

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, September 19, 2013

Work Order No.: NRC-263

Pages 1-334

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION
+ + + + +
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
(ACRS)

+ + + + +
DIGITAL INSTRUMENTATION AND
CONTROL SYSTEMS SUBCOMMITTEE

+ + + + +

THURSDAY

SEPTEMBER 19, 2013

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear
Regulatory Commission, Two White Flint North, Room T2B3,
11545 Rockville Pike, at 8:30 a.m., Charles H. Brown,
Jr., Subcommittee Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Subcommittee Chairman

DENNIS C. BLEY, Member

JOHN W. STETKAR, Member

MYRON HECHT, Consultant

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 NRC STAFF PRESENT:

2 CHRISTINA ANTONESCU, Designated Federal

3 Official

4 TANNY SANTOS, Acting Designated Federal

5 Official

6 LUIS BETANCOURT, RES/DE

7 SUSHIL BIRLA, RES/DE

8 THOMAS BURTON, RES/DE

9 DOUG ESKINS, RES/DE

10 MAURICIO GUTIERREZ, RES/DE

11 DEREK HALVERSON, RES/DE

12 MING LI, RES/DRA/PRAB

13 TIM MOSSMAN, NRO/DE/ICEZ

14 DAN SANTOS, NRO/DE

15 RUSS SYDNOR, RES/DE

16 BRIAN THOMAS, RES/DE

17

18 ALSO PRESENT:

19 DAVE BLANCHARD, EPRI

20 BRUCE GEDDES, EPRI

21 JOHN THOMAS, EPRI

22 RAY TOROK, EPRI

23

24 LIST OF PEOPLE LISTENING IN ON THE BRIDGE LINE (*):

25

26 SKIP BUTLER, GENERAL ELECTRIC HITACHI (GEH) NUCLEAR

27 JACK ADKINS, GENERAL ELECTRIC HITACHI (GEH) NUCLEAR

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 BISHARA KAKUNDA, GENERAL ELECTRIC HITACHI (GEH)
2 NUCLEAR
3 IRA POPPEL, GENERAL ELECTRIC HITACHI (GEH) NUCLEAR
4 SARA RUDY, GENERAL ELECTRIC HITACHI (GEH) NUCLEAR
5 PETER YANDOW, GENERAL ELECTRIC HITACHI (GEH) NUCLEAR
6 PATRICIA CAMPBELL, GENERAL ELECTRIC HITACHI (GEH)
7 NUCLEAR
8 TY D. ROGERS, GE HITACHI NUCLEAR ENERGY
9
10 MARTY RYAN, WESTINGHOUSE ELECTRIC COMPANY (WEC),
11 WINDSOR, CT
12 RICK WEBER, WESTINGHOUSE ELECTRIC COMPANY (WEC)
13 DAVE JAROSH, WESTINGHOUSE ELECTRIC COMPANY (WEC),
14 CRANBERRY, PA
15 STEVE SEAMAN, WESTINGHOUSE ELECTRIC COMPANY
16 (WEC), CRANBERRY, PA
17 DAVID TYLER, WESTINGHOUSE ELECTRIC COMPANY (WEC)
18 TOM MCLAUGHLIN, WESTINGHOUSE ELECTRIC COMPANY (WEC)
19
20 CHARLES ZENG, CANADIAN NUCLEAR SAFETY COMMISSION
21 (CNSC)
22 GILBERT CHUN, CANADIAN NUCLEAR SAFETY COMMISSION
23 (CNSC)
24 MARIUS CHIRILA, CANADIAN NUCLEAR SAFETY COMMISSION
25 (CNSC)
26 GUNA RENGANATHAN, CANADIAN NUCLEAR SAFETY COMMISSION
27 (CNSC)
28
29 JODI RAPPÉ, NUSCALE POWER, LLC
30 STEVEN MIRSKY, NUSCALE POWER, LLC
31 DANIEL J. CRONIN, NUSCALE POWER, LLC
32
33 YUICHI TANAKA, MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC
34 HAROLD PITTS, MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC
35 SHINJI KIUCHI, MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC
36 RICHARD SAMPLES, MITSUBISHI NUCLEAR ENERGY SYSTEMS,
37 INC
38 YUICHI TANAKA, MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC
39 KEN SCAROLA (CONTRACTOR OF MNES)
40
41 BRIAN ARNHOLT, GENERATION MPOWER
42 BOB ENZINNA, AREVA INC.
43
44 MARK JEKEL, NORTHROP GRUMMAN
45
46 JERRY MAUCK, INVENSYS
47 GLENN LANG, INVENSYS
48 *Present via telephone

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

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

I Opening remarks

Chairman Brown 4

Russ Sydnor 6

II EPRI Overview

Ray Torok 8

Update on Operating Experience (OE) Review 175

Overview of Digital Research Activities

by Mr. Sydnor 194

Research Information Letter RIL-1002

Identification of Failure Modes in Digital

by Mauricio Gutierrez 209

and Dr. Sushil Birla 215

RIL-1100. Technical Basis to Review

Hazard Analysis of Digital Safety Systems

By Luis Betancourt, RES/DE 256

By Sushil Birla, RES/DE 267

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

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

(8:34 a.m.)

CHAIRMAN BROWN: Everybody present and accounted for? I'm overly amazed we actually have people to come in to the Digital I&C subcommittee. It's a real joy so thank you and welcome everyone, hope you enjoy this day of fun and games.

This a meeting of the digital instrumentation and control system subcommittee. I'm Charles Brown, Chairman of the subcommittee.

ACRS members in attendance are John Stetkar, Dennis Bley, our consultant Myron Hecht and assistant to Christina Antonescu, while she is buried in beltway traffic is, what's your name again, Tanny Santos, filling in for Christina is the designated Federal Official for this meeting.

The purpose of this meeting is to discuss some specific accomplishments of the 2010, 2014 digital research plan, mutual of interest to the ACRS. In particular the staff will give an update of the digital system research activities on failure modes, hazard analysis and digital operating experience.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Also the Electric Power Research Institute
2 will discuss their research results on failure modes and
3 hazard analysis, methods for digital I&C systems.

4 The subcommittee will gather information,
5 analyze relevant issues, overweight proposed positions
6 and actions as appropriate for deliberation by the full
7 committee. The rules for participation in today's
8 meeting have been announced as a part of the notice for
9 this meeting previous published in the Federal Register
10 on August 19th, 2013.

11 We have received no written comments or
12 requests for time to make oral statements from members
13 of the public regarding today's meeting. Also we have
14 some folks on the bridge line listening to the
15 discussions.

16 The list of the names is long, like 20 or
17 25 so I am going to limit my comments to the organizations
18 they represent. They are from GE, General
19 Electric-Hitachi Nuclear, Westinghouse Electric
20 Corporation, Canadian Nuclear Safety Commission,
21 NuScale Power & LLC, Mitsubishi Nuclear Energy Systems,
22 Generation mPower, AREVA, Northrop Grumman and Invensys.
23 I'm not sure I said this right, Invensys.

24 MEMBER STETKAR: Invensys.

25 CHAIRMAN BROWN: Did I say, say that again?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MALE PARTICIPANT: Invensys.

2 CHAIRMAN BROWN: Thank you, I needed help.

3 Also we have with us today some representatives from the
4 IEEE Nuclear Power Engineering Society Working Group,
5 IEEE 7.4.3.2, so we welcome them to the meeting.

6 To preclude interruptions of the meeting
7 the phone line will be placed on a listen in mode during
8 the discussion and presentations and committee
9 discussions. It will be opened at the end of the meeting
10 to see if anyone listening would like to make any comments
11 and they can identify themselves personally at that time.

12 Transcript of the meeting is being kept and
13 will be made available as stated in the Federal Register
14 Notice. Therefore we request that participants in this
15 meeting use the microphones located throughout the media
16 room when addressing the subcommittee.

17 You should first identify yourselves when
18 you step up, speak with sufficient clarity and volume so
19 that you may be readily heard. We will now proceed with
20 the meeting and as a brief introduction I will call on
21 Russ Sydnor to give a brief statement about why we are
22 here.

23 MR. SYDNOR: Thank you, Charlie. The
24 Office of Research, well first of all Russ Sydnor Branch
25 Chief of Digital I&C for the Office of Research.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 We have a memorandum of understanding for
2 collaborative research with EPRI in many areas. Many
3 different disciplines, materials, area, electrical,
4 like cabling, cabling research. Many different areas.

5 About four or five years ago the Invensys
6 and I indicated and MOU for sharing and collective
7 research on digital implementation and control. And my
8 bias is that that's been very successful.

9 We've, in interfaces with our counterparts
10 will be speaking through the day. I think they've done
11 some, not only interesting work, I think it's important
12 work in moving forward in the area of understanding how
13 digital systems behave and how we can analyze them better
14 to ensure their safety.

15 And so that's really all I wanted to say.
16 And I welcome my counterparts who we've been, like I say,
17 we've been meeting with several times a year sharing
18 under the MOU.

19 We're allowed to share data information.
20 We're a branch reach independent conclusions under the
21 MOU. And under the MOU it's strictly a research effort.

22 We have not allowed to and avoid talking
23 about any specific licensing issue. And so it's a pure
24 collaborative research effort and I welcome the EPRI team
25 here this morning.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: On thing I would, just a
2 brief lead in before you start, Ray, is that we do have
3 a lot of information to cover, so we need to, I would say
4 be crisp and when folks have questions if they would be
5 very point with their questions as opposed to have some
6 soliloquys as lead ins. So good luck.

7 That last phrase, if you wanted to you got
8 to say it anyway just to try to set the stage and then
9 we'll go with the forward. Anyway, Ray, I turn it over
10 to you for starting this whole thing off.

11 MR. TOROK: A very good way and thank you,
12 Charlie. Thanks Russ for the intro. My name is Ray
13 Torok, I'm a project manager at the Electric Power
14 Research Institute.

15 And first I just want to say thanks for
16 giving us the opportunity to come back and talk to you
17 about some of the work that we've been doing. Now
18 getting on with my soliloquy I want to say, hmm, let's
19 see something here. Oh, yes, okay.

20 So what we're going to do here --

21 CHAIRMAN BROWN: It's the technology,
22 that's why you're here.

23 MR. TOROK: There was a delay time, you
24 know. So anyway, we're going to revisit some key topics
25 related to Digital I&C that we last discussed with this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Committee in August of 2009. For those who remember
2 that.

3 But basically the same topics but we've
4 continued to work in all these areas. So they're updates
5 and new information and so on.

6 And of course the purpose, our selfish
7 purpose for being here, is to gather feedback and input
8 and reactions and what not that are going to help us by
9 informing ongoing work and future work and so on. So
10 that's what's in it for us.

11 And now all three of these issues we're
12 talking about are really tied to a larger issue, a larger
13 digital system issue. And that's this notion of
14 assuring that you have adequate dependability of
15 critical functions in the plant that use digital
16 instrumentation control to make them happen.

17 Now since 2009 we have looked at additional
18 operating experience beyond what we had then. At that
19 point we have looked at digital operating experience in
20 U.S. Plants and now we've gone further than that, we'll
21 show you, we'll share with you the results of that.

22 As far as risk insights go, we continue to
23 believe that one can model Digital I&C in probably risk
24 assessment and gain useful insights. And so we have
25 developed some more information on that. Again, we'll

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 show you what we've done there.

2 However, most of the time, the great bulk
3 of the time really is going to be devoted to the failure
4 analysis, hazard analysis work where we also spend a lot
5 of time with Russ's group and under the MOU and so on.

6 Now, what's driving it for us is that the
7 feedback we get from our members, are EPRI member,
8 utility engineers and so on, is basically is that the
9 traditional methods for failure analysis are not as
10 effective as we'd like them to be when it comes to Digital
11 I&C. And so they're asking us to help them find better
12 ways to understand and manager potential vulnerabilities
13 that can come from this equipment. So that's really what
14 it's about.

15 Now you guys have the report that we
16 recently published on this subject. I hope you had the
17 time to look at it.

18 I apologize for the size of it, I know it's
19 pretty voluminous but we had a lot to say. And we think
20 there's a lot of information in there that we wanted to
21 make available to our members for their use and so on.

22 But most of the material you're going to see
23 here today was lifted right out of that report. So
24 that's really what it's about.

25 Now I wanted to share with you some of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 insights that we think we gained in doing this. And
2 we'll get into the details of that later on in the
3 presentation today, but I just wanted to hit a couple of
4 the high points.

5 One of them, the first one, has to do with
6 what we call level of interest. And this is the notion
7 that when you are analyzing for failure modes or hazards,
8 it's important to understand the level of interest, the
9 appropriate level of interest for the analysis.

10 What I mean by that is that, you know, we
11 tend to focus sometimes on low level failure modes,
12 failure mechanisms, that sort of thing, which is all well
13 and find and it's very useful in assessing the
14 reliability of a component, for example, or a box for a
15 vendor.

16 So a vendor of digital equipment is very
17 interested in looking at the low level failure modes in
18 his box because he wants to make sure it's as reliable
19 as it can be.

20 However, from the plant prospective it's a
21 different problem. The plant engineer maybe doesn't
22 care so much about the low level failure, what's in the
23 box, he cares what it's going to do to his plant system
24 at a much higher level.

25 So, and so it's important to understand that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 there's that difference going on when you look at these
2 failure modes and mechanisms.

3 In addition to that, if all I know is the
4 failure mechanism, failure modes of a component of a low
5 level, in general it's not possible to predict or
6 understand the high level effects of that unless you know
7 the details of how that system is being used in the plant.
8 An example would be a check valve.

9 If I have a check valve and I understand how
10 check valves fail, if you ask me, how's it going to affect
11 my plant system, I can't answer the question until you
12 tell me how that check valve is being used in my plant
13 system, right. The same game applies really to digital
14 equipment in the plants.

15 Now, let's come back to this whole level of
16 interest idea. We looked at a number of different
17 methods of failure analysis and hazard analysis and so
18 on and it's interesting to note that these different
19 methods approach this level of interest problem in
20 different ways.

21 For example, what we call a top-down method,
22 like a fault tree analysis, starts by identifying a high
23 level event, accident, loss, whatever, it's a bad thing
24 that you don't want to happen. And then it works down
25 through the system to understand what combination of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 lower level mishaps will lead to that high level event
2 that you don't want.

3 That's one way of looking at it is top-down
4 theory. On the other hand, what we call bottom-up
5 method, like design failure modes and effects analysis,
6 starts by assuming the failure of a low level component
7 and then working up to the system seeing where the effects
8 of that go.

9 Okay, now the bad news about that method is,
10 you know, it has certain advantages obviously but the bad
11 news is you're looking at, you'll end up looking at a lot
12 of failure effects that really have no bearing on safety,
13 on the thing you care about at the high level.

14 So you're looking at, you're basically
15 spending resources on a lot of things that maybe you don't
16 need to. What that suggests is that there may be
17 significant advantage to using a top-down method to focus
18 your bottom-up effort, right.

19 And in theory what that lets you do, which
20 is really kind of interesting, is the, both more
21 effective at finding things, the bad things, the
22 vulnerabilities less say and at the same time do it with
23 a smaller effort than what we're doing now. So a, where
24 as a bottom-up FMEA failure modes and effects analysis
25 might be a 1,000 pages long, a focus one use, taking

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 benefit of top-down incites, let's say, might be a 100
2 pages, I don't know.

3 But there could be some significant days
4 there. So those were all very important incites for us.

5 Now another thing that falls out of this,
6 this whole notion of levels, is that if I have, it's
7 perfectly reasonable that I can have software with faults
8 in it and it can be perfectly safe because those faults
9 or vulnerabilities can be managed at a level above the
10 software. And will show you examples of how that plays
11 out.

12 And that's interesting because what it
13 means is that while you're not likely to ever have fault
14 free software, you don't really need them. Now the
15 corollary to that is that you can have fault free software
16 and could still cause problems.

17 Imagine a case where there was an error in
18 the requirements specification --

19 CHAIRMAN BROWN: Can you go back a minute,
20 you said we don't really care whether we have fault free
21 software or not?

22 MR. TOROK: No --

23 CHAIRMAN BROWN: Is that what --

24 MR. TOROK: If I said it that way I was being
25 a little to --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: No, I don't disagree with
2 you. That's --

3 MR. TOROK: I think it's, you can --

4 CHAIRMAN BROWN: That ought to get your
5 attention.

6 MR. TOROK: You can have software with
7 faults in it and they can be perfectly safe from the
8 prospective of the plant because you can manage the
9 faults and avoid the faults in other ways with defensive
10 design measures and so on, okay. And I want to show you
11 some examples, okay.

12 CHAIRMAN BROWN: Oh, the reason I asked the
13 question is because I, just based on past experience in
14 my earlier life, that after months and months and months
15 and months of detail testing of the software, the
16 programs that we had installed in the equipment for the
17 plants I was familiar with --

18 MR. TOROK: Right.

19 CHAIRMAN BROWN: -- that we put it in
20 service and then over the next few months or years, as
21 we went through test programs, it was amazing how many
22 little nuances popped up of inconsistencies that we had
23 missed even though we had a full range of engineering
24 model equipment that virtually replicated the equipment
25 in the ship.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. TOROK: Yes.

2 CHAIRMAN BROWN: And it still had design
3 errors as well as, everybody says you don't have faults,
4 the software does what you tell it to do and that's
5 absolutely the case, except if you don't specify the
6 right number of characteristics, you know, how numbers
7 are represented or this or that --

8 MR. TOROK: Yes.

9 CHAIRMAN BROWN: -- or whether you have, is
10 that a design thing, is that, whatever, you can call it
11 whatever it is. But I have never ever seen any code that
12 ever got delivered that didn't have errors.

13 MR. TOROK: Right.

14 CHAIRMAN BROWN: And at, no matter how much
15 testing you did. And yet the systems worked.

16 MR. TOROK: That's right.

17 CHAIRMAN BROWN: Satisfactory. And from a
18 safety you can see that they did it, they made test and
19 little nuances.

20 MR. TOROK: Right.

21 CHAIRMAN BROWN: So anyway, that's why I
22 was interested in your specific comment.

23 CONSULTANT HECHT: I think the importance
24 of, what occurs with this work is that if you understand
25 the ways in which the software fails and can affect the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 system, which I, from which I use the term failure modes,
2 and at a higher system level you can detect and recover
3 from those failures. Then your system can achieve its
4 requirements and can achieve its objective.

5 CHAIRMAN BROWN: Yes.

6 CONSULTANT HECHT: So I think the need for
7 this general area is to understand what those failure
8 modes are in software systems used in the context of
9 nuclear power operation or something close there of that
10 could be used as a surrogate in getting that confidence.

11 CHAIRMAN BROWN: Yes. I want to make one
12 more observation because my primary interest in this is
13 at my old job I had tons and tons of resources to deal
14 with.

15 The NRC and its staff as a regulator, does
16 not have the type of resources to do, what I call the old,
17 I don't want to call it oversight, but detail review and
18 transformation and verification and validation, they
19 depend great deal on the processes that are put in place
20 for the vendors, the designers and other associated folks
21 that are called in by the plant designers.

22 And so what, in my own view, those of you
23 that have a set of processes in a design that accommodates
24 and can pass through and still operate satisfactory when
25 you have these glitches, faults, failures, whatever you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 want to call it. So that's, they're just not going to
2 be able to do the type of oversight that I would have
3 expected.

4 No, not that I would have expected but if
5 some perceive as necessary they could have fault free
6 stuff. It's just for a code, it's just not going to
7 happen.

8 MR. TOROK: Right.

9 CHAIRMAN BROWN: So they really need a
10 process that's very robust and they need designs that are
11 very robust that can ride through these things. And
12 that's why this type of thought process, in my own mind,
13 is setting the stage at the top level as opposed to down
14 in the lines of code level, is important.

15 MR. TOROK: I couldn't agree more. And you
16 touched on a number of things that we'd be struggling with
17 for awhile.

18 This notion for example that good process
19 does not guarantee good design. Right. You need to get
20 a handle on the design so we've worked a way to do that
21 and you'll see more of that in time.

22 CHAIRMAN BROWN: We've heard you talk about
23 architectures in past meetings with other nuclear design
24 plants. The architecture of these systems for safety
25 purposes, is absolutely critical and needs to have total

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 complete independence such that you cannot cross
2 contaminate on your basic safety and safe service.

3 That's the fundamental point. And that's,
4 I give the flavor sometimes that that's not fully
5 appreciated based on the level of communications and the
6 types of communication that are done between divisions
7 these days.

8 MR. TOROK: Yes.

9 CHAIRMAN BROWN: It's been kind of an
10 interesting five in a half or six years or so.

11 MR. TOROK: Right, I know what you mean.
12 That's not exactly our target for today --

13 CHAIRMAN BROWN: Well I know that, but I'm
14 saying the architectures give thyself, it provides the
15 softness for the software to be operational when you need
16 it to.

17 MR. TOROK: No, I got, I agree to a large
18 extent this architecture can provide the defensive
19 measures you need to protect against faults --

20 CHAIRMAN BROWN: Exactly.

21 MR. TOROK: -- right?

22 CHAIRMAN BROWN: That's the point I was
23 trying to make. Thank you. You did much better than I
24 did. Not so awkward.

25 MR. TOROK: Anyway so with all --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CONSULTANT HECHT: Wait, excuse me.

2 MR. TOROK: Oh, I'm sorry.

3 CONSULTANT HECHT: You made a statement
4 which I take issue with and that is that good process does
5 not guarantee good software.

6 MR. TOROK: No, I said it doesn't guarantee
7 good design.

8 CONSULTANT HECHT: Design, okay. Well
9 it's unnecessary not sufficient condition for it.

10 MR. TOROK: I'll agree with that.

11 CONSULTANT HECHT: I mean we have to have
12 traceability, we have to have configuration management.

13 MR. TOROK: Absolutely.

14 CONSULTANT HECHT: We have to have a means
15 of verification.

16 MR. TOROK: Yes.

17 CHAIRMAN BROWN: We don't disagree with
18 that.

19 MR. TOROK: I agree with all that.

20 CONSULTANT HECHT: Okay.

21 MR. TOROK: I agree with that.

22 CHAIRMAN BROWN: Still not a guarantee,
23 absolute guarantee.

24 CONSULTANT HECHT: No, it's not
25 sufficient.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: All right, we'll keep that
2 portion together.

3 MR. TOROK: Okay. Okay, so with all this
4 in mind, we set out to look at a number of different
5 methods for doing failure analysis and hazard analysis.
6 We looked at what goes on in some other industries and
7 so on.

8 The idea was we wanted to understand that
9 strength and weight in weaknesses and figure out if we
10 could offer suggestions on how our utility engineers
11 might improve what they're doing now. And our targets
12 were, be more effective.

13 In other words, be better at finding
14 vulnerabilities that can be there and figuring out how
15 to mitigate them. And also potentially be more
16 efficient about it.

17 You know, if you can do a better job and do
18 it with less resources, that's really good. So now the
19 good news, the good news from our standpoint is that it
20 appears that very significant data in what we're doing
21 now are possible in the short term.

22 And so we're optimistic and I would say
23 excited, but hey, engineers maybe don't get excited.
24 But we really are optimistic that significant things can
25 be made here.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 And I know you're going to challenge us on
2 this stuff but I'm hoping at the end of the day you will
3 share our optimism and maybe also encourage the staff to
4 be optimistic and look into, you know, continue to look
5 into new methods and what they might do for the industry.

6 Now what I wanted to mention here is, in
7 order to do the best job we can for you today, we brought
8 what I call my project team on this. The guys who really
9 know the details.

10 And so these had been the principle
11 investigators on our work. Bruce Geddes from Southern
12 Engineering Services has been involved in the nuclear
13 power industry for 30 plus years, I guess.

14 MR. GEDDES: About 30.

15 MR. TOROK: Anyway, a long time. As an I&C
16 engineer at plants, as an executive for a large company
17 that develops digital equipment, that sells digital
18 equipment, as a consultant after that.

19 In recent years he's been doing a lot of work
20 for us at EPRI. So he's got the right kind of mix of
21 experience here.

22 His colleague here, Dr. John Thomas, just
23 finished his PHD at MIT and not coincidentally his thesis
24 is on hazard analysis. And he is at, one of the world's
25 experts on one of the novel methods we're going to talk

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 about today. So he's the right guy for that.

2 We also have Dave Blanchard who is, been our
3 EPRI expert on risk methods and top-down analysis.
4 Including fault tree analysis for, from a PRA prospective
5 but also from a hazard analysis prospective. So I think
6 we've got the right guys here.

7 We're going to do this in sort of a tag team
8 approach where, you know, we'll flip back and forth to
9 get the right guys talking about each topic, okay.

10 So that's the team. Now then, I think I
11 said that we're going to highlight failure analysis and
12 hazards.

13 I want to give you a, just a little set the
14 stage kind of thing on EPRI. What we do is typically we
15 don't argue regulator issues, right. We try to generate
16 technical information, technical basis, guidance and so
17 on that is going to help our utility numbers, our
18 engineers do a better job.

19 Now in my little area, that means in regard
20 to digital I&C. Right. How can you do it better, what
21 can you do about I&C obsolescence. That's a big problem
22 for the plants right now.

23 There are a number of technical issues you
24 have to address when you get involve with digital
25 equipment like the failure analysis we've been talking

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 about. And we're trying to make that easier for them.
2 And we're trying to, and protect them from the
3 vulnerabilities, the potential vulnerabilities of the
4 new equipment.

5 Now I've got a line in about addressed
6 regulator issues. What that really means is there have
7 been times where we effectively generate a technical
8 basis that's used to support a regulator position.
9 That's where EPRI comes in here.

10 So we might help a utility or NEI, for
11 example, with the technical basis for something but not
12 the specific regulator issues themselves.

13 Now there's a list of other things going on
14 at EPRI on the right here. These are other topics we're
15 working on.

16 I'm not going to read the list, you can read
17 it faster than I can say it. But these are areas related
18 to Digital I&C that maybe of interest to you guys at some
19 date.

20 I just wanted that there for an awareness
21 issue, right, so that if those things become of interest
22 for the group, we'd be happy to get the right people back
23 here to talk to you about the EPRI work on that, okay.
24 Is that --

25 Okay, now getting on with it, our first

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 topic here is failure, digital failure, mechanisms mode
2 and effects. And going back in time now, 2008, ACRS
3 said, Digital I&C may introduce new failure modes that
4 are not well understood. So it was a big issue back then.

5 And at the time, 2009, what we said was,
6 okay, well based on our work there's this issue of
7 mechanisms versus modes versus effects. Mechanism at a
8 low level creates a failure mode, the next level up which
9 creates a failure or effect at a higher level still.

10 Now this sounds a lot like what we're
11 calling levels of interest now. And it is. So the good
12 news is at that time we were barking up the right tree,
13 I think, but now we continue to develop the idea. You'll
14 see more on that, so that's all good stuff I think.

15 In regard to PRA we were saying, look, from
16 the PRA prospective you don't need to understand all the
17 low level mechanisms to store, generate useful risk
18 insights. That's where we're worth the time.

19 And the last one really comes back to what
20 Myron was talking about here. When we looked at
21 potential digital system vulnerabilities and managing
22 them, we said, hey, process is good but it's not
23 everything and you have to somehow get it to design itself
24 to understand what protective measures you have built in.

25 And that's what this software and hardware

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 design features is about and that's what diversity is
2 about in terms of protecting against vulnerability. So
3 that's where we were.

4 Okay, now in terms of our current work, the
5 plants are still having problems with the digital systems
6 and they come back to us and say, look, we put these thing
7 in a year ago, it was fine, then it burped, it tripped
8 a plant, everybody got angry, we've got to do a better
9 job. And they did an analysis after the fact and
10 discovered that the system had a failure mode they missed
11 when they did their failure modes and effects analysis
12 or they misunderstood in some cases.

13 But there's another thing that also goes on.
14 There are cases where nothing failed. The components,
15 every component did exactly what it's supposed to do, but
16 the system at the high level did the wrong thing. Right.

17 Those are a little sneakier to deal with,
18 a little more interesting. Now, so --

19 CHAIRMAN BROWN: Are you going to talk
20 about any of those and your operating experience?

21 MR. TOROK: Yes.

22 CHAIRMAN BROWN: Okay.

23 MR. TOROK: Yes.

24 CHAIRMAN BROWN: Thank you.

25 MR. TOROK: Those are some of the most

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 interesting events that we know about in fact. Not just
2 in the nuclear power industry, in other industries.

3 But, so our objective was to find ways to
4 be more effective and more efficient in terms of finding
5 both potential vulnerabilities before these systems are
6 activated in the plants, right. How can you do a better
7 job?

8 So basically you find the vulnerabilities
9 before they find you. That was the game. And that means
10 failure modes but it also means undesired behaviors when
11 there are no failures.

12 Now there's a note here about failure
13 analysis versus hazard analysis. And in, most recently
14 for us we've been using some hazard analysis and the
15 reason is failure analysis implies that a component broke
16 or that kind of a thing.

17 Hazard analysis for us is broader than that.
18 It says, okay, things can break, we understand that, but
19 things can also misbehave even when nothing breaks.

20 So for us, having analysis is a bit of a
21 broader term and it's becoming, I suppose, the more
22 favorite term for us. Okay.

23 CONSULTANT HECHT: Ray?

24 MR. TOROK: Sure.

25 CONSULTANT HECHT: Just a comment that the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 IEEE and DoD definitions on failure is basically a
2 deviation from requirements. Now wouldn't that hold
3 true at any level and couldn't system fail even if the
4 underlying components haven't failed?

5 DR. THOMAS: It did, but the requirements
6 could be wrong.

7 CONSULTANT HECHT: Well --

8 MR. TOROK: Exactly.

9 CONSULTANT HECHT: -- so, I mean if the
10 requirements could be wrong that implies that those are
11 lower level requirements that deviate from a set of
12 higher level requirements, right?

13 DR. THOMAS: You can have requirements at
14 any level that are wrong. Hopefully not the highest
15 level, right, because that's basically the objective of
16 your system. But --

17 CONSULTANT HECHT: Right, so I guess that
18 means that the lower level requirements deviated from the
19 higher level requirements, which meant that even if your
20 system or your subsystem meet those lower level
21 requirements, there was still a failure.

22 DR. THOMAS: I think we could get into an
23 example of that.

24 MR. TOROK: That's an interesting way to
25 think of it and I'm not really disagreeing with you.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CONSULTANT HECHT: Yes.

2 MR. TOROK: Okay.

3 DR. THOMAS: Okay, a requirements conflict
4 is a little bit --

5 MR. TOROK: So yes, in my mind anyway you're
6 characterizing this a little differently. But the idea
7 is the same I think, right?

8 CONSULTANT HECHT: Yes.

9 MR. TOROK: For practical purposes.

10 CONSULTANT HECHT: Yes.

11 MR. TOROK: Okay. So --

12 MEMBER BLEY: So what you're really saying
13 is that you have to look at failure in an integrated
14 system. And that failure can occur anywhere whether, if
15 it's associated with software it's probably because of
16 some part of the design. The software in the
17 specification.

18 MR. TOROK: Typically true.

19 MEMBER BLEY: You've got to look at the
20 whole thing, the whole integrative plant.

21 MR. TOROK: Absolutely.

22 MEMBER BLEY: And I think you're saying
23 anything much different.

24 MR. TOROK: Yes. Well and that's a really
25 interesting point because sometimes we talk about

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 software failure analysis. What does that mean?

2 It might be more reasonable to talk about
3 system failure analysis or digital system failure
4 analysis. It gets into that discussion.

5 MEMBER BLEY: Yes, of course.

6 MR. TOROK: You're right. Okay, so where
7 we left off in 2009 there was this ACRS letter that said,
8 hey, look at this list of failure modes and I think
9 actually this was mostly in reference to the modeling
10 digital equipment in PRA saying, hey, what are you doing
11 about these in PRA?

12 And we looked at this list and we scratched
13 our heads and we said, well you know, that's a really
14 interesting list to go through if you're trying to
15 convince yourself or you're trying to figure out whether
16 or not you have a good design. A design that's robust
17 in regard to those things.

18 And that's a good thing to do right now.
19 Again, we're coming back to this things were we went
20 beyond process, we said, and IB have a good process for
21 software development, they still might have a lot of
22 these problems. I want to find out. So I went and
23 looked at the design.

24 So, and it turns out that in design what
25 those vendors and developers have figured out over a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 number of years, and I'm sure mostly through bad
2 experiences, is that you can implement design measures
3 that can help mitigate these things or can control them
4 or eliminate them and so on. And to make the effects
5 acceptable.

6 So here's some examples that you'll see in
7 a real-time system. You know, a high quality real-time
8 system will have a software architecture that
9 effectively is an infinite loop. They'll use watchdog
10 timers to figure out if something locked up or didn't
11 finish on time and those kinds of things.

12 And that's what addresses a whole bunch of
13 those failure modes that are on the list there. And
14 that's all good stuff.

15 And for some, also you've got, in typically
16 nuclear power plant safety systems you've got redundancy
17 requirements, independence and so on. And digital
18 systems use data validation routines to protect against
19 others of those.

20 I apologize for those words going out of the
21 box. You know, that looks great on my computer, I don't
22 know why it doesn't look right here.

23 But the point here is that of this list, I
24 think five there is the one that needs special attention
25 when all is said and done. Task incorrect response.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And that's the kind of thing where you come
2 back to this issue of, what happened in the requirements,
3 how do we know those are right, how do we know that we
4 just didn't implement bad requirement? But you want to
5 have a way to go after that as well.

6 But the point is that good design can deal
7 with a lot of those things. And when you're looking at
8 a digital system you want to convince yourself you have
9 a good design.

10 MEMBER BLEY: Or you --

11 MR. TOROK: Or you just apply your hazard
12 in design. I'm sorry?

13 CHAIRMAN BROWN: Before you leave that,
14 just one question. When you talk about an infinite loop,
15 I want to make sure we're on the, I've heard that term
16 and I know we think in terms of a main operating group --

17 MR. TOROK: Yes.

18 CHAIRMAN BROWN: -- where data is taken in
19 and every function of the application is performed and
20 once we finish this, it comes back and starts again.
21 There's no interrupts, there's no interjections anywhere
22 along the whole line.

23 MR. TOROK: Exactly.

24 CHAIRMAN BROWN: At any time, period.

25 MR. TOROK: Exactly.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: There's zero interrupt
2 yet vendors don't seem to, some of the have used platforms
3 which have an interrupt type design which is not an
4 infinite loop type. But we're talking the same type of
5 architecture.

6 MR. TOROK: You're exactly right. And
7 what we tell our guys is, you need to know enough about
8 this stuff to figure out if you vendor has a good design,
9 if your vendor has done those things well enough for your
10 application.

11 But you're right. And if you do that, what
12 you said, with this loop, no branching and all that,
13 again, the other thing that you're looking for is that
14 that system is what we call blind to plant transients.

15 It doesn't matter what's going on in the
16 plant, it can't trigger a fault in your system, in your
17 software because the software is not changing what it's
18 doing.

19 CHAIRMAN BROWN: But you don't want the
20 state, you don't want the operational software to be
21 dependent upon some state to the plant or some state --

22 MR. TOROK: Exactly.

23 CHAIRMAN BROWN: -- of data or some state
24 of anything.

25 MR. TOROK: And a good design --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: You want all this to
2 continue and just always go --

3 MR. TOROK: And a good time to do that --

4 CHAIRMAN BROWN: But I brought this up for
5 one reason because in terms of, I think I'm so old I almost
6 forgot my thought process here, is that today I hadn't
7 seen any software design rules, don't do these types of
8 things that have been put out by the regulator system.

9 And it was they, they don't put out a reg
10 guide or there's not a rule that says, do not use
11 interrupts, do not use global variables, do not use state
12 based information that can then change a particular
13 routine, this process as you go through your operating
14 work. Whether it's, regardless of what type of group you
15 have.

16 MR. TOROK: Exactly.

17 CHAIRMAN BROWN: In which, I mean the
18 argument is that, well gee we're regulators and therefore
19 we don't tell the vendors how to do this.

20 MR. TOROK: Right.

21 CHAIRMAN BROWN: Okay, well my mind just
22 doesn't get around that.

23 MR. TOROK: Okay.

24 CHAIRMAN BROWN: Seems to me that when you
25 talk about ensuring software that performs consistently,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I don't want to say perfectly, but consistently.

2 MR. TOROK: Yes.

3 CHAIRMAN BROWN: But that's what you're
4 looking for, consistently performing software that
5 without dictating some type of fundamental design rules
6 that you can use, you've opened yourself up to unknown
7 modes which the regulator will never be able to find.

8 MR. TOROK: Yes, yes.

9 CHAIRMAN BROWN: Or understand.

10 MR. TOROK: This comes back to that issue
11 of --

12 CHAIRMAN BROWN: Well I can see you all
13 recommending that either. I mean --

14 MR. TOROK: Oh.

15 CHAIRMAN BROWN: -- design a specific set
16 of design rules. I'm not saying you haven't, I'm just
17 saying I haven't seen it.

18 MR. TOROK: We published lists of those
19 things actually.

20 CHAIRMAN BROWN: But do you tell your
21 customers?

22 MR. TOROK: Oh, yes. And our
23 recommendations --

24 CHAIRMAN BROWN: Are they required to use
25 them?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. TOROK: We don't require anything.

2 CHAIRMAN BROWN: I'm sorry, but you can't.

3 MR. TOROK: What we say --

4 CHAIRMAN BROWN: I know that, I said that
5 just for a fact.

6 MR. TOROK: We say things like, hey, when
7 you're talking to your suppliers about their equipment,
8 here's some things to ask them about, right. And this
9 gets at that issue of design versus process.

10 And I know that NRC endorses a number of
11 software development standards, for example. And they
12 say use what requirements traceability matrix and do good
13 configuration management and those kinds of things,
14 which are all fine, but they don't get at good design
15 issues, right.

16 And now some companies do have a list of
17 design practices they follow to go after things like
18 this. But in general you're right.

19 And you guys are in a, I think a tough
20 situation because you don't want to dictate design,
21 right, that's not your role. But you do want to make sure
22 these guys have good design, so.

23 CHAIRMAN BROWN: But one of the arguments
24 I use in our other meetings is that in the absence of
25 those, you have to have an architecture that protects

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you. A hardware architecture that protects you from
2 that and the watchdog timers are relatively key --

3 MR. TOROK: Or something --

4 CHAIRMAN BROWN: -- if it's truly
5 independent of the software systems.

6 MR. TOROK: Yes. And we've looked at real
7 systems where the watchdog timers were not implemented
8 correctly and they missed important things.

9 CHAIRMAN BROWN: Yes.

10 MR. TOROK: Right. And we need to be able
11 to find those kind of things. Okay, I'm sorry.

12 CHAIRMAN BROWN: Go ahead, I'm sorry.

13 MR. TOROK: No problem. Okay, so now we
14 come back to this whole level of interest thing.

15 This is a figure right out of the report.
16 And what you see at the top there, we're talking about
17 plant functions and underneath that there's systems that
18 implement those.

19 There's a list in the fine print, main
20 turbine, main generator, feedwater and so on. The next
21 thing down is components of those.

22 And you'll see these bars going out like
23 form Plant System 2 out to the plant components showing
24 that there are multiple plant components within Plant
25 System 2. And similarly at the lower levels. As you go

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 down you can have multiple feeders to each level above
2 that.

3 So it's trying to express that. Now this
4 is sort of generic cartoon, it's not a fixed
5 representation of everything real.

6 But a thing to note here is that the way we
7 characterize this, in the green boxes up there we're
8 talking mostly hardware. And the blue boxes below are
9 talking about control at various levels.

10 Now what you want to keep in mind here when
11 you're doing failure analysis and hazard analysis, where
12 are you, what are you looking at?

13 Now that ACRS letter that talks about task
14 hang, task crash, those kinds of things, it's at the very
15 bottom level here, right. And looking at the software --

16 CONSULTANT HECHT: Can I suggest that it
17 can occur at higher levels as well?

18 MR. TOROK: Well yes. And in fact there's
19 software, I agree, there's software in levels, all those
20 blue boxes going up as well, we're right.

21 But we're talking, in those case we're
22 talking about a processor and failure mechanisms in a
23 processor, right, on that list?

24 CONSULTANT HECHT: Yes.

25 MR. TOROK: But you're right, in principle

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I agree. However it typically, from the plant engineer
2 prospective, the effective interest that the thing
3 you're trying to protect against is up near the top.

4 Does the safety function do what it's
5 supposed to do when you want it to do it, right? It's
6 at very much higher level.

7 And then you wonder, well if you got this
8 little hazard, where are you managing it? And in
9 principle, you can do it anywhere between the hazard and
10 the high level function you care about. And there are
11 different ways to go after those things, right.

12 And the point of this is that, I said this
13 earlier, it's not, in general, necessary to manage every
14 low level failure mechanisms you have, if you can
15 consolidate them and manage them at a higher level. And
16 good designers often do that kind of thing, right. Is
17 what you were talking about, really?

18 MEMBER STETKAR: Before you leave this --

19 MR. TOROK: Yes.

20 MEMBER STETKAR: -- I think that it's
21 important to kind of put some perspective on this.

22 That letter that you've referred to from the
23 ACRS regarding software failure modes was an effort to
24 try to get people to define a set of failure modes and
25 avoid, and you're guilty of this same process. You mix

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 terms, failure mechanisms, failure causes, failure
2 modes, failure this, failure that.

3 MR. TOROK: Yes.

4 MEMBER STETKAR: We struggled with this 35
5 years ago in the PRA business with a valve. What is a
6 failure mode of a valve?

7 MR. TOROK: Right.

8 MEMBER STETKAR: And people spent years
9 saying, well the packing could be too tight or somebody,
10 there could be a bur on the stem or there could be a minor
11 short circuit on the motor winding or, and finally after
12 a while people said, well no, there's sort of four failure
13 modes. Bail to open, bail to close, open spurious and
14 close spurious.

15 MR. TOROK: Yes.

16 MEMBER STETKAR: Everything else is
17 something that can result in one of those failure modes.

18 MR. TOROK: Right.

19 MEMBER STETKAR: The letter back in 2008
20 was focused at trying to consolidate the thought process
21 to define the equivalent set of failure modes for
22 software.

23 MR. TOROK: Right.

24 MEMBER STETKAR: And so it isn't
25 necessarily focused down there with your little circle

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 at the bottom with the implication that you don't think
2 about things with an integrated sense because those
3 failure modes of a valve. Valve opens spuriously.

4 And has the same effect all the way up to
5 a point of function. And can be mitigated by other
6 systems rather than protect it.

7 MR. TOROK: Yes.

8 MEMBER STETKAR: So I just wanted to make
9 that statement, kind of put things in perspective to say
10 that we weren't necessarily trying to focus on minutiae
11 of things way down at the bottom, we were trying to
12 provoke a thought process that's logically equivalent to
13 what took people probably several years to come to the
14 notion, that in a structured analysis of systems, their
15 interested for that valve in four failure modes.

16 MR. TOROK: Yes.

17 MEMBER STETKAR: Everything else, whether
18 the guy slipped when he wrote the design specification
19 and put 2.0 as far as a specification for, I don't know,
20 a torque limit or something limit or something like that
21 rather than 20.

22 MR. TOROK: Yes.

23 MEMBER STETKAR: So I just want to make
24 that --

25 MR. TOROK: No --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: -- before you go too far.

2 MR. TOROK: No, that's a good point.

3 And --

4 MEMBER STETKAR: You know, and I think
5 that's why we're having this meeting. It's not, but --

6 MR. TOROK: Yes. And, no, that's a good
7 point because even back then when we were looking at this
8 notion of mechanisms modes and effects, we went back to
9 the PRA handbook, which we thought explained it really
10 well, and we tried to follow that.

11 MR. GEDDES: Can I add something?

12 MEMBER STETKAR: I think we're, I mean
13 anyway, I think we're getting really close by the way,
14 so.

15 MR. GEDDES: If I can add something? I
16 believe the ACRS letter did provoke that discussion and
17 the researches, you're going to see today, are --

18 MEMBER STETKAR: I think that's why I said
19 that I think we're getting pretty dog gone close.

20 MR. GEDDES: And the only reason we put this
21 yellow oval at the bottom here is because in this
22 construct we had literally mean that the software is in
23 a device, in terms of a bits and bytes and where you find
24 software.

25 In reality software's more of an abstract

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 model. And it effects everything through that total
2 hierarchy.

