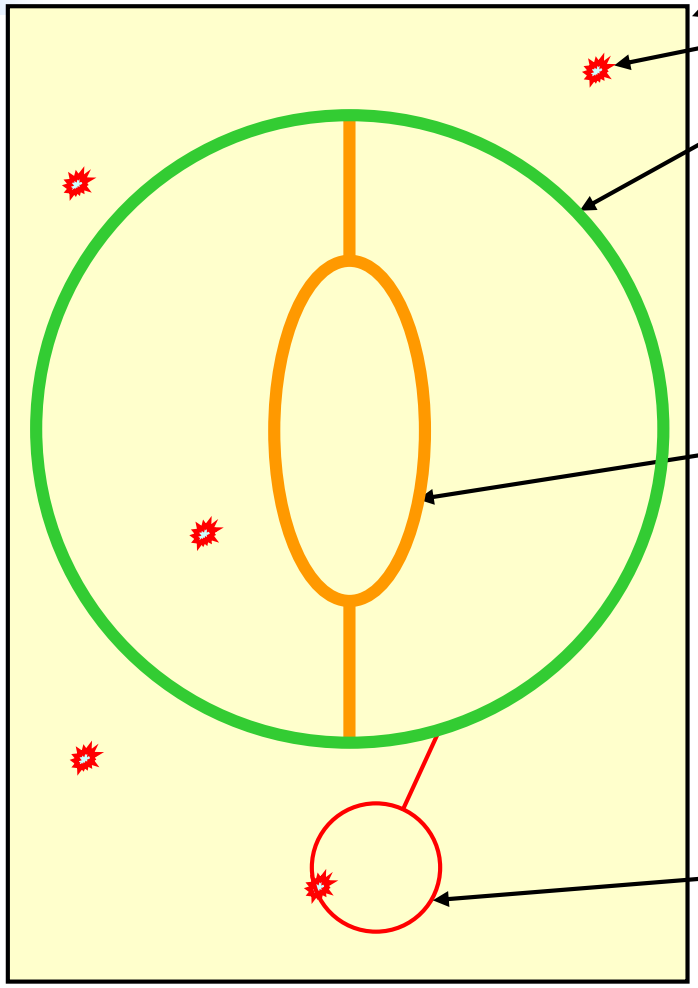




EPRI ELECTRIC POWER RESEARCH INSTITUTE

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

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

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

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

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

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

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

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

EPRI | 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

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

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

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

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)

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

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)

Palo Verde Exciter Hazard Analysis

9. Hazard Analysis Acceptance, Documentation and Maintenance
   - To be determined

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

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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]

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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].

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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