3 So it's a matter of semantics to say, where
4 is this software? But semantically we mean it's in a
5 device, it's a prop or a RAM or a CPU chip where it resides
6 and it becomes functionally usefully in a digital system.

7 But ultimately, and you'll see this in the
8 slides that are coming, how does that model effect the
9 plant components that it influences? And that's the
10 sweet spot, right.

11 And I think, John, that's the same point
12 you're making. If it's a bur on a valve stem or a bit
13 flip, what's the impact on the valve? And we're coming
14 to that same nexus here. And I hope you see it.

15 MEMBER STETKAR: And it's, this slide is
16 what Dennis mentioned also is that you can't do these
17 things in isolation.

18 MR. TOROK: Yes, absolutely.

19 MEMBER STETKAR: At all, okay.

20 MR. TOROK: Okay, moving on.

21 CHAIRMAN BROWN: I just want to --

22 MR. TOROK: Oh.

23 CHAIRMAN BROWN: I totally agree with what
24 John said. I was not here when that letter was written,
25 okay. I think that's a good --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BLEY: Yes, you came just after
2 that. Yes.

3 CHAIRMAN BROWN: About three weeks after.
4 Two, no --

5 MEMBER BLEY: That's right.

6 CHAIRMAN BROWN: -- the first of April,
7 what?

8 MEMBER STETKAR: 29th.

9 CHAIRMAN BROWN: 29th, I --

10 MEMBER BLEY: You're right.

11 CHAIRMAN BROWN: One day later. I didn't
12 get to present, participate in that thought process.
13 But to someone that's a little bit of the idea from what
14 John's saying, that the thought process when I came on,
15 trying to get people to think about it in a whole division
16 of reactor trip functions.

17 We got four channels, four divisions,
18 whatever it is. I'm interested in that reactor trip, no
19 reactor trip. That is the failure mode that I think
20 about. What, I really don't, I don't want to say I don't
21 care because that's not the case, but I don't want to get
22 lost in that. I want to say, what do I have to do no
23 matter what happens down here to ensure I've either don't
24 trip spuriously, okay, or I trip when I'm told to.

25 And if I've got four things and I need to,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 then I can have it do something spuriously and it's okay
2 as long as that's not replicated because I've lost
3 independence between the other three, the one that's
4 giving me the problem and the other three divisions or
5 trains or what have you.

6 So I really don't think about bit flips and
7 all that stuff, it's just what I trip or not trip if the
8 processing chain doesn't do what it's supposed to.

9 MR. TOROK: Right.

10 MEMBER BLEY: And that's just a focus, I
11 think, that needs to be brought from a higher level in
12 why, in most of our discussions we fundamentally focus
13 on redundancy, independence --

14 MR. TOROK: Environmental.

15 MEMBER BLEY: -- behavior, diversity
16 defense in depth and then try to make the design as simple
17 as you can. Don't put stuff into your code that doesn't
18 add value to the operation and monitoring of the plant.

19 MR. TOROK: And all those things are what
20 we would call defensive measures, defensive design
21 measures because they help make the option more
22 dependable. Right, that's why they're there.

23 MEMBER BLEY: Yes, okay.

24 MR. TOROK: Okay? Okay, so I get to stop
25 here in a minute. We're onto the report. Now here's the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 recently republished report, there's the EPRI report
2 number, I apologize for the length of that number but that
3 happens above my pay grade.

4 Anyway, so hopefully you guys have had a
5 chance to look at it in the report. In the investigation
6 we looked at six different methods that are listed here.

7 MEMBER STETKAR: By the, Ray, since you're
8 learned about, does EPRI change their fundamental notion
9 of how they're number the reports now?

10 MR. TOROK: Well that would --

11 MEMBER STETKAR: Use to be you could look
12 at the first two digits and figure out what year it was
13 issued.

14 MR. TOROK: Now those were the good old
15 days, yes.

16 MEMBER STETKAR: Okay.

17 MR. TOROK: No, what happened is EPRI has,
18 what transitioned to a, what do you call it, an enterprise
19 management system with SAP software.

20 MEMBER STETKAR: Yes.

21 MR. TOROK: SAP software likes long numbers
22 for some reason. Okay, and that's where we are.

23 MEMBER STETKAR: Okay, that explains it.

24 MEMBER BLEY: The numbers lack
25 intelligence, that's the point.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Yes. It appears to be
2 able to look at the report number and figure out what year
3 it was issued in.

4 MR. GEDDES: That's because they get paid
5 by the digit.

6 MR. TOROK: Because it turns out computers
7 don't struggle with long numbers like we do.

8 MEMBER STETKAR: No doubt.

9 MR. TOROK: Yes. Anyways, so that's
10 what's going on. Okay, so just the reports from last
11 year --

12 MEMBER STETKAR: No, yes, I noticed that,
13 okay, thanks.

14 MR. TOROK: Okay, all right, sorry.
15 Anyways, so the methods we looked at, this so called
16 functional FMEA, which, oh, and design FMEA, what we call
17 top-down method using fault tree analysis, HAZOP, which
18 is a method that's been developed primarily I think in
19 the chemical industry. They've been using it for
20 decades.

21 Now STPA, this is where it gets interesting,
22 systems theoretic process analysis. There will be a
23 quiz at the end to see who remembers that.

24 MEMBER BLEY: No, she use to call it STAMP,
25 didn't she?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. TOROK: Well it's related. It's not
2 the same but it's related.

3 MEMBER BLEY: Oh, okay.

4 MR. TOROK: John can explain all those
5 details if you need to.

6 DR. THOMAS: STAMP is basically the
7 theoretical model. STPA is the process, it's the
8 methods.

9 MEMBER BLEY: Okay.

10 DR. THOMAS: It's step by step, here's what
11 you do.

12 MEMBER BLEY: Sure.

13 MR. TOROK: There you go. And so that's
14 the method that Nancy Leveson, Dr. Nancy Leveson or
15 Professor I guess, at MIT had been working for a number
16 of years with grad students, of which John was one. And
17 so that's what I would call maybe a novel method or an
18 emerging method, those kinds of things.

19 PGA, purpose graph analysis, has been used
20 in a number of, I guess, DoD applications.

21 MEMBER BLEY: Can I interrupt you?

22 MR. TOROK: Yes.

23 MEMBER BLEY: Since you're talking MIT
24 people.

25 MR. TOROK: Pay attention, John.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BLEY: It wasn't a method but
2 another MIT guy, Daniel Jackson, lead a national academy
3 report a few years ago on dependable software. Did you
4 guys go through that too?

5 Now the thing he, the main thing they said
6 is keep it simple. They said no matter what else you do
7 if you don't keep it simple it ain't going to work?

8 MR. TOROK: It's hard to argue with that.
9 We were not involved at all, I don't, did you want to
10 comment on that?

11 DR. THOMAS: I don't think I saw this
12 specific report, but I'll --

13 MEMBER BLEY: It's a report worth looking
14 at.

15 MR. TOROK: Yes.

16 MEMBER BLEY: It came out about three years
17 ago or something.

18 MR. TOROK: Well we should --

19 MEMBER BLEY: So then you can get it on the
20 national academy website.

21 MR. TOROK: We should take a look at that
22 but there's nothing wrong with keeping it simple and it's
23 hard to argue. Now what I tried to do here was generate
24 a simplified version of a much larger table that's in the
25 report talking about strengths and weaknesses and things

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 like that. I'm calling attention to certain things.

2 So we've got this next column over,
3 characterizes these methods or top-down and bottom-up.
4 And I got to tell you this, this is somewhat qualitative
5 and even the group of us here, we don't always agree on
6 these things, okay.

7 So don't take these things as absolute, but
8 in general I say functional FMEA is where we consider
9 top-down approach. It looks at high level effects first
10 and tries to figure out what causes those.

11 Design FMEA is the opposite of that. It
12 postulates a failure of a low level component, let's say,
13 and see where, you know, looks for where that goes.

14 Obviously fault tree is a top-down method.
15 It talks about top events. HAZOP, we argue about HAZOP.
16 HAZOP could be either.

17 STPA, same thing, top-down. And purpose
18 graph, I characterize it as inside out, personally.

19 But why do we need to call attention to that?
20 And that's what I really wanted to point out here.

21 The point is that bottom-up methods start
22 with a low level failure of a component and just see where
23 it goes. Which means you're analyzing at the high level,
24 you're analyzing the things you care about and a whole
25 bunch of things you don't care about. And in that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 sentence, it's inefficient.

2 A top-down method can provide some focus by
3 first identifying the top, the high level things you
4 really care about. So for us, that's why that
5 distinction is of interest, okay. That's why it's on the
6 chart.

7 Now in terms of strengths of the individual
8 methods, if I look at, let's see the next column over,
9 the FMEA and the fault tree focus primarily on failures.
10 On failure of a component, that sort of thing.

11 And admitted they can under some
12 circumstances go beyond that, but in general, our
13 characterization was they don't. They focus on
14 failures.

15 Now we wanted to also go after things beyond
16 that. These unattended functions under certain
17 conditions and so on.

18 The next one, integrative view of the plant
19 design. That's where you get back to this whole issue
20 of context of that you guys have been talking about.
21 Understand how the digital system works in the big
22 picture.

23 Design FMEA, and when it starts out doesn't
24 really care. You're looking at low level behaviors.

25 Ultimately when you've got the whole thing

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 done maybe you understand it in the context of the plant.
2 But these other methods take it into account from the
3 start. They try to understand how the digital equipment
4 fits into the plant. That's good.

5 The last one over there. What's out there,
6 mature well documented. Well functional FMEA have been
7 heavily used in, with the automotive industry and they've
8 got exhausted procedures on how you do it and so on.

9 Design FMEA is the one that's best known in
10 the nuclear industry and it's what's most commonly done
11 on these digital upgrades. Also very well developed.

12 Fault tree, we've got a number of people in
13 the room who have been doing fault tree for 20 to 30 years,
14 I guess. So that's a well-developed method. Same thing
15 with HAZOP in the chemical industry.

16 These other two, the STPA and the PGA, we
17 characterize as like a emerging novel methods, okay.
18 And so that's probably the downside.

19 Now it's interesting to note that the most
20 prevalent one in our industry now for looking at these
21 digital systems has been design FMEA. Which in terms of
22 looking at hazards beyond failures and looking at the
23 integrated plant, is not so good.

24 You know, but FMEA or the design FMEA wasn't
25 developed for that. You know, I'm sorry, I can't blame

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the method, but the point is that I think we can do better.
2 That's what this chart is trying to say.

3 Now as we go forward here, we're going to
4 talk about selected ones here. We're not going to talk
5 about design FMEA because it's a well-established method
6 and these other ones are more interesting to us right now.

7 We're not going to talk about purpose graph
8 because of all these methods, it looks like the one that's
9 the farthest from practical applicability in our world.
10 Okay, but the others we want to talk about.

11 MEMBER BLEY: I'm just curious, you guys
12 can chip in on this too. The design FMEA is, if you've
13 got a system that's old style design that were not heavily
14 redundant and are designed to be highly reliable, you're
15 going to find all kind of things,

16 If you designed your system to have
17 redundancy, diversity, be highly reliable, I've rummaged
18 through some of those FMEAs, I mean piles of paper, and
19 I don't, I have yet to see anything especially useful,
20 because most of the low level things you spot don't do
21 anything expect fail something locally.

22 Have any of you seen much useful out of
23 those?

24 CONSULTANT HECHT: Can I answer that?

25 MEMBER BLEY: Sure.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CONSULTANT HECHT: The point is that if you
2 don't see anything, "interesting," out of a well done
3 FMEA, that's reassuring to a user or a customer or whoever
4 is depending on that system. The point in --

5 MEMBER BLEY: It's a hell of a lot of work.

6 CONSULTANT HECHT: It is a lot of work and
7 the purpose of the work is, once again, in the systems
8 that I mostly work, is to show that your failure detection
9 and recovery provisions, which are called defensive
10 measures here, do in fact address the failure modes of
11 the individual items. So for example, if you say --

12 MEMBER BLEY: No, no, I've heard a lot, it's
13 in.

14 CONSULTANT HECHT: Again, so what you want
15 at the end is you want no effect or you something in the
16 comments occasional says that --

17 MEMBER BLEY: What I'm asking is, do we get
18 that from the FMEA? I mean we get, well the thing that
19 says, yes, we looked and all is good. I don't think we
20 get that kind of good design from very much out of the
21 thousands and thousands of items in the FMEA. And I just
22 haven't seen it in the --

23 CONSULTANT HECHT: Well as somebody who
24 advocates them, they should be done, the designer maybe
25 doing it in his head. As that designer comes out with

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 whatever, it's a system which not only fulfills the
2 functions, but fails gracefully or has the means of
3 switching over or whatever is done.

4 But he has to be or she has to be thinking
5 about it that's why you put a fuse in a electrical
6 circuit. That's why there's --

7 MEMBER BLEY: And you do, in the document.
8 But anyway. Where we're we? The process has, yes, go
9 ahead.

10 MR. TOROK: That's some of the same thought
11 process we went through looking at these 1,000 page FMEAs
12 thinking, where are the good parts. And ideally you can
13 find the low level failures that contribute to things you
14 really care about at the high levels and then you go back
15 and see if you've adequate defensive measures for those,
16 right. But you've created this huge pool of information
17 that's not so easy to deal with.

18 Okay, now the last thing here that we're
19 also going to talk about is this notion of blended
20 approaches. Which really comes from the same
21 discussion, right.

22 What if we could use top-down methods to
23 focus the bottom-up part of it? That's what blended
24 methods is really about, blended approaches. And so
25 we'll come back to that where we talk about maybe using

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 combinations of some of those things to make the analysis
2 more efficient, more effective.

3 Okay, now I think I get to be quiet here for
4 a little and Bruce is going to explain what we did, what's
5 some examples we looked at and what they're telling us
6 for various methods and so on. So, Bruce, please.

7 CHAIRMAN BROWN: Can I ask one question
8 before you go relative to the interchange? You just, I'm
9 not agreeing on this kind of stuff so, but when you talk
10 about defensive measures, I've heard this term a couple
11 of times and I actually think I've heard it from one of
12 the design groups that we had, in other words they
13 monitored the software as it was doing its job and then
14 as they detected that something was awry, there was, part
15 of the thought process was, the defensive measure was to
16 correct the error within the software.

17 In other words it would be a self-correcting
18 loop. And I always get real nervous when somebody says
19 they now have figured out that my data is wrong, but I'm
20 going to tell you what the right data ought to look like.

21 MR. TOROK: Wow.

22 CHAIRMAN BROWN: Is that, do you see any of
23 that going on? I mean this is just information. I've
24 heard it talked about, but for instance, when I was trying
25 to boot up, bring up your all's presentation --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. TOROK: Yes.

2 CHAIRMAN BROWN: -- it worked fine at home
3 last night when I was looking at it, I brought it up on
4 the laptop as opposed to my desktop and it said, oh, we've
5 detected an error, can we recover your pages? We're
6 deleting some of the pages and putting blank pages in
7 their place, is that okay? I don't know, how am I
8 supposed to know why. How do I know they recovered the
9 pages? So my screen is blank right now.

10 MR. TOROK: They're going to fix it for you.

11 MEMBER BLEY: If you can find them, huh.

12 MR. TOROK: The answer to your question is,
13 I haven't seen that particular thing. Typically when we
14 talk defensive measures at a level like that, it might
15 be a data validation routine.

16 If you're worried that your software
17 doesn't know how to handle out of range data --

18 CHAIRMAN BROWN: Well I wasn't worried, it
19 was. I clicked okay and then something happened. But
20 I decided I was use the paper version because it doesn't
21 change while I'm looking at it.

22 MR. TOROK: Self-correcting sounds a
23 little, potentially a little dodgy though. You want to
24 be careful --

25 CHAIRMAN BROWN: I just, I heard you all

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 talking about defensive measures and I just wanted to see
2 how that, how you correct things or what have you. I
3 wasn't sure whether you all come onto that level, whether
4 anybody was really advocating that level.

5 MR. TOROK: No, cell phone does that too
6 when I try to do texts, it's really bad news. You know,
7 it doesn't like the word you put in, it puts in one it
8 likes. Which may have nothing to do with what you're
9 trying to say.

10 CHAIRMAN BROWN: I'll let you go on.

11 CONSULTANT HECHT: That's an example of bad
12 requirements. However, I will say that even electronics
13 does self-correction. Memory has, there's this error
14 detection and correction circuitry so that, and that's
15 done simply on the basis of including redundant bytes
16 that can be used to check consistency and we depend on
17 it.

18 Because when we have 8 gigabytes of RAM in
19 a PC, there's going to be failures in that --

20 CHAIRMAN BROWN: All I know is that I never
21 had any of that in the stuff I delivered. I mean if the
22 RAM got corrupted it was gone, we didn't try to recover
23 anything. The whole chain shutdown.

24 MR. TOROK: Except that right now the
25 software needs that in order to run.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: All right.

2 MR. TOROK: Okay, so --

3 MEMBER STETKAR: I was looking ahead, we're
4 going to get into nuts and bolts from MIT here, which is
5 essentially Chapter 4 of your report. I like to say
6 this, I like this report.

7 MR. TOROK: Thank you.

8 MEMBER STETKAR: One of the reasons I like
9 this report is not so much the inventory of the stuff that
10 we're going to be getting into, is that in Chapter 3, if
11 you go back to your Slide 7, which you put, you kind of
12 went through, well what's the level of interest here.

13 I looked at the report differently.
14 Because that Chapter 3 says, well we really need to focus
15 on an analysis of the plant functions. Which is what
16 this slide is getting into.

17 And I thought later in the presentation you
18 would talk a little bit more about that, but apparently
19 not. But it pervades everything.

20 MR. TOROK: Yes.

21 MEMBER STETKAR: You say, well I need a
22 function analysis and then within that construct, I need
23 you to develop sort of this highlight.

24 MR. TOROK: Yes.

25 MEMBER STETKAR: And that's one of the most

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 useful, I think, concepts in the whole report. I think
2 it presented really, really well.

3 And I just wanted to make that statement
4 because I think some of the discussion we had this morning
5 kind of glossed over that. And I think you're
6 characterizing it as level of interest may, that term
7 isn't used in the report or I don't recall seeing that
8 term in the report.

9 MEMBER BLEY: Oh, it's in there.

10 MEMBER STETKAR: Is it, okay. Perhaps I
11 glossed over it.

12 MEMBER BLEY: It must mean it made a lot of
13 sense to if you missed it.

14 MEMBER STETKAR: Well it did actually.

15 MR. TOROK: Maybe if you had emphasized
16 that more than if you're saying --

17 CONSULTANT HECHT: Can I suggest that for
18 other things that would make it cooler and stick out more
19 as one read it --

20 MR. TOROK: Yes.

21 CONSULTANT HECHT: The level of interest
22 seems to strike me as something that you're worried about
23 some 20-year-old singer doing something interesting,
24 that's a level of interest.

25 But other terms that are used are level of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 extraction, you know --

2 MEMBER STETKAR: No, no, you don't want to,
3 don't make this freaking theoretical --

4 (Simultaneous speaking)

5 MEMBER STETKAR: Keep the notion that it's
6 an integrated analysis that you're looking at functions.
7 Like this drawing shows.

8 CONSULTANT HECHT: Okay.

9 MEMBER STETKAR: You don't like the level
10 of interest. And don't, you know, trivialize it by
11 saying 20-year-olds or anything like that. It honestly
12 says to draw your attention to this construct.

13 CONSULTANT HECHT: Okay. Well, the point
14 I wanted to make is that there are two other terms of art
15 that are used in the industry. One is --

16 MEMBER STETKAR: And that's part of the
17 problem and that's the point I'm trying to make. Is the
18 terms of the art are both confusing and trivialize
19 things. Period.

20 CHAIRMAN BROWN: I agree with John on the
21 level of instruction just used in the word, the word
22 extraction is used in the report and I kind of got lost
23 on what the point was --

24 CONSULTANT HECHT: There's another term
25 which is used by the DoD and it's called level of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 indenture.

2 MEMBER STETKAR: That's fine. You know
3 I'll call it Rowdy rather than Ralph.

4 MEMBER BLEY: I have no idea, indenture?

5 CONSULTANT HECHT: Yes.

6 MEMBER STETKAR: You don't know what that
7 means?

8 MEMBER BLEY: Well --

9 MEMBER STETKAR: The concept is the
10 important concept and that's, the only reason I wanted
11 to raise this is I started flipping through the slides
12 and we're very quickly getting into FMEA's surf water
13 systems.

14 MR. TOROK: Yes.

15 MEMBER STETKAR: You know, all of those
16 examples that I think are really useful down in Chapter
17 4 to demonstrate benefits and perhaps weaknesses in these
18 various methods that you've presented.

19 MR. TOROK: Yes.

20 MS. SUBHAM: But as I read the report in
21 sort of a unifying theme, and perhaps I'm biased, was this
22 notion that no matter what of these tools you use, either
23 individually or in combination, you need to kind of keep
24 this, and I'm avoiding a particular term here by,
25 intentionally --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. TOROK: Yes, yes.

2 MEMBER STETKAR: -- this type of
3 perspective. So I just wanted to make that comment
4 because I thought perhaps you were going to talk a little
5 bit more about it later and you're not.

6 MR. TOROK: Yes. Bruce, you wanted to say
7 something?

8 MR. GEDDES: Yes, if I can, my background
9 is in plants and I work for some vendors, but I'm an I&C
10 guy. Born and raised dealing with various I&C issues.

11 I work with Dave, we've been working off and
12 on with various projects over the years and we find that
13 when I talk I&C, often that what's obvious to me is not
14 obvious to others. And then when Dave talks PRA, it's
15 obvious to Dave, it's not obvious to me.

16 So for six months we kept trying to come up
17 with some kind of unifying picture or terminology. And
18 these terms aren't sacred, you know, this is just a
19 construct that we found useful because I would say, well
20 we're analyzing the system failure modes, and Dave's
21 automatic response was, what system are you talking
22 about? The digital system or the plant system.

23 You know, I've worked with vendors. We do
24 FMEAs on the system. Well that's the platform, that's
25 the off the shelf technology that may not have any

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 application code in it yet. So that's the system from
2 their point of view.

3 And this is probably Rev 5 or 6. The first
4 four or five versions of this drawing were on the cutting
5 room floor. We don't want to show it to you because it
6 would confuse you as much as it would confused us.

7 MR. TOROK: Yes.

8 MR. GEDDES: So if resonates not with us,
9 and it's interesting that it seems to resonate with you
10 too. At least as a useful illustration of, what band in
11 this figure are you focused on?

12 And some methods are designed more at the
13 bottom. They're more applicable and useful at the
14 bottom and some methods of course are more useful.

15 And then some methods tend to span the whole
16 range, which is kind of a mind bending thing, so that's
17 where we ended up. And, John, I guess you had a comment
18 that you wanted to make?

19 DR. THOMAS: Well I think we might, I won't
20 to speak to all the methods but for STPA in Slide 21 I
21 think we may come back to this, talking about --

22 MEMBER STETKAR: Okay, that's fine. I
23 didn't --

24 DR. THOMAS: We'll come back to --

25 MEMBER STETKAR: -- leaping through this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 stuff.

2 MR. GEDDES: But John is right, there's a
3 whole subsection in Chapter 3 about this notion as a
4 precursor, before you get into any specific method.

5 I'd also like to comment, it's EPRI research
6 sponsored by EPRI members and we've learned to try to
7 avoid shelfware. And one of that --

8 CHAIRMAN BROWN: What's that? Shelfware?

9 MR. TOROK: Shelfware, that's when they
10 take a 400 page report --

11 CHAIRMAN BROWN: And put it on the shelf.

12 MR. TOROK: Yes.

13 CHAIRMAN BROWN: I see, I got it.

14 MR. TOROK: And say, I don't have time to
15 read that.

16 MR. GEDDES: And the feedback has been,
17 give us work examples, give us a procedure, give us a
18 rational explanation, avoid something that is too
19 academic.

20 For example, we talk about system theoretic
21 process analysis. When we're talking to utility
22 members, if we use the term, theoretic, it tends to evoke,
23 you know, I have to hire a PHD from MIT to do that. And
24 the answer is no, that's not true.

25 It's a very practical, implemental method

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that's accessible to a wide range of people. I was
2 skeptical when I first got involve and I went to an MIT
3 workshop and after a couple of days of listening to other
4 practitioners doing this, and it is mature in a lot of
5 ways.

6 It's novel, from our point of view in the
7 nuclear industry it's a new thing. But I was really
8 struck that this is something I might be able to figure
9 out how to do, with a little help from my friend, but we
10 feel compelled by these new approaches to attach the
11 notion of, where are the hazards and how can hazards lead
12 to losses or accidents or defeating or inhibiting safety
13 functions.

14 That seems to be the really payoff here.
15 And this picture helps us navigate those discussions so
16 we can always come back and get grounded when we get lost
17 in the minutiae. Does that help, John?

18 MEMBER STETKAR: Yes, it does, I think.

19 MR. TOROK: Okay and from a --

20 MEMBER STETKAR: I'm sorry, Charlie, I've
21 got to stop talking.

22 CHAIRMAN BROWN: No, no, I don't disagree
23 because I liked that diagram, that flow down diagram,
24 because it started with, what I want my plant to do and
25 then showed the elements as you went through.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BLEY: I just want to talk about this
2 a little bit because I saw it first because I started in
3 Chapter, in Appendix B or whatever the heck it is back
4 here.

5 MR. GEDDES: The tech --

6 MEMBER BLEY: Yes, and there when I ran
7 across it it was hard to grasp. When you go back and look
8 at Chapter 3 --

9 MR. TOROK: It's tech.

10 MEMBER BLEY: -- it's very natural and I've
11 worked in several other areas with multi-disciplinary in
12 coming up with a language that everybody can get along
13 with. And I think it's pretty transparent reading
14 through Chapter 3 and then on.

15 It's not something that gets in the way and
16 it helps. The old language is closer to the language I'm
17 use to but every one of those three terms use to use, have
18 different meanings to lots of different people.

19 MR. TOROK: Yes.

20 MEMBER BLEY: So, the other thing I really
21 like about it is it says you have to keep an integrated
22 system in mind when you're doing any of this analysis and
23 I think that's crucial.

24 MR. TOROK: Right, so --

25 MEMBER BLEY: That's the thing we forget.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. TOROK: From EPIR's standpoint here
2 we're trying to find methods that work, but then maybe
3 the bigger challenge for us to communicate those to the
4 guy, our guy who need them, and to convince them that they
5 can actually go out there and do it themselves.

6 And that's why the report has things like
7 this. It's got procedures, step by step procedures and
8 worked examples. And so what we're trying to do is
9 communicate. Okay, so, are we okay with this for now?

10 CHAIRMAN BROWN: Yes, I want to ask, before
11 you get into the nitty gritty, just one other relative
12 to the higher level. Back to the animal of goodies
13 before we started doing digital stuff in 1978 for the
14 Naval nuclear program, we used a, we required FMEAs as
15 part of our generally specifications for all of the
16 hardware, regardless of what the system, each system for
17 the plant monitoring, for the protection, for the level
18 controls, etcetera.

19 MR. TOROK: Sure.

20 CHAIRMAN BROWN: And every time we got into
21 a money bind, in other words the price for doing the
22 whole, you know, all the designs, you go back to the
23 vendors and say, hey, look guys, all of you are a little
24 bit pricey, what was, the first thing they grabbed was
25 the FMEA requirements.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Get rid of it because it was laborious, time
2 consuming, personnel consuming and the dollars, once you
3 start throwing people at it, particularly in the '70's,
4 we didn't have the computers that you have now. And I
5 don't know if that helps it or makes it worse, probably
6 makes it worse, and that's what they want.

7 But we kept it and tried to reduce the scope
8 so that we could fundamental say, hold it. Back in those
9 days we thought the more parts you had and stuff the less
10 reliable you were going to get.

11 That was the mindset of some folks, not all
12 of use subscribed to that but we did get some of the
13 systems simplified by looking at parts failures going up
14 from the bottom up. And made the system, made the
15 compliments, the boards a little bit simple.

16 But I haven't heard anything, we did make
17 mention in here in your report about cause. And is
18 there, well I forget, maybe it was one where the NRC
19 reports, you know, that followed this. I don't remember
20 which one it was after reading them all or part of them.

21 Did you all address that at all in this
22 general thought process? In other words, if I'm going
23 to implement these methods, how do we prepare
24 recommendations that make sure the value added, we put
25 in the value added parts of these things and don't have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 all the, back hold the tales?

2 MR. GEDDES: I think that's a great segue
3 into a portion of this presentation that talks about
4 blended approaches. Given any given method, you can
5 take it to some infinite degree and get to some asymptotic
6 limit on value, some results.

7 And I give Dave a lot of credit, he really
8 forced us to address that problem. And so the idea is
9 maybe there is a blend of methods where a good reasonable
10 effort on one method combined with a good reasonable
11 effort on another method, takes less effort overall than
12 taking any single method to the nth degree.

13 And that doesn't speak to cost or
14 necessarily level of effort, but there is an objective.
15 One of the objectives of this project was to come up with
16 guidance and do some research and development, develop
17 guidance so that there is a more practical pragmatic and
18 cost effective way to get a higher level of coverage.

19 Can we find these corner cases and edge
20 cases or hazards things happen and the OE bares that out
21 without turning over the science project or a 10,000 page
22 FMEA? That was the feedback that we got.

23 And that's been experienced by the way. So
24 we think the blended approach, and jump in if I'm not
25 getting this right, but the blending of two or more

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 methods gets to that problem, we think.

2 MR. TOROK: We'll, Dave will talk about
3 that later but --

4 MR. BLANCHARD: We'll talk about strengths
5 and limitations of each approach.

6 MR. GEDDES: All right.

7 CHAIRMAN BROWN: All right, well we've done
8 nine pages here in an hour and a half and we've got 32
9 more to go, if I do the math right in this, aside from
10 the operating experience part.

11 MR. TOROK: Yes.

12 CHAIRMAN BROWN: So we need to get on to it.
13 So I will ask you to proceed.

14 MR. TOROK: So the approach we took here,
15 we were not that familiar with some of these methods and
16 we said, hey, let's look at these methods as applied to
17 realistic new way to find problems. So we ended up with
18 a, sort of a simple one and more complex one.

19 We saw difference depending on that and so
20 we'll get into that stuff. So with that I want to turn
21 this over to Bruce who will explain the first set of
22 example anyway.

23 MR. GEDDES: Okay, this example is --

24 CHAIRMAN BROWN: Wait a minute, one thing.
25 As you go through these we're going to take a break at

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 some point, but I want to finish one, at least I don't
2 want to break in the middle of one of your, if you go from
3 example to example. So tell me when is the appropriate
4 time to break because we're kind of into that zone right
5 now.

6 MR. GEDDES: Well --

7 CHAIRMAN BROWN: A lot of you guys have
8 had --

9 MR. GEDDES: Now could be a good time if you
10 like? There is some continuity through the, at least the
11 next few slots.

12 CHAIRMAN BROWN: Pardon?

13 MR. GEDDES: There is some continuity in
14 the next three or four slides. So now could be a good
15 point or we could wait until the next break point.

16 CHAIRMAN BROWN: Okay, if you want we could
17 take, we'll take a break now for 15 minutes. We'll come
18 back at 10:12. How about that?

19 MEMBER STETKAR: Jesus.

20 CHAIRMAN BROWN: I don't have a --

21 (Simultaneous speaking)

22 CHAIRMAN BROWN: -- and this clock is off
23 by about --

24 MEMBER STETKAR: Oh, yes, I noticed, it's
25 off by about five minutes as a matter of fact, so.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 (Whereupon, the foregoing matter went off
2 the record at 9:53 a.m. and went back on the record at
3 10:11 a.m.)

4 CHAIRMAN BROWN: The meeting will come back
5 into order and we will proceed. I believe Bruce Geddes
6 was chatting at the time and I believe he's still up.

7 MR. GEDDES: All right, so this is one of
8 our first examples. We have two examples baked into the
9 report, the EPRI report.

10 And the idea was pull real-life examples
11 from the OE data that we'd already done research on that
12 we thought might be interesting and then apply each of
13 the six methods to each example to see what we learned,
14 and that's how we helped identify strengths and
15 limitations through our own practical experience.

16 This particular example's based on a
17 reported event with a turbine speed control system that's
18 part of a larger nested flow control system. Here we see
19 a BWR with pumps and valves in a turbine and the flow
20 control system's the blue box in the middle of the
21 diagram.

22 Essentially it takes a flow signal from the
23 output of the pump, the pump discharge flow, and
24 calculates a response to a fixed setpoint. For
25 high-pressure coolant injection, we came up with 5,000

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 gpm. For reactor core isolation cooling, Dave, what's
2 the typical setpoint?

3 MR. BLANCHARD: For?

4 MR. GEDDES: For RCIC.

5 MR. BLANCHARD: Flow?

6 MR. GEDDES: Flow.

7 MR. BLANCHARD: Yes, around 400 gpm.

8 MR. GEDDES: Four hundred gpm. So the
9 output from the flow control system is a demand signal
10 that goes to a governor valve. Now, in this system there
11 are three valves that are in series to provide steam to
12 the turbine.

13 The first valve coming in is what we're
14 going to call the steam admission valve. That takes a
15 signal, a safeguard signal, and opens when there's a
16 demand. For example, Dave, what's a typical demand for
17 HPCI? What's an initiating event?

18 MR. BLANCHARD: Low reactor level.

19 MR. GEDDES: Low reactor level. So
20 there's a low reactor level. That system initiation
21 signal comes in, opens the steam admission valve.

22 Now, you notice there's a limit switch on
23 that valve. When that switch changes state, it provides
24 an enable signal to the flow control system. Now, this
25 is a digital flow control system. This is after an

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 upgrade has been done in an actual operating plant.

2 The trip and throttle valve, if things are
3 reset, that valve is open and in the new digital system
4 the governor valve starts from a closed position, so
5 that's the setup.

6 Of course, other valves are in this system.
7 Those valves also change position on a demand signal but
8 our interest is in this digital flow control system and
9 how it might behave, or how we could assess its design
10 and characteristics using different methods, all right?

11 So one of the six methods in this report is
12 called the functional FMEA. We have an EPRI member who
13 came to several of our project meetings and said I just
14 got back -- sorry?

15 CHAIRMAN BROWN: Do we have a problem with
16 the slides?

17 MR. GEDDES: No.

18 CHAIRMAN BROWN: Oh, you shifted pages,
19 okay.

20 MR. GEDDES: Yes.

21 CHAIRMAN BROWN: I thought that was the
22 first -- oh, that's your next slide.

23 MR. GEDDES: I'm on the next page. I'm on
24 Slide 10.

25 CHAIRMAN BROWN: Go ahead, go ahead.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. GEDDES: Okay.

2 CHAIRMAN BROWN: I apologize.

3 MR. GEDDES: So in a project meeting
4 recently, before we published the final results, she said
5 I just got back from FMEA school. I said okay, what was
6 that? She said, they introduced the concept of a
7 functional top-down FMEA.

8 And I'm a bottom-up, design up -- I was born
9 and raised as an I&C guy. I've done FMEAs. I've
10 reviewed FMEAs. I've required them and looked at them
11 from vendors. I said this is a different idea. This is
12 something new to me.

13 So we explored it on this example and came
14 up with some interesting results. This functional FMEA,
15 you take this example and lay it next to this construct,
16 what we call the level of interest construct, and now
17 we're looking from the top down at failure effects,
18 failure modes and the mechanisms or causes. Functional
19 FMEA is causal to some extent.

20 So we evaluated postulated functional
21 failures at the plant system level and dug in and found
22 some potential causes of those functional failures.

23 Now, this is an I chart. This is a
24 functional FMEA worksheet for this example. We're not
25 going to go into every row and every column, but we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 provided a template in the guideline and a procedure for
2 how to fill out the template and generate the results and
3 make use of them.

4 In this case, now we're talking about a
5 basic function. That first column is high-pressure
6 injection. That's a basic function. We're not
7 allocating functions to hardware or software. We just
8 want water in the core. We want to inject water under
9 high pressure.

10 There are four processes listed in the next
11 column and then functional requirements in the next
12 column and then we get into potential failure modes at
13 the functional level.

14 We're not talking about digital processors
15 or RAM or ROM or task crash or any of those things. This
16 is from a top-down, functional abstract point of view,
17 functionally abstract.

18 Now, what's interesting in this functional
19 FMEA process, we did find an industry standard that comes
20 out of the automotive industry where a lot of interesting
21 work is being done with automation. John's been
22 involved in some of that in his work at MIT.

23 There are key words in this method, you
24 know, and we can say what can go wrong? So given a
25 functional requirement, what happens if that functional

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 requirement's not met? What happens if it's partially
2 met? What happens if there's too much of it? What
3 happens if it's degraded or intermittent or unintended
4 or maybe spurious?

5 And then we go from left to right across the
6 worksheet and we get into, you know, what are the effects
7 of those functional failures? So these key words guide
8 the analyst through these various scenarios.

9 And then we get into potential failure
10 mechanisms and then what methods of prevention or
11 detection are already available for dealing with those
12 functional failures, and then the analyst can provide a
13 recommended action.

14 I found a functional failure mode,
15 notwithstanding hardware/software, but in this proposed
16 control system I found a functional failure mode that
17 bears further investigation because I haven't found a
18 readily available design measure or method of prevention
19 or detection. It could be an administrative control or
20 other feature in the system.

21 So the end result is to inform the design,
22 inform the plants on the functional failures that are
23 manageable or not and carry forward into the design
24 process for the proposed upgrade. Myron.

25 CONSULTANT HECHT: I just wanted to say

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that the functional hazards, what you call functional
2 FMEA, is called the functional hazard analysis and it's
3 called the SAE-4754, which is used by the FAA for aircraft
4 certification.

5 And it's also referred to as a subsystem
6 hazard analysis in MIL standard 882 so it does have, you
7 know, heritage.

8 I was kind of intrigued by the fact that you
9 are calling it a top-down method because if I certainly
10 look from the fourth column over it looks like any other
11 FMEA.

12 MR. GEDDES: Well, we had that discussion
13 amongst ourselves. Let's go back to this level of
14 interest diagram. When we say top-down, we're proposing
15 functional failures at the top of this diagram and then
16 getting into the details. That's all we mean by top
17 down.

18 CONSULTANT HECHT: Okay, because both the
19 values of the FMEA is that, you know, when you want to
20 blend methods, each method gives you a certain level of
21 --

22 MR. GEDDES: Coverage.

23 CONSULTANT HECHT: -- of coverage that you
24 completed something so that you can say that you've
25 touched every item.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. GEDDES: Yes, that's what we're after.

2 CONSULTANT HECHT: So the point is that I
3 think about a top-down approach as not necessarily
4 touching every item but touching every concern.

5 MR. GEDDES: Well, we have a section in the
6 report on blending the results of various methods to get
7 to that full coverage from the top to the bottom of this
8 hierarchical diagram. That's why we wrote that section.

9 CONSULTANT HECHT: Right, I'm aware of that
10 but perhaps it's maybe a, I mean, maybe it's a discussion
11 that we don't need to get into but it seems to me that
12 from the place where you have requirements, which I guess
13 is the third column to the right, you can say whether
14 you've gotten every requirement or not.

15 MR. GEDDES: John, how would you respond to
16 that?

17 DR. THOMAS: Well, I mean, there is a little
18 bit of semantics going on here. But the way that I would
19 classify this, it does start with a functional
20 decomposition which you could argue is top down.

21 But a lot of the analysis itself proceeds
22 just like FMEA, starting from that decomposition and
23 moving forward, so as a bottom-up. The analysis itself
24 kind of proceeds in a bottom-up fashion, starting with
25 a specific function, identifying the modes of failure and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 then identifying the effects.

2 So, yes, so there is a little bit of
3 semantics going on but I think where this comes into play,
4 the part that we're getting at with top-down versus
5 bottom-up, it's going to come into play after we review
6 all the methods and we summarize them and we discuss
7 potential ways to put them together or try to leverage
8 benefits of multiple methods and things like that.

9 MR. GEDDES: Okay, moving on. We play the
10 same game with the same example but now using another
11 method in the report, what we're calling top-down using
12 fault trees, and I'll throw it to Dave to explain this
13 example.

14 MR. BLANCHARD: Okay, and obviously this
15 method uses fault tree logic in order to do a very similar
16 review of the system as was shown earlier in the
17 functional FMEA.

18 We begin with plant functions. They're
19 important for this plant system, the HPCI or the RCIC
20 system, and we work our way down to the trains of
21 equipment that make up the HPCI and RCIC system for each
22 of the functions it provides, and then down to the point
23 where we find the components that are controller actuated
24 by the digital instrumentation and control system.

25 Now, the guideline itself does not

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 encourage the development of new fault trees. When
2 implementing the top-down fault tree approach to
3 performing hazard analysis, I'd suggest you go talk to
4 the PRA folks because they've got a lot of these already
5 developed.

6 MEMBER STETKAR: Dave, let me stop you
7 right there because I read that and we're not developing
8 a tutorial here for fault tree analysis for pumps and
9 pipes and valves. We're trying to struggle with the
10 notion of digital systems and software.

11 One of the things I found is that if --
12 forget digital systems or software for the moment and
13 just think about fire analysis. Many times when we start
14 doing a detailed fire analysis of a plant, we find that,
15 indeed, the developers of the PRA models who focused only
16 on internal events and particular failure modes have
17 missed things.

18 For example, a normally open valve that
19 could close spuriously might not be in that fault tree
20 and yet that failure mode might be excited by many
21 different fires in many different locations, so people
22 have needed to go back and think carefully about those
23 models.

24 MR. BLANCHARD: Right, they didn't, they
25 function like --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MEMBER STETKAR: I didn't get quite that
2 notion reading through the report. It said basically it
3 presumed that the PRA fault trees had 100 percent
4 coverage of every conceivable failure mode for every
5 conceivable -- my experience is that's not necessarily
6 always the case.

7 MR. BLANCHARD: Right, for the sake of
8 building fault trees that are manageable in applications
9 in the future --

10 MEMBER STETKAR: No, no, no. We're
11 talking about --

12 MR. BLANCHARD: -- we leave things out that
13 we know ahead of time --

14 MEMBER STETKAR: No, we don't know.

15 MR. BLANCHARD: -- don't necessarily
16 contribute to risk of the internal events period.

17 MEMBER STETKAR: We don't know that
18 necessarily unless we examine. I've found people who
19 have left failure modes out because they didn't think
20 they were going to be important and didn't examine
21 whether they were and, lo and behold, when they put them
22 in they were important.

23 So be careful, I think, a little bit about
24 you picking up something that somebody has created and
25 presuming that, indeed, it covers everything that you're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 interested in. That's just one of the dangers that come
2 about.

3 MR. BLANCHARD: I agree with that but,
4 nevertheless, the PRA at this point in time already
5 develops a structure that is very useful in continuing
6 the hazard analysis.

7 MEMBER STETKAR: It certainly is very
8 useful. My only caution is it's not necessarily always
9 complete --

10 MR. BLANCHARD: Right, I agree with that.

11 MEMBER STETKAR: -- because it still
12 depends on the individual analyst's decisions, and
13 sometimes they're not written decisions, about creating
14 those models and we have a lot of experience with them.

15 And only reason I bring it up is because some
16 of the types of, I'll try to be careful here about using
17 words, conditions that can be created by instrumentation
18 and control system malfunctions are pretty doggone
19 subtle and they're things that, as you mentioned, an
20 analyst might decide, well, that can't be very important
21 if I'm only looking at a specific set of other conditions.

22 MEMBER BLEY: You're going to get here
23 eventually but you don't have to back up to your
24 functional failure modes and effects analysis, if that's
25 what you called it. Something very similar to that, to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 me, is a precursor to doing the PRA kind of analysis.
2 However you organize it, it's the very things that are
3 on here.

4 If you've done a really good job, it's got
5 these other failure modes and the reason why you've
6 dismissed them. There might be clumps of them but if we
7 left out pipe breaks of a certain size, we left out valves
8 that are normally open, they won't get signals normally.
9 But then you've got a catalogue so if you come to do the
10 fire analysis or something else, you know what you left
11 out and you got to put back in.

12 Or if you do fixes to the plant and all of
13 a sudden your risk drops real low, well, maybe there were
14 things you left out that would make that not so.

15 So the idea of blending is something I
16 think's always been there and something like that
17 functional failure modes and effects analysis should
18 have preceded fault tree analysis all the time. Now, it
19 might not have been so formal and laid out just the way
20 you did it, but it's always in there.

21 And just one last aside, I like what Myron
22 said, except the failure modes and effects analyses I was
23 talking about that I've seen, and I've seen them in
24 several industries, they didn't start from there, from
25 the functional point of view.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 They started with every little widget in the
2 plant and that's thousands and thousands and thousands
3 of them, and if you start from that point, that's where
4 you get the ones I was talking about that I don't see much
5 gain from.

6 If you start from something like the fourth
7 column here where you're thinking of what things have to
8 happen and how you can then develop failure modes that
9 can get you in trouble, that's extraordinarily helpful
10 I would think so clarifying what I said earlier. And I'm
11 sorry for the diversion but head back into it.

12 MR. BLANCHARD: No, that's fine.

13 CHAIRMAN BROWN: Okay, now I'm going to ask
14 a question because I'm trying to look and connect between
15 the functional FMEA presentation that you gave, the
16 worksheet and where you started, and then I shift to the
17 top-down, the fault tree analysis approach.

18 And I look at that worksheet and I can't
19 connect a start point back into -- was this a part of the
20 blended approach or was just a fault tree analysis
21 approach? And I think it was just an FTA approach to the
22 HPCI system which --

23 MEMBER BLEY: Right, but just to a piece of
24 it.

25 CHAIRMAN BROWN: Well, but this is just one

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 page, I mean, one piece. I understand that. But when
2 I look at the two diagrams, not being a weenie on this
3 stuff, it's a subset.

4 Instead of the whole system you showed
5 before, you have only the little corner of the system over
6 here without focusing on the final things, which was the
7 high-pressure injection. It's only the producing
8 system itself. I just couldn't connect this diagram
9 with the others.

10 MEMBER BLEY: Before you answer, that
11 bothered me too. The first four columns of that
12 functional failure modes and effects table to me is the
13 top part of the fault tree, the functional definition of
14 it, and you don't get the connection without some
15 storybook.

16 MEMBER STETKAR: Well, but I think for the
17 purposes -- one is Chapter 4 and one is Chapter 5.
18 They're trying to demonstrate different methods and I
19 think we're suffering a bit from this presentation --

20 MEMBER BLEY: Nevertheless, just looking
21 at the other slide, it's hard to get a grasp that it is
22 knocked down except for the governor valve itself.

23 MR. GEDDES: This one?

24 CHAIRMAN BROWN: No, no.

25 MALE PARTICIPANT: No, the next one.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: The top down, the FTA
2 worksheet. Yes, right there. I mean, it just seemed to
3 start in the middle of the system over here. There's a
4 valve so I've got to operate those valves --

5 MR. BLANCHARD: If you go into the report,
6 what it actually does is it starts at the top of the plant
7 listing all the safety functions.

8 CHAIRMAN BROWN: Okay, so this is a --

9 MR. BLANCHARD: This is just a comment on
10 the --

11 MALE PARTICIPANT: This is just a snapshot.

12 MR. BLANCHARD: Right.

13 CHAIRMAN BROWN: All right, all right.

14 MR. BLANCHARD: And so there's about 15
15 pages of fault trees that precede this which I'm not sure
16 you would be interested in.

17 (Simultaneous speaking)

18 CHAIRMAN BROWN: You answered my question.

19 MEMBER BLEY: Well, what it really does is
20 sort of the logic you saw in the other chart to get down
21 to this one.

22 CHAIRMAN BROWN: But, yes, I'm looking for
23 a segue from this other chart over to this and I'm not
24 connecting those dots.

25 MR. GEDDES: Yes, we examined each method

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 in isolation to see what each method could tell us and
2 then later we looked at how to possibly blend methods,
3 and that's when we came up with this level of interest.
4 Where do they intersect?

5 And we struggled for a long time until we
6 came up with that hierarchy to show where there might be
7 points of intersection where the digital system can
8 actually start to influence plant components and plant
9 systems. That seems to be the nexus that Dave can get
10 to in this slide.

11 CHAIRMAN BROWN: All right. You can go on.

12 MR. BLANCHARD: All right? Well, once we
13 worked our way down from the plant-level functions
14 through the systems down to the point where we now want
15 to identify the components within the plant and within
16 the fault trees that are controller actuated by the
17 digital system, now there are quite a number of functions
18 other than injection to the reactor that the HPCI and RCIC
19 systems play a role in.

20 There's containment isolation. There's
21 primary cooling system isolation. There's even
22 pressure control functions in some situations. And so
23 all the functions are listed here on the table and, again,
24 we encourage taking advantage of information that exists
25 in the form of the PRA using the fault tree analysis

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 approach.

2 And so what we have listed here in this table
3 is a list of quite a number of the basic events that are
4 in the PRA with respect to the HPCI system, translating
5 that into their tag IDs and the failure modes that are
6 modeled in the PRA.

7 Now, there turns out to be another column
8 in our guideline that doesn't show up on this particular
9 slide that has to do with what plant-level function is
10 this particular component and tag ID failure mode playing
11 a role in?

12 And so out here on the right side what the
13 guideline suggests you do is you identify the function
14 you're talking about. Is it containment isolation? Is
15 it primary cooling system isolation? Is it reactor
16 inventory control? So there is an additional column in
17 the guideline that relates it back to the plant-level
18 functions.

19 And then if you can advance the slide a
20 little bit it turns out not all of these particular
21 components and their failure modes are affected by the
22 digital I&C that we're investigating.

23 In this particular example, only the
24 governor valve and its failure modes will be affected by
25 the digital I&C and so this component and its failure mode

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 would then become the focus of a further analysis,
2 perhaps using fault trees, to then get into the digital
3 system itself.

4 Now, the fault tree analysis part of the
5 guideline at this point says this is a possible
6 transition point to one of the other methods if you would
7 like.

8 If you're installing brand-new digital I&C
9 system, you likely don't have any logic in your PRA right
10 now associated with this. You can continue the approach
11 with a fault tree analysis on the digital I&C system
12 itself if you like or you might like to transition to one
13 of the other methods.

14 We don't go into detail in the guideline on
15 how you create fault trees. We do refer to other EPRI
16 reports on the development of additional fault trees if
17 you want to do that and, in particular, there's a couple
18 of EPRI reports that talk about modeling digital I&C
19 systems using fault trees with a reference at this point
20 in the guideline.

21 CHAIRMAN BROWN: At this point, though, I
22 still haven't seen a connection to the actual control
23 system itself, other than --

24 MR. BLANCHARD: That's right. What we do
25 at the bottom line on this table here is the next step

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 in the process is to translate this failure mode into the
2 digital system-level failure modes or behaviors, I
3 should say misbehaviors, that would cause this failure
4 mode of this component to occur.

5 At that point we move into the digital
6 system itself and having identified the digital system
7 misbehaviors that could cause these failure modes,
8 continue the analysis, either with developing a new fault
9 tree or by going to one of the other methods to doing a
10 hazard analysis.

11 MR. TOROK: But the point was the fault tree
12 focused you on the one thing. It could hurt you from the
13 high-level perspective.

14 MR. BLANCHARD: Right, and then force you
15 to translate that into a digital system behavior that
16 you're now most interested in continuing.

17 CHAIRMAN BROWN: So it's knowing.

18 MR. BLANCHARD: Yes. The top-down
19 approach, the purpose of it is to get a focus on what you
20 care about from a function and system level and the
21 functions and systems that are performed by plant
22 components that are controller actuated by the digital
23 I&C.

24 CHAIRMAN BROWN: Okay, now, why didn't the
25 FMEA, maybe I'm asking because I just don't understand.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 If I look at the worksheet, that approach, why wouldn't
2 that approach --

3 MR. BLANCHARD: Functional FMEA would do
4 something very similar.

5 MALE PARTICIPANT: Very similar, yes.

6 CHAIRMAN BROWN: Okay.

7 MR. BLANCHARD: The detailed FMEA
8 wouldn't.

9 CHAIRMAN BROWN: I would expect it to, but
10 go ahead. I'm sorry.

11 MR. BLANCHARD: The detailed FMEA
12 wouldn't. The detailed FMEA --

13 MALE PARTICIPANT: I'm talking about the
14 functional.

15 MALE PARTICIPANT: Right, right.

16 MR. GEDDES: You'll notice there's a
17 comment in the functional FMEA worksheet that says we
18 might want to look at this particular functional failure
19 mode when we go do a design FMEA, the bottom-up FMEA, on
20 the digital system. That's the connection point. In
21 other words, this method only gets you through the upper
22 half of that hierarchical structure.

23 CHAIRMAN BROWN: So you're looking at that
24 last column then where it says, "Evaluate flow control
25 system failure modes via design FMEA."

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. GEDDES: Yes.

2 CHAIRMAN BROWN: That's the point you're
3 talking about?

4 MR. GEDDES: Yes, sir. And I think the
5 functional, sorry, the top-down fault tree analysis
6 method is another way to get there.

7 So the reason why we included both methods
8 is that if an engineer has a preference for functional
9 FMEA because it's something that he can grasp and
10 implement, there's a procedure and some work examples on
11 how to do that.

12 To Dave's approach, if you have fault trees
13 that are readily available, the I&C engineer needs to go
14 find the person who owns that fault tree and ask a couple
15 of good questions and then start with a set of information
16 that doesn't require a bunch of additional analysis, it's
17 readily available, and then take it from there.

18 So it gets to the cost and level-of-effort
19 issue. If you have readily available information, maybe
20 there's a way to use it to narrow the search for the
21 critical failure modes that you need to be concerned
22 about. Isn't that right, Dave?

23 MR. BLANCHARD: Yes. So the strengths of
24 this approach are that it gives you an integrated view
25 of plant design. It's not limited to single failures

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 like the FMEA may be.

2 MEMBER STETKAR: Get to the next slide.
3 I've got a few, and I hate to do this because I'm kind
4 of a detail -- right there. That's good.

5 MR. BLANCHARD: The circ water?

6 MEMBER STETKAR: Right.

7 CHAIRMAN BROWN: You're shifting that,
8 right?

9 MR. BLANCHARD: Yes.

10 MALE PARTICIPANT: No.

11 MR. BLANCHARD: No, no. We're going to --

12 MEMBER STETKAR: Just bear with me here.
13 Just look at this picture, please.

14 CHAIRMAN BROWN: I have. I looked at it a
15 lot.

16 MEMBER STETKAR: It's the circ water
17 system.

18 CHAIRMAN BROWN: Yes.

19 MEMBER STETKAR: Not the HPCI system.

20 MALE PARTICIPANT: Right. It's different
21 systems now, what I'm saying.

22 MEMBER STETKAR: First time we've seen
23 this. Now, the reason I wanted to do this is that it's
24 a little, in some sense, less complicated than the
25 HPCI/RCIC systems, the way they're presented. And it a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 little bit better illustrates some of the higher level
2 I&C stuff that Charlie likes to focus on. In today's
3 presentation you didn't walk us through the FMEA for this
4 system.

5 MR. GEDDES: The design FMEA?

6 MEMBER STETKAR: You didn't walk us through
7 the FMEA for this system.

8 MALE PARTICIPANT: That's right.

9 MEMBER STETKAR: Notice I didn't use the
10 word design or function because I get confused about
11 those things, so you didn't walk us through an FMEA for
12 this system.

13 In the examples, and it's a good example and
14 I like this picture because you can see it a little bit
15 easier. In the examples in the report, the FMEA for the
16 circ water system, there's only one, it says the
17 functional FMEA, just like the design FMEA, if I follow
18 correctly, when it gets to things like -- now, Charlie,
19 in this system the stuff on the left is normally running.
20 The stuff on the right is redundant.

21 CHAIRMAN BROWN: Got it.

22 MEMBER STETKAR: The pink stuff is
23 redundant.

24 CHAIRMAN BROWN: Okay, I got that.

25 MEMBER STETKAR: It's stand by. The FMEA,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 limitation of the FMEA says, well, if I have failure of,
2 let me just call it Logic Cabinet A kind of stuff, the
3 FMEA conclusion is slave controller in service or slave
4 controller takes over and there's no affect on the
5 system. That's the end of the FMEA.

6 In other words, it says if I have a failure
7 in the little blue boxes there, there's no problem on the
8 system because the pink boxes are guaranteed to always
9 work.

10 And that's a limitation of the FMEA because
11 the FMEA process, as it's presented in this report,
12 strictly focuses only on single failures.

13 MR. GEDDES: Single failures.

14 MEMBER STETKAR: Now it didn't, for some
15 reason, and I don't know why it didn't ask when there's
16 a failure in the pink box which would give you also a
17 failure in the blue box and a failure of the whole system.
18 So I'm not sure why nobody asked that question in the
19 FMEA, which is a question I would have asked. You didn't
20 ask it.

21 CHAIRMAN BROWN: Okay, can I -- are you
22 done?

23 MEMBER STETKAR: I am done with this.

24 CHAIRMAN BROWN: Okay. Let me add, that
25 brings up a question in terms of the thought process.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: These are the thought
2 process. That's where I'm going to get to here.

3 CHAIRMAN BROWN: Yes, no. Well, I'm good.
4 Okay, well, I was involved with a system where we needed
5 to maintain output voltage for a turbine generator --

6 MEMBER STETKAR: Let's focus on this
7 system.

8 CHAIRMAN BROWN: Hold it. It's the same.

9 MEMBER STETKAR: Okay.

10 CHAIRMAN BROWN: It had a dual voltage
11 regulator, sitting right like this. Had an A and a B,
12 but it didn't do what you just said. When we looked at
13 it we said, okay, here A is running. We know whether B
14 is running or not because there's a little bit of thing
15 going on.

16 And if A fails, it'll transfer to B if it,
17 you know, if this interrelation communication says B is
18 okay. B is not okay for some reason, it did something
19 else.

20 In other words, we covered that but not, it
21 was just a thought process. We said, well, gee, what if
22 the backup of the slave is not -- because you had to make
23 this transition in about five milliseconds to not dump
24 the plant, so it had to be very responsive.

25 And I gather from your comment that, gee,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I would have just stopped right there and I'm just
2 wondering don't people think about what if the other box
3 is not working or didn't you just get there and I
4 interrupted you?

5 MEMBER STETKAR: Yes, you did and that's
6 why I wanted to keep focusing on this, that you're here.

7 The point is that the example, given the
8 fact that you defined an FMEA is to look at only single
9 failures from one perspective, has that limitation.

10 MALE PARTICIPANT: Yes.

11 MEMBER STETKAR: It presumed that the pink
12 always works.

13 MALE PARTICIPANT: Yes.

14 MEMBER STETKAR: Because it's only
15 developed from the perspective of if this normally
16 running thing fails what is the effect?

17 Now, I don't know why the FMEA did not
18 challenge anything in the pink, and it didn't. It did
19 not challenge anything in the so-called standby backup,
20 whatever you want to call it, controller.

21 MALE PARTICIPANT: But it could.

22 MEMBER STETKAR: It could, in principle,
23 but it didn't. So that perhaps is a limitation in, and
24 here's the important thing, the person implementing the
25 FMEA process, not the FMEA itself.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CONSULTANT HECHT: That's what I would have
2 thought.

3 MEMBER STETKAR: That's fine. That's
4 fine, but it is important. It's also important, I think,
5 if you're developing -- one of Ray's initial comments was
6 he wanted to make this a practical set of guidance for
7 people who are actually doing things.

8 And I think as soon as you say that, your
9 examples become very, very important, okay, because I,
10 as a marginally trained poor power plant analyst, would
11 say, okay, EPRI just told me this is the way to do an FMEA,
12 right?

13 MALE PARTICIPANT: Yes, well --

14 MEMBER STETKAR: Okay, I was taught now not
15 to think about failures in the pink that could also feed
16 back into the blue and affect the whole system by your
17 example.

18 MR. GEDDES: That's true.

19 MEMBER STETKAR: Okay, thanks.

20 MR. GEDDES: But we also advocate that it's
21 not the only way to skin a cat.

22 MEMBER STETKAR: Right. Right, you're
23 absolutely right and the benefit from the fault tree
24 approach that I'm going to start dealing with in a second
25 here --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. GEDDES: Given multiple concurrent
2 failures.

3 MEMBER STETKAR: -- is that the fault tree
4 approach would look at both of those values. It would
5 allow the pink to fail in combination with the blue for
6 a variety of different causes. One cause might be a
7 common fault in the same software that's used and, in
8 fact, the fault tree example develops some of that.

9 MR. GEDDES: Dave showed us some cuts sets
10 --

11 MEMBER STETKAR: So that's one of the
12 benefits of that fault tree approach and it's one of the
13 limitations on the FMEA and the reason I want to go to
14 this is at a high level it sort of shows you that
15 difference.

16 MR. TOROK: FMEA doesn't necessarily look
17 at multiple faults, although it could, right?

18 MEMBER STETKAR: It could in principle.

19 MR. TOROK: But fault tree does.

20 MEMBER STETKAR: Fault tree does.

21 MR. TOROK: We saw that as a big advantage
22 for fault tree.

23 MR. GEDDES: In practice. We had seen some
24 what we'll call design, bottom-up FMEAs that begin to
25 attempt to address the issue of common cause failure or

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 multiple concurrent failures. And the way the
2 worksheets and the procedures are laid out, they're
3 really designed to help you assess against a single
4 failure --

5 MEMBER STETKAR: Right. Exactly right,
6 and the report makes that point, by the way, quite well.

7 MR. GEDDES: Yes. That doesn't mean you
8 can't go beyond that but in practice it becomes difficult
9 and probably easier to transition to something like fault
10 tree and start to look at cut sets.

11 Dave looked at this and pulled out some
12 fault trees and gave us some cut sets and I guess, Dave,
13 your immediate reaction was holy cow, look at this. We
14 have some pairs that should direct the attention of the
15 I&C design people to those pairs.

16 This is based on some OE, okay? This
17 example's also based on a plant trip that we evaluated
18 with a researcher from that utility who gave us some
19 tremendous insights, so it's compelling and this
20 particular example also gets into some architectural
21 issues.

22 But notwithstanding, Dave showed us some
23 cut sets and I said, well, gee whiz, there it is. It's
24 right there. We didn't have to spend six months and a
25 small fortune to get the cut sets to direct our attention

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 to where it needs to be directed, whereas this system
2 could result in thousands of pages of FMEA --

3 MEMBER STETKAR: Yes.

4 MR. GEDDES: -- and never get to the pairs.

5 MEMBER STETKAR: Never get to those pairs

6 --

7 MR. GEDDES: Exactly.

8 MEMBER STETKAR: -- because of that
9 constraint and that's the reason I wanted to bring it up
10 here, because it's a good example. It's actually a
11 little better example than the HPCI/RCIC stuff, try to
12 demonstrate those differences. That's why I tended to
13 focus on this one a little bit more than the other.

14 Now, Dave, in this example in the fault tree
15 process there's a couple of things, and I hate to do this
16 but I have to because this -- well no. It's part of this
17 sort of philosophy, if you will, of -- I don't care about
18 the circ water system.

19 I care that the EPRI report is giving me as
20 a marginally informed analyst some decent guidance about
21 how to think about the problem. Examples are important
22 because I can actually look at different things and
23 understand that.

24 But in, and this is kind of a, I hate to do
25 it, but it's in the report and it just really bothered

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 me.

2 As you lay out this sort of systematic
3 functional approach, there's a long discussion in
4 Example 5-2, kind of tabular form, you know what I'm
5 talking about. It seems to say that the function of --
6 I'll read it for you. "The focus of the top-down
7 analysis is on circulating water."

8 If you're looking for a page number, it's
9 on Page 5-44. If you're a PDF guy, it's 178 in the PDF
10 file.

11 "The focus of the top-down analysis is on
12 circulating water but it is not considered to be a
13 front-line system in the PRA and does not appear in Figure
14 5-2," which was a high-level PRA guideline.

15 "However, review of the fault tree logic and
16 dependency matrices for the front-line systems shown in
17 Figure 5-2 show that the main condenser, which is
18 supported by circulating water, ultimately provides
19 support to two plant-level safety functions, reactor
20 inventory control through operation of the
21 turbine-driven feedwater pumps, which required
22 condenser vacuum, secondary heat removal through
23 maintenance of CST inventory, for example avoiding the
24 need to make up to the CSTs from systems such as
25 demineralized water or fire protection in order to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 maintain an adequate long-term auxiliary feedwater pump
2 suction source. This, by the way, is an example for a
3 pressurized water reactor."

4 How does the main condenser support reactor
5 inventory control through the feedwater system for a
6 pressurized water reactor?

7 MR. BLANCHARD: That should have bothered
8 you. That's a BWR/PWR mixture of --

9 MEMBER STETKAR: Yes. Well, that's really
10 clear, that you're talking about these functions from a
11 BWR perspective and not a PWR. So, EPRI, be careful
12 about this, because this high-level function process
13 works really well --

14 MR. TOROK: So we're mixing and matching.

15 MEMBER STETKAR: You're mixing. These
16 models --

17 MALE PARTICIPANT: The poor guy in one of
18 the plants may have trouble.

19 MEMBER STETKAR: HPCI/RCIC is strictly a
20 BWR system.

21 MALE PARTICIPANT: Right. That's right.

22 MEMBER STETKAR: So it's developed from
23 people who have a lot of BWR experience because this is,
24 like I said, I'm trying to learn how to think about this.

25 MR. BLANCHARD: The circ water example

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 should have been developed for either.

2 MEMBER STETKAR: Yes, because actually it
3 doesn't make any difference here but since -- I like the
4 process because it says start at a high-level function.
5 What am I trying to achieve? I'm trying to not melt the
6 core.

7 You know, and work your way down into these
8 subsidiary functions, subsidiary systems. What do they
9 do? How do they contribute to that overall function of
10 not melting to core, if that's what I'm interested in.

11 MALE PARTICIPANT: Right.

12 MEMBER STETKAR: And you're right. On
13 this picture it doesn't make any difference whether this
14 is for --

15 MR. BLANCHARD: Right. Had we said the
16 steam generator inventory control, you would have
17 probably had no problem with the paragraph.

18 MEMBER STETKAR: I do because the circ
19 water system doesn't contribute to that.

20 MR. BLANCHARD: The steam generator
21 inventory?

22 MEMBER STETKAR: Not for CST make up.

23 MR. BLANCHARD: Yes, it does. If you have
24 a small CST, you don't have a regular emission time.

25 MEMBER STETKAR: For a little bit of time.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 For a little bit of time. I'd give you that.

2 MR. BLANCHARD: Right.

3 MEMBER STETKAR: Give you that one.

4 MR. BLANCHARD: Some of the older plants
5 are like that.

6 MEMBER STETKAR: Anyway, that's a little
7 nit. But, again, if you're presenting examples, you
8 know, please try to get them right.

9 MR. BLANCHARD: We could be confusing
10 people here.

11 MEMBER STETKAR: And don't confuse them,
12 because somebody will read that and say, well --

13 MEMBER BLEY: Worse than confusing.

14 (Simultaneous speaking)

15 MEMBER STETKAR: They'll dismiss it.
16 They'll say, well, obviously these people don't know how
17 really power plants work so why should I follow their
18 example?

19 MALE PARTICIPANT: Exactly.

20 MEMBER STETKAR: They'll put it aside.
21 They'll just dismiss it. Now, more importantly you take
22 5-9 which, you know, kind of walks you through the
23 process.

24 For the circ water pump discharge valves,
25 and just keep the drawing open there, you define three

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 failure modes for the circ water pump discharge valves
2 and examine them systematically, fail to remain open,
3 fail to close and fail to open.

4 I noted that that list did not include the
5 fail to remain closed failure mode. So I thought, well,
6 why do I not care about that failure mode for this
7 particular system?

8 And then I thought about those two little
9 red valves that you have there that are normally closed.
10 Said, gee, what happens if one or both of those valves
11 opens spuriously?

12 If they open spuriously, I need to start up
13 some extra circ water pumps because I'm short-circuiting
14 flow in the same way that if one of the normally open
15 valves fails to close for your presumed type of system
16 response.

17 And, gee, because I have common software
18 that can affect both of those, that might be something
19 that I've overlooked by simply not including that one
20 failure mode. So my question is why didn't you examine
21 the fail to remain closed for the two red valves?

22 MR. BLANCHARD: It is.

23 MEMBER STETKAR: If this is an example to
24 teach people how to systematically think about this
25 process and if you go back about three slides in the FMEA,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 too much, too little, not enough, you know, that type of
2 systematic thought process.

3 It's also an example of what might not be
4 wired into a preexisting fault tree model because the
5 person who drew that fault tree model didn't think about
6 that failure mode or didn't think it was important for
7 the purposes of that particular fault tree that was being
8 drawn for that particular purpose.

9 MR. BLANCHARD: I believe the actual fault
10 tree did include.

11 MEMBER STETKAR: Oh it did, okay.

12 MR. BLANCHARD: Why it did not end up in the
13 table I can't tell you at this point, so. Yes, all the
14 combinations of valve and pumps, valves open and pumps
15 not running were a part of the fault tree because that
16 causes the flow diversion issue which does precisely what
17 you said, is it requires additional flow from the other
18 pumps.

19 MEMBER STETKAR: The point is during one,
20 see, you developed a model, this particular example, from
21 a pump trip, need to get a different pump running
22 perspective.

23 MALE PARTICIPANT: Yes.

24 MEMBER STETKAR: But in terms of a thought
25 process, again, from the top-level function, what can

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 give me a problem with circulating water?

2 MR. BLANCHARD: Yes right, so that's --

3 MEMBER STETKAR: Spurious opening of those
4 valves could be important and if that thought process
5 identifies some type of, I'll call it failure mechanism,
6 if you will, in the software such that everything is
7 running normally but something would give you a signal
8 to open both of those valves.

9 MR. TOROK: You know, seems like I recall
10 talking about this and I thought there was an interlock
11 between the pump and the valve that somehow dealt with
12 that in the real system.

13 MR. BLANCHARD: But that could fail too.

14 MEMBER STETKAR: But that could fail too.

15 (Simultaneous speaking)

16 MR. TOROK: Yes, yes, yes, right.

17 MEMBER STETKAR: And the FMEA doesn't look
18 at spurious open and close valves either.

19 MR. GEDDES: John, I think you're hitting
20 on something that we need to take to heart. These
21 examples are not fully developed, detailed design
22 examples.

23 Although the detailed designs are out
24 there, we didn't go beyond development of these examples,
25 you know, to the full extent. We developed enough

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 information in these examples to be able to demonstrate
2 the methods and see what we could learn, and that's a
3 great observation.

4 MEMBER STETKAR: And that's why I almost
5 didn't want to make these comments in this meeting,
6 because I think the examples are very, very good to
7 demonstrate concepts. But the concern that I have is
8 people tend to pick up these examples --

9 MALE PARTICIPANT: And take them for
10 granted.

11 MEMBER STETKAR: -- and use them as
12 cookbooks and the danger is that if I pick up, you know,
13 I'm baking a cake and you left the flour out, I have a
14 problem.

15 MEMBER BLEY: But the other hand, John's
16 example could be picked up here, is that this table only
17 has three main components and you would expect the
18 failure modes to be complete. So if you were studying
19 it, and especially when it's a little subtle, it could
20 lead people astray on this one.

21 MEMBER STETKAR: The only reason I come
22 back to this, and we'll hear more about this when we get
23 to the real things, is that if we're trying to develop
24 a notion that valve has nothing to do with software at
25 the level of a red circle there.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 But the subject of today's meeting is to
2 talk about software failure modes and to get people
3 thinking about a coherent set of failure modes in a
4 systematic process, so it's one of the reasons why two
5 hours ago I brought up this notion fail to open, fail to
6 close, spurious open, spurious closed.

7 It took hardware people years back in the
8 late '70s to kind of settle on, gee, okay, those are
9 failure modes that I'm interested in and now I should
10 systematically think about how can those failure modes
11 affect the system all the way up through the systems, to
12 the functions, to the top.

13 And if, you know, if your examples are not
14 enforcing that process of looking at failure modes
15 systematically, they may not serve the purpose.

16 MR. TOROK: That's a good observation.

17 MEMBER STETKAR: And now I'll be quiet.

18 MALE PARTICIPANT: Really?

19 CHAIRMAN BROWN: You can do whatever you
20 need to do, but let's go ahead.

21 MR. BLANCHARD: All right, the circ water
22 system is the next example in the guideline beyond the
23 HPCI and RCIC system and, you know, several approaches
24 were taken to evaluating the circ water system in the
25 methods in the report and among them was the fault tree

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 analysis.

2 In this particular case we didn't stop the
3 fault tree analysis at the hardware that the
4 instrumentation and control system, the digital I&C
5 system controls. We continued the fault tree analysis
6 into the digital I&C system.

7 So in the HPCI and RCIC system case, there
8 was a transition point to one of the other methods. In
9 this particular case, we took it down into the I&C system
10 so there is an example of modeling the digital I&C system
11 in the guideline.

12 Now, to kind of jump to the results and Bruce
13 has mentioned that we provided cut sets for this
14 particular system. In a minute Bruce I think will
15 describe the system and how it works.

16 There's a lot of redundancy built into this
17 system and it became a little bit surprising when we built
18 the fault tree that while, you know, you need multiple
19 pumps to fail before you don't have sufficient circ water
20 to maintain this plant at power, there are pairs of
21 instrumentation and control components that can cause
22 that very thing to occur.

23 And that was kind of surprising thing that
24 came out of the analysis, something that might not be
25 found in an FMEA or one of the other methods but just kind

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 of fell out of the fault tree analysis. So you want to
2 describe the --

3 MR. GEDDES: And it's in the basic design
4 of the system. In fact, the next method we're going to
5 show you is HAZOP.

6 And after dealing with design FMEA on this
7 system and then the hiccup of the cut set information from
8 Dave, we tried to see if another method might find the
9 actual OE that was reported.

10 And I'd like to show you the HAZOP approach
11 and then how that method found what was reported and it
12 was a bit surprising and we'll come back to this diagram
13 and show you exactly what happened in the plant that
14 caused the trip.

15 So, now we're talking about deviations from
16 design intentions. There's a HAZOP worksheet that I'm
17 going to show you next and now we can see the functional
18 relationship between the circuit breaker tied into a
19 digital input module and then some software in the
20 controller that's communicating with remote I/O and
21 affecting the position of the motor-operated valve.

22 We evaluated those deviations and then you
23 could argue that HAZOP is top down or bottom up or inside
24 out or forward or backward. You see arrows going in two
25 directions here.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 If we evaluate deviations of the digital
2 components, so we focus specifically on the
3 communication modules, then you can evaluate what the
4 consequences of those deviations from the design
5 intention. Let's go to the next slide.

6 Here's the HAZOP worksheet. HAZOP has some
7 standards and guidance available out there. We've
8 adapted it and incorporated it in this guideline but it
9 uses a series of guide words against design intent.

10 If you look at the top of this worksheet,
11 you can see the design intent. We're talking about
12 communication modules. The design intent is to
13 communicate data in and out of I/O modules in I/O Cabinet
14 Alpha or Bravo.

15 The success criteria was no data errors or
16 losses of data links to other cabinets, and then you can
17 systematically identify the elements that are imported.

18 In this case we've identified one of the
19 elements or attributes is the signal and voltage and then
20 the deviation in the first row was what happens if there's
21 no carrier signal.

22 And as we went through this thought process,
23 and we had to get some help from a facilitator. This is
24 a different way of thinking. One of our EPRI members
25 from Rolls-Royce is trained as a facilitator in HAZOP and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 very patiently walked us through this how many times?

2 MALE PARTICIPANT: Two.

3 MR. GEDDES: At least twice, until we began
4 to get it. And then we got it and we found, well, what
5 happens if there's a failed backplane? We did not
6 identify a failed backplane as a potential failure mode
7 in the design FMEA example. We could have, we should
8 have and we would have, but we didn't. And these are,
9 you know, 30-year people that have been doing design
10 FMEAs for a long time.

11 CONSULTANT HECHT: Those backplanes never
12 fail.

13 MR. GEDDES: Well, they do. But they do,
14 right? You know, on a dark and stormy night, backplanes
15 fail, right? And this is actually what happened in the
16 OE but the way it failed was unique and I'll explain.

17 But if you lose two COMM modules in one
18 cabinet, you basically isolate one half of this control
19 system from the other half and it's an attribute of the
20 architecture and the way the system integrator put it
21 together for this plant.

22 So let's go back, the picture, the circ
23 water example. Dave already showed us if you lose two
24 COMM modules bad stuff happens. The HAZOP method shows
25 how two COMM modules can fail due to a common cause.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 In the OE, one of the COMM modules in the
2 logic cabinet had failed and the system was in service.
3 They wrote a work order. The I&C techs went to the logic
4 cabinet, opened it up, pulled the failed, you know, the
5 offending module out and I guess there were some captive
6 screws or something.

7 But they dropped a screw somehow in the rack
8 and it shorted out the backplane, took out the other COMM
9 module, isolated one half of this architecture from the
10 other half, the data communication path.

11 This is not a software issue. This is a
12 hardware failure mode. It's all it is, and Dave's cut
13 sets demonstrated how this can happen. The HAZOP method
14 showed exactly, you know, the underlying way you can
15 influence system operation.

16 And, in fact, it closed. It resulted in a
17 closure or isolation of two active pumps in one of the
18 basins. So in this plant design you need four running
19 circ water pumps to maintain condenser vacuum, 100
20 percent load, 100 percent power. If you drop to two
21 pumps, Dave, what happens?

22 MR. BLANCHARD: Well, you don't have enough
23 left to maintain condenser vacuum.

24 MR. GEDDES: And the plant tripped on
25 condenser vacuum?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. BLANCHARD: Right. One of the other
2 aspects of this design is the I/O modules that feed the
3 motor-operated valves on the discharge of the pumps.
4 When there's no signal, its automatic state is close the
5 valve.

6 MALE PARTICIPANT: Close it?

7 MR. BLANCHARD: Yes. Which is --

8 MALE PARTICIPANT: Oh yes, that's right.

9 MR. BLANCHARD: Right. And so that was
10 another design feature that fell out of the fault tree
11 analysis. That did get modeled. It didn't seem to have
12 a whole lot to do with, you know, reducing the redundancy
13 of the system.

14 But once that default failure mode ends up
15 in your model, you know, you end up in situations where
16 you're losing two COMM modules. Leaves you with only
17 three pumps and you need four to run the plant, so.

18 MEMBER BLEY: I like HAZOP a lot and have
19 used it in many places and especially like when you're
20 doing PRA of a new system looking for the ways you can
21 get in trouble.

22 But it was developed in the UK for chemical
23 processing plants. It's looking at piping systems
24 usually. Did you give much thought to whether the guide
25 words are great as they are or if they need to be expanded

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 for looking at I&C systems?

2 MR. GEDDES: Well, the Rolls-Royce member,
3 he's in the nuclear submarines part of Rolls-Royce, so
4 he grew up in the UK. You know, he's in Upper Derby, you
5 know, Derbyshire, and this is baked into what they do in
6 the Royal Navy submarine force.

7 We asked him that question. It was
8 difficult for us to determine without a lot more research
9 and trial and error to see if these guide words were
10 adequate or not.

11 MEMBER BLEY: Obviously they do a lot but
12 I don't know if they do everything.

13 MR. GEDDES: But we took it on, you know,
14 on the strength that it's been around for a long time.
15 It's been used in a lot of ways. It's mature and proven
16 in those other industries, chemical industry and the
17 defense industry in the UK, at least from the exposure
18 that we got.

19 MR. TOROK: You know, we asked him if he'd
20 seen situations where those guide words were not adequate
21 and he said no.

22 MEMBER BLEY: Not so far.

23 MR. TOROK: Right.

24 MEMBER BLEY: That's good.

25 MALE PARTICIPANT: We've even tried using

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 them in some human reliability kind of work. It's a very
2 helpful way to look for ways things can fail and have a
3 lot of history.

4 MR. GEDDES: So moving on to the next
5 method. This is the one that was getting a lot of buzz,
6 systems theoretic process analysis. John is one of the
7 researchers in the lab at MIT working with Dr. Leveson.
8 He taught us a lot.

9 We think it has some practical, immediately
10 applicable use in our industry but we had to learn, you
11 know, a few basic principles or relearn some basic
12 principles before we really grasped what this is about.

13 So first, there's the notion of accidents
14 or losses. We gave you here, reference 19 is Dr.
15 Leveson's new book. This was published, what, last
16 year, John?

17 (No response)

18 MR. GEDDES: So this is not the definition
19 of a nuclear accident. This is an accident at MIT and
20 Nancy says, well, you can call it a loss. I don't care
21 what you call it, in her words, anything that you don't
22 want to have happen.

23 So if you're concerned about loss of
24 generation, loss of life, nuclear safety, that goes in
25 that box. That's your starting point.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Next step is identify potential hazards
2 that can lead to those accidents or losses and typically
3 a list of accidents or losses or a list of hazards that
4 can lead to those accidents or losses is a short list.
5 John, typically five to ten at most?

6 DR. THOMAS: Yes.

7 MR. GEDDES: It doesn't take long. It's a
8 tabletop exercise to do this. We did it on a couple of
9 examples and we got it. We understood, you know, these
10 points.

11 The next step is to systematically find the
12 control actions and the nomenclature here are considered
13 unsafe. By definition an unsafe control action leads to
14 a hazard or is hazardous, and we'll get into what a
15 control action is next.

16 And then this is step two. The first step
17 was identify unsafe control actions. Part two of STPA
18 is to find the control flaws that can lead to those unsafe
19 control actions. So I'd ask you to think of this mental
20 model as we go through these next few slides.

21 Control systems can issue lots of control
22 actions, a very, very long list, but not all are unsafe.
23 So this method helps you narrow the search to the ones
24 that are potentially unsafe and then assess for control
25 flaws.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 The alternative is a checklist. What are
2 all the control flaws that we've ever seen in our
3 lifetimes or in prior, you know, in other domains? Well,
4 we make a list, don't do this, don't do that, don't do
5 that, don't do that, or assure this, assure that.

6 From a technical point of view, this is a
7 paradigm shift that helps us assess a proposed or
8 existing system design, see if it has the potential for
9 unsafe control actions and then narrow the search for
10 flaws that can lead to those control actions. In a way
11 it's almost like doing root cause analysis before the
12 event.

13 Assess the design for potential causes of
14 events rather than applying your checklist, which we
15 advocate. There's lots of things that we want to do on
16 our digital systems to assure safety and reliability.

17 But we can also look for these corner cases
18 and edge cases, the things that we've missed using
19 traditional methods and, lo and behold, we found one in
20 one of these examples.

21 And then we can mitigate, prevent,
22 eliminate, design out or take administrative controls,
23 whatever works, to mitigate those control flaws and
24 assure a safer system before it's put into service, so
25 that's the power of this method.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CONSULTANT HECHT: Question.

2 MR. GEDDES: Yes.

3 CONSULTANT HECHT: You said you don't need
4 checklists but --

5 MR. GEDDES: No, I didn't say that. I said
6 they have their place, but checklists aren't enough.

7 CONSULTANT HECHT: Okay. Well, I guess
8 the point I was leading to is that when you do this kind
9 of, I'll call it decomposition for lack of a better term,
10 hazard decomposition as opposed to functional
11 decomposition, don't you really have to know how things
12 fail and doesn't it pay to have that kind of a list in
13 mind as one does those?

14 MR. GEDDES: Yes, it does but we're going
15 to show you an example where nothing failed. Everything
16 worked exactly as it was designed to work. You had to
17 do the wrong thing at the wrong time.

18 CONSULTANT HECHT: Okay, I'll amend that to
19 say when I said failed what I really meant was do
20 something wrong.

21 MR. GEDDES: Okay. Well, this gets back to
22 semantics. When we say failure, what do we mean?

23 CONSULTANT HECHT: Yes.

24 MR. GEDDES: Right? I think if we work
25 through the example, we can get to your point. So STPA,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 am I doing so far so good, John?

2 DR. THOMAS: Yes.

3 MR. GEDDES: Okay. STPA is rooted in
4 control theory. When I went to the first MIT workshop
5 two years ago, I was skeptical. I didn't go to MIT. I'm
6 not that smart. I didn't get in. I tried. And I was
7 thinking, well, I'm going to go to the center of academia
8 and just see if there was any practical work that we could
9 bring into nuclear power.

10 John gave a presentation and he showed this
11 is a control structure. I said that's something I can
12 recognize. I'm a control system guy. There's
13 controllers and control processes.

14 John started talking about unsafe control
15 actions. I said do you mean a down arrow in this picture?
16 He said yes. That's something I can recognize. That's
17 a down arrow. That's a control action.

18 Controllers can be machines or people. A
19 human operator in a control room is a controller in this
20 model. So we act on control processors through control
21 actions so that's the down arrow. There's going to be
22 a quiz later, so pay attention.

23 Feedback signals are models in this method
24 and they're called process model variables, okay? So we
25 have up arrows and down arrows. Notice there's a box in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the controller called process model. That's the
2 software, or the firmware in the operator's head through
3 training and procedures, simulation and experience.

4 There's a side row there called other inputs
5 or conditions that can act or influence a controller.
6 That could be another controller or it could be a state
7 in the environment that the controller needs to be able
8 to discern and make decisions to act on the control
9 process.

10 For example, operators are trained to
11 recognize that there's a LOCA. That's a condition that
12 human operators are trained to recognize and take action
13 if the automatic systems don't mitigate or take
14 confirmatory action in addition to automatic systems
15 that mitigate an accident.

16 So control actions, there's terminology
17 here. Control actions might increase, decrease, open,
18 close, hold, switch. Now we're acting on components of
19 the field, motor control centers, fans, pumps, valves and
20 we express control actions this way.

21 Process model variables, pressure, flow
22 temperature, voltage, current. These are things that we
23 know and understand. We're taught these things as
24 engineers.

25 Each of those process model variables also

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 have states, normal and accident, increasing,
2 decreasing, just right, too much, not enough. It's an
3 abstraction but it's something we can understand.

4 And then, of course, other inputs and
5 conditions might be an aggregation of information. What
6 mode are we in, Mode 1 or Mode 5? Is the plant condition
7 accident or normal? So this is the construct, up arrows
8 and down arrows and methods for expressing what they
9 mean.

10 Okay, back to our high-pressure coolant
11 flow control system. We found some OE where on command
12 this system turned itself off during the surveillance
13 test. Everything worked exactly as designed.

14 Yet when the operators entered the
15 surveillance test, they hit the go button and the system
16 stopped, so why is that? Design FMEA's not going to tell
17 you how that happened. You won't see it. Fault trees
18 won't show it to you.

19 We gave this block diagram to John Thomas,
20 sitting next to me, and Blandine Antoine, another
21 researcher at MIT, because we'd met them. I handed them
22 a business card. I said can you help us figure out how
23 to do this?

24 And John's advice was can you give me an
25 example? So we gave him this block diagram. Came back

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 three days later with a list of things that could make
2 this system misbehave and on that list was the root cause
3 of the failure and now, mind, we're talking about
4 functional failures. If it doesn't go on demand, that's
5 a functional failure.

6 In two or three days we had a conference
7 call, Ray and I, and I said, okay, stop. You found it
8 and we'll show you where it is and the results that they
9 gave us within just a couple of days. I was shocked.

10 So here's the OE. You've got the block
11 diagram on the bottom right. It's a handy reference.
12 Remember there's three valves that affect delivery of
13 steam to the turbine.

14 You want the turbine to spin to make the pump
15 go and pump water, right? If those valves aren't
16 behaving correctly, you don't get high pressure coolant
17 injection.

18 The initial conditions for this event --
19 well, let me back up. Turbine speed's on the left-hand
20 axis. Governor valve position's on the right-hand axis.

21 The green dotted line is governor valve
22 position. You can see it's wide open. The blue line is
23 the actual turbine speed. The red line is what the
24 operators are expecting.

25 The flow control system has a flow

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 indicating controller in the control room. There's no
2 indication of turbine speed. Flow is indicating at a low
3 rate. The system is isolated.

4 They hit the go button. It's a
5 surveillance test to simulate demand on the system and
6 a recirc mode and the turbine's rolling around 700 rpm.

7 The red line is what the operators' expect.
8 They don't see the red line. They want flow to come up.
9 Like when the turbine starts to roll, flow comes up.

10 In the flow indicating controllers, the
11 needles come off zero and they come up to setpoint. In
12 this case if it's HPCI it's 5,000 gpm and life is good.
13 They pass the surveillance test.

14 One of the software features in the digital
15 flow control system is a reset setpoint. If turbine
16 speed, and there's turbine speed feedback in this local
17 governor and positioner system, if turbine speed is not
18 below that reset setpoint, the governor valve won't
19 reset. Stays open.

20 So the first question is why is it open?
21 This is the second or third attempt to run the
22 surveillance test. The operators didn't know that it
23 had not reset itself and there's no indication of reset
24 in the control room. It's a flow-indicating controller,
25 not a turbine speed system in the control room. Everyone

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 with me so far?

2 CHAIRMAN BROWN: No.

3 MR. GEDDES: Okay.

4 CHAIRMAN BROWN: What's the blue line
5 again?

6 MR. GEDDES: The blue line is actual
7 turbine speed.

8 CHAIRMAN BROWN: Yes, I read that. And is
9 that, that back here on the left-hand side, that's still
10 above the reset point --

11 MR. GEDDES: Yes, sir.

12 CHAIRMAN BROWN: -- at this point you're
13 talking about?

14 MR. GEDDES: At the start of this event, the
15 turbine's rolling. Operators don't know it.

16 CHAIRMAN BROWN: That's above the reset
17 speed?

18 MR. GEDDES: Correct.

19 CHAIRMAN BROWN: Now, I understand.

20 MR. GEDDES: And the governor valve is wide
21 open. If it had achieved reset, the governor valve would
22 be closed. But because of prior maintenance work on this
23 system, it was left in this state at the start of the next
24 surveillance test and nobody knew it.

25 CHAIRMAN BROWN: That ramp up of the blue

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 line is where it started to try to do something?

2 MR. GEDDES: Well, we'll get there.

3 CHAIRMAN BROWN: Okay. All right, I'm
4 ahead of you then now.

5 MR. GEDDES: Okay. At the initiation
6 point, you know, the surveillance test is mash the
7 button, initiate HPCI. Remember that valve on the
8 right, the system initiation signal is the signal we're
9 talking about in this blue box. The operator hits the
10 button. That valve begins to open. When that limit
11 switch changes --

12 CHAIRMAN BROWN: The governor valve?

13 MR. GEDDES: No, steam admission valve.

14 CHAIRMAN BROWN: Steam admission valve
15 now, okay.

16 MR. GEDDES: That valve is closed. The
17 trip and throttle valve is open and the governor valve
18 is open, right? So the first question is why is the
19 turbine rolling at 700 rpm if the steam ignition valve
20 is closed? Why? Myron, why? It's not the first time
21 --

22 CONSULTANT HECHT: If it's closed that's
23 the -- I don't --

24 MR. GEDDES: I'm an I&C guy. I've got a
25 P&ID that says that valve is closed.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MALE PARTICIPANT: Why are you picking on
2 Myron?

3 CONSULTANT HECHT: Obviously it's not
4 closed.

5 MR. GEDDES: Why would the turbine -- it's
6 closed.

7 MALE PARTICIPANT: No, it's not.

8 MR. GEDDES: The operator on that valve has
9 mashed the plug into the seat. It's closed.

10 MALE PARTICIPANT: Is it actually closed or
11 is indicator just closed?

12 MR. GEDDES: It's actually closed.

13 (Simultaneous speaking)

14 CHAIRMAN BROWN: The governor valve is
15 closed?

16 MR. GEDDES: The governor valve is open.
17 The steam admission valve is closed at the start of this
18 event. Why is the turbine rolling at 700 rpm? Because
19 valves leak.

20 CONSULTANT HECHT: Oh, okay.

21 (Simultaneous speaking)

22 MR. GEDDES: I have the system manager in
23 mind that's certain that that valve is closed but
24 leaking. This is a paradigm shift. As I&C engineers,
25 we look at a P&ID and schematic and we make assumptions

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 about how equipment behaves and those assumptions aren't
2 always true.

3 Now, John pointed this out and I said but
4 we have PMs and we have surveillance tests and we have
5 -- he said, Bruce, you don't get it. You don't get it.
6 Your assumptions aren't always valid.

7 So let's keep going. Let's see what
8 happened. The turbine's rolling. They hit the button.
9 The steam admission valve is closed. The indicated
10 position is 0 percent open. That's closed.

11 Now, the graphic is a little garbled here.
12 Remember, I said when the limit switch hit 17 percent it
13 changes state and it's a contact closure input to the
14 digital flow control system and it takes it as an enable.
15 That means go.

16 That valve takes a certain amount of time
17 to get to 17 percent and then the flow control system
18 says, aha, I have a demand. You want me to go, okay?

19 There's another software feature built in
20 to protect the equipment in a case of a leaky steam
21 admission valve because turbines really shouldn't be
22 rolling in an uncontrolled way. The set point for this
23 protective function is 1,000 rpm.

24 So it's in the no-man's land between 100 rpm
25 and 1,000 rpm and nobody knew it. They hit the demand,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 and guess what? It hit 1,000 rpm before it got the enable
2 signal and closed the governor valve to protect the
3 turbine. It's exactly the wrong thing to do when there's
4 a valid demand. This is where maybe priority logic is
5 helpful because now you have a demand signal --

6 MEMBER BLEY: What kind of logic?

7 MR. GEDDES: Priority logic.

8 MEMBER BLEY: Okay, sure.

9 MR. GEDDES: This is a stovepipe
10 architecture. It's a purpose-built system to make the
11 turbine, you know, do its function. So you have an
12 independent demand signal at odds with an independent
13 equipment protective function.

14 So the designers of the box know that
15 turbines shouldn't spin when there's leaky valves
16 because they get reports of leaky valves in terms that,
17 you know, aren't behaving correctly.

18 So their point of view is to protect the
19 equipment, the turbine, and we've lost sight of the
20 larger view to protect the plant. We're trying to
21 protect the core.

22 So there's two different purposes now at
23 odds and it's baked into the software. Everything
24 behaved exactly as it was designed to behave.

25 MEMBER BLEY: Except for the steam

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 admission valve.

2 MR. GEDDES: Well, that's an interesting
3 point. We've given this presentation a few times and we
4 teach a class on some of these concepts. From an I&C
5 guy's point of view, you might say fix the valve. Make
6 the valve work so I don't have to protect the core in a
7 case of a leaky valve.

8 But valves leak, and this is where digital
9 systems can help turn around equipment issues that could
10 influence the plant. Take advantage of the software
11 and, in fact, there are some software and hardware
12 changes going on right now to fix this problem, right?
13 Software can be the cure here as well. It's not the
14 culprit.

15 MEMBER BLEY: Well, yes. But the guy
16 designing the software has to understand the context in
17 which it's safe in the plant.

18 MR. GEDDES: Well, there's the level of
19 interest.

20 MEMBER BLEY: I mean, both things need to
21 be fixed.

22 MR. GEDDES: Right, exactly.

23 DR. THOMAS: Yes, and I have a couple
24 comments. When it was designed, the designers knew that
25 valves leak. I mean, that wasn't what's surprising

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 about this, that a valve leaked and that's, in fact, one
2 of the reasons they have three valves there. The trip
3 valve is there in case they have a problem and they need
4 to shut it down.

5 What was surprising was that the system,
6 somehow with the leaking valve, the logic of the system
7 was designed inadvertently to shut itself off in this
8 situation.

9 MEMBER BLEY: But this isn't the only place
10 in the plant where we have protective logic on equipment
11 that needs to be overridden in the case of an accident
12 demand. But somewhere in the specification or the
13 implementation of the software, somebody didn't
14 understand the overall function, the high-level
15 function.

16 MR. GEDDES: That's a great segue and
17 that's the next few slides. They systematically get
18 there.

19 MEMBER BLEY: But the guys, they didn't
20 know it was rolling?

21 MR. GEDDES: The operators didn't know.

22 MEMBER BLEY: They have no indication of
23 rpm on the thing.

24 DR. THOMAS: Correct.

25 MR. GEDDES: Right.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BLEY: Well, they didn't know it was
2 rolling so they didn't know to send somebody down and
3 check that. The system's going to be hot if they're
4 going to go near it but something was going on.

5 DR. THOMAS: So let me summarize this in a
6 couple words in case anybody got lost. What happened
7 here is the turbine basically sped up too fast. It hit
8 the trip point before the enable signal came in.

9 Normally that's impossible. Normally that
10 doesn't happen. It starts from zero and it speeds up to
11 the physical limitations. It can't hit that trip point
12 before it gets the enable.

13 But what nobody knew is in this case it was
14 starting from a rolling start so it got a head start and
15 it was able to hit that trip point first, and that means
16 every time you try this, and they tried it two or three
17 times, it shut itself off every time. You turn it on.
18 It shuts itself off.

19 And so the operators are sitting there
20 scratching their heads trying to figure out what's going
21 on. It's shutting itself off, right? The automation is
22 doing the wrong thing.

23 And this is something that we would have
24 loved to know about before we started the STPA analysis
25 but Bruce wouldn't tell me.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MR. GEDDES: It was a blind test to see if
2 they could find the cause and they did. They actually
3 found a longer list and we said stop. You found the one
4 that actually caused this particular issue and we'll show
5 it to you. We have some more slides on that. Fair
6 enough? Okay.

7 So we identified the losses and we have a
8 list that's in the report. The hazards, it's another
9 list. It's in the report. And then we got into
10 systematically identifying the hazardous control
11 actions like closing the governor valve at the wrong time
12 and then the flaws that could cause that to happen.

13 Here's the process model, sorry, the
14 control structure, excuse me, the control structure,
15 which is one of the prescribed steps in the STPA
16 methodology.

17 So here's the test and between the flow
18 control system and the control process, where's the
19 control action? I'll give you a hint. A control action
20 is a down arrow.

21 CONSULTANT HECHT: Yes, the open/close
22 commands on the governor valve.

23 MR. GEDDES: Correct. What are the
24 process model variables? Those are up arrows.

25 CONSULTANT HECHT: Valve position, turbine

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 speed and system flow rate, system enable.

2 MR. GEDDES: All right. Notice the flow
3 control system gets signals so it can close the loop and
4 establish the right speed in response to a flow demand
5 from the human operator. The operator has a process
6 model, plant conditions, and the process model they also
7 know the system flow rate.

8 Notice you don't see the turbine speed up
9 arrow between the flow control system and the operator.
10 That's basically the human system interface, the
11 display. The display only displays the system flow
12 rate, not turbine speed.

13 It could display turbine speed if you have
14 a more integrated system and the operator could have
15 access to an override feature or some administrative
16 control to say, yes, I see you'd rather close the governor
17 valve but I really want it open. So the operator's blind
18 to this and maybe shouldn't be.

19 So there's two different process models,
20 one in the software in the governor box and another one
21 in the operator's head. Maybe the process model's
22 incomplete. That's one of the potential flaws that you
23 can uncover with this methodology.

24 Now we're getting into human factors
25 engineering. How do we combine the strengths of digital

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 technology and human factors in a way that we have a more
2 effective process model? In fact, the STPA method is
3 very well suited for requirements engineering.

4 Hazard analysis is almost a secondary
5 outcome. It's better used to evaluate conceptual
6 designs and come up with a more complete and correct set
7 of requirements for a system. That's it's real payoff.

8 In this report we're only examining its
9 ability to uncover hazardous design problems. Did I get
10 that right, John?

11 DR. THOMAS: Yes, yes. It provides both as
12 an output. You get the hazard analysis, the traditional
13 results, which is what can go wrong in the system.

14 But you can also get a set of requirements
15 which says what do I have to do to be right? And this
16 is really helpful for software where we have a big problem
17 a lot of times with the cursive software, which is that
18 it always does what we tell it to do. It always obeys
19 exactly the commands that we give it.

20 And so trying to get that right is a huge
21 problem. So when we talk about getting it from hazard
22 analysis, getting what can go wrong in the system, to
23 requirements, that's one of the areas that it can be very
24 helpful. It's almost exactly what software needs to do.

25 MR. GEDDES: Okay, so this is the control

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 structure. That's one of the steps in the process. Now
2 we have the process models. The operator has a process
3 model. The flow control system has a process model.
4 The process model is a table. You have the process model
5 variables and their possible states. It's not too
6 complicated.

7 For example, the plant conditions. The
8 operator can assess are plant conditions normal or
9 accident? You know, am I in the main control room or the
10 remote shutdown panel? It turns out there's two
11 different flow-indicating controllers. Are we in
12 manual or automatic mode, and is the system flow too low,
13 too high or just right? Pretty simple process model.

14 Down in the software and the digital boxes,
15 there's a little bit more going on. Do I have an enable
16 or not? Is turbine speed too high or too low or just
17 right? This is basic functional closed-loop control,
18 basic control theory acting on the governor valve
19 actuator and ultimately the governor valve.

20 You'll notice on the left-hand side we have
21 two, sorry, four control actions between the operator and
22 the flow control system and between the flow control
23 system and the actuator.

24 We're going to focus on control action
25 number three. We did not systematically analyze all

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 control actions in this system. We stopped with control
2 action number three just to demonstrate how to use the
3 method.

4 So this goes to the point is this example,
5 you know, 100 percent complete? It would be about 500
6 or 600 pages if it were. I'm sorry, the report would be
7 500 or 600 pages if we completed each method on each
8 example. We just did enough to demonstrate and learn.
9 The process --

10 MALE PARTICIPANT: The EPRI report, right?

11 MR. GEDDES: The EPRI report, yes. And the
12 process model variables, of course, are on the right-hand
13 side.

14 So we evaluate each control action for each
15 combination of process model variable states. This does
16 or can lead to large sets of tables, spreadsheets. We
17 both use spreadsheets. Next slide.

18 The definition of a hazardous control
19 action requires four ingredients. When John gave this
20 talk at MIT, I was like okay, now I'm getting it. At the
21 bottom you have the source, the behavior, the control
22 action and the context. Context is critical. It gives
23 you a glimpse into where misbehaviors occur.

24 So the source in this case is the governor
25 box. It's the digital box. It behaves certain ways and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the list of behaviors is up above, control actions
2 provided, not provided, provided too early or too late,
3 or stopped too soon. And I think there's another case,
4 stopped too late?

5 MALE PARTICIPANT: Yes.

6 MR. GEDDES: Okay.

7 MALE PARTICIPANT: Probably too long.

8 MR. GEDDES: Or too long, applied too long.

9 So you take a source, you evaluate it five times for five
10 different behaviors on a control action. This is
11 control action number three. Increase the valve
12 position.

13 So here's another quiz. If turbine speed
14 is too high and we open the governor valve, is that
15 hazardous?

16 MALE PARTICIPANT: Is that what?

17 MR. GEDDES: Is it hazardous? If turbine
18 speed is already too high and the controller issues a
19 command to open the governor valve even more, is that
20 hazardous?

21 MALE PARTICIPANT: Could be.

22 MALE PARTICIPANT: It depends if the flow
23 is affected.

24 MEMBER BLEY: Hazardous to what?
25 Hazardous to what?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. THOMAS: So one of the hazards would be
2 --

3 MEMBER BLEY: Might be hazardous to the
4 pump.

5 DR. THOMAS: Yes, one of the hazards is
6 equipment damage including damage to the pump, right,
7 yes.

8 MEMBER BLEY: Yes, sure.

9 CHAIRMAN BROWN: Well, the turbine's also
10 of interest, right?

11 (Simultaneous speaking)

12 DR. THOMAS: So it's clearly hazardous.

13 MALE PARTICIPANT: Well yes, okay.

14 MALE PARTICIPANT: Could be.

15 MALE PARTICIPANT: Depends on how much.

16 MR. GEDDES: Okay. Now we're building
17 tables. If we're talking about the flow control system,
18 control action number three, I'm going from the top down
19 here, control action 3 is increase governor valve
20 position. That's one of five behaviors that we can
21 postulate here and it's providing the increase governor
22 valve position command.

23 Now let's look at the columns from the left
24 to the right. Process model variable one is plant
25 conditions, normal or accident. Process model variable

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 number two, governor valve position, too high, too open,
2 too closed, or just right. Process model variable
3 three, turbine speed, too high, too low or just right.
4 System flow, too high, too low or just right and then
5 system enable. We have five process model variables.

6 We evaluate each combination of each state
7 of each process model variable against the postulated
8 behavior providing control action number three.

9 So the next couple of columns say is the
10 situation already hazardous? In other words, if system
11 flow is already too high, before we even consider issuing
12 a control action command is that already hazardous and
13 are we going to make it worse? That's the next column,
14 is the control action behavior hazardous?

15 So you see in the first row system flow is
16 too high and by our construct we deem that to be
17 hazardous. If we increase governor valve position,
18 we're not making it less hazardous. We're probably
19 making it more hazardous.

20 And the related hazards are listed across
21 the top. H3 is equipment damage and, Dennis, that's what
22 you hit on. You could destroy equipment and that's a
23 loss that we've identified that we don't want.

24 So there's a lot of tables. This is an
25 excerpt, but it demonstrates the methodology and how to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 identify a hazard. This is basically the result of STPA
2 step one, identify the hazardous control actions.

3 Now, there are some special cases here where
4 it says no response. Every other row is no response
5 because that means you didn't get a system enable.
6 That's what happened at the plant that tripped the
7 turbine before it got the system enable, so that's kind
8 of low-hanging fruit.

9 You could cut this table in half by calling
10 that a special case and now you have a method of reducing
11 the results to something more practical and useful rather
12 than handing a stack of spreadsheets to a system designer
13 and say please make these hazards go away. You want to
14 comment?

15 DR. THOMAS: Yes, what we're showing here
16 is kind of a brute force approach which is helpful for
17 understanding the method and understanding the fact that
18 it considers all these combinations.

19 But there are more efficient ways to go
20 about it. You could go row by row through this table and
21 some guys that I've worked with actually love to do that,
22 but there are also ways to be more clever about it.

23 This particular table, I don't remember if
24 we had this in the report, but it reduces down to actually
25 about seven rows.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. GEDDES: It's in the report but we don't
2 have a slide on it.

3 DR. THOMAS: Yes, right. So this is just
4 an example to show the fact that these were all the things
5 that are considered.

6 MEMBER BLEY: Just a comment. The
7 systematic way this lays things out is very nice. I like
8 it. But your little two-box controller, control process
9 model is a lot like the information processing model from
10 psychology that's used in some of the more advanced human
11 reliability --

12 DR. THOMAS: Yes. That is a great point,
13 yes.

14 MEMBER BLEY: Your control actions are
15 really close to the HAZOP words.

16 DR. THOMAS: Yes, they are.

17 MEMBER BLEY: Whatever they call those
18 words.

19 DR. THOMAS: Guide words.

20 MEMBER BLEY: They're very similar and just
21 noticed that. I don't know if that's good or bad --

22 DR. THOMAS: There's nothing that's
23 missing.

24 MEMBER BLEY: -- the cases we're looking at
25 so.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. THOMAS: Right, right. And the HAZOP
2 was a kind of drive based on experience and people, you
3 know, sitting together. What do we think are the
4 appropriate guide words to include?

5 MEMBER BLEY: And they're based on looking
6 at typing systems really?

7 DR. THOMAS: Yes, right, right. These
8 guide words, maybe I shouldn't call them guide words, but
9 these --

10 MEMBER BLEY: Control actions.

11 DR. THOMAS: Yes, the control action can be
12 unsafe are derived from control theory. Okay, so
13 there's nothing mathematically or logically that you can
14 identify that wouldn't fit into one of these categories
15 from control theory, so it's two different approaches.

16 Also I want you to keep in mind this is only
17 the first half of STPA, which is actually very powerful
18 by itself, but there's a whole other part that I think
19 Bruce is about to get into which is step two.

20 This is looking exactly on the control
21 actions that are provided so it's very much looking at,
22 like, flaws in things that you provide that are unsafe
23 or things that happen on the down arrows, like Bruce said.

24 There's a whole other part of STPA that
25 looks at physical component failures, looks at valves

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 that get stuck open, that look at feedback that gets
2 garbled when it gets provided to the operator.

3 Maybe we're confusing the operators and
4 they don't have the information to make safe decisions.
5 Like in this case, they had no idea that it was rolling,
6 the turbine was rolling.

7 And it looks at, you know, missing feedback.
8 Maybe the design was flawed or the requirements were
9 flawed and we don't have the right feedback in the system
10 to do what we need to do.

11 So I just want to point out that there's a
12 whole other part of STPA. That slide isn't everything,
13 but --

14 MEMBER BLEY: Well, Mr. Chairman, as we
15 start to get to the rest of these examples, I note we're
16 halfway through the slides for this morning, although
17 continuing with this seems to me really useful but I don't
18 know how much --

19 CHAIRMAN BROWN: I'm about to address that.
20 My game plan as we go on is to try to get through Slide
21 31 before we go on to the last topic.

22 MR. GEDDES: I can pick up my pace.

23 CHAIRMAN BROWN: Now, we need to kind of
24 step -- yes, we're about an hour behind when you hit that
25 point. I will talk to the staff afterwards to see --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 we'll continue after lunch and finish that and we'll then
2 speed that part up.

3 I think the operating experience and the
4 other part I think you can kind of go through and show
5 us how you relate those and then we'll see if we can
6 accommodate a little bit more this afternoon.

7 So if you could use the remaining 12,
8 actually you've got about 15 minutes because that clock
9 is about four or five minutes fast.

10 MR. GEDDES: To get to Slide 31?

11 CHAIRMAN BROWN: To get through Slide 31.

12 MR. GEDDES: Okay. Hold on to your hat.

13 CHAIRMAN BROWN: I took a quick look at
14 those and seen that we don't have to have, based on the
15 earlier comments, that seem to repeat a little bit about
16 what we've all been doing.

17 MR. GEDDES: I think so.

18 CHAIRMAN BROWN: Or emphasize, so go ahead.

19 MR. TOROK: After that, at that point we've
20 gotten through the important part of the presentation so
21 we can shorten up the rest of it as well.

22 MR. GEDDES: Okay, so John gave us a good
23 segue. This is part one. Part two is coming up. I'd
24 like to just briefly point to row seven on this slide.
25 Conceptually row seven represents turbine speed is too

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 low but system flow is too high.

2 John said, yes, that's something we need to
3 consider as potentially hazardous and I said that can't
4 be. He said, Bruce, you don't get it. Things break,
5 valves leak, shafts, bearings, equipment damage, things
6 that, you know, we have to account for that we don't
7 normally think about.

8 So in the next step, we go back to the
9 control structure and after step one we have identified
10 which control actions are hazardous. That's the prior
11 table.

12 Now we overlay the concept of control flaws.
13 I won't go over each one of these but this is a systematic
14 way. This is probably a more difficult way. It takes
15 more judgment and experience to think about these issues.

16 And before you throw anything out you have
17 to stop and think, for example, if a sensor on the
18 right-hand side has inadequate operation, well, could
19 that contribute to the hazardous control action? Maybe.

20 But this is why we have sensor PMs and tech
21 spec surveillance and all the measures and
22 administrative controls and setpoint calcs and all those
23 things to account for sensory operation, response time
24 testing, all those things.

25 Now we can begin to take credit for the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 things that we have at our disposal and if we find
2 something that we can't take credit for we take design
3 steps or administrative controls or a combination of
4 both.

5 Now in the case of the plant that had the
6 actual trip where the governor valve closed when there
7 was a demand signal, they focused on this upper
8 right-hand corner where it says feedback delays.

9 That was the stated root cause of that
10 event, that the enable signal came in from a limit switch
11 sensor too late. Now, we could also focus on other
12 control flaws maybe, but that's the one that they chose
13 as the root cause.

14 They bypassed the limit switch so that when
15 ESFAS initiates a command signal, you get an enable
16 signal immediately without any delay. So here John
17 showed us this list of possible causes of delayed
18 feedback and here's the limit switch interaction.

19 We said stop. You found it. You found the
20 cause of the event before, you know, using the conceptual
21 design information where, of course, the plant found it
22 after it happened. That's very compelling.

23 So we have a couple of slides on blended
24 approaches. Dave, do you want to talk to this briefly?

25 MR. BLANCHARD: Sure. All right, we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 introduced you to the six methods that are in the EPRI
2 guideline and the objective of the EPRI guideline was to
3 try to make some of these hazard analysis approaches as
4 complete as they could be but also perform them with a
5 reasonable level of effort.

6 We've kind of gone through the strengths and
7 limitations of some of them as a part of this presentation
8 and it's not clear that if you pick any one method that
9 you could meet both of the objectives on the EPRI
10 guideline.

11 And so we attempted as the report came
12 together to recommend that, you know, you ought to look
13 for the beneficial aspects of some of these approaches
14 and combine them together, such that you take the
15 advantages of the benefits of several approaches and
16 minimize the impact of the limitations.

17 And here is one possible way to blend some
18 of the techniques we've seen this morning. We have a
19 top-down approach with fault tree analysis and possibly
20 FFMEA going down to the plant-component level and
21 translating the hardware, the failure modes, that I&C
22 controls into digital system-level behaviors that we
23 want to avoid.

24 That then, in turn, becomes the defined loss
25 for a technique such as STPA and then we can go through

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the process like we just saw for the HPCI issue with STPA
2 to continue the analysis into the digital system itself.

3 Now, this transition here between the
4 components and the digital I&C system is not just a
5 one-way street. We wouldn't necessarily have to do a
6 top-down approach, say, with a fault tree analysis or an
7 FFMEA and then hand it off. The communication can go
8 back the other way.

9 The STPA is set up such that it identifies
10 hazards and it's worthwhile going back at that point when
11 you've identified those hazards to see if it's in the list
12 that was handed to you, see the impacts it has on the plant
13 that was handed to you as a part of some of these top-down
14 approaches.

15 This gets to, in part, to the completeness
16 issue we were discussing earlier. If I don't happen to
17 have a failure mode in my fault tree analysis yet it's
18 identified in STPA as something that could happen, the
19 right thing to do is for the STPA folks to come back to
20 the PRA folks and say, hey, I found this hazard. I don't
21 see it in my list.

22 MEMBER BLEY: You just said something that
23 I'm sure in a couple years will drive me nuts if we really
24 proceed with this. There ought not be PRA folks and STPA
25 folks.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MALE PARTICIPANT: I agree with that.

2 MEMBER BLEY: This is an integrated
3 analysis. There's nothing in any of these that's
4 automatic. You don't use a fault tree and get an answer.
5 You got to understand the whole damn system and how it
6 interacts and how it works if you're going to use any of
7 this.

8 And if different people are doing the
9 different parts, why can a PRA if you've got somebody else
10 doing the HRA who doesn't understand the plant model,
11 doesn't work. And this isn't going to work either.
12 They've got to be linked together. You got to look at
13 this as a whole piece.

14 And there's nothing, I really think what we
15 saw in the example you gave us systematizes things, but
16 no matter what tool you're using the person doing the
17 analysis has to think about carefully one way or another
18 and it would really help out.

19 But, you know, I kind of think back to what
20 happened in physics where you had the guys taking the
21 probabilistic approach and they'd get together and
22 they'd solve the same problems and they'd both get
23 answers and they were wrong.

24 And in statistics you had the Bayesians and
25 the other guys, the really best ones that solved the same

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 problems very differently but they'd all adjust what they
2 were doing to take care of what was important by
3 understanding the problem. Get the same answer.

4 I think we can do the same thing here but
5 I think the idea that you get help from the organizational
6 and computational capabilities of the different methods
7 is important and you ought to always depend, I mean, all
8 the tools you have at hand. It really shouldn't be
9 different people.

10 MR. BLANCHARD: They need to communicate.

11 MEMBER BLEY: To me, the same analyst needs
12 the tools and needs to understand what's going on.

13 MR. BLANCHARD: Or a team.

14 MEMBER BLEY: Or a team, but it has to be
15 tightly integrated so somebody sees how all the pieces
16 are fitting together and understands it all.

17 MR. BLANCHARD: And we also see STPA having
18 a very good capability to get into the software.

19 MEMBER STETKAR: Bruce, let me stop a
20 little bit because Dennis got his thing. STPA, when I
21 look at it, is nothing more than a truth table. Thirty
22 years ago he used to yell at me for laying out these
23 godforsaken truth tables. It's nothing conceptually
24 new.

25 It is, I agree, it's a systematic process

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to look at combinations of things. There still needs to
2 be in your nice table here in all of those pink boxes a
3 human being that sits down and says this combination, 37
4 things in a row, is that already hazardous?

5 MR. GEDDES: That's not what I'm saying.

6 MEMBER STETKAR: STPA doesn't do that for
7 you. The spreadsheet doesn't do that for you.

8 MR. GEDDES: Yes, a human being --

9 MEMBER STETKAR: And if you lay it out and
10 you've got 12 billion combinations, by the time your
11 human being gets through number 38, they've lost
12 interest.

13 So just be careful about saying that this
14 methodology -- this methodology got it for your
15 particular example for a simple, single system, pretty
16 doggone simple control.

17 People designing diesel generators
18 bypassed those kind of control functions 50 years ago
19 when they started a diesel because they didn't want this
20 thing to happen. So, you know, some idiot who designed
21 this system who didn't have that experience forgot that.

22 The whole point I think we're making here
23 is that don't rely on these methods as crutches, as Dennis
24 said. It's not the STPA method versus the fault tree
25 method versus the FMEA method. It's a thought process,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 and what's the most efficient tool to implement that
2 thought process?

3 MEMBER BLEY: Well, not just efficient but
4 what can help you avoid missing things?

5 MEMBER STETKAR: Well, yes. Well, when I
6 say, the presumption is you want not to miss things.

7 (Simultaneous speaking)

8 DR. THOMAS: I absolutely appreciate your
9 comment about not relying on methods as crutches. I want
10 to make a couple comments.

11 First, that table that we talked about that
12 I think you said is a truth table, I just want to point
13 out because we started to rush through, that was only half
14 of STPA. The other half doesn't look anything like a
15 table.

16 The other thing is what you said about
17 someone going through the final column and looking at
18 this combination, saying is this hazardous or not.
19 You're absolutely right. It's dependent on the person
20 to do that.

21 One of the differences I want to point out
22 is this is where the method is trying to provide more
23 guidance to the person doing the analysis and that's what
24 it's all about as opposed to, for example, a fault tree
25 where you have a box and now you know you've got to go

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 to the next level.

2 You know you can use an AND gate or an OR
3 gate, but there's not a whole lot of guidance telling you
4 think about, you know, here are the things that you could
5 put -- so that table was trying to provide exactly that
6 kind of guidance in STPA, to help a person think, help
7 an expert, an engineer who's experienced, make sure they
8 don't miss anything.

9 MALE PARTICIPANT: Why don't you talk about
10 methods of reducing the tables too?

11 DR. THOMAS: Yes. So we didn't have time
12 to put this in but there is some material out there and
13 some of it is in my thesis and there's some presentations
14 that we can send you.

15 But there are ways to be really intelligent
16 about these tables where you don't want to deal with
17 thousands or even hundreds of rows, but you can logically
18 reduce these tables quite a bit, down to seven rows,
19 something that's very manageable and something that
20 makes sense intuitively there.

21 You can say, you know, if the flow rate is
22 too high, then maybe the position of this thing doesn't
23 really matter and so you can do this kind of logical
24 reduction and it ends up being very powerful.

25 I actually worked with a nuclear engineer

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 from Brazil and he enjoyed going through the hundreds of
2 rows of these tables and I was very surprised. I
3 disagreed with him. But the first time I went to him he
4 said, you know, I'm learning the process. I didn't know
5 if I was doing anything right.

6 MEMBER BLEY: I'm sorry for laughing.

7 MALE PARTICIPANT: If it were a 10,000-row
8 table, he would --

9 (Laughter)

10 DR. THOMAS: So my experience was really
11 strange. This guy, he loved it and I said how can you
12 love it? It's 200 rows. And he said, well, first of
13 all, I'm learning the method. I don't really know if I'm
14 doing anything right and what was nice is that any given
15 row I knew exactly what the next step was going to be.
16 It was going to be the next row.

17 And he did it in two days and I said, well,
18 you wasted, what, eight hours a day on two days. And he
19 said you don't understand. This is nothing compared to
20 a full-blown hazard analysis that we spend on a FMEA where
21 we generate 3,000 or 10,000 pages of a FMEA.

22 And I said but, still, it's 200 rows. How
23 can you go through this? And he said, well, you know,
24 I liked it and it helped me. So, anyway, I went back and
25 found these ways to reduce the problem and so we don't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 have to do those 200 rows but there are people that like
2 it.

3 MR. BLANCHARD: And interestingly enough,
4 in reducing the size of the table, my reaction to that
5 table is exactly yours.

6 DR. THOMAS: This is an event tree.

7 MR. BLANCHARD: It's got consequences on
8 the end. I can reduce this and --

9 MEMBER STETKAR: You can. The only danger
10 is be careful about getting too automated.

11 MR. BLANCHARD: Oh yes, right.

12 MEMBER STETKAR: Some of these differences
13 make a difference.

14 MR. BLANCHARD: Well, we only got together
15 yesterday afternoon and compared our notes on how we
16 reduced the table, and guess what? It's fact tree.

17 (Simultaneous speaking)

18 DR. THOMAS: Right, right, yes. And for
19 the record, I wouldn't say event tree. I would go so far
20 as to say it's a tree structure maybe but, yes.

21 (Simultaneous speaking)

22 CHAIRMAN BROWN: Once Dennis finishes, I
23 have some stuff to go over for a few minutes and I'll
24 implement it someplace else.

25 But one of the things I took out of looking

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 at these various documents was all the examples and all
2 the discussions fundamentally dealt with feedback
3 control systems, actual plant systems that I put in.

4 But I didn't see any applicability to
5 systems that were set up to do kind of like once-through
6 functions like a reactor trip function and that had
7 multiple redundancies.

8 And so how do you treat a system like that
9 in terms of identifying and fixing the single most
10 critical issue with independent redundant systems as
11 they are really independent? If you use that somewhere
12 and it's not visible, then you no longer have that and
13 I didn't see any of that in the methods.

14 I mean, the method, I like the method. I've
15 seen these type of things for decades and the thought
16 process is, and I agree totally with John and Dennis in
17 terms of the overall integrated look of the thing.

18 But that was a piece I've been struggling
19 with for the last few years, to try to figure out how do
20 we focus and how does the regulatory body enforce that
21 level of independence and the understanding of how
22 important that independence is in the fundamental
23 reactor trip type functions? You've got to have these
24 other systems work but I got to trip when I want it to.

25 MR. GEDDES: John evaluated an example of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 an ESFAS system --

2 CHAIRMAN BROWN: Well, that's ESFAS.
3 That's still got, in a way, it's not the same. I mean,
4 you don't trip those when they -- if you have a failure,
5 you fundamentally don't want them to trip and fail to
6 actuate. You want them to fail to not actuate.
7 Otherwise you're doing, you really can have some unusual
8 circumstances in the plant. Now, maybe some systems
9 it's okay and others it doesn't. How do you
10 differentiate?

11 DR. THOMAS: So there's two ways to use STPA
12 and the application that Bruce was talking about we had
13 an existing design and he wanted to do a blind study to
14 apply STPA and see if it could find the accident, so that
15 was the background for that project.

16 So STPA can be applied to an existing design
17 and when that's the case the existing design has some
18 redundancy that some engineers decided was important
19 here or they assumed independence there.

20 STPA says, well, basically let's question
21 the assumptions, and that's an ongoing theme throughout
22 the STPA analysis as Bruce was mentioning a couple times.

23 And one of the assumptions that it questions
24 is are these things really independent? So if you apply
25 STPA after the fact, after the system is designed, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the basis of the design is that these systems are going
2 to be independent and you apply STPA, STPA is going to
3 try to attack that independence assumption and it's going
4 to try to find ways, find causes that might violate that
5 assumption of independence.

6 MR. GEDDES: Or dependencies and
7 influences between controllers --

8 DR. THOMAS: Right.

9 MR. GEDDES: -- is, I think, what you're
10 talking about.

11 DR. THOMAS: Right, but let me say that STPA
12 is really designed to do a much better job than that.
13 It's designed to help you in the early development
14 process before you have a finished design because this
15 is kind of an efficiency problem, right?

16 If we wait till we have the design already
17 finished and already built and all the major decisions
18 already made, then we're really limited in what we can
19 do. It's very expensive to have changes.

20 CHAIRMAN BROWN: To answer your question,
21 I'm really looking at how you develop that basic,
22 fundamental functional architecture. How do you use
23 these tools to come up with an architecture that has and
24 maintains the independence, does not result in
25 dependencies that are very, very expensive and time

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 consuming to fix later?

2 After the fact, after the stuff's designed
3 and built and installed, it becomes very expensive to fix
4 some of these because those other dependencies are now
5 built in on that very thing that gave you the lack of
6 independence but they're there for other fundamental
7 purposes and it's too late to come up with an alternate
8 approach to doing those.

9 The design stage is what I'm really, I was
10 kind of looking when I was reading these, is there
11 anything in the design stage, particularly the reactor
12 safety world, you know, from both the ESFAS and the
13 reactor trip systems that these tools could allow us to
14 find those in the very beginning when folks bring those
15 systems to us for review, because that's when we see them.
16 That's when they commence in their conceptual level.
17 They're fleshed out.

18 You know, how then can we come to the
19 conclusion that, yes, they, in fact, will operate that
20 design and be as independent as supposed to be
21 functionally? After the fact, in my mind, is already too
22 late.

23 DR. THOMAS: Exactly. Yes, yes.

24 MR. TOROK: We haven't gone that far but it
25 has been suggested that we start applying these methods

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to some new plant designs maybe and looking at it that
2 way.

3 CHAIRMAN BROWN: To some what kind?

4 MR. TOROK: New plants.

5 CHAIRMAN BROWN: Yes, new plant, yes okay.

6 (Simultaneous speaking)

7 MR. GEDDES: And if you can show the two
8 controllers that might share information don't have a
9 hazardous influence between each other, then maybe
10 that's a way to satisfy the independence criteria.

11 CHAIRMAN BROWN: Never make me agree with
12 that.

13 (Simultaneous speaking)

14 CHAIRMAN BROWN: Pardon me? What now?

15 MEMBER BLEY: I was looking at these guys
16 and saying don't take that one, not from you.

17 DR. THOMAS: So I think absolutely STPA can
18 be used for that purpose, to try to pursue those goals.
19 I don't know of an example that's been done in the nuclear
20 -- I think the nuclear examples of STPA we have so far
21 have been after the fact and it's just you got to start
22 somewhere, right?

23 In other industries they have been using it
24 to drive the design and it's been very successful so I
25 think it's something that definitely could help.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: Okay. We're going to
2 have to stop unless you've got some really crisp things
3 you can blow our minds with. This is your next steps
4 slide, right?

5 MR. TOROK: Yes.

6 CHAIRMAN BROWN: I already read it.

7 MR. TOROK: Yes. Okay, well.

8 (Simultaneous speaking)

9 MR. TOROK: Well, I want to say just a
10 couple things really quickly. We have another project
11 where we're looking at applying this method to
12 requirements engineering which gets, talking to your
13 point, how do you get the requirements right so you have
14 everything you need? There's also this notion of tools
15 to reduce the matrix size and those kinds of things.
16 That's fine.

17 Our advisor said, hey, first you guys got
18 to do some more demonstrations and convince us that this
19 really does what you say. So we're working toward that
20 and after that we'll get into this notion of training and
21 whatnot. That's it, so.

22 MEMBER BLEY: Charlie, before you bang the
23 gavel, are we coming back today or are we not?

24 CHAIRMAN BROWN: Yes, they've got a --

25 (Simultaneous speaking)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. TOROK: We'll keep that really brief.

2 CHAIRMAN BROWN: Okay. Yes, right. All

3 right, we're adjourned until 1:00 p.m.

4 (Whereupon, the foregoing matter went off

5 the record at 12:06 p.m. and went back on the record at

6 1:03 p.m.)

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

(1:03 p.m.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: The meeting has now come
2 back into order. We will commence with the
3 EPRI again. Proceeding on with the operating experience
4 review.

5 MR. TOROK: Okay, I'd like to make one more
6 point before we leave this slide. I just want to thank
7 you guys for taking the time to look at this carefully,
8 because you really gave us some great feedback. So,
9 that's my point. Okay, thank you.

10 MR. TOROK: That is very helpful for us.
11 Okay, on failure analysis, we did some other work on
12 common cause failure. Like this was in the, in fact, I'm
13 pointing out this one only because Charlie brought it up
14 earlier. This notion of figuring out design measures
15 that protect you against bad stuff. That's what this
16 report's about.

17 There's defensive measures, there's
18 diversity, and what we've said in here, is hey, you're
19 looking for the right combination of those things. And
20 that's what this report is about. Right?

21 There's no consensus on how you do that
22 right now. But that report's out there. There's a
23 report number, and that's all I wanted to say about it.
24 So it's an awareness thing, okay?

25 Now operating experience wise, back in 2009

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we showed you a bunch of data from U.S. operating plant
2 experience. And the focus here was on common caused
3 failure because that was a kind of a hot-button issue at
4 the time.

5 And this group and the commissioners as I
6 recall said, both said, hey, what's the operating
7 experience? Tell us about this. Go figure it out. So
8 we came back with data from U.S. operating experience.
9 And the bottom line was that, the, software wasn't the
10 big offender. There were other things that were more
11 prevalent in the data.

12 Now since then, we went and did a similar
13 evaluation using operating experience from Korea, from
14 South Korea. Because their methods of -

15 -

16 CHAIRMAN BROWN: When you say you had no
17 more problems, was no more problematic than other CCF
18 contributors.

19 MR. TOROK: What do I mean?

20 CHAIRMAN BROWN: Yes. What do you mean by
21 software in itself? I mean, is there some
22 characterization of what --

23 MR. TOROK: Oh, for our purposes in our
24 reports, software meant, software and digital were
25 almost interchangeable. The idea was, is there a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 problem that happened or an undesired behavior that
2 happened because the system was digital?

3 Had it been analog, would that problem not
4 have happened? It was that kind of thing. And so
5 anything that was digital specific, we called software.

6 CHAIRMAN BROWN: Yes, the fundamental
7 processing was now accomplished with software VICE and
8 analog --

9 MR. TOROK: Yes.

10 CHAIRMAN BROWN: -- op amp type? And that,
11 within that part of it, not necessarily all the other
12 output parts of it. Well there might have some output,
13 but I mean the other actuating type things.

14 MR. GEDDES: For example if there's a
15 memory leak, that's a unique failure mechanism in a
16 digital system. If you enter the wrong set point, you
17 could do it an analog equipment or digital equipment, we
18 didn't call that a software issue.

19 MR. TOROK: That's not called a software
20 problem.

21 CHAIRMAN BROWN: That's okay, that's so far
22 it's -- I understand. I have a vague understanding.

23 MR. TOROK: So it had to be things that were
24 specific to digital that got the system into trouble.

25 CHAIRMAN BROWN: Well specific to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 software, I mean you can have combinational logic, which
2 is analog logic producing digital processing, which is
3 not subject to software failure because it's a hardware
4 based system. So that's another form.

5 MR. TOROK: Yes. It gets subjective in
6 some of these things.

7 CHAIRMAN BROWN: If, I'm not worried about
8 them, I'm just saying when you said digital, digital has
9 two components.

10 MR. TOROK: Yes.

11 CHAIRMAN BROWN: The software based
12 digital, there's hardware combinational logic based
13 digital which --

14 MR. TOROK: That's right.

15 CHAIRMAN BROWN: -- are totally different
16 in terms of their behavior.

17 MR. TOROK: Right.

18 CHAIRMAN BROWN: One's fixed programming
19 software is what that is.

20 MR. TOROK: Yes. For the most part, we
21 meant digital stuff that has software in it.

22 CHAIRMAN BROWN: Yes, okay. Thank you.

23 MR. TOROK: For our purposes. Okay, so we
24 looked at that for the Korean data. We're also
25 continuing to look at operating experience. With this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 project we're just starting to look at the lessons
2 learned from a plant wide upgrade in the Czech Republic.

3 And of course, and after that we expect to
4 look at more operating experience from other non U.S.
5 utilities. So that's, so I think I've got one slide that
6 summarizes and compares the data from Korea with the U.S.
7 data.

8 And just looking at the table, we had 322
9 events. They had 97. So ours was over a 20 year span.
10 Theirs was 26 years, with fewer plants but longer time.
11 Safety related, they did theirs, let's see about 20
12 percent of theirs were safety related. About 15 percent
13 of ours.

14 And in terms of the actual potential CCFs,
15 and safety systems, they didn't see any. We saw some.
16 We saw 11 of which, one we attributed to software
17 problems.

18 CHAIRMAN BROWN: Was that a translation?
19 They said they had none.

20 MR. TOROK: They had none, now --

21 CHAIRMAN BROWN: Is that a translation, or
22 they just don't bother to count them, or?

23 MR. TOROK: Well, yes. We questioned
24 those kind of things. I mean they have different
25 protocols for recording information and those kinds of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 things. So that could be a factor here.

2 But in general we sat down and went through
3 all of the digital events that they identified with their
4 subject matter expert. We stepped through them with our
5 team.

6 In fact, well yes these guys and, I guess
7 Dave was involved. Bruce was involved, and Tween Wynn
8 from BDF was involved, and their principal investigator.
9 And we went through them the same way we went through
10 ours. So we got as close as we could to apples to apples
11 comparisons.

12 On the non-safety side, let's see. We
13 showed 56 events in which there were actual or potential
14 common caused failures at the system or subsystem level.
15 Of those, 14 were, involved software.

16 They had a very similar ratio. Four out of
17 17 for them, involved software. So in that respect, the
18 results were quite similar enough --

19 MEMBER BLEY: Can you tell us anything
20 about this? We've had designers here telling us,
21 they've never seen common caused failures in their
22 software.

23 MR. GEDDES: In safety or non-safety
24 systems?

25 MEMBER BLEY: That's a good point.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 (Simultaneous speaking)

2 MR. GEDDES: Generally speaking, the
3 design centers come here, and they're usually talking
4 about safety systems.

5 MEMBER BLEY: Yes, you're probably right.
6 You didn't find any there?

7 MR. GEDDES: Right.

8 MR. TOROK: Well and there are a bunch of
9 reasons why safety systems are --

10 MEMBER BLEY: Well he did, he found one.

11 MR. TOROK: -- traditionally more robust.

12 MR. TOROK: We found one potentials common
13 caused failure related to software in the U.S. but it --

14 MR. GEDDES: It was in a platform that I'm
15 pretty sure it's not --

16 MR. GEDDES: That's in your old report that
17 you guys, that's the old report.

18 MEMBER BLEY: That's right. That's the
19 old report.

20 MR. GEDDES: But that letter that is from
21 1992, it's with some obscure technology that's not part
22 of one of the design centers we've talked to today.

23 MEMBER BLEY: Oh, okay.

24 MR. TOROK: Okay, anyway so it's, so the
25 point was that, the results were pretty comparable, we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 felt.

2 CONSULTANT HECHT: In the non-safety side,
3 did you look at things like the system platform's, the
4 vertical stacks, the windows operating systems, the
5 graphical interfaces, the plant historians, things like
6 that?

7 MR. GEDDES: Anything that was reported
8 about a digital system, we looked at. And then we
9 narrowed down to these criterion that you see here. If,
10 we did see some cases where the operating system had a
11 misbehavior.

12 But where there was software related system
13 or subsystem common caused failures, they were almost all
14 in the application code. The application software that
15 makes the box do something useful.

16 CONSULTANT HECHT: Does that mean that the
17 things like windows crashes weren't recorded?

18 MR. GEDDES: They were. And we found some
19 of those, but they were not the dominate part of the data.
20 Most of the software common caused failures were
21 incorrect logic, when the box was, you know, when the
22 solution was developed and integrated.

23 MR. TOROK: So it's the application code,
24 not the code that resides in the --

25 MR. GEDDES: Not the one on the operating

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 system.

2 CONSULTANT HECHT: So those failures were
3 independent. You could consider, you know, when windows
4 going down, not causing another operating system on
5 another --

6 MR. GEDDES: Oh, I don't know that we
7 concluded that either way.

8 MR. TOROK: We saw it, we saw it, we didn't
9 see any examples where that happened. We'll put it that
10 way.

11 MR. GEDDES: Okay.

12 MR. TOROK: And the other thing is we saw
13 a number of examples, cases where certain forms of
14 diversity proved very effective. What am I trying to
15 say? Signal diversity, functional diversity, those
16 two, there were a number of events where those two saved
17 the day.

18 For others we didn't see much. Like, for
19 example we didn't see any cases where platform diversity
20 turned out to be a key attribute. You know, for the ones
21 we looked at. Admittedly, it's not a huge data base.
22 Okay?

23 And so we're going to skip, we're going skip
24 PRA. Am I correct? The whole point here was there are
25 some reports we published since the last time we came,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 and titles and the numbers are there. And there are
2 brief summaries of what's in the report that, the focus
3 of it. And I think that's as far as we want to go with
4 the discussion today on those. Okay?

5 We, yes, and one of them had to do with
6 estimating failure rates for digital systems. So we did
7 look harder on that. There's a report on that. And oh,
8 and then, and there's one on modeling digital in PRA.
9 And this was actually, it's interesting because what it
10 emphasizes is the need for that I&C's engineers to work
11 together with the PRA guys to make sense of it. And
12 there's a step-by-step form to do that.

13 So I just want you to be aware of that. You
14 know, again there's a report number and that's --

15 CHAIRMAN BROWN: Okay, I want to go
16 backwards one more time. Back to your CCF table.

17 MR. TOROK: Oh, I thought I was so good for
18 you.

19 CHAIRMAN BROWN: No, you did fine.

20 MR. TOROK: Okay, where do you want to go?

21 CHAIRMAN BROWN: No, I just needed to ask,
22 when you talk about the one on safety related, you had
23 a potential common cause failure.

24 MR. TOROK: Yes.

25 CHAIRMAN BROWN: And the example you gave

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 was a logic. And when Myron asked the question --

2 MR. TOROK: Is the potential CCF from
3 safety on this?

4 CHAIRMAN BROWN: Yes.

5 MR. TOROK: Yes.

6 CHAIRMAN BROWN: That there was, you know,
7 you talked about a logic error or whatever.

8 MR. TOROK: Well I can tell you
9 specifically what it was in this case. Is that what you
10 want to know?

11 CHAIRMAN BROWN: Yes. Because it has a
12 special related to it.

13 MR. TOROK: It's a software and a diesel
14 sequence serve? So there were multiple trains of diesel
15 sequence serves. And it had, they had a diagnostic
16 routine that it went through and checked on the health
17 periodically.

18 And it turned out that, and there were, I
19 think there were four channels here, and they, these
20 diagnostics were staggered in time. So they weren't all
21 happening in every channel at the same time. But there
22 were overlaps in time.

23 And it turned out that one, during this
24 diagnostic sequence, that channel, whatever channel was
25 out at that time, was, would ignore an incoming safety

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 actuation signal.

2 MR. GEDDES: Block safety injection.

3 MR. TOROK: And there were times when two
4 or even three channels were effectively out of service
5 during those times.

6 MR. GEDDES: The requirement was to --

7 CHAIRMAN BROWN: I think you call that a
8 design issue. I mean if fundamentally if --

9 MR. GEDDES: There's an implementation issue.
10 Absolutely, the requirement was to allow a safety
11 injector signal to stop or halt the diagnostic, and then
12 go back into the safety functions, but there was some,
13 a logic problem, but it didn't, it just didn't
14 implemented to the requirements.

15 MR. TOROK: So apparently the requirements
16 were correct. They didn't do an adequate job of checking
17 to make sure that requirement had been met in the final
18 design.

19 CHAIRMAN BROWN: Okay, so it wasn't, I was
20 just wondering if it was the result of a demand or an
21 action that this particular design logic overlapped
22 whatever you wanted, you know whatever the diagnostic
23 being used all the time. And but then there was a demand,
24 and two or three diesels didn't start because of it.

25 MR. TOROK: The famous surveillance test.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: I think it kind of
2 actually happened during a surveillance test?

3 MR. GEDDES: They found it during the
4 surveillance test.

5 CHAIRMAN BROWN: Okay.

6 MR. TOROK: Something didn't --

7 MR. BLANCHARD: The annunciator, didn't
8 come in that should have. I think is the way to look at
9 it technically.

10 CHAIRMAN BROWN: The annunciator did come
11 in?

12 MR. BLANCHARD: Didn't come in that should
13 have.

14 CHAIRMAN BROWN: That should have.

15 MR. BLANCHARD: And in investigating it,
16 they uncovered the root cause.

17 MR. GEDDES: So they initiated safety
18 injection through a, in a test line up and safety injector
19 doesn't come out the other end. Or the diesel sequencer
20 stopped with a --

21 CHAIRMAN BROWN: As a result of a common
22 design --

23 MR. GEDDES: Yes, so in all four divisions
24 in multiple --

25 CHAIRMAN BROWN: Even though they were

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 independent.

2 MR. GEDDES: And they found because of the
3 overlap in time, these are random effects, but there's
4 a 50 percent of the time failure --

5 MR. BLANCHARD: Well, what happened is they
6 would do the automatic surveillance test, and then it
7 would not reset, such that the safety injection wouldn't
8 start the diesels until the next cycle.

9 MEMBER BLEY: Started.

10 MR. BLANCHARD: Started. So there was a
11 period of time of about an hour.

12 MEMBER BLEY: Between the tests.

13 MR. BLANCHARD: Where the safety injection
14 signal wouldn't have started it.

15 CHAIRMAN BROWN: So each of those software
16 loops had X amount of time for diagnostics, that overlap
17 and it's --

18 MR. BLANCHARD: It's the time in between
19 tests.

20 CHAIRMAN BROWN: I'm thinking this, that it
21 just so happened that --

22 MR. BLANCHARD: Right.

23 MR. TOROK: And it was in the plant,
24 operating for what, two or three years before they
25 discovered it?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. BLANCHARD: Well they were doing manual
2 tests and it didn't have a problem during the manual
3 tests. And then they ran for a year doing the automatic
4 tests.

5 And if it was setup to automatically do the
6 sequencer tests, then it had an issue. So they ran for
7 about a year with occasional overlaps between some of the
8 diesels on the sequencer from the board prepper.

9 MR. BLANCHARD: No, it would --.

10 CHAIRMAN BROWN: Do you have any idea how
11 long their diagnostic period was when they doing this?

12 MR. TOROK: I think it was about an hour.
13 I mean that one would go for about an hour.

14 MR. BLANCHARD: No. No. The tests would
15 not take very long, and then the next cycle would start
16 about an hour later.

17 CHAIRMAN BROWN: How long would the tests,
18 theoretically have taken?

19 MR. GEDDES: There's a series of tests. To
20 get through the whole series takes about an hour.

21 CHAIRMAN BROWN: Yes, but how many, how
22 long was it in any operating, main operating, was it a
23 main operative loop or an infinite loop?

24 MR. BLANCHARD: I don't remember.

25 CHAIRMAN BROWN: Probably not. But was it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 a, was this time during the testing, was that like a
2 minute?

3 MR. BLANCHARD: It's, yes.

4 CHAIRMAN BROWN: For that particular test.

5 MR. BLANCHARD: The test didn't take very
6 long, but the tests were staggered about an hour apart.

7 CHAIRMAN BROWN: I understand that, yes,
8 you do them over a period of time to complete the whole
9 series.

10 MR. BLANCHARD: But the problem would not
11 clear until the next test sequence started.

12 CHAIRMAN BROWN: Okay, I got it.

13 MR. TOROK: As I recall over all the system
14 was disabled roughly 15 percent of the time.

15 MR. BLANCHARD: And the 15 percent of the
16 time because they needed two trains of ECCS. And so you
17 had to have combinations of these out before you had a
18 problem.

19 MR. TOROK: And this one, we're with 20-20
20 hindsight. Our digital expert looked at that and said
21 that really wasn't a very good design. They violated a
22 number of design considerations, you know. But it was
23 a learning curve event for them.

24 CHAIRMAN BROWN: The reason I ask, is I'm
25 used to something like a 50 millisecond operating loop

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 of about 15 percent of it taken for a subset of
2 diagnostics, which takes about, what's 15 percent?
3 Seven and a half milliseconds to --

4 MR. BLANCHARD: These are not --

5 CHAIRMAN BROWN: Which is a non-issue in
6 terms of, but if you had that time it takes a minute to
7 do that particular rural segment of tests then you had
8 --

9 MR. BLANCHARD: But it wasn't it during the
10 tests that the problem was --

11 MR. GEDDES: It wasn't that kind of
12 diagnostic test. It wasn't a baked-in feature in the
13 digital operating system platform. It was application
14 logic, developed by the integrator, to self test parts
15 of the system. And it was 15 different tests, all
16 designed to test different parts of the system.

17 So it'd initiate a test. Some tests might
18 take a few cycles, some might take a couple of minutes.

19 CHAIRMAN BROWN: Yes.

20 MR. GEDDES: Right? But to Dave's point,
21 once this blocked condition --

22 CHAIRMAN BROWN: I got you.

23 MR. GEDDES: -- essentially latched, until
24 you reran the tests. So if it's 15 milliseconds or 15
25 hours, its out of service.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Okay, I was worried about
2 something that I had done in the past.

3 MR. GEDDES: Oh, well.

4 CHAIRMAN BROWN: And now you've just told
5 me that I didn't do that. So I'm not worried about it.

6 MALE PARTICIPANT: That's really --

7 CHAIRMAN BROWN: Yes, hold it, is there
8 something we didn't think about?

9 MALE PARTICIPANT: Now he's good for the
10 day.

11 CHAIRMAN BROWN: Okay, that's all, that was
12 all I had on that.

13 MR. GEDDES: Okay.

14 CHAIRMAN BROWN: So you, you're done, then?

15 MR. TOROK: Yes, I am if you are.

16 MALE PARTICIPANT: If you say so.

17 MEMBER STETKAR: Question, I haven't seen
18 the Korea report, but does the Korean experience report,
19 you talked about briefly here, include detailed
20 descriptions of the events themselves?

21 MR. TOROK: They include descriptions of
22 the events, yes.

23 MEMBER STETKAR: That's all I asked for,
24 it's, it is in general more useful than any of the
25 statistics that we derive from things. Just wanted to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 make sure that it wasn't just a brief summary of the
2 report.

3 MR. TOROK: Oh, no, no. There's a
4 description of each event.

5 CHAIRMAN BROWN: Okay, I take it you all are
6 done. Russ if you would like to -- again thank you very
7 much. I want to thank you all very much for putting this
8 together. And then coming here and taking you know, the
9 time to lay all this out in a summarized form, in which
10 some of us can even understand. So it was a very good
11 one, a good report. I mean, I thought it was a good
12 report. So thank you very much.

13 MR. TOROK: Thank you again, for your
14 feedback.

15 (Off microphone comments)

16 MR. SYDNOR: You ready?

17 CHAIRMAN BROWN: Yes, ready when you are.

18 MR. SYDNOR: Okay, I'm Russ Sydnor, Branch
19 Chief of the I&C and Electrical Engineering Branch in the
20 Office of Research. And we collaborated with EPRI, like
21 I was saying this morning, in setting up today's
22 presentation. Our intention was to talk about the areas
23 where we've had collaborative research and we have mutual
24 interests.

25 In looking at digital system failure

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 behaviors, looking at FMEA practices, and looking at
2 hazard analysis. Our purpose and objectives for the
3 staff's presentation here this afternoon. We're not
4 requesting a letter, but we are obviously very interested
5 in your feedback. And that's primarily why we're
6 presenting at this point.

7 Both of the documents we've provided you,
8 both of the research information letters are draft forms
9 so there's a chance for input before we finalize those.
10 And so we're looking for your feedback today.

11 (Off microphone comments)

12 CHAIRMAN BROWN: Gentlemen, if you would,
13 provide some conclusions, summary conclusions, and stuff
14 like that you would , so we'll know what your thought are
15 --

16 MR. SYDNOR: I wanted just to, and I'll keep
17 this short because we're running behind today, leave some
18 context of why we're even doing work in this area. And
19 we, most of our research, or most of our work we do in
20 research is driven, in my area, is driven by research,
21 primal research plans.

22 But we also have user needs and other things
23 we do. In our research plan there's five major topic
24 areas. The two that are highlighted are where the,
25 today's topics fall, into either where we have a number

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 of projects that are looking at the safety aspects of
2 digital systems.

3 And some of our knowledge management
4 initiatives, which is where we put our operational
5 experience assessment piece in that area. Go ahead.

6 The last time we spoke with ACRS was in, or
7 I'm sorry, I got ahead of myself. We issued the research
8 plan in February of 2010, and it was based on previous
9 research plan and results, License Office input, which
10 we went through and extensive review process.

11 But I wanted to really focus on, it was the
12 specific topics we're talking about today had
13 considerable input and feedback from ACRS. Both asking
14 us to look at digital system failure modes and
15 operational experience in a number of letters.

16 And the Commission SRM that specifically
17 asked for investigation of digital system failure modes.
18 And ultimately to look at, can they be, can there be
19 quantified for use in PRA approaches. And so we're going
20 to address that topic today.

21 The other thing I wanted to mention with the
22 current research plan, we try to have a flexible and an
23 iterative research approach. Whereas maybe previous
24 plans had specific research projects outlined and they
25 were just executed.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 The current plan allows for us to learn as
2 we go. To flexibly change from another, a number of
3 standpoints, either from input from the staff, or input
4 we gain from talking to external experts. Go ahead.

5 We last spoke to the committee, in June
6 2011, it was pretty much an overall update of the plan
7 at that time, but we really focused, three areas we
8 focused on, we're revisiting today and want to report
9 further progress in these areas.

10 The first was, we reported on an Expert
11 Clinic that we convened and documented the results from
12 in our research information letter 1001. It really
13 dealt with software uncertainties.

14 In other words, what sort of uncertainties
15 still remain after you've got the good design process and
16 the good software development process. What
17 uncertainties might still remain? And what can you do
18 about those?

19 And so some of our research that we're
20 currently doing, is driven by expert input from that
21 clinic. And as documented in that research information
22 letter.

23 We also issued and talked about it in that
24 meeting, a very specialized look at software FEMA and
25 whether that can, has any feasibility, viability for use

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 by the NRC? And we concluded that in that work, that it
2 didn't.

3 We revisited that a little bit in one of the
4 topics we're going to talk about today. And got some
5 additional input from other experts on that. And
6 operational experience, we also talked about our plans
7 for dealing with that, which were quite extensive.

8 And some of those plans have worked out,
9 some of them haven't. We're going to try to give you an
10 update today. And I understand for time limitations, we
11 may have to cut that part of the agenda, so we'll see.

12 CHAIRMAN BROWN: Until we get there, you
13 can keep it on the list.

14 MR. SYDNOR: But to reiterate again, we
15 refocused our research when needed, based on expert
16 input, which we've over the last several years, we've
17 been getting extensive input from external experts
18 internationally, both regulators, University experts,
19 experts in the field, practitioners.

20 License Office experience, there's been a
21 lot of feedback and experience. Most of which you're
22 well aware of, you don't need me to tell you that from
23 reviews of new reactor designs. And some of the
24 challenges there. Especially with integrated digital
25 systems.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 We also have been responding to specific
2 License Office user needs. One of which is supporting
3 a specific user need from NRO, on hazard analysis. And
4 when we talk, get to that topic today, we'll reiterate
5 how we're supporting that specific user need.

6 And finally ACRS feedback in general, not
7 just what I mentioned before, but go ahead to the next
8 slide. You know, when you guys give us feed back in the
9 Office of Research, and you do that I think bi-annually.
10 Your last report was in 2012, NUREG-1635, a volume of
11 that, these are some of the things you told us in that
12 report.

13 And we believe that we are taking those to
14 heart. We believe that we are addressing those in our
15 research. The red items are things that you
16 specifically feed back to us, as concerns that you had.

17 And so, I think you can judge for
18 yourselves, I'm not going to put words in your mouth,
19 whether we're following these, doing these things when
20 you hear the presentations. I think we are. I think we
21 got the message on these, and I think we are responding
22 to your recommendations and concerns.

23 Finally, today's topics we wanted to talk
24 about three things. Research information letter 1002,
25 which specifically deals with identification of failure

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 modes in digital systems. And reports on work that we've
2 done, primarily from investigating, from talking to
3 external experts and investigating what has been done by
4 a lot of other people in this area.

5 And so it is the second of three research
6 information letters. The first one I already mentioned,
7 which was the Expert Clinic results, which talked about
8 software uncertainties and the problems and concerns
9 with developing safety critical software.

10 And so this one specifically deals with
11 failure modes. And can you or can you not, come up with
12 a distinct set of failure modes that could be used for
13 multiple digital systems. And so that's going to be our
14 next presentation.

15 And we plan a third one, that's really going
16 to address the issue of quantification of such failure
17 modes. And I'm sure we'll get a chance to talk about that
18 one in the future.

19 The second topic and may end up being our
20 last topic if we run out of time, we're going to talk about
21 work we're doing to provide a technical basis for
22 reviewing hazard analysis of digital systems.

23 But this was an area that we were working
24 in, and in our collaborations with EPRI under the MOU,
25 you know, we started sharing information including

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 knowledge about, with the work at MIT and other methods.
2 They were already looking at methods for failure mode
3 analysis, and so we think our collaboration benefitted
4 both organizations in that area.

5 Our work is different from EPRI's. EPRI's,
6 EPRI is focused on providing deliverables and products
7 that the industry can use to do a better job in design,
8 construction, operation. Lots of areas.

9 Our research is focused on providing the
10 staff some technical basis, technical knowledge,
11 technical background for reviewing these hazard
12 analysis, when we would see those.

13 And the first potential use of that, is
14 although it's not finalized yet, is the design specific
15 review standard for small modular reactors,
16 specifically mPower. And so NRO asked us to develop a
17 technical basis for that. To help them in that area.

18 So that was part of the reason we were doing
19 the work. We were also doing that work because of the
20 research plan in investigating better methods of
21 reducing this software uncertainty. And other methods
22 that we could add to our means for reviewing software
23 systems for safety assurance.

24 And so we had several reasons we were doing
25 that work, and the collaboration with EPRI has worked out

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 very well. I think for both parties there. And finally
2 I was going to, we were going to talk about operational
3 experience.

4 It's, we don't have a deliverable to give
5 you there. We wanted to give you a status update on what
6 we're doing, and what type of analysis approach we're
7 thinking about taking. If we don't get to it, that
8 information is in the handout, so feedback would be
9 useful there too.

10 We think right now, we're confident that we
11 can learn from nuclear digital I&C operational
12 experience. We've got, we're starting to build a data
13 base. We've got significant number of events in there.
14 Maybe as many as, I think 600, if I remember right.
15 Potential digital events that we are going to be looking
16 at.

17 So we're confident that we can learn, and
18 our learning is going to be focused on what sort of
19 lessons learned we can throw out of that, from a
20 regulatory standpoint. And how can it help us in the
21 regulatory process?

22 MEMBER STETKAR: There again, because of
23 time, we may not get to that operating experience. You
24 mentioned 600 or so --

25 MR. SYDNOR: And we're not through

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 screening, we're still, we're screening, I don't know,
2 like 20,000 LER's.

3 MEMBER STETKAR: It's 600, it's not 272,
4 however many, have you talked to EPRI, that's, to me it's
5 a notable difference.

6 MR. SYDNOR: Well, I think EPRI's work, I'm
7 not sure you looked at events after 2009, there were
8 events that, where as we continued on. And we're --

9 MEMBER STETKAR: Is it simply a data base
10 snapshot issue? Or is it?

11 MR. SYDNOR: This is one of the things that
12 we faced 30 years ago, the RA, that Ralph might call that
13 a failure of the pen, and Sally might call the explosion
14 of the pen, a failure of the pen. Are you, are we getting
15 into an arena where we're starting to fight about things
16 because of the way we're categorizing events?

17 MEMBER STETKAR: Six hundred, if you'd said
18 300, I would have said, oh okay, sounds like that's
19 probably --

20 MR. SYDNOR: Well some of the, the biggest
21 difference between their number and our number is time
22 difference right now.

23 MEMBER STETKAR: Okay, if that's the case,
24 then --

25 MR. SYDNOR: We're continuing on, and I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 think also, we've gone further back in time in looking
2 at LERs. And we're, right now we're focusing on
3 licensing event reports over the last 20 years, I think.

4 MEMBER STETKAR: But again --

5 MR. SYDNOR: And what I've done --

6 MEMBER STETKAR: -- there are some people
7 who looked at only licensee event reports, where somebody
8 said, help, help. Response, we fixed the pump. The
9 pump broke really because it had a little bit high
10 vibration that's out of spec on a regulatory -- and it
11 was still running. So I'm curious, just to keep that in
12 mind. We're not going into the operating experience
13 today, but --

14 MR. SYDNOR: Okay.

15 MEMBER STETKAR: But that difference just
16 caught my attention, that --

17 CHAIRMAN BROWN: We're close to being back
18 on schedule, so.

19 MR. SYDNOR: I wouldn't focus too much on
20 the number differences at this point, there's different
21 time frames and our initial screening was taken at a
22 pretty high level so we don't miss anything.

23 MEMBER STETKAR: I would hope there's some
24 eventual meeting of the minds on that, because that's one
25 of the lessons that we learned a long time ago. Lots of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 loss, like power events for example. People argued
2 about, you know, did we have 3 or 300 over a similar period
3 of time.

4 Just because of what one person might have
5 assigned to that set of words. And that can create real
6 problems for reviewers who are looking at operating
7 experience and looking at perhaps quantitative
8 assessments. And licensees who are using other
9 references to do the same thing.

10 MR. SYDNOR: That's good, that's good
11 feedback.

12 MEMBER BLEY: Part of that, definitional
13 problems, John, talking about from the past, it might be
14 applicable here. One person looking at it was defining
15 it in a way such that electric power is lost and stays
16 out more than some time.

17 Where that was really mixing the model in
18 with an event, the response model. And that kind of
19 thing, you've got to be careful about.

20 MEMBER STETKAR: There's other things.

21 MR. SYDNOR: There's lots more.

22 MEMBER STETKAR: I saw this thing, and it
23 might have happened, this other thing might have
24 happened, so I'll count it as a possible event.

25 MR. SYDNOR: The feedback's welcome.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: That's just feedback.

2 MR. SYDNOR: Just real quickly. Just the,
3 and the last bullet there. The reason that's a negative,
4 is that when we talked to you two years ago, we had high
5 hopes for utilizing some non-nuclear data that we'd
6 gotten from NASA.

7 And we're also still at that point,
8 participating in an international effort called COMSYS,
9 which the organization of economic development NEA was
10 sponsoring. Since that time, COMSYS is now not
11 operating any more. We never could get the cooperation
12 from the other countries, even the number of countries
13 participating, and even the ones that were participating
14 were not really reporting data.

15 The U.S. had 90 percent of the data that was
16 in the data base, and it got to a point where my office
17 director said why are we, we can do this ourselves, we
18 don't need the participation.

19 MEMBER STETKAR: It's really interesting
20 because in your initial lead in to this introduction, you
21 said there's been a whole lot of interest in this,
22 internationally, from and domestically --

23 MR. SYDNOR: Well we are still doing more
24 in one on one collaborations with individual countries.
25 We tried to solicit from them their operational

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 experience.

2 I'm just pointing out that this particular
3 initiative because it, number one it required funding,
4 it required travel, and so countries weren't supporting
5 it adequately and then, so the organization essentially
6 shut it down.

7 I just wanted to make you aware of that,
8 because we had talked about it a number of times. And
9 in the case of the NASA data, there was a lot of good data
10 there. Translating that to something in our domain
11 proved to be virtually impossible.

12 Because of the way they categorized the
13 data. It was different from missions, and became very
14 complex and something we eventually had to give up on.
15 Because we were just never going to be able to translate
16 it usefully to --

17 MEMBER STETKAR: That's just really sad.
18 Because of the, you all know there's a lot more operating
19 experience with digital software systems in nuclear
20 plants internationally, many more years anyway.

21 MR. SYDNOR: Well like I say we have
22 collaborations with Koreans, we have collaborations with
23 the French. Actually through our contacts with the
24 French, they've made us aware of significant, actually
25 it would be with EPRI too. And so via what their, because

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 we have an MOU with them, we also get feedback on some
2 of the same information they're seeing. I think it was
3 --

4 CONSULTANT HECHT: Russ, can I ask a
5 question? With respect to the COMSYS data, one of the
6 things that it had with it, was not only the specific
7 records, but the fields in the records. And it was
8 rather extensive list of fields. So, I thought too many.
9 And that might be one of the reasons why other countries
10 didn't want to participate.

11 But one of those things the fields did, is
12 it did give you enough specific information, which has
13 a tendency to get kind of aggregated in the description,
14 are you using any of that information in the?

15 MR. SYDNOR: Well we still have that. And
16 actually the data base still exists and we still have
17 access to the information that was in there. It's just
18 that people weren't contributing new information, other
19 than the U.S.

20 We had Karl Sturzebecher, who you may
21 remember, worked for me in research before he moved to
22 NRR, and actually entered a lot of event data, U.S. event
23 data.

24 CONSULTANT HECHT: So are the additional
25 LERs being entered in that format, or what?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SYDNOR: We're still looking at that.
2 At the, that was part of what the discussion was going
3 to be, to talk about what we are doing in that, and
4 solicit feedback. So if we can get to it, we'll, we can
5 talk about it.

6 Do I have another slide there? I don't
7 even remember. No. That was it, so with that I'd like
8 to introduce Dr. Sushil Birla and Mauricio Gutierrez.
9 We're going to talk about research information letter
10 1002, on digital system failure mode identification.

11 MR. GUTIERREZ: Okay, good morning, and I
12 thank you, Russ. I'll just say again, my name is
13 Mauricio Gutierrez. I'm with the Instrumentation
14 Controls and Electrical Engineering Branch. I'm here
15 with Dr. Sushil Birla. And we're here to present to you
16 the work we're presenting in research information letter
17 1002. And it's on the topic of identification of failure
18 modes and digital safety systems.

19 I guess I, before I start, I'd like to
20 acknowledge some of our other team members who have
21 supported this work. I came in and began work on this
22 in 2011. And a lot of work was done before I came on
23 board, Luis Betancourt, Derek Halverson, of course
24 Sushil and Russ Sydnor here.

25 And I guess as we developed this product,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 we've also received feedback from other staff within
2 research and also the licensing offices. And we believe
3 that's made it a better product.

4 So the research information letter at this
5 point, is in draft form. I will present it to you, and
6 we're happy to get your feedback and to address any
7 comments that you may have before we issue a final
8 version.

9 So just a quick outline of the talk. First
10 I'll give you a brief background, information on RIL.
11 I will state our objectives. I'll present the research
12 method we used, the findings, what we found from our
13 review of different documents and from information from
14 different experts. Present the results and
15 conclusions, and I'll discuss some of our next steps.

16 So quick background here. This, these
17 concerns that the ACRS has had on failure modes, go back
18 a long way. They have their roots, I guess with the
19 commission direction to risk inform the licensing
20 process.

21 But these concerns really came to fruition
22 to us, beginning this work that we're presenting here,
23 in 2008. When the ACRS reviewed digital I&C interim
24 staff guidance 03, on the review of new reactor digital
25 instrumentation and control probabilistic

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 risk assessment.

2 Your letter and your meeting with the
3 commission, lead to a staff requirements memorandum,
4 which it at the origin of this work. There's been some
5 other concerns that have come about as time went on.

6 In 2010, you sent us a letter, or you sent
7 a letter to the, sent the letter and you had a
8 recommendation in there, that software failure modes and
9 effects analysis methods should be investigated and
10 evaluated, to exam their suitability for identifying
11 critical software failures that could impair reliable
12 and predictable digital I&C performance.

13 So the, purpose of this presentation here,
14 we're really trying to link it back to the staff
15 requirements memorandum, which is, which was issued in
16 2008. The commission directed the staff to report the
17 progress made with respect to identifying and analyzing
18 digital I&C failure modes. And to discuss the
19 feasibility of applying failure mode analysis to
20 quantification of risk associated with digital I&C.

21 So I believe in 2009, the commission was
22 briefed. NRR took the lead, and basically at this, at
23 this meeting in June 6, 2009, it was stated that research
24 would work on this issue.

25 So at the last meeting here, we began to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 present to you some of our findings. And these findings
2 are directly linked to the first part of the staff
3 requirements memorandum here. The first part was
4 presented in RIL-1001, which is on software
5 uncertainties.

6 The next part here, that's greyed out here,
7 NUREG/IA-0254 was a collaborative effort with IRSN. And
8 we presented some work on software fault modes and
9 effects analysis, the suitability for regulatory
10 assurance.

11 Here in RIL-1002, we're going to present
12 information mainly on identification of failure modes in
13 digital safety systems. The second part will be
14 addressed in RIL-1003, and we hope to have that at least
15 in draft form by February 2014.

16 CONSULTANT HECHT: Can I make a comment?
17 You use the term fault mode.

18 MR. GUTIERREZ: I'll come to that in two
19 slides.

20 CONSULTANT HECHT: Yes.

21 MR. GUTIERREZ: Yes.

22 CONSULTANT HECHT: Thank you.

23 MR. GUTIERREZ: So just another view of
24 what's, what happened, I guess after 2008 when we
25 received, when you issued your letter and we got the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 direction from the commission. The letter was input to
2 our digital research plan, and then we formulated
3 different activities to address what was in that research
4 plan.

5 The first effort we had, was we held an NRC
6 expert elicitation process. And we presented to you the
7 work in RIL-1001. Around the same time, or a little bit
8 after RIL-1001, that work began, and the expert
9 elicitation process began there.

10 IRSN reviewed the digital research plan and
11 we found that we could collaborate in some of these
12 topics. The last bullet in the background there, about
13 software failure modes and effects analysis methods, was
14 also input into NUREG/IA-0254.

15 And I think part of this, the reason for
16 having this slide up here is to communicate that, you
17 know, everything isn't in it's own bubble. I mean we are
18 learning through our efforts, and it is impacting other
19 work.

20 So this issue about, you know, how do we
21 evaluate digital safety systems? We're learning
22 something in each one of these activities that we have.
23 We're trying to logically present that information and
24 some of that information is also impacting other work.

25 So for example, you'll hear about RIL-1101

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 later today. Luis Betancourt and Dr. Birla here, will
2 present that information. The results of some feedback
3 here, you'll see the safety demonstration framework in
4 green, that was some specific feedback that we received
5 at the NRC expert elicitation clinic, for I guess
6 throughout the process.

7 And that's something we're beginning to
8 explore. It's another way of demonstrating that a
9 safety goal has been met. I guess you make a case by
10 presenting evidence to demonstrate that you've met a
11 claim that you're making.

12 And we're not losing sight of the overall
13 goal of what we're trying to do with all these projects.
14 And that's improve regulatory guidance.

15 CONSULTANT HECHT: Can I ask a question?
16 That, you used the term safety case. Do you mean the
17 safety cases such as originally proposed at the
18 University of York, and subsequently explored in Europe
19 and used here, or just, is that a more general?

20 DR. BIRLA: More general.

21 CONSULTANT HECHT: Okay.

22 DR. BIRLA: So the project is in the user
23 need stage, meaning acquiring the needs, understanding
24 the issues from other regulatory experts. Via
25 experiences in Finland, France, UK, Sweden, and in RCNRO.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 And then determining what the common pattern of issues
2 is, and how a better framework could address these
3 issues.

4 So we don't think that the traditional
5 safety case paradigm that you've seen, published
6 literature, or in Tim Kelly's work at the York University
7 is going to hit on the issues directly, as they have been
8 manifest in the last five, six, years. That's not what
9 we're reporting on today, just in answer to your
10 question.

11 CONSULTANT HECHT: All right. Thank you.

12 MEMBER STETKAR: Before you read this,
13 let's you know, a couple of statements here in the report
14 that I guess, bother me. Or make me curious. In the
15 executive summary, it says, "Results and conclusions
16 presented in this RIL concern assurance of digital safety
17 systems. The results and conclusions are not intended
18 to address issues related to quantifying the reliability
19 of digital systems.

20 As such, results and conclusions about DI&C
21 failure modes and software fault modes discussed in this
22 RIL may not be applicable to NRC research on the
23 development of probabilistic models for DI&C systems for
24 inclusion in Nuclear Power Plant Probabilistic Risk
25 Assessments."

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 And back in the Appendix E, there's a
2 statement, "While these two areas of research (i.e.,
3 digital I&C PRA and analytical assessment of digital I&C
4 systems) are closely related in many ways, it should be
5 emphasized that they are intended to support very
6 different applications.

7 The research in the body of this RIL is
8 focused towards assurance of safety critical digital
9 systems while the PRA research is focused on quantifying
10 failures caused by software in terms of failure rates and
11 probabilities.

12 As such, the conclusions about the methods
13 discussed in RIL-1002 may or not be appropriate for the
14 intent of the PRA research and vice versa."

15 Could you explain why? To me that sounds
16 like the PRA and this are divergent, rather than
17 convergent. If you're defining failure modes for one
18 purpose, and you're saying well that purpose may not
19 satisfy the needs of PRA, because all they're interested
20 in doing, is quantifying numbers.

21 I'd say that research should probably get
22 together and develop research that's consistently
23 focused on one issue. And that's determining how
24 hardware and software can fail. And understanding the
25 importance of those failures.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So I'd like some explanation about those
2 statements that say, we're doing this over here. And
3 research is doing this over here for PRA, and almost
4 sounds like we're not talking to one another.

5 DR. BIRLA: I'm looking at the EPRA expert
6 back there, if he wants make comment? Did I --

7 MEMBER STETKAR: I know that for some
8 reason, PRA is only interested in, as it said back there,
9 in all of those numbers. Six significant figures, times
10 ten to the minus three, is what they're interested in.
11 And you're interested in something --

12 DR. BIRLA: Assurance, security.

13 MEMBER STETKAR: Okay, I'll get to
14 assurance later, when we're all finished, because I don't
15 understand any of those statements about assurance
16 either.

17 DR. BIRLA: Okay.

18 MEMBER STETKAR: But first, I'd like you to
19 address this issue about why, what you're doing, may or
20 may not, could be or might not be, relevant to what
21 research, it says research, is doing for PRA, for digital
22 systems.

23 DR. BIRLA: Yes, so the work that Mauricio
24 is reporting on, and the conclusions that he has
25 reported, are focused on utility in licensing,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 deterministic licensing reviews.

2 MEMBER STETKAR: So failure modes for
3 digital I&C for deterministic licensing, are different
4 than failure modes for digital I&C, for PRA?

5 DR. BIRLA: The purpose is different. So
6 there may be a utility, some utility for PRA purposes --
7 (Simultaneous speaking)

8 MEMBER STETKAR: Let me bring you back, I'm
9 going to keep bringing you back to my favorite little
10 motor operated valve, because that's simple. Fail to
11 open, fail to close, spurious open, spurious closed.
12 How are those failure modes different for doing a
13 deterministic licensing based evaluation of a system,
14 versus a risk assessment of that system?

15 DR. BIRLA: Well we can not address how a
16 PRA activity would use failure modes. That's just a
17 different research direction. And you have had separate
18 meetings with them on what utility they had served.

19 MEMBER STETKAR: Part of our problem is
20 separate meetings.

21 DR. BIRLA: Yes.

22 MEMBER STETKAR: And here, I hear,
23 separation continual.

24 DR. BIRLA: Yes.

25 MALE PARTICIPANT: Institutionalized.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Institutionalized,
2 separation continued.

3 DR. BIRLA: Our focus is on supporting the
4 domestic licensing issues.

5 MEMBER STETKAR: Let me ask you this
6 Sushil.

7 DR. BIRLA: Yes.

8 MEMBER STETKAR: Of those four failure
9 modes, which I'm kind of interested in, if I'm drawing
10 a fault tree, which of those are not relevant when you're
11 making a safety determination, in a deterministic
12 licensing applications?

13 DR. BIRLA: Okay, listen to the rest of the
14 presentation.

15 MEMBER STETKAR: I'm asking you about that
16 now. I'm not asking about the --

17 DR. BIRLA: Yes, we're not talking about
18 valves, we're talking about I&C, particularly
19 programmable I&C.

20 MEMBER STETKAR: Part of the ACRS's concern
21 for the last ten years, has been this notion of we'll look
22 at it for our purpose one way, we'll look at it for another
23 purpose a different way. And what I believe the
24 committee has been trying to do, is to reach some sort
25 of consensus in closures. So I'll bring you back to that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 valve.

2 DR. BIRLA: Yes, so this is what drives the
3 research path. And you can not have well bounded
4 economic research if you drive to pursue too many
5 purposes. And in this case, that is the situation.

6 MEMBER STETKAR: You can't have well
7 bounded economic research if you try to pursue divergent
8 approaches either.

9 MR. SYDNOR: May I comment?

10 MEMBER STETKAR: Spending my dollar twice,
11 to have two different people decide that slightly
12 different nuances on the same failure mode, might apply
13 to two different applications --

14 DR. BIRLA: I don't think that's happening.

15 MEMBER STETKAR: -- doesn't seem to be
16 efficient expensive research.

17 DR. BIRLA: That's not happening.

18 MR. SYDNOR: May I address that?

19 MEMBER STETKAR: Sure.

20 MR. SYDNOR: I disagree we're divergent, we
21 work in the same office. And we collaborate with Kevin
22 Coyne, Ming Li is here, who has now taken over that effort
23 from Alan Kuritzky. We, they, when they do research we
24 talk about what they're doing. We review what they're
25 doing.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 They reviewed this product. Some of the
2 words that are in there, are words that they asked us to
3 specifically add to differentiate --

4 MEMBER STETKAR: Okay. Maybe I'm speaking
5 to the wrong people.

6 MR. SYDNOR: No, I'm just saying, you're
7 saying we're divergent, I don't agree with that. I'd say
8 we're on parallel paths. In that they're focusing on PRA
9 methods, which I have no body in my group who's an expert.
10 I do have people that are expert on digital systems and
11 how they behave.

12 DR. BIRLA: And your concern that the
13 agency's spending money two different places and two
14 different directions for the same failure modes is not
15 correct. They're not.

16 MEMBER STETKAR: I hope that's the case.

17 DR. BIRLA: They're not.

18 MEMBER STETKAR: As we, as I said the --
19 that I saw there --

20 DR. BIRLA: Both divisions have cost
21 populated reviews and are aware of what each is finding.
22 So anything they have done with the risk --

23 MALE PARTICIPANT: Is included here.

24 DR. BIRLA: -- at least six people know
25 about that. They review that work. Anything that we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 produce, they review our work.

2 CONSULTANT HECHT: Can I offer, just some
3 insights from defensive industry work. I do most of my
4 work. There is a place, or there is a precedent for
5 separating qualitative failure mode studies from
6 quantitative probabilistic estimates of success or
7 failure. We call it reliability, in that world.

8 And when we get a failure rate, when we try
9 to do probabilistic estimates, we speak about an
10 aggregate failure rate. And we don't necessarily try to
11 say what the failure modes are.

12 In most cases the failure modes are, the
13 thing stops working. So that in the parlance of the
14 failure mode discussion that was presented earlier, that
15 would be a crash. Or a hang. And we didn't, we don't
16 do that. We just say the thing, it's not providing the
17 service overall. And statistics aggregating it that
18 way, are often much easier to collect than they are to
19 say how many, what the distribution is in, within that
20 overall failure rate.

21 And so we do have both qualitative analysis,
22 which is the FMEA, and the quantitative analysis, which
23 is the reliability prediction. And those are both
24 delivered, and those are both used to establish the
25 operational suitability of the system.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 So I, there is some basis, some reason for
2 keeping things together. There's some reasons for
3 keeping things separate. And it's a difficult problem
4 to --

5 MEMBER BLEY: Well before we leave this,
6 look we, the reason we do quantitative analysis, the
7 reason we do qualitative analysis is to understand how
8 things work, how they fail, and to do something about it.
9 And this morning we heard from EPRI about what they've
10 put together and their levels of interest approach.

11 And that's looking at how these things fit
12 within the systems they work with, and how the failure
13 modes they can exist, be they software platforms or be
14 they the software itself, or be they huddler. How
15 they're all interrelated, and neither.

16 I like when you say that you're interacting.
17 Some of the words here, and some of where Sushil was
18 speaking earlier, trouble me, as they troubled John.

19 And I guess I look at the studies that have
20 aggregated so far you don't know what to do about
21 failures, as not being particularly helpful. And we're
22 trying to avoid that. So I'd let you go ahead, but I --

23 DR. BIRLA: Yes, you --

24 MEMBER BLEY: -- I really think we're talking
25 about the same thing on both sides of this whether you're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 in regulatory deterministic analysis, or PRA, which you
2 can't do very well in some of these systems just yet. And
3 the thing we've been pushing in that previous letter, is
4 about making sure people have a common understanding of
5 how things work, and how they fail, and how they interact.

6 DR. BIRLA: Yes, and I --

7 MEMBER BLEY: So, I really hope we're
8 heading that way, and I thought we were when I looked
9 through most of the material, but -- go ahead.

10 DR. BIRLA: Yes, John's point was, are we
11 doing failure modes, studies, research, how things fail
12 in two different divisions, in a divergent way, and we're
13 not.

14 MEMBER BLEY: Okay. That's fair.

15 MEMBER BLEY: Some of the words sounded that way,
16 and some of what you said earlier sounded that way, that's
17 what got us started.

18 DR. BIRLA: Well the, and the statements
19 that John read, were really put together in collaboration
20 with the other divisions, but they were --

21 MEMBER BLEY: But see if that's the case,
22 if the other --

23 MEMBER STETKAR: If the other division, the
24 risk assessment people are saying well, qualify what
25 you're doing, because we're interested in something

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 different. The reason that, I'm interested in
2 understanding why different arms of research need to have
3 that difference and what's the fundamental basis for that
4 difference?

5 DR. BIRLA: Difference in using --

6 MEMBER STETKAR: That brings me back to my
7 goofy valve example.

8 DR. BIRLA: Yes, the difference in using
9 the information. So they're not doing any research in
10 understanding how things fail. They're using that --

11 MEMBER BLEY: Well they're using yours, so
12 there ought to be a common basis.

13 MEMBER STETKAR: That's right.

14 MEMBER STETKAR: That's what we're saying.

15 DR. BIRLA: But they are also using other
16 people's, or at least being part of the probabilistic
17 risk group, which could be producing some other
18 information.

19 MEMBER STETKAR: Well but, I'll play the
20 devil's advocate.

21 DR. BIRLA: Yes.

22 MEMBER STETKAR: And if they're only
23 interested in putting numbers into bins to create failure
24 rates, and then hoping that they will then look at things
25 and see, oh, here's something I can call a failure mode.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 There's a real danger.

2 DR. BIRLA: Well, Ming's there to answer.

3 MR. LI: Hi, my name is Ming Li, and I'm
4 office research, PRA division and PRA branch. I believe
5 the reason we put that statement. We recommend to put
6 that statement in the report.

7 We believe that we do not have a solid ground
8 of how to do the digital and the PRA. So we want to leave
9 room. We're not saying that definitely, will show their
10 work, we can not use.

11 We just try to leave room in there for
12 future. Because we don't know where there are
13 difference. We don't know how to use our research to
14 allow each other. But definitely, I believe there are
15 common ground we can share each other, for failure mode
16 perspective.

17 And the failure mode is a very key concept
18 to reliability and the PRA. So we also, the PRA also
19 studied, the you know, like the event train. We
20 studied how system fails, but at the very high level.

21 So we do care how systems fails, but
22 normally we don't care for understand their statement,
23 they're incorrect operator in that statement. How that
24 incorrect operator influence the overall power plant
25 operations.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 We don't go that level of detail. Normally
2 we stay at a little bit higher level. So I think that's
3 where --

4 MEMBER BLEY: You working on the level
5 three PRA too?

6 MR. LI: No, I don't.

7 MEMBER BLEY: Okay.

8 MR. LI: So I work on the --

9 MEMBER STETKAR: Probably for the purpose
10 of this meeting, we should just proceed here. There's
11 some troubling things that have been said. And I'll just
12 put that on the record.

13 MR. SYDNOR: Well I think your asking
14 questions, that we don't have the right people here to
15 answer your questions on this. And that's not fair to
16 DRA and to the --

17 MEMBER STETKAR: Right. That's why.
18 Thanks.

19 MR. GUTIERREZ: So I'll proceed. So the
20 two objectives here. The first one is directly tied to
21 the SRM, and that's really the focus of our effort here,
22 to report the progress made, excuse me, with respect to
23 identifying and analyzing digital I&C failure modes.

24 The second objective is to report the
25 findings resulting from the staff investigations on the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 efficacy of software fault modes and effects analysis,
2 as a method for identifying faults leading to system
3 failures, impairing a safety function.

4 Dr. Hecht, you had asked the question about
5 the terms failure, fault and fault mode, I think,
6 earlier. So I can briefly go to aside here.

7 The use of the terminology in the literature
8 that we reviewed, and in the information that we obtained
9 from our experts. At some times, I guess it wasn't
10 always as consistent. And we tried to choose terms that
11 would facilitate how we communicate what we learned.

12 So we chose definitions that were based on
13 our regulation, on our regulations, and from standards
14 of authoritative bodies such as IEC, or IEEE. And just
15 to go over some of these definitions here, we restricted
16 our use of the term failure, to mean that it's the
17 termination of the ability of an item to perform a
18 required function.

19 A failure mode, we understand to mean it's
20 the effect by which a failure is observed to occur.
21 Another way of understanding that, is that it's the
22 manner in which failure occurs.

23 A fault is restricted to mean that it's the
24 state of an item characterized by the inability to
25 perform a required function. Excluding you know, during

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 preventive, during activities such as preventive
2 maintenance, other planned actions or lack of external
3 resources.

4 And a fault mode was defined for, as one of
5 the possible states of a faulty item. And these
6 definitions, specifically a fault and fault mode, have
7 their origins in an IEC standard. I believe it's 60050,
8 if I have that correct.

9 CONSULTANT HECHT: Okay, so far, so good,
10 but I would argue that, when we say software failure mode,
11 we're being a little bit sloppy, but I think it's
12 generally understood that when my computer crashed, you
13 know, using windows or whatever.

14 That was a failure. It's true that, the
15 software didn't suffer any fracture, didn't burst,
16 didn't fail to close or open, it's just there. But the
17 integrated system, which is what we're really interested
18 in, failed.

19 And if, let's face it, it's a little bit
20 awkward to say a system failure induced by software
21 failure. So that's I think why we say software failure
22 mode. And the reason why I would recommend conforming
23 to basically, you know, the universally used industry
24 usage.

25 Is that when you start communicating with

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 others, and they say well the NRC does software fault mode
2 analysis, but we do software failure mode analysis. And
3 depending on what the motivations of the speaker are,
4 they say that's something completely different. And in
5 fact it isn't, and it shouldn't be. Is you know, it's
6 going to cause problems.

7 And you know, I was thinking about an
8 extreme case, so I was thinking about some hapless
9 engineer, who accepts the failure modes and effects
10 analysis by a platform vendor such as Siemens, or
11 Rockwell or whomever.

12 And it's called the failure modes effects
13 analysis, and he includes that, and that's provided by
14 the applicant as part of the whole licensing basis, and
15 he approves that design. And later on something bad
16 happens.

17 And he gets, and he's called to answer for
18 what he's, his decisions were. And the first question
19 will be from the indignant lawyer from the proponent of
20 the other side for whatever reason, saying you stupid
21 idiot.

22 NRC uses software fault modes analysis, and
23 here you are accepting a software failure modes. Now I
24 understand you haven't yet gotten to the point that the
25 NRC does that, but in this environment, I would recommend

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 that, conforming to the industry terminology.

2 The other thing I would say is that we had
3 an example a little earlier today, about the common mode
4 failure caused by the interleaving of the testing and
5 operational sequences in the digital sequencer. And
6 that's an example of some software actually damaging
7 other software.

8 Because we have the operating system, and
9 we have the timing loop, basically saying, we're going
10 to allow you this amount of resources to do your job,
11 which is test. And we're going to allow you less
12 resources to do your other job, which is respond to a
13 safety injection signal.

14 And the software actually, even though the
15 instructions and the change of software actually did
16 suffer a failure, because resources that it should have
17 had, or that were intended to have, it didn't have.

18 Just as you could have the same situation
19 with a valve not closing and there would be more water
20 flowing, or more steam flowing through the system, we
21 heard early.

22 So the distinction between a fault and a
23 failure are sometimes very difficult to establish. So
24 for that reason if nothing else, I would suggest that you
25 conform to the usage that everybody else uses.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 DR. BIRLA: So we don't have to respond to
2 that, just continue.

3 MR. GUTIERREZ: Okay, so continuing on, our
4 research method here, and we, Sushil briefed you on this
5 in 2011. It's very well summarized in Appendix, I
6 believe it's Appendix B of RIL-1001.

7 We basically went out and sought out
8 information from subject matter experts. We conducted
9 interviews. We held an expert clinic and we followed up
10 on any references they suggested, while we consulted
11 them.

12 In addition to, improve the validity of what
13 was told or to verify and to make sure that it was
14 consistent across the broadest community possible, we
15 performed supplemental activities that included
16 reviewing over 150 public and non-public articles,
17 reports, journals, conferences.

18 We held the collaborative effort with IRSN,
19 which resulted in NUREG/IA-0254 and we also communicated
20 both formally and informally with experts that were not
21 part of the initial expert elicitation process in 2010.

22 So what did we find? What did we report in
23 this research information letter? Well we found ten
24 sets of system level digital failure modes. And the
25 information comes from a broad set of experts and from

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 a broad set of efforts.

2 We have several NRC collaborative efforts
3 there. We present the failure mode set that was reported
4 in NUREG/IA-0254. We present the information that has
5 been obtained through the WG risk activities, which we
6 touched upon before.

7 We list the, and consider the failure modes
8 that you listed in your letter. We consulted the
9 automotive industry. We looked at cross industry
10 surveys, but our feeling was it included better
11 information from the aerospace industry and also from
12 academic researchers.

13 And with this information, we synthesized
14 the information that we found, the failure mode sets, in
15 order to facilitate communicating what we've learned.
16 So what did we learn?

17 The technical community does not consider
18 any of the sets that are reported as standard or complete.
19 We found that some of the failure modes, they could
20 potentially be construed as being a different
21 characterization of the same failure mode, so we
22 synthesized that.

23 We report that in set K. And we can't make
24 any claims that set K, is complete. There may be missing
25 failure modes, and other legitimate characterizations of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 the failure modes that we synthesized are possible.

2 MEMBER STETKAR: Are you going to talk more
3 about set K, or?

4 MR. GUTIERREZ: Yes, so. And I can present
5 them here. There is a list that we synthesized from the
6 ten sets. Is there any?

7 MEMBER STETKAR: Let me, let me, I've
8 looked through all of this slides here. I'd wanted to
9 talk about set K a little bit. It is the appropriate time
10 to do that now? I guess it is.

11 By-the-way, I like what you did. I think
12 it's really, really useful. Set K, I looked at that as
13 a set of distilled things, that the staff is calling
14 failure modes. I'll call him Ralph.

15 Ralph is better because it avoids, failure
16 caused, failure all of this jargon stuff that just drives
17 me crazy. It's great. If I look at those nine, and I
18 have questions about, gee, are they really a mutually
19 exclusive set?

20 You're concerned about are they complete?
21 One can never demonstrate completeness. I mean people
22 do the same research for another 100 years, and will still
23 say, well it might not be complete. But if I look at
24 those and I look at the set that EPRI had in their report,
25 there's a lot of similarities.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 And you didn't mention EPRI, so I'm assuming
2 that these were developed in a fairly, I know you talked
3 to them, so it's obviously not in a vacuum. There's a
4 lot of agreement. There's some differences, but the
5 differences are relatively small.

6 So it strikes me that if you developed this
7 set of, you've listed eight here. And in the report, you
8 list nine, which one did you drop from this presentation?

9 CHAIRMAN BROWN: There's eight listed in
10 this presentation and there were --

11 MEMBER STETKAR: One, two, three, four,
12 five, six, seven, eight, I can check nine in the report,
13 so --

14 MR. GUTIERREZ: Go ahead, I'll find it.

15 MEMBER STETKAR: Anyway, there's some,
16 less than 100 and more than two.

17 DR. BIRLA: Yes, so the too sharp and too
18 long, are on one row. At least it was my definition of
19 it.

20 MEMBER STETKAR: Five, there's a 5A and a
21 5B, which is --

22 MR. GUTIERREZ: Oh, yes.

23 MEMBER STETKAR: Now it doesn't make any
24 difference. The point here is that it seems that NRC
25 research, from whatever your perspective is, and the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 industry, from whatever their perspective is, seem to be
2 focusing now on something that, I can't speak for the
3 ACRS, but I can speak for me.

4 Seems to start making sense. Something
5 that might be trackable and useable, and serve as a focal
6 point, like my simple valve. And I view that as
7 something really good. There might be some fine tuning
8 required.

9 DR. BIRLA: And we just talked about one,
10 too long and too short here in one row.

11 MEMBER STETKAR: Right, and I have you
12 know, if you want feedback on individual ones, that's
13 fine, I could give you that, but in terms of timing here.
14 The point is the feedback that I had, didn't expand this
15 list to 25, nor did it collapse it to two.

16 But there seem to be, the process that
17 you've worked through, through all the different sources
18 and rationale that's in this report, seem to make an awful
19 lot of sense.

20 And all, you know, that's all I'm saying is
21 that this seems to be good, and it's, when I compared the
22 two reports, not knowing how the different people came
23 up with the different lists.

24 There's a very, very strong, and in some cases direct
25 correlation, and certainly a very large overlap, which

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 gives me confidence that we're close.

2 Now you go on in your report, and maybe we'll
3 hear more about this, to say, no we're not close because
4 we can't be assured that this is a complete set and we
5 need to do more searching, and you can't take this as
6 something that's given. I'm saying --

7 DR. BIRLA: We're not recommending doing
8 more searching. It just that, so basically you might
9 want a verification. Don't take this as a complete set,
10 and you all are getting knowledge that this -- should be
11 it.

12 But if you were to take this as complete set,
13 and that was one of the questions our PRA group asked us.
14 How do you assure this. You can't.

15 CONSULTANT HECHT: You can if you had ninth
16 one saying everything else.

17 DR. BIRLA: Well and again, there are ways
18 of packaging, and construing. We've seen all the way
19 down to two, omission and commission, and everything can
20 be construed to packaging, why not the other two? We can
21 construe to a package and four, five, six.

22 MEMBER STETKAR: I'm not as I said, I've
23 got, when I went through this and thought about them. I
24 had questions about GRB's. I'm trying to think of a
25 mutually exclusive set, that's less than 10 million, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 more than two.

2 And this is a good start. You know this is,
3 I think that from my perspective what the ACRS has
4 struggled with, is trying to focus people down to this
5 level. That's why I say, I personally like this.

6 Because this table is getting to that point.
7 This table, if I look at this table, if I look at what
8 EPRI had in their report, says there seems to be pretty
9 strong consensus about what it is that we will call Ralph.

10 I didn't say fault causes, I didn't say
11 misappropriations, I didn't say --

12 DR. BIRLA: So if you think of what these
13 are, a set of ways in which the safety function can get
14 degraded, we just don't know if it is all the different
15 possibilities that the safety function can get degraded.

16 But if we use this, as you mentioned EPRI's
17 work, as a set of key words in HAZOPs, or as a set of
18 systematic queries.

19 MEMBER STETKAR: That's the whole, that's
20 the whole point.

21 DR. BIRLA: Yes.

22 MEMBER STETKAR: I'll come back to this, to
23 my valve example until people started to think in the
24 sense of, fail to open, fail to close, spurious open,
25 spurious closure, you had people running around saying,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 oh, there could be a burr on the stem of the valve, and
2 that's a failure mode. How do we get data for that?

3 And there could be a nick on the winding of
4 a motor, and that could be a failure mode, how do we get
5 data on that? And you could have a short circuit or a
6 little bit of corrosion on two contacts and that's a
7 different failure mode. How do we get data on that?

8 People run, and how do we know that, that's
9 complete because oh, a rat crawled into the motor and got
10 burned up, and that's a different, that's an external
11 failure mode.

12 The whole point is that this set or some
13 cohesive set that looks like a combination of EPRI and
14 this, tends to focus those discussions. It gives you a
15 set of coherent boxes, if nothing else, to put things in.

16 And a set of consistent boxes that modelers
17 can then use as a potable point, for expanding their
18 models. Now whether those models are fault tree models
19 that develop different causes, or whether they just put
20 data into those boxes to develop failure rates, that's
21 up to different people.

22 DR. BIRLA: Right.

23 CONSULTANT HECHT: Can I make a comment on
24 your point, that some people only establish two,
25 commission and omission. That, there's a work being

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 done by the SAE in a language called AADL, the
2 Architecture Analysis and Design Language. And they
3 have an error annex.

4 DR. BIRLA: Right.

5 CONSULTANT HECHT: And that's very good
6 work. I didn't see it on your set of references, but I
7 would recommend that you to the Software Engineering
8 Institute and see how they have the error annex.

9 DR. BIRLA: Yes, and you'll see that in the
10 next report.

11 CONSULTANT HECHT: Okay. And what they
12 have in that error annex, is they have a hieratical
13 decomposition. So they start with omission and a
14 commission, and they actually add timing, and I think
15 there's one more fourth category that they have.

16 But then they decompose that. And the
17 value of this decomposition, is it allows you to
18 instantiate and specialize your failure modes, which
19 they're using primarily for their design purposes and for
20 their analysis purposes.

21 But you can use that as well, in terms of
22 how you would classify failure experience in different
23 domains. So whereby NASA may be speaking about an
24 attitude control system failure, you may be able to speak
25 about that as an indirect result, and at a higher level

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 as an error of commission.

2 And still be able to include that in your
3 statistics. If we are so lucky as to actually be able
4 to generate those failure rates by failure mode.

5 DR. BIRLA: Dennis, were we done with set
6 K? Myron, I'm sorry.

7 MEMBER BLEY: It's okay. It's a common --

8 MEMBER STETKAR: We're eventually just
9 going to poke it into a blender and squeeze out sausage,
10 I think.

11 CHAIRMAN BROWN: Want to go back to swat A,
12 is what you're talking about. Or doing swat A.

13 MEMBER STETKAR: No, you can go to some.

14 CHAIRMAN BROWN: Okay.

15 DR. BIRLA: I think that discussion can
16 produce a result --

17 MR. GUTIERREZ: Okay. Okay.

18 DR. BIRLA: Yes, just go to the
19 conclusions.

20 MR. GUTIERREZ: So the conclusion's here,
21 with respect to Objective 1. We can't --

22 CHAIRMAN BROWN: Hold it, what happened to
23 9, 10 and 11?

24 DR. BIRLA: Well, the key point was made.
25 He jumped to set K, and recognized that we are on a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 convergence path.

2 MEMBER BLEY: What path?

3 MR. GUTIERREZ: Convergence.

4 DR. BIRLA: Convergence path, yes.

5 MEMBER BLEY: They skipped over pieces that took
6 them to K, that's all I'm saying.

7 CHAIRMAN BROWN: Yes, yes.

8 DR. BIRLA: So you don't have to labor you,
9 with all the different --

10 MEMBER STETKAR: And we heard some of the
11 stuff on failure mode, and effects analysis.

12 DR. BIRLA: Yes, yes.

13 MEMBER STETKAR: Okay.

14 MR. GUTIERREZ: So our conclusions,
15 completeness of a set of failure modes is not assurable.
16 There are major obstacles to identifying all critical
17 failure modes for a moderately complex digital safety
18 system.

19 With respect to Objective 2, on software
20 fault modes and effects analysis, we didn't find a sound
21 technical basis to require any of the techniques that we
22 reviewed from NRC applicants and licensees. And we have
23 no suggested changes to DI&C regulations or guidance for
24 SFMEA.

25 MEMBER BLEY: That's about the most

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 negative set of conclusions, from a positive piece of
2 work, I've ever seen --

3 (Simultaneous speaking.)

4 (Laughter.)

5 MEMBER BLEY: I'm okay. That could be a
6 footnote, you know, you've got a big story, and what you
7 did, and what's good about it?

8 DR. BIRLA: Yes, so the positive is in the
9 next report.

10 MR. GUTIERREZ: Yes, remember this is just
11 part of the story. And so --

12 DR. BIRLA: If we can wrap up all the
13 negatives and say now that's behind us.

14 (Simultaneous speaking.)

15 MR. SYDNOR: He's talking about hazard
16 analysis, not the third reel.

17 MEMBER BLEY: Oh, okay, the report we've
18 got.

19 (Simultaneous speaking.)

20 DR. BIRLA: Yes, in this overview of the old
21 map of research, he mentioned that we're learning from
22 one, and adapting the path in the next piece of work. The
23 next piece of work, is we have analysis, with new
24 guidance, technical basis for that. So the digital set
25 that you caught onto, that set K, basically we took that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 into the next report.

2 MEMBER BLEY: The next report, which
3 probably gives the answer to my question, but I'm going
4 to say it anyway. You know, I've heard about the
5 cooperation with EPRI. You saw the EPRI work, and I see
6 this, and as John says, when you get to K there, there's
7 a lot of similarities, but there's a lot of it isn't here.
8 And EPRI's not wrapped up.

9 I'm guessing you finished this a while back,
10 and EPRI finished their report and we're on parallel
11 paths but not clearly --

12 (Simultaneous speaking)

13 MEMBER BLEY: -- on one path. Anyway we'll
14 leave it at that.

15 DR. BIRLA: Yes, so no, EPRI's work was
16 finished in June. And the set of, let's call them key
17 words that they used, was from a preestablished method.
18 They did not do any other piece, as we discussed this
19 morning.

20 This report went to them the end of August.

21 MEMBER BLEY: Oh, just a few weeks.

22 DR. BIRLA: And this report did not get
23 finished, it's a draft.

24 MEMBER BLEY: Okay.

25 DR. BIRLA: And we, as I said earlier, you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 see nine, eight, could be repackaged into four, five.
2 The same four, five that EPRI had.

3 MEMBER BLEY: Yes you could.

4 DR. BIRLA: So you have to take that
5 intermittent. So intermittently we've got on or off.
6 So at anytime it's on, you can say look, it's on when it's
7 not supposed to be. If it's off. It's off when it's not
8 supposed to be. Well, does it help?

9 So we talked that, Myron used the word
10 decomposition, or giving a little bit more breakdown,
11 might be a little bit more helpful in stimulating the
12 analyst into thinking about the different ways things
13 can go wrong.

14 Now is eight the right number, is nine the
15 right number? Should we have this further decomposed as
16 he was mentioning in the error annex? Six?

17 MEMBER BLEY: You can stop. It doesn't
18 matter. The idea is, here now it, thinking of their
19 report, functional failure modes that apply to certain
20 levels of whatever you call them, you're over here aren't
21 you?

22 Whatever EPRI calls their levels of
23 interest, I guess. And these are functional failure
24 modes that affect certain or maybe all, levels in this.

25 DR. BIRLA: Yes, yes. We look at it that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 way. So when their analyst, any one of the three that
2 you saw up here, if they were to think about how something
3 can go wrong, regardless of whether it was packaged in
4 those four, or five, they'll think of all these things.

5 MEMBER BLEY: That's right.

6 DR. BIRLA: So in that respect, I agree with
7 John's observation that, yes conceptually we are very
8 close. And what you call them, yes, this will continue
9 to be an open ended debate. And we don't want to get hung
10 up on that debate.

11 MEMBER STETKAR: Don't get hung up on the
12 semantics.

13 DR. BIRLA: Yes.

14 MEMBER STETKAR: That's I think that's part
15 of the message, for me. Unfortunately, we do need to be
16 in debate, but sometimes those nuances are real
17 impediments.

18 DR. BIRLA: So a key message from the
19 morning presentation, in EPRI's case, was that they, no
20 component failed, yet something went wrong. And that's
21 really the message we want to drive across. If people,
22 if we use the word failure, failure modes, and people just
23 look for something that broke down, we have done them a
24 disservice.

25 Think more broadly than that. And so they

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 are shifting from their older terminology of failure
2 analysis to hazard analysis, and that is exactly what we
3 are doing. It is really to change that mind set.

4 MEMBER STETKAR: It's certainly, from my
5 perspective would be nice under this MOU, to come to a
6 coherent set. I think you're close, that EPRI and the
7 staff can agree upon, and I think you're close.

8 DR. BIRLA: Yes.

9 MEMBER STETKAR: If I read, I excerpted it
10 on a piece of paper here, a list of bullets from EPRI's
11 report. And I excerpted your nine in the report, and
12 there, there's an awful lot of one to one correspondence.
13 And some difference.

14 But I, but it strikes me that the
15 differences, I don't know whether they're part Lindberg
16 semantics, or whether they're really something that
17 might be better split?

18 DR. BIRLA: Yes, so the differences you're
19 seeing are from nuances or semantics.

20 MEMBER STETKAR: That could very well be.
21 But as I say --

22 DR. BIRLA: Analysis, conceptually, no.

23 MEMBER STETKAR: That they're really, but
24 there are an awful lot of, closer than similarities.

25 DR. BIRLA: Yes, yes. So that leads us

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 into our concluding slide here.

2 MR. GUTIERREZ: Yes, our next steps are
3 to track external research and identification of digital
4 I&C system failure modes. We don't plan to perform any
5 further work on SFMEA techniques. We'll complete the
6 work on RIL-1003.

7 You're going to hear a little bit about
8 hazard analysis next, and we're just beginning this work
9 on the safety demonstration framework. That concludes
10 this --

11 MR. SYDNOR: From our third bullet, John,
12 I'll commit to you that, you know, when we come back with
13 that, we'll come back with the DRA too. We'll come
14 together. And that really we'll do it.

15 (Simultaneous speaking)

16 DR. BIRLA: And that's really why the third
17 piece is a separate report. Because that covers
18 overlap, territory. So we will bring information from
19 the perspective of how things go wrong. And we'll
20 collaborate with them on what that means to our ability
21 to quantify.

22 MEMBER STETKAR: That's different.

23 CHAIRMAN BROWN: Before you leave, after I
24 make, after I've asked my question, we're going to take
25 a break, just to let you know. Since that we're roughly

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 in that time frame.

2 But on Appendix C, to this thing, there was
3 a, at the end, around page 79, there was a, I think C1.1,
4 system and detailed level SFMEA. And this was
5 literature review.

6 And you provide quite a dissertation about
7 on what -- where you summarized, I guess from someone,
8 that detailed software failure modes and effective
9 analysis, that's again page 79, last paragraph, that this
10 is applied late in the design process, when you possibly
11 have pseudo code available.

12 Then you go on to say, performing the
13 analysis, fault modes for each variable and each
14 algorithm need to be postulated. In other words, you
15 need to have some information to do this. The effects
16 must be traced through the code. And in this review that
17 you did, and you enter in an interview with NRC, that PG?

18 DR. BIRLA: Pete Goddard.

19 CHAIRMAN BROWN: Okay, stated that
20 detailed level SFMEA is becoming moot, because it is
21 labor intensive. In particular SFMEA may not be cost
22 effective for systems with adequate hardware
23 protections, which triggered my thought processes a
24 little bit, based on some earlier discussions we had.

25 DR. BIRLA: Right.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: During his interview, he
2 stated that the intent of the software, the FMEA is not
3 to verify the quality of the software. The intent is
4 to demonstrate that it should, if something should go
5 wrong, whether it's hardware or software induced, and,
6 that the software architecture is such that it will catch
7 that something went wrong, and it will handle it in a safe
8 manner.

9 DR. BIRLA: And your example of continuing
10 to hardware protection is --

11 CHAIRMAN BROWN: Yes, okay. It said the
12 important assumption, after that, is, this is your all's
13 writing now, not his quote.

14 Is that it is possible to move to a safe
15 state once something goes wrong. And he further noted
16 that showing you can detect something, a discrepancy, is
17 miles away from showing that you can isolate it
18 correctly, make some kind of recovery and push forward.

19 And that there's no indication that methods
20 in this reference are suitable for assuring or for
21 identifying. I guess I was trying to connect the dots,
22 so see if my thought process was, that I had lost
23 something. Or that I, maybe I was way off base.

24 Because I have definitely been talking
25 about a hardware architecture that helps protect against

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the software. Because it is so difficult to build in
2 enough, whatever it is, diagnostics, or other
3 methodologies in the software itself, to ensure that you
4 can protect something.

5 Fix it, and not have some off side picture,
6 diverse means, it's independent, that take care of you.
7 Is that the message? Was that the message he was trying
8 to send, when he said that?

9 DR. BIRLA: That is part of the message.
10 Basically, he was saying that --

11 CHAIRMAN BROWN: I want to know who he is,
12 so I my thought --

13 DR. BIRLA: Basically then we tried to
14 engage him again, but he didn't want to come back to work.

15 CHAIRMAN BROWN: Is he an NRC employee or?

16 DR. BIRLA: But he was a, very
17 knowledgeable person. He had worked for Hughes Aircraft
18 Company, and then turned into Raytheon. Then Raytheon
19 started a business, in some were saying the auto
20 industry. So he began doing hazard analysis for the auto
21 industry.

22 And finally he retired from that. But this
23 statement was about 15, 16 years ago. And he through his
24 work experience came to the conclusion, that this higher
25 level was more rewarding. In terms of return on your

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 effort. And that higher level is what you heard this
2 morning, described as functional leveling.

3 CHAIRMAN BROWN: Yes, that's kind of what
4 I heard. Okay, so it's consistent with what we heard,
5 and the kind of what I see maybe the direction you guys
6 are heading? Is that?

7 DR. BIRLA: Yes, yes, yes.

8 CHAIRMAN BROWN: Okay. It's not that
9 you're throwing all the babies out with the bath water,
10 or the bath water out with the babies, whatever the
11 terminology is. You're just moving on to a how do we take
12 this information we've got, in perspective, and where we
13 go from here?

14 DR. BIRLA: That's right.

15 CHAIRMAN BROWN: Because your statements
16 were pretty, I agree with John and Dennis, run through
17 and then slam dunk, in these nice negative comments.

18 MEMBER STETKAR: Before you finish the
19 paper, I mean I, obviously you do a lot of scrutiny of
20 the words that, the conclusion does sound really negative
21 there. I think you've done a heck of a lot of good work.

22 And the caveats that you've put in the
23 conclusions about, gee it's not complete, we're not sure
24 what it can be used for, we're not sure that we can
25 determine licensing assurance based on this information,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 is perhaps a bit negative.

2 DR. BIRLA: Yes, but part of it the modesty
3 of the author here. He didn't want to take credit from
4 the next piece of work, but basically the positive
5 message is in the next piece of work.

6 So your observation is well taken, we
7 will, even though you didn't do the work on the hazard
8 analysis, I think it is appropriate to say we've got a
9 positive outcome, and we are moving forward with it.

10 MEMBER STETKAR: Good comment.

11 DR. BIRLA: We can take care of that.

12 CHAIRMAN BROWN: Yes, I would have taken
13 it, that because of that, you we're going to do anything
14 else, if that really works?

15 DR. BIRLA: Well the first bullet says,
16 track external research, and we're not doing any more
17 internal research. So basically we're not doing an
18 active, literal search, and for the interviewing, to look
19 for it. Is there's another 10th, or 11th, or 12th that
20 we missed?

21 But for example, that we just continue to
22 work. There is a recent project in Scandinavian
23 countries where they are doing something very similar.
24 Whatever we are aware of, and can become aware of, to
25 draw the connections, we'll continue to have our antenna

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 out there. That's about all we're doing. That's what
2 we're trying to say and wrap this up.

3 CHAIRMAN BROWN: Okay, well you didn't have
4 that hardware figure piece you kind of see folded into
5 the conclusions either, you just kind of left that there,
6 with the thought that we can't do with the others, there's
7 nothing here. And I--

8 DR. BIRLA: That was, he was strictly very
9 disciplined within the scope of the objectives that he
10 wrote in there, and the proofs of his hard work are going
11 to show up in the next piece of work.

12 CHAIRMAN BROWN: And we anticipate it, so
13 we're going to see that next?

14 DR. BIRLA: Yes.

15 CHAIRMAN BROWN: Okay, all right, with that
16 we will recess for 15 minutes.

17 (Whereupon, the foregoing meeting went off
18 the record at 2:40 p.m. and went back on the record at
19 3:04 p.m.)

20 CHAIRMAN BROWN: Okay. I'll hit it one
21 more time and we should be ready to go. We'll commence
22 again with Sushil and Luis. Are you all ready to take
23 off on the next session?

24 MALE PARTICIPANT: Yes.

25 CHAIRMAN BROWN: Okay, get on with it.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Let's go ahead.

2 MR. BETANCOURT: Hello. Good afternoon.
3 My name is Luis Betancourt. I'm the NRC project manager.
4 I know some of you might not really have a such an
5 agreement with many of the specific information there on
6 the recent research.

7 This research was actually performed under
8 -- we needed a quick turnaround of this because the mPower
9 --

10 CHAIRMAN BROWN: You don't have to talk too
11 fast to get us through. Just --

12 (Laughter)

13 CHAIRMAN BROWN: I understood. I
14 understand trying to keep us on schedule.

15 (Laughter)

16 (Simultaneous speaking)

17 MR. BETANCOURT: Thank you. I will
18 actually take that into account and I apologize. So to
19 be clear, this research actually is to support the design
20 specific review standard for the mPower design and how
21 to review an applicant's hazard analysis.

22 On a post-hazard analysis, I know the ACRS
23 is concerned that from the last NRC's recent program
24 review, that you guys wanted for us to that we look for
25 some things, one is specifically to understand the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 sources of uncertainty better.

2 Second was to provide you sound technical
3 basis to be resolve the foreseeable sector issues.
4 Number 3, I think this is very important to develop and
5 maintain the NRC internal expertise on Number 4 to see
6 if it can stand the collaboration basically to learn from
7 whether applications remain or mission critical remains.

8 Specific to the system, one thing you were
9 concerned of, it was about how to preserve independence,
10 how to preserve the domestic behavior, and the effects
11 in that.

12 Also you have some concerns about the design
13 reviews not being integrated, so after we move into the
14 presentation we will be talking about how we actually
15 address your concerns on the this approach.

16 Please remember this is only like an entry
17 status briefing. This really is still like a work in
18 progress. So the document that you actually have been
19 reviewing has been updated since then. Not many changes
20 have been done, but I just wanted to let you know.

21 MEMBER BLEY: I'm sorry. Say that again.
22 We have, you've made the number of changes?

23 MR. BETANCOURT: Yes, but this was only
24 understanding, just on the --

25 MEMBER BLEY: Oh, okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. BETANCOURT: -- that is actually
2 already in the public domain. We're trying to, and I'm
3 going to be talking about that later in the presentation,
4 but we want the NRC stakeholders to engage with the
5 applicant and this is actually going to be one of those
6 ways.

7 So we are going to be updating our guidance
8 in RIL-1101. We're going to be putting that in the
9 public domain. So a little bit of the, for the
10 presentation to a little bit of the background about the
11 current states and trends. We already discussed that in
12 the morning part.

13 And I already gave you a little bit of the
14 motivation, why we did this project. Then why this
15 hazard analysis, it asks us that question on, through the
16 NRO when actually they brief you on the mPower DSRS, so
17 we're going to be telling you what is a hazard analysis.

18 Sushil take off on the areas of the
19 dependencies, after that I will be talking about what was
20 the recent method that we actually employed as well as
21 the scope for this limit of purposes.

22 After that Sushil will be going back again
23 on the evaluation of a hazard analysis and on the
24 envisioned roadmap, basically where we headed for on this
25 research. So I will go really quick over here since we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 already touched up on some of the discussion in the
2 morning.

3 As the ACRS may have noted already from the
4 last evaluation we have been some seeing some trends in
5 the system that is actually shown in the safety
6 evaluation.

7 And on some of the reports we have been
8 seeing an increase in interconnections and our feedback
9 paths in the current designs which is leading to an
10 increase in complexity and it's actually making more
11 difficult for the system to understand, to verify, to
12 analyze, and to conform the behavior that is actually
13 deterministic.

14 As a side of that we have been seeing an
15 increase of unwanted interactions and this is actually
16 causing an increase of unwanted hidden independencies
17 which is creating a compromise of independence and an
18 increase of non-common causes.

19 Therefore, these are such as compromising
20 redundancy, diversity, defense in depth, and safety
21 margins. That means that we cannot count on the
22 traditional techniques -- but again is on normal
23 generated efficiencies.

24 As you may have heard earlier today from the
25 other presentations such traditional hazard analysis,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 sources from FMA and FTA have become ineffective under
2 this condition that I just described.

3 The NRCs longstanding chemical basis is for
4 the Reviewer, however you may note that some various FTA
5 and FMA combinations and our patience will still be
6 useful for a simple system that don't have
7 interconnections and feedback paths, often make or limit
8 the purposes.

9 So starting with the motivation for
10 RIL-1101, also what I talked before, we were supporting
11 NRO for my use and the request that they needed authentic
12 base to review an applicant's hazard analysis. The
13 curtail is already contained in Appendix A from the DSRS
14 which we already reviewed in 2011 in our November
15 meeting.

16 We also believe that this will be useful for
17 the Reviewer as a technical reference document in order
18 to support additional review. However, we see some
19 value to others in this. We think that this can be used
20 as an organizing an analytical framework for three
21 purposes.

22 One, for the applicant who are going to have
23 their safety analysis report. Another one will be to
24 improve the necessary regulatory guidance, which I will
25 be talking about that later. Finally, the framework to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 learn from operating experience.

2 We also believe as I was stating before that
3 we're going to be polling these drafts on the public
4 domain so this will be used as a technical reference for
5 the industry.

6 So now we come to the fun part. What is a
7 hazard analysis and what it means. So hazard analysis,
8 so if you look in the book under the commission and it
9 provides a definition of why a hazard analysis is, a
10 hazard.

11 So we define as a hazard as a potential for
12 harm and is basically characterized in three things. It
13 is a condition, a circumstance, a scenario, or state. We
14 use definition of a hazard by binding the scope of the
15 system that is actually being analyzed.

16 At least normal information that we're
17 going to be using is bounding the system to its boundary
18 in relationship to the embodiment and interaction that
19 it has with the environment.

20 Also when we have that environment it
21 includes logical as well as physical aspects. Also, you
22 --

23 CHAIRMAN BROWN: Was that logical as well
24 as physical aspects?

25 MR. BETANCOURT: Correct.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Okay.

2 MR. BETANCOURT: Also, the second
3 definition that we have over here from the system of
4 software engineering is seemingly under the scope to harm
5 or damage which we refer as the loss, basically the
6 protection to cause a degradation.

7 So now we going to be talking about to the
8 eyes, the analyses Criterion 4H and this is why we need
9 to have a hazard analysis. Criterion 4H basically says
10 the following, a specific basis shall be established for
11 the design of each safety system of the nuclear power
12 generation station and the design basis shall commence
13 immediately with the following.

14 One, what are all the conditions for having
15 the potential for the regulation of a safety performance,
16 basically what we mean about the conditions, basically,
17 what are all of these things can actually go wrong.
18 That's what we mean about a hazard.

19 DR. SUSHIL BIRLA: The conditions are the
20 set?

21 MR. BETANCOURT: Yes.

22 DR. SUSHIL BIRLA: Okay.

23 MR. BETANCOURT: Yes. Do you want me --

24 DR. SUSHIL BIRLA: So if you see this set
25 that's from what is Set K. Okay, go back.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. BETANCOURT: Okay.

2 CHAIRMAN BROWN: So is this a backup slide

3 --

4 MR. BETANCOURT: Yes.

5 CHAIRMAN BROWN: -- that you just showed?

6 MR. BETANCOURT: Yes.

7 CHAIRMAN BROWN: Okay. It wasn't in the
8 package though?

9 MR. BETANCOURT: It is on Slide Number 34.

10 CHAIRMAN BROWN: This is the same --

11 MR. BETANCOURT: It is the same set of the
12 more.

13 CHAIRMAN BROWN: I'm presuming you have
14 Slide 34?

15 MALE PARTICIPANT: We only have 30 through
16 37.

17 MR. BETANCOURT: Yes.

18 CHAIRMAN BROWN: So somehow --

19 MR. BETANCOURT: I apologize. I already
20 printed that stuff.

21 MS. ANTONESCU: So we should get that copy
22 because we need to give it to them --

23 MR. BETANCOURT: Sure. But if you look
24 under the electronic copy that it was given to you is in
25 Slide Number 34.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: Yes, okay. It's in the
2 electronic version?

3 MR. BETANCOURT: Yes.

4 CHAIRMAN BROWN: Okay. Thank you.

5 MR. BETANCOURT: Okay. Now to go back over
6 here and you could read it on the Criterion 4H that
7 suggests also why are all the provisions that needs to
8 be incorporated to retain the capability to perform the
9 safety analysis functions, just that we mean that the
10 hazard controls.

11 So as the result of a hazard analysis is the
12 fulfillment of this Criterion 4H basically to identify
13 what are all the conditions that can go wrong around the
14 provision to actually control the hazard. So this is
15 what we mean about a hazard analysis through the eyes of
16 313 Criterion 4H.

17 Now as you might recall from the criterion
18 of System 34H, this does also contain our regulations on
19 the density for our 52.47(a) which specifically states
20 that all the evaluations must contain to show that the
21 safety function will be accomplish.

22 Basically if you look at Criterion 4H that
23 is the hazard analysis and that is part of this
24 evaluation. As part of this we will be looking, the
25 applicant will actually have to define, to identify, what

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 are all the principle design criteria that are from this
2 hazard analysis.

3 From this hazard analysis we will also be
4 looking if the hazard analysis leads from this principle
5 design criteria to the design basis and from this design
6 basis to somebody filing the requirements and
7 constraints.

8 This requirement and constraint may
9 actually become part of the license and basis and this
10 will actually be the result of a hazard analysis. So by
11 definition, hazard analysis is part of the revelation.
12 So what we wanted to say, this is nothing new.

13 If you recall from the definition of what
14 we meant about a hazard, as a potential for loss, if you
15 recall from the last presentation, this is what we mean.

16 The loss connection could be from three
17 different source or form, harm to the human, as damage
18 to the environment, or as an economic loss. So the same
19 analysis that you will actually lead a system to a loss,
20 the potential for any kind of loss as such as is shown
21 over here.

22 On the analysis there are varied conditions
23 that can actually lead to such a loss. This is another set,
24 unwanted intrusion, inference, or interaction. So you
25 can actually see hazard analysis can actually encompass

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 all of this together so we're now in focus within the
2 safety point of view.

3 This is like an analytical framework that
4 can actually lead from the non-safety to the safety side.

5 CHAIRMAN BROWN: On just the last part?

6 MR. BETANCOURT: What I'm saying over here
7 that the loss or concern is not only, as you might heard
8 from the other presentation before, it's not only concern
9 from the safety point of view, it's also a concern from
10 the safety and the non-safety.

11 So the applicant can actually have this.

12 DR. SUSHIL BIRLA: And your other concern
13 was about integrated review design, reviews, if you look
14 at the block at the bottom. John, Dennis, you might
15 remember in the November 16 mPower DSRS Review with the
16 subcommittee and December 6 full committee, this
17 discussion had come up and in the DSRS Appendix A there
18 is this line.

19 MEMBER BLEY: I don't remember, but it
20 makes sense.

21 DR. SUSHIL BIRLA: This is how we covered
22 the integrated design review.

23 MEMBER BLEY: Well, let me let you go ahead.

24 MR. BETANCOURT: Sure.

25 CHAIRMAN BROWN: Before you do, about the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 harm, you equate down to human. That's the only, I
2 presume you're saying a harm equates to a human harm. Is
3 that, a harm two units?

4 DR. SUSHIL BIRLA: Yes. So --

5 CHAIRMAN BROWN: With the environment we've
6 all got all that --

7 DR. SUSHIL BIRLA: Right. So that's just
8 a distinction, not all the capabilities make that
9 distinction. Some have extended into the meaning of the
10 word harm, damage to the environment also and any other
11 kind of harm, economic harm too.

12 But the point we're trying to make was that
13 whether it is something that injures people or something
14 that hurts the environment or something that caused
15 economic loss, the paradigm of this analysis allows you
16 to utilize the same method, therefore you can have
17 integrated analysis.

18 As you heard this morning, there was a
19 conflict of goals. On the one hand they were trying to
20 protect equipment, on the other hand there was a call for
21 the safety function. And because that analysis was not
22 integrated it got missed. So this is just an example.

23 CHAIRMAN BROWN: Okay.

24 MALE PARTICIPANT: Oh, wow. Okay,
25 wonderful.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. BETANCOURT: Now we're going to be
2 talking about how RIL-1101 relates to the planned hazard
3 analysis. If you look on the plan hazard analysis, this
4 is actually the non-labor losses of concern.

5 In this case, let's take for example the
6 unwanted interaction activity. In the current practice
7 of the hazard analysis or the plan label is atypical from
8 using a combination of event re-analysis as well as FTA.

9 From this plan label hazard analysis there
10 are some system constraints and they allocate some of the
11 current functions which are identified over here as on
12 the sample.

13 And they're allocated to some respective
14 systems. Let's take, for example, the RPSDS systems.
15 Our corresponding hazard analysis is actually performed
16 in each one of these systems.

17 In current practice as you may have noted
18 from the presentation today these are actually performed
19 using a design FMEA, which is used actually used to,
20 basically to comply with the single criterium.

21 CHAIRMAN BROWN: Is that the actual
22 practice that you see in the design world?

23 DR. SUSHIL BIRLA: This is what we had
24 learned from --

25 CHAIRMAN BROWN: I was going to ask if this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 was identical to the functional SFAS --

2 DR. SUSHIL BIRLA: Yes. Basically this is
3 what we learned from our discussions with EPRI and you
4 heard that in the morning, too.

5 MALE PARTICIPANT: Yes.

6 CONSULTANT HECHT: Charlie, I'm just
7 wondering if the distinction between the design and
8 functional FMEA is all that clear?

9 CHAIRMAN BROWN: Well I guess I kind of
10 viewed the design was more from a, that the component
11 bottom up type thing as opposed to a --

12 MALE PARTICIPANT: Yes, it is.

13 CHAIRMAN BROWN: -- system functional
14 down, I want the thing to trip and what are the --

15 MALE PARTICIPANT: Correct.

16 CHAIRMAN BROWN: -- little lines that
17 branch out from that. So that's the way I viewed it.

18 CONSULTANT HECHT: Well, one person's
19 component is somebody else's function. For example --

20 CHAIRMAN BROWN: Yes, I don't work in that
21 world. A component is a piece of stuff I can go throw
22 down and smash.

23 CONSULTANT HECHT: Yes.

24 CHAIRMAN BROWN: A function is just
25 amorphous little thing called an algorithm that resides

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 inside the stuff or an analog process that says I put
2 something in, I've got a function and it gives me some
3 voltage level and it varies going out.

4 DR. SUSHIL BIRLA: Yes. So --

5 CHAIRMAN BROWN: That's my view.

6 DR. SUSHIL BIRLA: Yes. So my point is is
7 that we'll have clear, and we agree that different
8 communities, different people, even people in the same
9 organization use these terms in very different ways.

10 Today there's a great confusion out there.
11 We've chosen to narrow the definitions, write our
12 definitions in the policy and be consistent with those
13 definitions.

14 CHAIRMAN BROWN: With which definitions,
15 consistent with which ones? What I just said or what he
16 just said?

17 DR. SUSHIL BIRLA: What you just said, yes.

18 CHAIRMAN BROWN: Okay.

19 CONSULTANT HECHT: So is a function an
20 equipment rack or is a function something smaller on the
21 equipment rack or --

22 CHAIRMAN BROWN: It's a component.

23 DR. SUSHIL BIRLA: I think you don't even
24 need equipment. You can start a functional FMEA just on
25 a concept where you don't even know what the equipment

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 is just on interrelationships of functions. You can
2 start it at that stage.

3 MEMBER BLEY: I think it just shows use of
4 functions is closer to mine than Charlie's and it's the
5 tasks that a system has to perform.

6 CONSULTANT HECHT: Right, because that
7 task ultimately gets allocated to a thing.

8 MEMBER BLEY: And lower levels then.

9 CHAIRMAN BROWN: I'm actually, I'm looking
10 at it the same way you do.

11 CONSULTANT HECHT: Okay.

12 CHAIRMAN BROWN: I mean when I look at it
13 in the early stage, a block diagram to me is not function,
14 it's a box, but it's a box with function. It's things
15 that process things not just certain, you don't know it's
16 not just hardware, and that's true.

17 DR. SUSHIL BIRLA: That's right.

18 CHAIRMAN BROWN: So when I think functional
19 FMEA I think of the block diagrams we get that represent
20 what the system's supposed to look like after you design
21 it with real stuff or hardware --

22 MALE PARTICIPANT: Yes.

23 CHAIRMAN BROWN: -- with components. I
24 used to have this component argument all the time with
25 people, so we'll stop right here.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 DR. SUSHIL BIRLA: And I still don't
2 disagree with your other comment that one person's
3 component is another person's system and it will come to
4 that.

5 MR. BETANCOURT: So to continue the
6 presentation this hazard analysis will be actually done
7 at every level for this area. They will be done at the
8 plan level. They will be done at the system level and
9 so on.

10 One may find that to perform the hazard
11 analysis we may need some changes into the design. Maybe
12 one of those changes has to feedback all the way back to
13 the plan design. So these are things that we're going
14 to be discussing in RIL-1101.

15 With that, I'm just going to Sushil for the
16 dependency section.

17 DR. SUSHIL BIRLA: Okay. So as you see in
18 the outline, it's a little overview of types of
19 dependencies and then we'll take a look at some examples.

20 DR. SUSHIL BIRLA: To understand the
21 various ways the safety function can get recreated? We
22 need to understand what the safety function depends upon.
23 So here you'll see, you're seeing some examples of
24 various types of dependencies ranging from functional to
25 conceptual.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 We'll also show you examples of
2 dependencies on conditions in the environment, and
3 remember the environment is logical, too. The last
4 bullet here is the, and one of great concern, if you don't
5 know what it is, how do you avoid degradation from it?

6 And with more interconnections and feedback
7 paths, that is a great concern not only, across in many
8 application domains. So we'll look at the dependency
9 path and the system architecture dimension.

10 Yes, so I do distinguish between a human
11 mistake, error for failure, but that's a discussion for
12 another time. A hazard which may cause degradation of
13 a system may arise from a dependency internal to the
14 system or external to the system, so that's the two paths
15 that you're seeing here.

16 As the hazard analysis examines various
17 ways in which a safety function can get degraded from its
18 environment. As you recall in that Set K interference
19 was one of those ways and some external system can
20 interfere with the performance of the safety function.
21 That's what this is trying to show, so therefore it needs
22 to be examined.

23 As the hazard analysis examines various
24 ways in which a safety function can get degraded from
25 within the safety system, recall that they, again in our

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Set K, a function not provided when required was one of
2 those ways.

3 Let's say that Element I, an element in the
4 vocabulary of systems engineering as adopted in the IEEE
5 Standard 1012, could be another system, subsystem,
6 sub-subsystem, component, hardware, software, we chose
7 to use the word element so that it could mean any of this,
8 it's the next lower level of integration that I'm talking
9 about when I say Element I.

10 And it did not provide a wide function. So
11 if you're a provider of Element I, the provision of that
12 function becomes a safety requirement. So here we are,
13 a lot of your team, Myron, and this again not well agreed
14 upon.

15 A lot people say look, the safety function
16 is only at the plant level and everything else is not a
17 safety function. You can't do a safety analysis when you
18 start from a plant level. Well, how does the engineering
19 get broken down into manageable pieces?

20 You do have to have a clear allocations.
21 And the reason people talk about, talk against this kind
22 of a thinking is that in the allocation process if you're
23 allocations are not right something gets missed.

24 So I just wanted you to be aware of that
25 controversy going on, but here we'll say that at least

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 this function got allocated, this didn't perform it, so
2 now we've got to analyze Element I. You need to have an
3 analysis on Element I like this water system.

4 CONSULTANT HECHT: Well I guess when we
5 can't say that functions can get decomposed and then
6 allocated to some functions and you could still argue
7 that you're at the functional level.

8 DR. SUSHIL BIRLA: Yes, exactly. Exactly,
9 and we don't dispute the diagram. But, again, as soon
10 as you start using the term safety goal, safety
11 requirement, some people get worked up and say well
12 that's not proper at the top level only.

13 Okay. So you perform a hazard analysis at
14 this level and liking you get the point that the next
15 lower level and we call it Element IJ, you may again think
16 about that Set K, another one of those ways things can
17 go wrong is you provide it too late.

18 So this just shows applying the same Set K
19 at every level of integration. So you are following the
20 dependency path or propagation path of what can go wrong,
21 whether you want to call it prior propagation path, be
22 a propagation path, whatever.

23 Okay. Let me just make one more point here.
24 So what we saw in this example was dependency through
25 levels of integration following a functional dependency

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 path and there can be other contract dependencies, too.

2 The elements or sub-elements can be the
3 hardware or software, combinations, so the hazard
4 analysis is examining at each level of integration
5 whatever it comes across. This may also be viewed as the
6 casual pathways leading to the degradation of a safety
7 function.

8 Eventually we'll come to a root effect and
9 in RIL-1101 we use the term contributory hazard or
10 everything that you're seeing going wrong in these red
11 arrows until you get to the bottom.

12 Now some people will want to call them
13 causes, some want to call them contributory causes, some
14 just want to call them contributory factors. You'll see
15 these terms, we chose to refer to them as a contributory
16 hazard consistently regardless of what level we were,
17 other than the one closest to the safety function where
18 we use the term hazard.

19 But, again, if your whole world is at that
20 sub-subsystem level, then for you anything that degrades
21 its function is the hazard for that system.

22 So eventually you come down to some
23 engineering deficiency and therefore to do further
24 investigation now you've got to do the hazard carrying
25 out this analysis into the process level.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 So this picture shows life cycle process
2 model and this reference model is inspired by IEEE
3 Standard 1012 of the 2012 version. So in the middle
4 block you see the mainstream system engineering life
5 cycle from planning through implementation and so on.

6 And in the bottom block you see the
7 verification validation activities in their life cycle
8 phases following the, these are the mainstream
9 development. And in the upper block which is labeled a
10 safety analysis, you see a parallel flow of activities
11 which include independent hazard analysis.

12 So what's independent hazard analysis that
13 this is now a part of a safety analysis responsibility
14 as contrasted with whatever hazard analysis verification
15 validation that is included within the system
16 development process itself.

17 So for systems of highest level of
18 criticality, IEEE Standard 1012 says your V&V should be
19 independent. That is what you see at the bottom tract,
20 separate, and safety analysis in the top tract, separate.

21 And these red arrows that you see are the
22 feedback path, change paths which Luis talked about in
23 an earlier slide. So in RIL-1101 in Appendix C you will
24 see a more complete description of the acceptance model
25 and then there is an accompanying table, Table 20, which

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 lists the corresponding activity tasks and for each task
2 there is a set up inputs and there's a set of outputs.

3 And when we reach the evaluation segment of
4 this presentation we'll talk a little bit more about the
5 outputs. So by performing hazard analysis on the work
6 product of each phase, contributory hazards can be
7 discovered as early as possible in the life cycle, but
8 this is, again, from the IEEE Standard 1012 reference
9 model.

10 It asks for hazard analysis activity at
11 every phase in the life cycle. This way we can also
12 identify contributory hazards nicely during two
13 particular phase so that we can do the diagnosis and
14 deeper dive in the development process activities of that
15 phase.

16 The work product of a particular phase in
17 the development process now depends upon the process
18 activity. So if we need to take a deeper dive, we need
19 to look at process activity model and this activity model
20 is a little bit of an elaboration of a process activity
21 model that you see in the IEEE Standards, series of
22 standards for software engineering.

23 So the middle block is the process activity,
24 right is its work product, left is the incoming item which
25 could be a part of the proceeding phase, and the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 activities performed by applying resources which include
2 people, tools, aids, information, others.

3 So what you're seeing here is called a
4 model. What can affect the work product and you might
5 think of these as dependencies and the process
6 diminishing.

7 CHAIRMAN BROWN: Before you, okay, the
8 generality of this is why I don't have a Ph.D., okay, and
9 the abstraction you use for, okay, and fall asleep before
10 I got there. When you talk about a process activity, how
11 do I relate that back to the previous phase?

12 DR. SUSHIL BIRLA: So if you look at the
13 center bar the concept is one phase. So --

14 CHAIRMAN BROWN: Is that in the process
15 activity?

16 DR. SUSHIL BIRLA: That's the process
17 activity. Requirements definition, architecture,
18 specification, detail design, implementation --

19 CHAIRMAN BROWN: Okay. So those are all
20 part of the, what I what would call the main design
21 process, and you are just generically calling this a
22 process activity?

23 DR. SUSHIL BIRLA: Activity.

24 CHAIRMAN BROWN: It's not the, although the
25 other ones could be, like the hazard analysis is an

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 activity also --

2 DR. SUSHIL BIRLA: Yes.

3 CHAIRMAN BROWN: -- in some form.

4 DR. SUSHIL BIRLA: Yes. And there could be
5 a hazard analysis performed internal to the mainstream
6 development activity, but because it's a highest
7 criticality system we show in the block above an
8 independent hazard analysis.

9 CHAIRMAN BROWN: That's independent,
10 that's different people doing it?

11 DR. SUSHIL BIRLA: Yes.

12 CHAIRMAN BROWN: Regardless of what the
13 design guys do to satisfy themselves that they've
14 developed a satisfactory product --

15 DR. SUSHIL BIRLA: Right. Exactly.

16 CHAIRMAN BROWN: -- at that point?

17 DR. SUSHIL BIRLA: Yes. And this is also
18 a process activity.

19 CHAIRMAN BROWN: Okay.

20 DR. SUSHIL BIRLA: So that --

21 CHAIRMAN BROWN: I just wanted to
22 understand. I just wanted to understand that
23 extraction, as you had it in here.

24 DR. SUSHIL BIRLA: Right. And this holds
25 good at all levels. So whether you're talking a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 hardware, software system, system or systems. Okay,
2 please.

3 MEMBER STETKAR: So before you switch
4 topics because I know the next slide is a new topic. I
5 think I was following all of this stuff and I tend to hang
6 up on some words here and there because this is guidance
7 for reviews of pattern system analysis --

8 DR. SUSHIL BIRLA: A technical basis to
9 support the guidance.

10 MEMBER STETKAR: Okay, yes. That's true.
11 It's basis is to support the guidance, I'm sorry. In
12 some of the notes on, in particularly this area that
13 you've been talking about, dependencies, there are
14 statements like the following, "the extent of
15 dependencies on processes including the physical
16 processes in the plant may not be fully understood."

17 "From an NRC Reviewer's perspective a third
18 party certification of the system could provide the
19 requisite assurance that all dependencies have been
20 identified and their effects analyzed." What do you
21 mean by a third party certification of the system to
22 identify --

23 DR. SUSHIL BIRLA: What it's getting at --

24 MEMBER STETKAR: -- from an NRC Reviewer's
25 perspective?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. SUSHIL BIRLA: Yes, from a Reviewer's
2 perspective right now, historically, we've not focused
3 on product characteristics such as an architecture
4 design. So what you saw in an earlier slide was a hazard
5 analysis in the architecture dimension.

6 Ideally speaking that should be sufficient.
7 You shouldn't really have to go into the process
8 dimension as an independent reviewer, as I already told
9 you that you were.

10 But if you saw a lot of unanswered questions
11 and the applicant claimed that those questions are
12 answered by the process and offered you process
13 everything, should you look at it?

14 But on the other hand if the applicant said
15 look, I've got my processes all evaluated and assessed
16 by a third party process assessor and here is my
17 assessment. I'm at a HHOCMMY Level 4 and ISO 9000,
18 whatever.

19 And this assessor says that I meet all your
20 dependency criteria, too, and I've given you all the
21 product evidence. So don't waste my time with your
22 process arguments.

23 MEMBER STETKAR: I understand that. I
24 don't quite know how it works in factories, but --

25 DR. SUSHIL BIRLA: All right. So this is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 one of the ideas within NRO right now of how do you shift
2 the resources available internally to focus more on the
3 product characteristics? They're spending thousands of
4 hours on the process side if you recall the presentation
5 on the 16th of November.

6 CHAIRMAN BROWN: Okay. Let me, I thought
7 I understood something a minute ago, let me go back. I'm
8 going back to your document itself, the lead in. Is this
9 trying to develop a, the right phrase, to review the
10 hazard analysis that's been prepared by an applicant?

11 So is this your staff guidance for them to
12 do the review or is this for you to develop some guidance
13 for the applicants to prepare their hazard analysis?

14 DR. SUSHIL BIRLA: This is a technical
15 basis to support to reviewing of an applicant's hazard
16 analysis.

17 CHAIRMAN BROWN: Well your staff?

18 DR. SUSHIL BIRLA: Yes.

19 CHAIRMAN BROWN: It's the staff.

20 DR. SUSHIL BIRLA: Yes.

21 MR. BETANCOURT: Every research
22 information letter --

23 CHAIRMAN BROWN: But right now you don't do
24 that is that what you're telling me?

25 MR. BETANCOURT: No this --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. SUSHIL BIRLA: Remember that right now
2 the way the submittals are coming in at the INC level it's
3 typically FMEA to show that they've met every single
4 point, single digit factory.

5 CHAIRMAN BROWN: Yes, got it.

6 DR. SUSHIL BIRLA: And then we have met all
7 these other regulatory guidance, clauses that you have
8 and if you have a checklist of all those clauses
9 implicitly the plan is that by satisfying all these
10 clauses you've satisfied all your hazard concerns.

11 Unfortunately with new kinds of
12 configurations these interconnections, feedback paths,
13 unwanted interactions, there are new situations coming
14 up for which we do not have explicit clauses and at the
15 rate technology changes and configurations change up we
16 can't stay ahead.

17 So rather than depend upon exhaustive,
18 explicit clauses for every kind of hazard --

19 CHAIRMAN BROWN: Exhaustive what? You
20 said explicit --

21 DR. SUSHIL BIRLA: Clauses in the
22 regulatory guidance.

23 CHAIRMAN BROWN: Yes, yes, okay.

24 DR. SUSHIL BIRLA: What this process is
25 trying to do is with the owners or the applicant, you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 discovered the hazards and it will create controls for
2 those hazards.

3 CHAIRMAN BROWN: So you want to put this
4 requirement out to the applicants to convince you. So
5 this is, okay.

6 DR. SUSHIL BIRLA: All right.

7 MR. BETANCOURT: It's just already part of
8 system --

9 DR. SUSHIL BIRLA: So that the --

10 (Simultaneous speaking)

11 MEMBER STETKAR: -- eventually all the
12 regulatory guides are implemented. It's regulatory
13 guidance to the staff --

14 CHAIRMAN BROWN: Yes, right.

15 MEMBER STETKAR: -- that were evolved from
16 this.

17 CHAIRMAN BROWN: Yes, but they don't have
18 it right now is the point. That's what I was trying to
19 --

20 DR. SUSHIL BIRLA: Yes.

21 CHAIRMAN BROWN: -- I didn't ask it
22 eloquently enough. Okay, so that's what I said when I
23 said for you to, somehow they had to develop, they had
24 to put in the effort, at some point they'd have to be told
25 to do it within some boundary levels whether it would be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 for some standards or what have you that you endorse or
2 not endorse and then you review those when they're
3 completed and they demonstrate that they've met your
4 requirements via these analyses.

5 DR. SUSHIL BIRLA: Right now,
6 historically, we have seen it this way in the I&C arena,
7 that first the regulator puts out some guidance and then
8 the industry responds with here's how we meet them.

9 But there has been a precedent in the hazard
10 analysis, the seismic analysis, where industry took the
11 lead and said look, we like this NUREG better than what
12 we already had and this is what we want to do and came
13 to the NRC.

14 And here's an area where you heard it this
15 morning and that they conduct a couple of investigative
16 projects in the field and the plants like what they see
17 and the plants say look, this is where we want to go. You
18 could see this happen in the other direction, too.

19 CHAIRMAN BROWN: Okay. All right. I just
20 needed a little bit more calibration. Thank you.

21 DR. SUSHIL BIRLA: Yes.

22 MR. BETANCOURT: So as part of this matter
23 this was basically what we did. We are not developing
24 any new guidance. We all know that actually what we've
25 found for the leadership, so we actually went and we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 reviewed 150 papers, documents.

2 And where we found little information about
3 how information about review criteria on how to evaluate
4 a hazard analysis. Most of the information that we found
5 is about how to perform a basic process of research. So
6 we read a little beyond that, what we did is basically
7 we supplemented information that we had.

8 We acquired this from some subject matter
9 experts in the area of hazard analysis. Whether we know
10 that due to the limited time of scope of this project,
11 there may be some comments from the experts as well as
12 from the interacts with the public that may meet for
13 future research in this arena and we are going to be
14 discussing about that in a later slide on the envisioned
15 roll out.

16 So as part of the scope for RIL-1101 this
17 is basically what we actually did. And we're able to
18 with every hazard there is actually a rule if any systemic
19 goes through the development of field it is. The scope
20 is focused on evaluation rather than performance of a
21 hazard analysis.

22 You've already heard earlier today with
23 EPRI that they're doing some work in that area. And also
24 it focused on the digital safety function. Basically in
25 implementing an element of condition that made the safety

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 function basically.

2 And the element of condition may be internal
3 or external. That goes back to 603 and we also exclude
4 in the quantification aspects in RIL-1101.

5 CHAIRMAN BROWN: Okay. That's fine. I
6 just wanted to ask a relevant, an irrelevant question,
7 maybe I'm not sure which.

8 MR. BETANCOURT: Go ahead.

9 CHAIRMAN BROWN: The use of that hazard
10 analysis approach, I mean what you're trying to develop
11 is to be used in conjunction I presume still with other
12 review techniques or method like reviewing, functional
13 diagrams, et cetera, to understand what the system looks
14 like.

15 This is another means of looking at that
16 overall functional system and see what people have
17 developed out of it but you still need to understand
18 basically how it's configured functionally, you know,
19 from an architecture standpoint.

20 DR. SUSHIL BIRLA: Yes, they need to
21 understand that, yes.

22 CHAIRMAN BROWN: Okay.

23 DR. SUSHIL BIRLA: And you use that
24 information to perform the hazard analysis.

25 CHAIRMAN BROWN: Well you want him to, the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 applicant to be able to perform the evaluation so that
2 you can then connect the dots between them.

3 DR. SUSHIL BIRLA: Yes. Right.

4 CHAIRMAN BROWN: Okay.

5 DR. SUSHIL BIRLA: Okay, so --

6 CHAIRMAN BROWN: Sorry to interrupt, go
7 ahead.

8 DR. SUSHIL BIRLA: Yes. So this RIL is not
9 covering the whole waterfront. It is covering only
10 what's not been addressed in our earlier guidance.

11 So if you look at absolute no guidance and
12 no design rules and, Charlie, you mentioned this morning
13 about you haven't seen any design rules, then you can see
14 well the size of the contributory hazard space is very
15 large by the length of this arrow.

16 So we are going to see two access pictures
17 here in which as you start applying these constraints or
18 as you call them design rules, we should be reducing the
19 size of the contributory hazard space. So the first
20 level is unconstrained which means the design is giving
21 whatever they want, particularly in softwares, that's
22 exactly what's happening in software as you were saying
23 this morning you haven't seen local design rules
24 explicitly.

25 So if there's good design practice and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that's what industry has, we as Regulators don't repeat
2 every bit of what they have in their design practice.
3 It's taken as granted, as understood this is the baseline
4 and the regulatory guidance assumes that this good design
5 practice is in place.

6 So how would you distinguish good design
7 practice from additional guidance that you need. One
8 criterion one of my licensing office colleagues gives me
9 is, well if it's published in a book that's premature.

10 You shouldn't have to have more standards
11 and reg guides on that, and there is such a situation in
12 hazard analysis. In fact one of the most prolific
13 authors, Cliff Erickson, has published so many books on
14 safety analysis and hazard analysis.

15 If you just take the hazard analysis
16 framework and the safety analysis framework, you should
17 have all the basics. We shouldn't have to give that.

18 And then you apply NRCs regulatory guidance
19 framework which consists of the reference standards in
20 our reg guides, assuming that this good design practice
21 is in place. In other words, not repeating everything.

22 Yet we know with new kinds of conditions,
23 configurations, interconnections, feedback paths, they
24 are residual uncertainties. So that's what we are
25 addressing in RIL-1101, in fact that's we address in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 RIL-1001 which we published more than a couple of years
2 ago.

3 And we are assuming conformance and safety
4 to everything below that, so that we don't have to repeat
5 what's already in.

6 CHAIRMAN BROWN: Before you switch new
7 grass, I mean the pictures, back to the good design
8 practice. I mean what, at least what I observed in our
9 discussions, what's good design practice to one vendor
10 or design developer is not necessarily good design
11 practice for another design developer.

12 And a prime example of that is a design that
13 it was presumed to be perfectly satisfactory that shares
14 data between divisions from processor to processor to
15 evaluate the goodness of incoming data and all that where
16 it which tends to go against the principle of
17 independence.

18 Yet other vendors will come in and say oh,
19 no, no. We don't do that, that's just not a good idea.
20 And that's a different version of good design practice.
21 So you all have to adjudicate that in some manner in your
22 alls reviews.

23 DR. SUSHIL BIRLA: Right.

24 CHAIRMAN BROWN: So how --

25 DR. SUSHIL BIRLA: Yes. So --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: You don't specify a
2 compendium or a good design practice or a bracket or a
3 bin of here's some methodologies which we agree are good
4 design practices and if you go outside that we're, you
5 know, we're not going to review the design or whatever.

6 DR. SUSHIL BIRLA: Yes. So right now on
7 the industry side there are some publications of good
8 design practice and the case that you mentioned is not
9 covered in there because these are recent evolutions,
10 systems with more interconnections into the safety
11 system.

12 So we don't consider that as excluded from
13 our scope, in fact that is part of our scope.

14 CHAIRMAN BROWN: I know you all review for
15 that. I mean you've done a considerable amount of
16 discussion on that, so --

17 DR. SUSHIL BIRLA: Yes, but what I'm trying
18 to say here was that even our baseline regulatory
19 guidance framework, including the standards reference
20 therein, are not identifying every item of good design
21 practice. There's an assumption out there.

22 And you're absolutely right sometimes what
23 you assume turns out to be false and then you have to make
24 things explicit and that's the reactive process we are
25 in at the moment.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 CHAIRMAN BROWN: Okay. So you recognize
2 that?

3 DR. SUSHIL BIRLA: Yes, recognize that.
4 So here's one of those examples, interconnections of
5 safety system with some non-safety system, and that
6 non-safety system is connected to the plan data network
7 and so on.

8 So this is a scenario. We aren't saying
9 that this what people are doing, but if this scenario
10 occurs it's not covered in that good design practice.
11 It's not covered in our existing guidance, we address
12 that in RIL-1101.

13 So we address things in terms of scenarios
14 and then what are the conditions that reduce the hazard
15 space of this scenario. And how did we pick the
16 scenarios? Basically listening to NRO in the last five,
17 six years, the kinds of issues they have run into and this
18 was one of them.

19 The dotted line that you see are the hidden
20 dependencies because the wires, and the lines only show
21 as to direct dependencies. Here's another kind of new
22 configuration where there are interconnections across
23 divisions to share censored data.

24 This was not envisioned in the past. This
25 has arisen, when you have that in redundant systems that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 becomes a distributor systems with interconnections and
2 it is a set of 12 byzantine behavior. This is why in our
3 Set K we listed byzantine behavior a separate item.

4 CHAIRMAN BROWN: You listed what? Say
5 that again?

6 MEMBER STETKAR: I had a curiosity about
7 that because I think --

8 CHAIRMAN BROWN: What kind of behavior did
9 you say?

10 DR. SUSHIL BIRLA: You remember the story
11 of the byzantine generals --

12 CHAIRMAN BROWN: Byzantine, yes, I
13 remember that in the list.

14 DR. SUSHIL BIRLA: Yes. So what happened
15 to the byzantine generals is happening in digital
16 electronic systems today when you have these kinds of
17 configurations.

18 So they are very difficult to detect and
19 very difficult to overcome, but the subject has been
20 studied so there is knowledge available, we reference
21 that.

22 MEMBER BLEY: Those last two slides bother
23 me a bit because I think you're trying to draw a
24 distinction maybe to make people feel good that you're
25 not going to revisit something you've looked at before.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 In a way I don't see an application and you
2 can clarify, and I, you talk about analyzing these
3 systems and you talk about tools to do it and you don't
4 say here's a set of things so you don't have to look at
5 it because they were covered before. And I just don't
6 --

7 DR. SUSHIL BIRLA: No, no, no. That's not
8 --

9 MEMBER BLEY: -- know if that, because they
10 don't tell me anything.

11 DR. SUSHIL BIRLA: This is not saying hey,
12 Mr. Applicant, we don't have to look at them. This is
13 saying RIL-1101's scope is limited to address these new
14 kinds of issues. It doesn't cover the whole waterfront
15 from ground zero.

16 MEMBER BLEY: Okay.

17 DR. SUSHIL BIRLA: That's what --

18 MEMBER BLEY: It's not saying what, okay.
19 That's fine.

20 DR. SUSHIL BIRLA: Okay. So how does one
21 evaluate the results of hazard analysis? So at the
22 superficial level we can look for the phase whiteout,
23 which remember I mentioned Table 20 in Appendix C which
24 has a list of top tasks for every phase in the life cycle.

25 If you don't even have the logbooks right

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 there you got the, making a request for additional
2 information, RAI.

3 MEMBER BLEY: By the way, Table C20 follows
4 Table C1 and the text refers to Table C2 and there is no
5 such thing.

6 MR. BETANCOURT: Yes. That is our mistake
7 and we revised that in the review sheet.

8 MEMBER BLEY: Table C20 should be Table C2,
9 right?

10 MR. BETANCOURT: Yes.

11 MEMBER BLEY: Yes, okay.

12 MR. BETANCOURT: That is the same.

13 MEMBER BLEY: There is no Table C20.

14 MR. BETANCOURT: We revised that. We
15 noted that.

16 MEMBER BLEY: Go ahead.

17 DR. SUSHIL BIRLA: I'm impressed how
18 minutely you have read this thing, thank you.

19 MEMBER BLEY: I just couldn't find direct
20 links to the Table.

21 DR. SUSHIL BIRLA: Our apologies on that.
22 Okay, so let's say the item is not missing. The items
23 listed in the output for that phase and it's available
24 for review, then the next thing to do is you examine its
25 basis.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 Its basis is the inputs and the competence
2 which is what this slide shows and what it's trying to
3 say is that just looking at a technique and saying if you
4 applied this technique your good is not good enough, and
5 this is what you folks said in the morning, too, don't
6 get too hung up on the technique.

7 More is at stake if you don't have the right
8 competence and if you don't have the appropriate quality
9 of information that you're working with. So let's say
10 that you have the results of an analysis and let's take
11 a reasonable example that you have a hazard log that shows
12 we identified a hazard and then some entry that
13 identifies the control for that hazard, okay.

14 That design rule, that will eliminate that
15 hazard. Anyone to examine the validity of that, what do
16 you do? So what we've included here is a reasoning
17 model, so what I just mentioned was an assertion that the
18 hazard that was identified has been controlled, hazard
19 or contributory hazard.

20 And now we look for the reasoning to support
21 that assertion. So as a Reviewer you should challenge
22 that reasoning, you look for the factors that could
23 influence its validity and you identify qualifiers or
24 conditions.

25 I don't have enough information to make a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 definitive conclusion or a reasonable conclusion that
2 this assertion is correct. Let's start tracking all
3 those conditions, could be a thousand assumptions that
4 have to be satisfied.

5 So some things depend upon specific hard
6 evidence, other things in the reasoning could be just
7 there's some rule. Let's say the rule here, the hazard
8 here is that we don't know what the position of this valve
9 is and this is a contributory hazard.

10 The control for that hazard is that we want
11 to track where the, we'll track the position of the valve,
12 but we'll track it at the other end of the stem and the
13 rule is that if we see movement, measured movement, at
14 the other end of the stem then at the ball end of the stem
15 there's an exact same movement, or that same rule.

16 And on the surface of it it seems very
17 reasonable, but in the analysis, of the review of the
18 analysis you could say look, this is an assumption that
19 needs to be satisfied. There is a stem in between, what
20 if the valve got jammed and the stem broke?

21 And you heard some similar story this
22 morning, but that's just an example of how you evaluate
23 the reasoning. This model is not new. The original
24 model was developed by Tolman in around the early 1950s.

25 This model has been used in the safety case

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 paradigm, but you don't really need to have, need to
2 commit to a whole safety case paradigm, you can apply this
3 reasoning in the evaluation model to even a very small
4 assertion like if I moved the other end of the stem then
5 the valve will also move the signal.

6 MR. BETANCOURT: I guess we shall now go to
7 the final part of the presentation. What I want to show
8 here is actually how research has actually supported NRO
9 in their activities.

10 As you will see from the top, anything that
11 is in green it's actually related to NRO activity and
12 anything that is actually yellow relates to research
13 activity.

14 We basically took all the lessons learned
15 form, the lessons we've reviewed from NRO and we actually
16 incorporated that into RIL-1101. As part of the use and
17 the request that came from NRO in 2011, it took us around
18 seven months to have a product for NRO to pick and choose
19 whatever they wanted from the RIL and to publish the, an
20 informal drop of the DSRS.

21 That was the DSRS that you actually reviewed
22 back in 2011 in November or December. As part of the
23 ongoing process we are currently in the escrow
24 acquisition activity, now we expect to finalize in around
25 December of this year.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 We already showed this RIL to EPRI. We
2 already had like an EPRI MOU meeting back in July that
3 we shared this knowledge to them as well as we have been
4 sharing this to some of the IEEE working group member of
5 7-432 has seen today.

6 Currently right now NRO is actually having
7 these pre-application meetings and we expect this
8 RIL-1101 to be used a technical reference to support this
9 interaction with them. We expect to finalize this RIL
10 by the end of the year.

11 We expect for the final DSRS to be actually
12 published, and when I was talking to the plan manager she
13 told me that this is actually now moved to somewhere in
14 2014. We expect these applications to come in around
15 Fall 2014.

16 Finally we want to show you how we plan to
17 address some of the unresolved comments and we also want
18 to talk about a little bit of your concern about on how
19 to develop and maintain the NRC internal expertise within
20 the NRC.

21 As you may know over here, RIL-1101 is
22 actually the first milestone of a long roadmap. NRO can
23 actually pick and choose whatever they wanted and
24 included that to the mPower DSRS Appendix A for hazard
25 analysis.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 We're going to be developing some trust
2 knowledge type of resources for the start on how to
3 evaluate a hazard analysis. As part of these unresolved
4 comments we expect that this future research will
5 actually be fair upon this NUREG for HA which actually
6 we'll be supporting the next small model reactor in, and
7 then as knowledge becomes mature we expect that we can
8 get this knowledge and actually influence some of the reg
9 guides on some of the standards that we reference in our
10 regulations.

11 Also, as you may notice over here we have
12 what we call experts on tap. The idea is very simple.
13 The idea is actually for, and as a Reviewer to have a
14 contract in which the NRC Reviewer can call anytime to
15 an external expert which will be plain or brief in what
16 are basically our current issues.

17 Also on the industry side we have been this,
18 and now we're on the understanding with the NRC and EPRI
19 which Russ already said before that has been quite
20 successful. They'll also be having their experts on tap
21 and they're currently developing the guidance on how to
22 perform a hazard analysis.

23 Currently they're working on how to
24 actually get this knowledge to the licensees and the
25 applicants.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MEMBER STETKAR: Before we leave this, and
2 I ask Russ, put him on the hot seat rather than you. I
3 see this process and I kind of get it and I think about
4 something that I'll just call NFP- 805, and don't laugh
5 because there's a lot of parallels here.

6 It's a, back in the early 2000s EPRI and the
7 staff worked together and developed the infamous
8 NUREG/CR-6850 and parallel others, NFP-805, and finally,
9 you know, here's a methodology for doing risk informed
10 fire protection.

11 And that methodology was then applied the
12 first time for Shearon Harris and Oconee and people
13 discovered how really difficult it was to really do one
14 of those, but here we are today with now real licensees
15 doing real analyses under conditions that were quite
16 honestly not well vented before they're being applied and
17 practiced.

18 I guess I'd express a concern that I see the
19 same path developing here. So one of the things I wanted
20 to ask you, because you in, and it's not shown here, but
21 in RIL-1101 as part of the future research activities you
22 mention pilot applications and indeed EPRI mentions in
23 their report pilot applications.

24 Have you thought about that in terms of the
25 time line? Is mPower the pilot application? Because if

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 they are that sounds an awful lot like Shearon Harris and
2 Ocone. They will have time schedules. That will be a
3 real license in that approval.

4 So have you all thought about this? One of
5 the lessons learned that we hear from both the staff and
6 the industry is gee, we really wish we had seriously
7 piloted both the doing of the analysis, the blue things
8 up above, and gee, we the staff really wish we had sorted
9 out how to review one of these things before we got it
10 real time.

11 (Simultaneous speaking)

12 MEMBER BLEY: And feedback into the method
13 before lots of people are trying to use it.

14 MR. SANTOS: Can I field that? This is Dan
15 Santos from NRO, the licensing offices. I agree with
16 your statement and we are very sensitive to everything
17 you said and yes it's a concern.

18 But we're looking at the status quo today
19 and the challenges and the effort it's taking to get
20 through some of these licensing review and new reactors
21 and there was a big incentive to look for a better
22 alternative to increase safety focus and efficiency of
23 reviews.

24 You heard Russ before report on the number
25 of hours and unresolved safety issues to get through the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 licensing process. So it's not balanced between looking
2 for an alternative to the current status, the status quo,
3 and the sensitivities to bring up.

4 So, yes, we have to be careful, cautious,
5 you know, cautiously optimistic, that's how we move
6 forward. But I feel it's time to start looking at
7 alternatives and that's why the push for this now.

8 And another criticism we got is sometimes
9 until you do it on a real application, on a real license,
10 is all academic. So --

11 MEMBER STETKAR: That's actually true, but
12 I'll still fall back to my analogy with NFP-805 and
13 applying the guidance in the NUREG which in this sense
14 I'll point at the EPRI report as the first elements of
15 that and the fact that the staff hadn't worked out
16 reasonable guidance for expectations or how to review one
17 of those things, whatever it was, once they got it.

18 MR. SANTOS: I think a difference also is
19 the level, I want to thank BMW in our project office, the
20 level of interaction that we're having with them I think
21 is significant and it's going to help a lot --

22 MEMBER STETKAR: Well let me ask you this
23 --

24 MR. SANTOS: -- in the pre-application --

25 MEMBER STETKAR: Okay. I hear all of that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SANTOS: Yes.

2 MEMBER STETKAR: What I'm asking for is BMW
3 going to do a hazards analysis starting oh, like January
4 1, 2014, and use that as a pilot application for which
5 you will then do a staff example review of that hazards
6 analysis so by the time the real world starts kicking in
7 you've got all of the bugs worked out, which might be five
8 to six years from now.

9 NUREG/CR-6850 was published in 2005 and,
10 you know, people are struggling with that process now
11 eight years later.

12 MR. SANTOS: Yes. Our current schedule
13 shows pre-application audits, okay, that goes into a
14 hazard analysis, and we feel we'll have sufficient
15 activities pre-application to try to work that out and,
16 again, we're working closely with the applicant, BMW,
17 they're, I don't want to speak for them, seeing that we
18 have some representatives here, and their willingness
19 and commitment to actually try to do this.

20 And keep in mind we are presenting hazard
21 analysis on our organizing framework over the existing
22 regulatory framework and requirement. We're not short
23 circuiting our review nor our current regulatory
24 requirements so the fallback position is the current
25 status quo, that's all I'm trying to say.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 MEMBER STETKAR: Well as it was back in,
2 I'll pick a number, 2006, there was still the
3 deterministic appendix, our fire program reviews that
4 you could read.

5 MR. BETANCOURT: If I may interject, I
6 think what your concern is a little bit about the
7 competence of the staff and how when they were --

8 MEMBER STETKAR: No. I'm not concerned
9 about competence of staff. It's something to think
10 about, it's something new that nobody has ever done
11 before. The industry has never done a comprehensive
12 hazard analysis. They probably don't even know what
13 that is.

14 You've never reviewed a comprehensive
15 hazard analysis because you don't know what that it is.
16 So the only way to learn is not by developing guidance,
17 it's by actually trying to do something.

18 And that's, again, it's lessons learned
19 that we hear, ACRS hears, from both the industry and the
20 staff about gee, we really wish we should have done this
21 way back eight to ten years ago and learned all of those
22 lessons and worked out the bugs before we got pushed into
23 a situation where we're needing to do it real time.

24 And there may be industry pressures because
25 they may feel that that one approach using more emphasis

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 on hazard analysis may be a benefit. There may be
2 regulatory pressures. I don't know, but it's something
3 new and it doesn't say anything about competence I mean,
4 you know, there are smart people everywhere.

5 MR. THOMAS: If I may, Brian Thomas, NRC
6 Research, point well taken. Very, very good point.
7 They've got a lot of work to do. The point is we are where
8 we are.

9 MEMBER STETKAR: Yes.

10 MR. THOMAS: We are at a certain stage in
11 the development of the hazard analysis, you know, are
12 confronted with challenges with respect to advances in
13 the state of the art technology and so here we are.

14 And so this is where we are in the process
15 of, you know, developing a technical basis, developing
16 guidance that would hopefully, you know, we'll be able
17 to get the guidance established in a timely enough manner
18 to facilitate the reviews that we've got that are
19 forthcoming.

20 The projection right now is for the Fall of
21 2014 for a mPower submittal. Who knows it could be
22 later, nonetheless we've got to start sometime. So
23 we've got to get behind this and get going.

24 But, you know, the point is well taken.
25 What it does is it points out there's a lot of challenges

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that are forthcoming. We really will have to explore a
2 lot of opportunities to the extent we can to advance
3 whatever it is we're doing, advance the exposure to the
4 industry with what we're doing, you know, interact with
5 them extensively so that they get an understanding of
6 what it is we're doing.

7 So that, you know, as Dan said, they, you
8 know, in some manner get a head of what's needed and get
9 something before the staff, so we all have a sense of
10 what's forthcoming going forward, but your point is very
11 well taken.

12 MEMBER BLEY: Charlie, if you don't mind
13 I'd like to slip in a couple comments and questions before
14 they get to the recap and let them have a clean recap.

15 CHAIRMAN BROWN: Okay, well then let me
16 make, is it on this subject or did it --

17 MEMBER BLEY: No.

18 CHAIRMAN BROWN: Okay. Can I make a
19 comment on this, what you all were discussing?

20 MEMBER BLEY: You're the boss here. I'm
21 not the boss.

22 CHAIRMAN BROWN: I am.

23 (Laughter)

24 CHAIRMAN BROWN: I just, well and I agreed
25 with them, I mean I agree with them relative to what

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you're trying to do. I understand what you're trying to
2 do and this is just an observation that you're trying to
3 implement a kind of a process with a bunch of things that
4 you'd like to see in it, the industry develops that then
5 you want to see that and then go do something with it.

6 The problem is you approve it. You agree
7 with it. You say go use that and it's never been done
8 and you don't, within the NRC, you don't have a model for
9 dealing with problems on the spot as they come up that
10 allow you to change what is in that guidance that you've
11 issued.

12 In 1978 there were no, I can tell you this
13 from experience, we had two, two aircraft carriers got
14 authorized, the CVN-72 and 73, Abraham Lincoln, I forgot
15 George Washington, and we decided we had a set of analog
16 specifications for their INC systems and protection
17 systems.

18 We had no specifications that applied
19 microprocessors with which was a Z80 in those days, but
20 we issued the analog specs and said build it with
21 microprocessors. Try that one on.

22 There were no software standards. There
23 were no low level standard of big software packages, they
24 were all little, very specialized software packages
25 everywhere and we also issued a document which we called,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 what was it, SS473, which was a set of software standards
2 technically.

3 And we put everything in there we thought
4 we really knew about and then over the next five years
5 we were making changes on a weekly, if the vendor would
6 identify difficulty with well, you're asking for this,
7 but you can't really do it if you want to do that.

8 And so if we wrote one letter over that five
9 years we wrote five dozen letters changing those
10 documents in real time while we were designing and
11 applying it.

12 You don't have a process for doing that and
13 that's what screws up, excuse me, that's what messes up,
14 pardon me please, your ability to really execute this.

15 I mean that's the difficulty you have and
16 that's what I've seen in several of the, over the last
17 four or five years was when you've tried to certain
18 things, you don't have a real time process for issuing
19 something like this and then dealing with difficulties
20 and problems submitted by the vendors, whether it's
21 mPower or NuScale or whoever in this case or the other
22 design projects, and getting those fixes changed and into
23 the guidance in real time.

24 And that's probably, I'm guessing, but I
25 suspect that's a little bit of what you saw in the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 NFPA-805 application because you didn't have --

2 MR. SANTOS: Still the pilot's overseeing
3 it.

4 CHAIRMAN BROWN: Yes. The pilot program
5 doesn't necessarily help that because you've got to
6 finish the pilot program which is specific. Unless you
7 have a real time process for executing and changing it
8 you're really going to run into a wall.

9 It's going to very difficult. I think
10 you'll see the same problem they saw.

11 MEMBER BLEY: Well and one other trouble
12 they had was the pilot programs ended up not being
13 representative of what was going to happen elsewhere.

14 CHAIRMAN BROWN: Yes, and I agree with Dan.
15 You need to do it on a real project, okay. He's 100
16 percent, if you don't do it on a real project, doing on
17 a theoretical project, I'm just passing that on as
18 observation.

19 I would suggest if you want to do this, you
20 identify a process where you can execute things on, you
21 know, every few months or whatever it is to say yes, we're
22 going, we agree with you. We didn't phrase that right,
23 here's the new thing.

24 And I don't know how you, but based on
25 observations that's going to be difficult to do in your

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 old world.

2 MR. SANTOS: Yes. I appreciate that. Dan
3 Santos, again, and I'm fully supportive of your comments.
4 I just want to caveat a little bit because if something
5 bad that, the goal is not achieved, the goal is assurance
6 of safety and conformance with their regulation.

7 We want to use the JSM method to try to help
8 with that case where today we basically are relying on
9 the variability and judgment and expertise of the
10 Reviewers to request for additional information. So
11 that's the main goal, safety assurance.

12 So, yes, to improve the HA guidance on how
13 to evaluate a shape, yes, we need to figure out a better
14 way to more quickly about to making it better as we,
15 lessons learned, but we're not, because of that we're not
16 losing focus on our mission.

17 CHAIRMAN BROWN: I'm not saying you are,
18 but if you want to use that, you want to --

19 MR. SANTOS: Yes.

20 CHAIRMAN BROWN: -- use that to give you
21 part of your safety assurance and it's --

22 MR. SANTOS: We got to start some.

23 CHAIRMAN BROWN: It's just I, I'm not
24 disagreeing with your start --

25 MR. SANTOS: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: -- I'm trying to give you
2 a thought process for execution.

3 MR. SANTOS: Yes, I know.

4 DR. SUSHIL BIRLA: Yes.

5 CHAIRMAN BROWN: That's all I'm talking
6 about.

7 DR. SUSHIL BIRLA: Yes, but that's an
8 excellent suggestion, but I want to remind you what we
9 just reviewed. Today we reviewed a technical basis
10 document. It is not a regulatory guide. It is not a
11 review guide.

12 On the 16th of November you reviewed the
13 mPower DSRS that had Appendix A in it. That Appendix A
14 was the draft for industry comment at that time. That
15 is the review guide, the guide for Reviewer.

16 CHAIRMAN BROWN: That's the what? The
17 guide --

18 DR. SUSHIL BIRLA: For the Reviewers.

19 CHAIRMAN BROWN: Yes.

20 DR. SUSHIL BIRLA: The reviewers are going
21 to use that and that's right now at the final stages of
22 commenting. So there has been some dialogue cycle
23 between NRO and industry on that document.

24 The reason why hazard analysis was placed
25 in an appendix, and you know there are three or four

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 appendices, was just to give that flexibility. Now you
2 heard this morning from industry, from EPRI, that the
3 increase in effectiveness and the increase in
4 efficiency, the incentives are so great that they want
5 to move forward.

6 So if the applicant chooses, and this is
7 voluntary, the applicant may say look, this is so much
8 more effective with so much less effort, we want to use
9 this as the organizing framework for our whole safety
10 analysis report. The applicant had the freedom to make
11 that decision or not to.

12 CHAIRMAN BROWN: All right. Well I've
13 said my piece and I'm going to pass on over to Dennis so
14 you can make your comments without --

15 MEMBER BLEY: I wonder what I was going to
16 say?

17 (Laughter)

18 MR. SYDNOR: Can I just say one thing to
19 address John's comment? I have a background in Appendix
20 R and I remember 20 years ago when we though NFPA-805 was
21 the golden pot at the end of the rainbow from dealing with
22 Appendix R type of, so I take your comments seriously.

23 My management, NRO management, have asked
24 us to develop a much more formal research roadmap and we
25 can factor that comment into that roadmap and I know

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 exactly what you're talking about.

2 DR. SUSHIL BIRLA: The quick response turn
3 around process, those learning cycles have to be very
4 quick for anything to change that's a very good point.

5 CHAIRMAN BROWN: And even though it's
6 sometimes on a daily basis in some circumstances that's
7 how fast we could respond, it could be a couple days. I'm
8 viewing this from an old guy and it was 34 years ago.

9 DR. SUSHIL BIRLA: So the intent of this
10 slide in its cycle envision roadmaps, this is a vision
11 and the intent is to show that they're the seas of
12 learning cycles.

13 And with each learning experience the next
14 work product will be improved with that experience.
15 That's what this slide was trying to show and the pot at
16 the end of the rainbow is this thing at the extreme right
17 of the slide and there's no time line on that.

18 MEMBER BLEY: Well since you said that, do
19 you foresee over the next year or so as this interaction
20 continues that this document and the EPRI document will
21 become more tightly aligned or do you think they're
22 already tightly aligned?

23 DR. SUSHIL BIRLA: Well our memorandum of
24 understanding for research collaboration has a provision
25 that our work products will be independent. So we will

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 maintain our work products as independent work products,
2 but we will continue to share information.

3 MEMBER BLEY: I didn't say it would be the
4 same document, I said be more closely aligned and will
5 they be referencing each other or something like that?
6 Right now they seem to stand apart.

7 And just a couple comments, first, there's
8 a lot of good stuff here and I'll say that again later.
9 There's a lot of good information in here. Second, it's
10 still pretty rough for me. It's jagged as you go through
11 it. Back at Appendix C you have a very short section,
12 C6, on hazard analysis techniques.

13 Well maybe that just got thrown together
14 quickly to have something in here and maybe, it's a little
15 bit short. It doesn't flag the methods that are over in
16 the EPRI document. Here's a place, I can see a reference
17 there where you get some discussion of them.

18 Just a comment for you, I suspect the
19 comment about the similarity between HAZOP and STPA might
20 not sit well with the STPA folks. I mean there's some
21 basic things similar, but there's a lot that's very
22 different.

23 Then you have a short section where you talk
24 about how great it might be if we have automated hazard
25 analyses. I'll just tell you, the thing we talked about

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 this morning, with to do a good job here, you really got
2 to have a person who understands this system and its
3 relationship to the overall plant.

4 And, you know, years ago I had people bring
5 in software products they had that I could feed in the
6 P&ID and it would feed out of the fault tree. That fault
7 tree's useless because it doesn't know anything about
8 operation of that system and limits on it and it just
9 doesn't work.

10 Be really careful what you recommend there
11 because this is eventually going to be something that
12 people have to really pay attention to. A little like
13 Myron's comments about use of language and definitions
14 with respect to the industry, on Page A9 you have
15 "definitions of mistake" that are taken from references
16 about electronic computation and software and error.

17 You might bounce this off your human
18 performance people. It's not the definition of mistake
19 that you'll find they're using and is really common in
20 those areas. I think that's a fairly important one and
21 I think you ought to try to align with them.

22 I think the guys from EPRI talked something
23 about their inclusion of humans, at least in the STPA,
24 and that was much more consistent with those two worlds.

25 And finally, this report mentions that back

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 in your peer review section and Safer Engineering was
2 your neutral agent to pull all of that together.
3 Something else I read this week and I've been thumbing
4 through everything and I can't find it, also said they
5 were continuing to give you repair guidance for you on
6 the overall program.

7 I don't know if that's true or where I even
8 saw. If that's true I'm interested in when you're going
9 to get that. Whether it's true or not as far as I know
10 EPRI has now got the MIT Levenson Lab helping them and
11 you had Safer Engineering who I think are the same folks
12 just down the street in a commercial operation so you're
13 hanging on, your hat's on the same post.

14 But that's not bad, they have a lot of good
15 ideas. Do they owe you something? Are they giving you
16 guidance on the whole program or did I --

17 MR. SYDNOR: No. We don't --

18 MEMBER BLEY: -- maybe I read something
19 that was a little, I can't find it. I was going to show
20 it to you and ask you. Okay.

21 MR. SYDNOR: Their role is different than
22 that.

23 MEMBER BLEY: Okay.

24 DR. SUSHIL BIRLA: Just to clarify that we,
25 even before the contract was awarded, this was a very

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 small business contract set aside. We had mentioned to
2 the contract officer that because of this potential
3 conflict of interest, we're going to place certain
4 restrictions.

5 MEMBER BLEY: Oh, okay. Good.

6 DR. SUSHIL BIRLA: And we had --

7 MEMBER BLEY: Just so you thought about it.

8 DR. SUSHIL BIRLA: Yes. And we had to
9 convince the contract officer to allow us to place those
10 restrictions. So, for example, the choice of experts,
11 the contract officer wanted them to have a freedom of
12 choice.

13 Before the award we had a discussion, look
14 here's the issue, if you bring in Nancy, we have a
15 conflict of interest.

16 MEMBER BLEY: Okay.

17 DR. SUSHIL BIRLA: We can't have that.
18 Also as a part of the review team in here, there is nothing
19 in here form Safer for Nancy.

20 MEMBER BLEY: Okay. Whatever I read made
21 me think there was more involved in there.

22 DR. SUSHIL BIRLA: Yes, because of this
23 conflict of interest everyone's perception of a conflict
24 of interest, we made an early decision on that. And then
25 we also told Nancy and Safer that our technical work is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 not going to recommend any particular technique or show
2 one is better than another.

3 MEMBER BLEY: Okay, that's good. And the
4 last thing, would you pop up Slide 33 in your backup
5 slides. This is just what Charlie was asking about and
6 I thought that would save a -- 33.

7 MEMBER BLEY: That one. I thought that put
8 in perspective what you were asking about how does this
9 fit in their process. It just kind of dangles over their
10 device right now.

11 CHAIRMAN BROWN: Yes, I agree. Thanks.

12 MEMBER BLEY: Yes, so I had that, I've been
13 looking at their slides --

14 DR. SUSHIL BIRLA: Yes. So just a reminder
15 that in DSRS, in the mPower DSRS, Appendix A is review
16 guidance on hazard analysis.

17 MEMBER BLEY: Yes.

18 DR. SUSHIL BIRLA: And the contents of
19 that Appendix A were based on an earlier version of this
20 rule.

21 MEMBER BLEY: Yes, okay.

22 DR. SUSHIL BIRLA: So they picked and
23 choose what they felt comfortable with from an NRO review
24 perspective.

25 And that's what they put out for early

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 public comment. Now they're not done yet and they may
2 choose to add more or subtract something, but that's the
3 second one.

4 MEMBER BLEY: They is NRO?

5 DR. SUSHIL BIRLA: NRO, yes.

6 MEMBER BLEY: Okay.

7 MR. MOSSMAN: This is Tim Mossman from NRO.
8 We have received public comments on the DSRS and we are
9 in the midst of resolving those and we owe final comment
10 resolution in December I'm pretty sure.

11 MEMBER BLEY: Okay, thanks.

12 DR. SUSHIL BIRLA: Yes. So thank you for
13 pointing that out that on this slide we tried to clarify
14 that.

15 MEMBER BLEY: Yes. I was looking at that
16 thinking that it would maybe help you.

17 DR. SUSHIL BIRLA: But still Charlie's
18 point was in your process in the NRC you need to have very
19 fast learning cycles like on a daily basis.

20 CHAIRMAN BROWN: That's kind of an
21 extraordinary, I wouldn't expect it, I would say, you
22 know, just you want to be able to respond in a few weeks
23 to a concern to say yes, we understand that, that's not
24 what we meant, and not six months, not a year, not two
25 years, or three years which seems to be, and I'm not

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 saying, it's just the process --

2 DR. SUSHIL BIRLA: Right.

3 CHAIRMAN BROWN: -- you've got it written
4 in so many stages and you have to delegate authority down
5 from whoever signs that step to the level at which
6 somebody can respond in real time, that's all.

7 DR. SUSHIL BIRLA: Yes. So that's the
8 advantage of keeping this as a technical basis. There's
9 no recommendation even here on what the regulatory
10 guidance should be or the review guidance should be.

11 CHAIRMAN BROWN: Okay. Now are you all
12 finished with this? Is that the last --

13 MR. BETANCOURT: Yes.

14 CHAIRMAN BROWN: Yes, you're past, you're
15 in the backups. We got some time so if you would like
16 to take about, I will need about at least 15 or maybe 20
17 minutes for requesting public comments off the phone line
18 and from anybody in the peanut gallery, anything, other
19 comments that somebody might come up with here at the
20 table.

21 So you've got about 20 minutes or so if you
22 want to bring your op experience guys up and have them
23 give us a quick summary.

24 MR. SYDNOR: That may cut their time so much
25 that it might be ineffective.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 DR. SUSHIL BIRLA: Yes.

2 CHAIRMAN BROWN: That's fine.

3 MR. SYDNOR: Because they were looking for
4 a kind of interactive, one of the things they had in their
5 presentation was an actual event analysis and we were
6 hoping to get some interactive discussion. I'm not sure
7 we have time to do it justice.

8 CHAIRMAN BROWN: Okay. That works.

9 MR. SYDNOR: And if we can do it another
10 time because like I said that's a work in progress so
11 you'll hear about it again.

12 CHAIRMAN BROWN: Okay. That's fine.
13 When it's a little more refined just let us know and we'll
14 toss it into another one. With that let me turn to the
15 audience, is there anyone here in the public that would
16 like to provide guidance, erudite comments, information
17 that we can't pass up.

18 I'm hearing nothing. Okay then let's get
19 the phone line. We will open the phone line and see if
20 anyone's there so be patient gentlemen when we hear the
21 snap, crackle, and pops, I will ask you to talk,
22 hopefully.

23 Is anyone on the phone line? Would
24 somebody, even if you don't have anything to ask, would
25 you say something so we can confirm that the phone line

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 is open.

2 MR. INDITTER: Bob Inditter's here from
3 AREVA.

4 CHAIRMAN BROWN: Thank you very much. Is
5 there anyone on the phone line that would like to make
6 a comment or an observation?

7 MR. JOHNSTON: Johnston from CNSC.

8 CHAIRMAN BROWN: Go ahead.

9 MR. JOHNSTON: Oh, we don't have a comment.

10 CHAIRMAN BROWN: Oh, okay.

11 (Laughter)

12 MEMBER BLEY: Thank you very much.

13 CHAIRMAN BROWN: Thank you. Hearing no
14 comments or no requests to make comments from the phone
15 line we will put that back on mute. Can you go turn that
16 back off? Go around the table, Dennis?

17 MEMBER BLEY: Nothing to add beyond what
18 I've already said and what other people have said, yes.

19 CHAIRMAN BROWN: John?

20 MEMBER STETKAR: I'm the same way. I don't
21 have anything to add. I thank both EPRI and the staff
22 for taking the time to give us this briefing. I thought
23 it was really, really useful.

24 I've said it before and I'll say it again,
25 I'm encouraged by what I'm seeing and I just would further

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 encourage both the industry and the staff to bring some
2 of these thoughts to fruition as soon as possible because
3 if this process is going to be applied in the real world
4 it needs, it's going to take some work to get there.

5 MEMBER BLEY: You just triggered my mind.
6 There was one thing I did want to say earlier and I didn't
7 leave myself a note. Despite what we might think was a
8 mischaracterization of our letter earlier, I think what
9 we've seen today goes a long way to addressing the things
10 we've raised in several letters over the past many years
11 and I really appreciate it. Where you're headed I think
12 we have unlimited opportunity --

13 DR. SUSHIL BIRLA: So can we consider that
14 part of the SRM closed then?

15 MEMBER BLEY: It's not my job to see if the
16 SRM is finished or not.

17 DR. SUSHIL BIRLA: No. I mean from your
18 perspective is that --

19 MEMBER BLEY: No. You're not done yet.
20 You're on your way.

21 MEMBER STETKAR: A, you're not done yet,
22 and B, you're hearing feedback from three individuals who
23 happen to be members of the ACRS. You're not hearing
24 ACRS feedback.

25 CHAIRMAN BROWN: We can only speak through,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 yes, once there's some other full meeting where you want
2 a formal, formal --

3 DR. SUSHIL BIRLA: Right.

4 CHAIRMAN BROWN: -- response to where we
5 have to say yes or no.

6 MEMBER BLEY: The ACRS only speaks through
7 our letters and that's only by the full committee.

8 DR. SUSHIL BIRLA: Right.

9 MEMBER BLEY: So three of us are here.

10 MEMBER STETKAR: Three of us are here and
11 if we were all in agreement we still could be outvoted
12 12 to three.

13 DR. SUSHIL BIRLA: Yes. My question was
14 really whether all three of you were in agreement on that
15 level of satisfaction that you --

16 (Laughter)

17 MEMBER BLEY: I'm not walking into that
18 mine field right now so I couldn't answer because we
19 haven't had a chance to discuss it privately within that
20 --

21 DR. SUSHIL BIRLA: Yes. So --

22 CHAIRMAN BROWN: And you're not finished.
23 I just think you're getting at the core issues that we
24 were hoping you would drive for.

25 DR. SUSHIL BIRLA: Okay. So let's just

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 talk about the first part of the SRM that was
2 identification of failure modes in a digital INC and they
3 left the next part blank, but it's, we created the system.

4 The sense I got from the earlier discussion
5 was that you felt you come a long way, are pretty close,
6 and you were a little disappointed that we had a
7 disclaimer in there that this is not a complete set, for
8 God's sake how long are we going wait before you put this
9 to use.

10 And then when I show it to you how we were
11 using Set K in the next step you felt better about it.
12 So if you want to talk in terms of that asymptotic stage,
13 the impression I got was that you felt we were there.

14 So although we'll work in keeping aware of
15 developments outside, what others are discovering who
16 are investing R&D in this direction. More than an
17 awareness level search, we're not intending to do anymore
18 work and we'd like to conclude that that part of the SRM
19 has been filled.

20 MEMBER BLEY: You have a conceptual
21 framework for these failure modes. You haven't, in a
22 practical sense, applied them to real world events to the
23 extent that you engender confidence that everything's
24 going to work out using it.

25 It's a nice conceptual framework. Let's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 see if it can be used.

2 MR. THOMAS: And I want to, yes, I like the
3 way you phrase that. Thank you, I think you know that
4 that is where we are and I think we don't necessarily at
5 this point not want to snatch defeat and enjoy the
6 victory.

7 MEMBER BLEY: There you go.

8 (Laughter)

9 MR. THOMAS: We heard though, we heard it
10 loud and clear, we're going to be subjecting and we have
11 a lot more work to do. So with that, I thank you.

12 MEMBER BLEY: Okay.

13 CHAIRMAN BROWN: Myron?

14 CONSULTANT HECHT: I also wanted to echo
15 that I think progress is being made. I think the two
16 foundations of success in this work are number one a
17 architectural framework that you can apply consistently
18 across multiple designs and that would be something like
19 what we saw this morning from EPRI.

20 And the other thing is that you have failure
21 modes and perhaps the failure modes are generic and then
22 get tailored for each application, for each
23 architectural level with a way of looking at the
24 architecture and with the way of thinking about how each
25 level of the architecture behaves in the presence of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 failures, anomalies, whatever you want to call them.

2 You have the basis for being able to perform
3 hazard analyses and no matter which methods you use I
4 think once a disinterested Reviewer or something like
5 that understands the methodology and understands the
6 system under analysis and understands how it can fail,
7 I think a case can be made. The basis can be established
8 and a basis for assessing compliance can be reached.

9 CHAIRMAN BROWN: I'll just make, but number
10 one I want to thank you. I appreciated all of this
11 because I found the reports, the EPRI report was very good
12 that you all sponsored. I've found the presentations
13 and the stuff you all put together, those were very
14 useful.

15 I actually was able to understand them and
16 I'm not a PRA or a cut case or a set case, or whatever
17 these things are called, type person. So I thought they
18 were very, very useful and I'd only like emphasize why
19 I think it's been a really good effort since we started
20 writing these letters and trying to, you know, see
21 something come out of this research was that, and I'm
22 going back to memory again, but about 25 years ago or
23 whatever, one of our laboratories in my program had
24 proposed using hazard analysis as one of the basis for
25 making determinations and agreements on certain things

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 and we popped up in the meeting and says well, what is
2 a hazard analysis? And the room went silent.

3 And with that we decided we weren't going
4 to use hazard analysis approaches for trying to make a
5 determination, that our designs were satisfactory. We
6 would rely on the old-fashioned engineering approach
7 which was not necessarily all that good all the time, but
8 it was what's there.

9 And I want to thank you for a very good
10 presentation today. I thought it went very, very well
11 and it was well done. So with that, have I missed
12 anything? John? Dennis?

13 MEMBER BLEY: Just the gavel.

14 CHAIRMAN BROWN: Just the gavel. The
15 meeting is adjourned.

16 (Whereupon, the above-entitled meeting was
17 concluded at 4:41 p.m.)
18
19
20
21
22
23
24
25

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1
2
3
4
5
6

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com



Update on Digital Instrumentation & Control Projects

- Failure Modes – Hazard Analysis Methods**
- Operating Experience Review**
- PRA Insights**

Ray Torok
EPRI

Bruce Geddes, Dr. John Thomas
Southern Engineering Services

Dave Blanchard
Applied Reliability Engineering

ACRS Subcommittee on Digital Instrumentation & Control Systems
September 19, 2013

Content / Purpose

Introduction/Background

- Review EPRI role
- Digital I&C research topics

Update August 2009 presentation to Subcommittee

Topic 1 - Digital Failures - Mechanisms, Modes and Effects

Topic 2 - Operating Experience

Topic 3 - PRA Insights

Highlight recent failure / hazard analysis work

Introduction / Background

EPRI Research on Digital Issues

Provides technical bases and guidance to help utilities:

- Manage I&C obsolescence
- Implement advanced I&C technologies
- Enable plants to use digital technology capabilities to:
 - Maintain safe operation
 - Enhance reliability
 - Reduce operating costs
- Address regulatory issues

Areas for future discussion?

- Human factors engineering (HFE)
- Cyber Security
- Testing digital systems
- Configuration management
- Field programmable gate arrays (FPGAs)
- Electromagnetic compatibility (EMC)

Topic 1 – Digital Failures - Mechanisms, Modes and Effects

“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

Key points from 2009 EPRI presentation

- Failure **mechanisms** produce failure **modes** which, in turn, have **effects** on plant system operation
- PRA models do not need exhaustive treatment of low level digital failure mechanisms to generate useful insights
- Fault avoidance and fault tolerance important in designing robust systems
 - Software and hardware design features
 - Diversity

Digital Failures – Focus of Current EPRI Research

- Issue - Plants still experiencing unexpected/undesired behaviors
 - Failure modes missed or misunderstood
 - Nothing failed but system did the wrong thing

Research objective -

- More effective and efficient ways to find and manage vulnerabilities **before** system is operating in the plant
 - Failure modes **and....**
 - Undesired behaviors in the absence of failures

Failure analysis or hazard analysis?

Failure Mechanisms / Modes / Effects

- Where we left off in 2009

“Application-independent processor failure modes” (ACRS letter to Chairman of NRC Commissioners, 4/29/08)

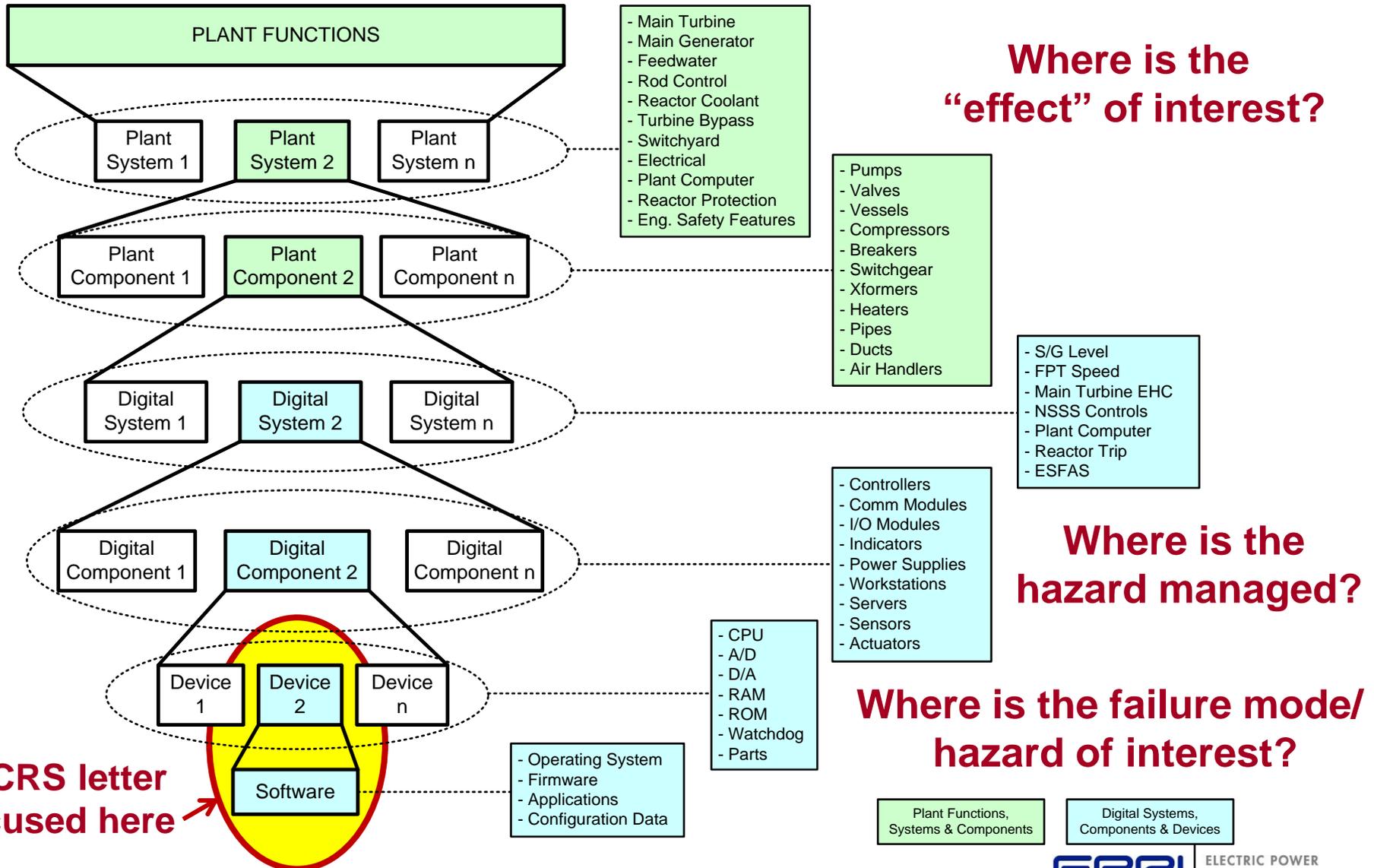
1. Task Crash
2. Task Hang
3. Task Late Response
4. Task Early Response
5. Task Incorrect Response
6. Task No Response
7. Processor Crash
8. Corrupted Input
9. Corrupted Output
10. Out of Sequence Data

Example defensive measures

- *Infinite-loop* software architecture with watchdog timers to detect problems and put system in a safe state
 - ➔ **Items 1,2, 3, 4, 6, 7 and 10 are N/A**
- Items 8, 9 addressed through redundancy, independence, data validation
 - ➔ **Item 5 needs special attention**

Defensive design measures constrain many potential failure “mechanisms/modes” to acceptable “effects”

Key to Focusing Failure / Hazard Analysis - “Level of Interest”



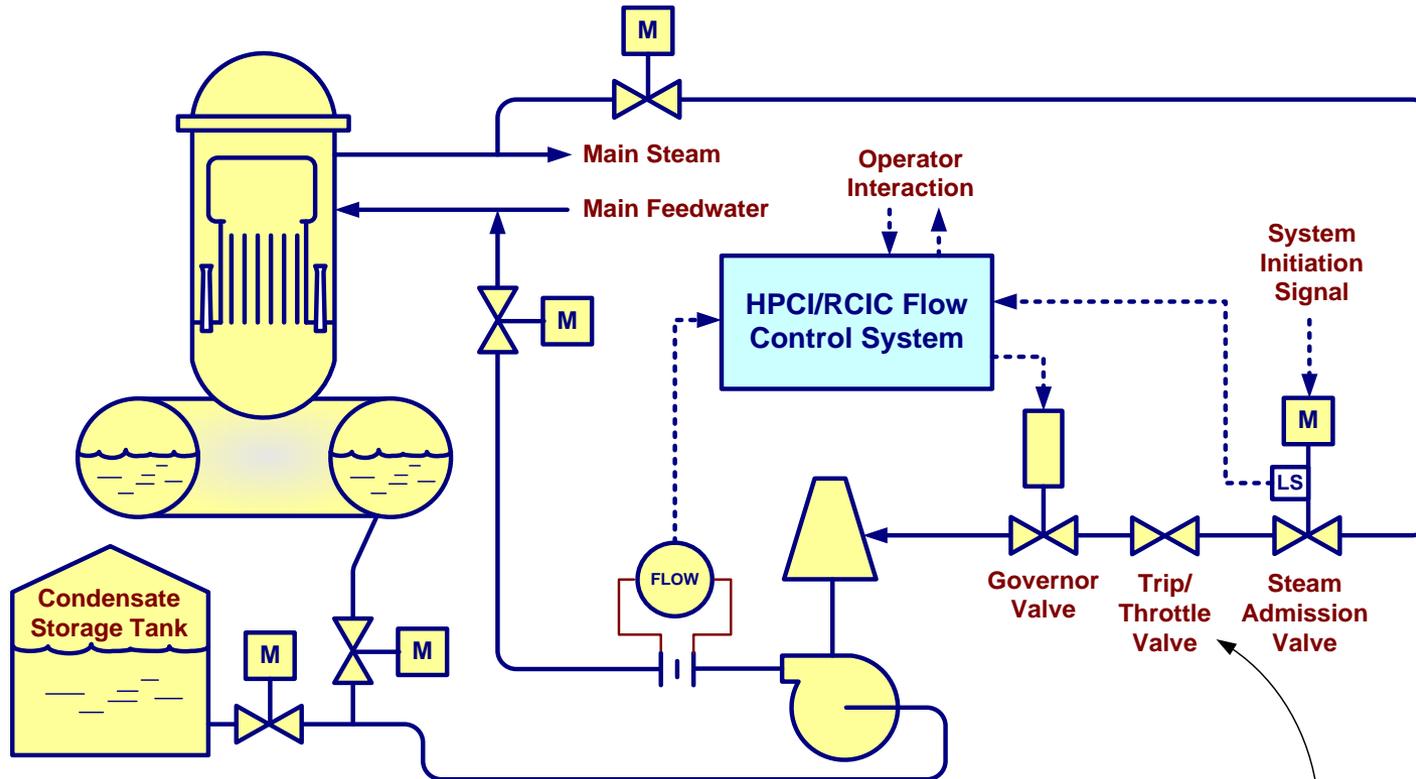
Hazard Analysis Methods for Digital Instrumentation and Control Systems (EPRI 3002000509)

| Six Methods Investigated | 'Top-Down' or 'Bottom-Up' | Strengths | | |
|--|---------------------------|--|---------------------------------|-------------------------|
| | | Considers Hazards Beyond Faults/Failures | Integrated View of Plant Design | Mature, Well Documented |
| Functional FMEA (Failure Modes & Effects Analysis) | T | | X | X |
| Design FMEA | B | | | X |
| Top-Down using FTA (Fault Tree Analysis) | T | | X | X |
| HAZOP (HAZard and OPerability Analysis) | T/B | X | X | X |
| STPA (Systems Theoretic Process Analysis) | T | X | X | |
| PGA (Purpose Graph Analysis) | N/A | X | X | |

Blended approaches may combine strengths of multiple methods

Example – BWR Flow Control System

High Pressure Coolant Injection (HPCI) or Reactor Core Isolation Cooling (RCIC)



System Initiation Signals

(Open Steam Admission Valve & Process Valves)

1. Low Reactor Level (-48")
2. High Drywell Pressure (HPCI only; +2 psig)

System Isolation Signals

(Trip Turbine & Close Process Valves)

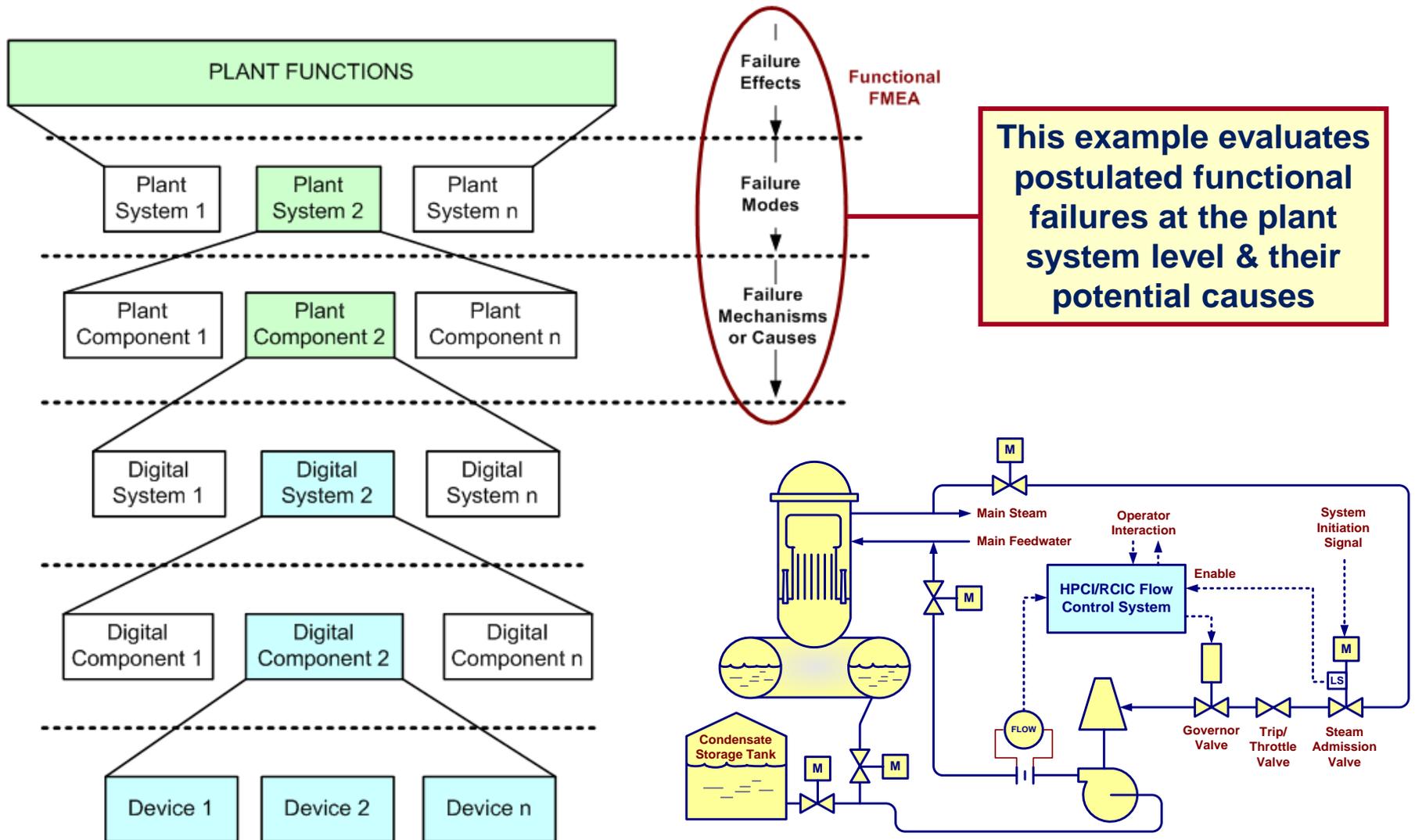
1. High Steam Line Flow
2. High Area Temperature
3. Low Steam Line Pressure (HPCI only)
4. Low Reactor Pressure (RCIC only)
5. Manual

Turbine Trip Signals

(Close Trip/Throttle Valve)

1. Any system isolation signal
2. High Steam Exhaust Pressure (150 psi)
3. High Reactor Level (+46")
4. Low pump suction pressure (15" Hg)
5. Turbine overspeed
6. Manual (local or remote)

Functional FMEA Method Applied to HPCI



Functional FMEA Worksheet for HPCI

| 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: HPCI/RCIC Flow Control System | | Checked by/Date: | | Lifecycle Phase: Conceptual Design | |
| | | | | | | Approval/ Date: | | Rev: 0a | |
| Row No. | Function | Process | Requirement(s) | Potential Effect(s) of Failure | Potential Causes(s)/ Mechanism of Failure | Current Prevent/Detect Method | | Recommended Action | |
| | | | | | | Prevention | Detection | | |
| 1 | High Pressure Injection | Turbine/pump provides required coolant flow | 5000 gpm (HPCI) or 500 gpm (RCIC) @ 1000 psi, on demand, within 60 seconds | Loss of Rx inventory, leading to core damage | 1. Failed initiation signal 2. Tripped turbine (no reset) | 1. Software V&V 2. ESFAS PM 3. Turbine PM | 1. ESFAS Test 2. System Flow Test | Evaluate flow control system failure modes via DFMEA | |
| 2 | | | | 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 PM 3. Turbine PM | 1. ESFAS Test 2. System Flow Test 3. Alarms | | |
| 3 | | | | More than 5000 gpm (HPCI) or 500 gpm (RCIC) | Too much inventory, possibly leading to core damage | | | | |
| 4 | | | | 5000 gpm (HPCI) or 500 gpm (RCIC), but after 60 seconds | Less than adequate inventory, possibly leading to core damage | | | | |
| 5 | High Pressure Injection | Steam Supply to Turbine | Supply high quality saturated steam at 1000 psig | No steam flow | Loss of steam to core damage | | 1. Section 11 Test 2. Alarms | | |
| 6 | | | | Poor steam quality (high moisture) | Turbine loss of R | | 1. System Flow Test 2. Turbine PM | | |
| 7 | | | | Steam pressure too low | Less than adequate inventory, possibly leading to core damage | | 1. Section 11 Test 2. Alarms | | |
| 8 | | | | Steam pressure too high | Relief valve pressure | | Alarms | | |
| 9 | High Pressure Injection | Suction Supply to Pump | Supply clean, demineralized water with adequate NPSH | No water flow | Loss of water to core damage | | 1. Alarms 2. CST/Torus Surveillance | | |
| 10 | | | | Foreign material in water | 1. Pump adequate 2. Clogged less than | | 1. System Flow Test 2. Chemistry Samples | | |
| 11 | | | | Less than adequate NPSH | 1. Pump damage, flow | | CST/Torus Surveillance Test | | |
| 12 | High Pressure Injection | 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. Intersystem leak | | | |
| 13 | | | | Capacity less than 5000 gpm | Less than adequate Rx inventory, possibly leading to core damage | | 1. H ₂ O Chemistry 2. Human Performance | | Alarms |
| 14 | | | | Less than 1000 psi | Less than adequate Rx inventory, possibly leading to core damage | | 1. Pipe leak 2. Intersystem leak | | |

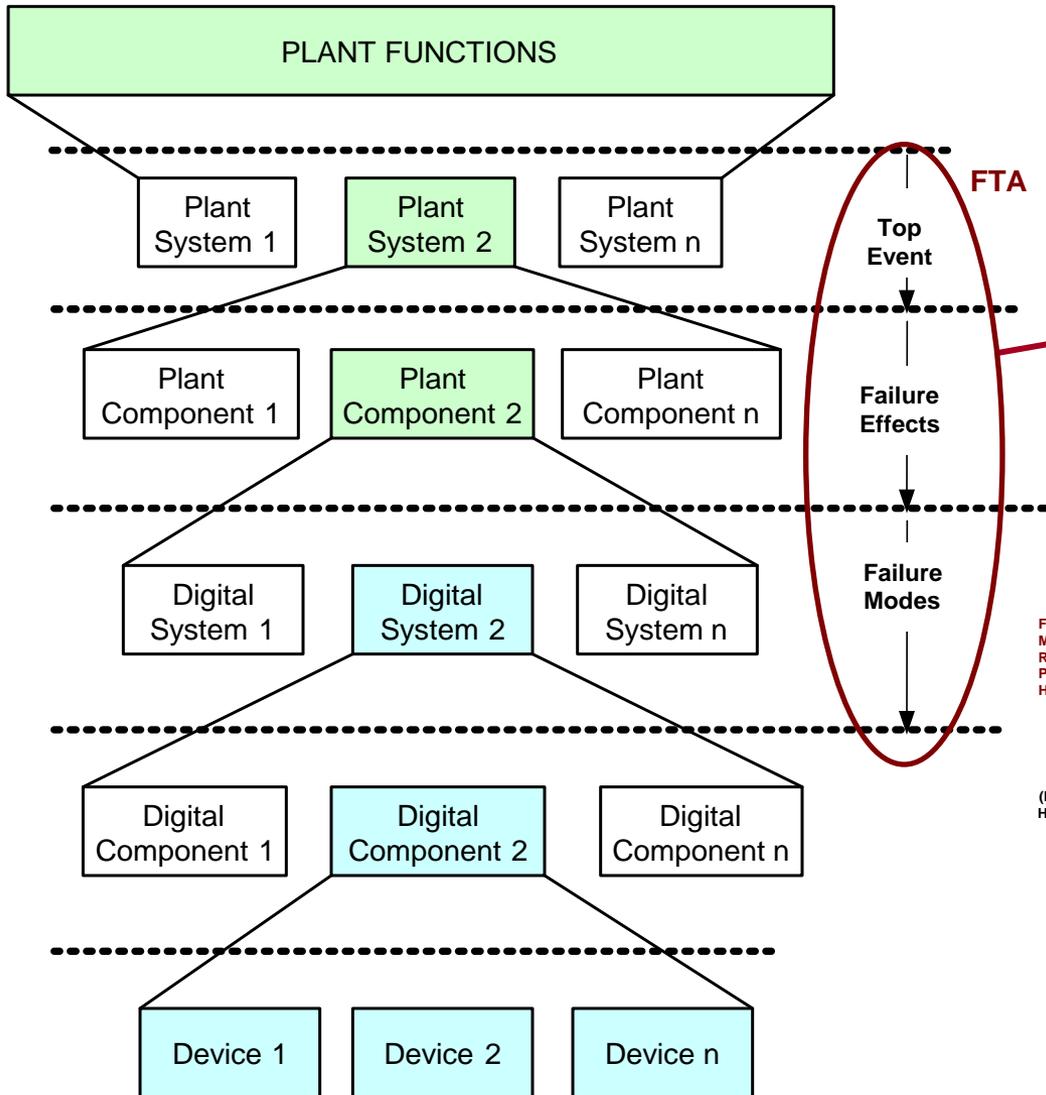
Potential Failure Mode

Key Words

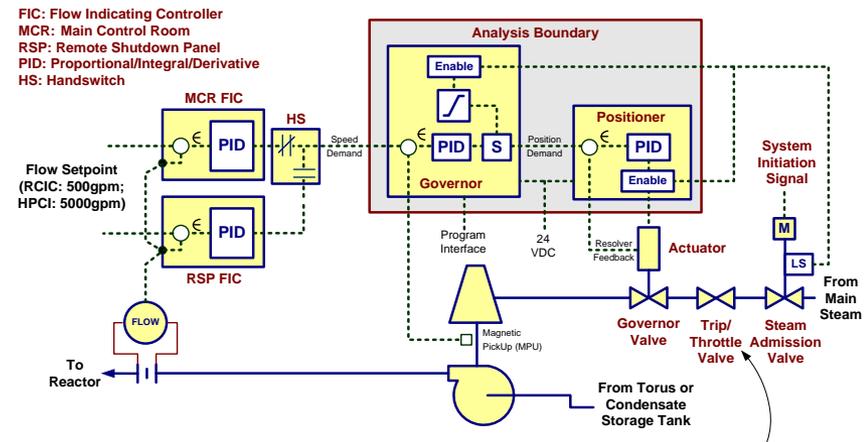
What can go wrong?

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

Top Down (FTA) Method Applied to HPCI Example



This example evaluates plant component failure modes that can be caused by the digital control system



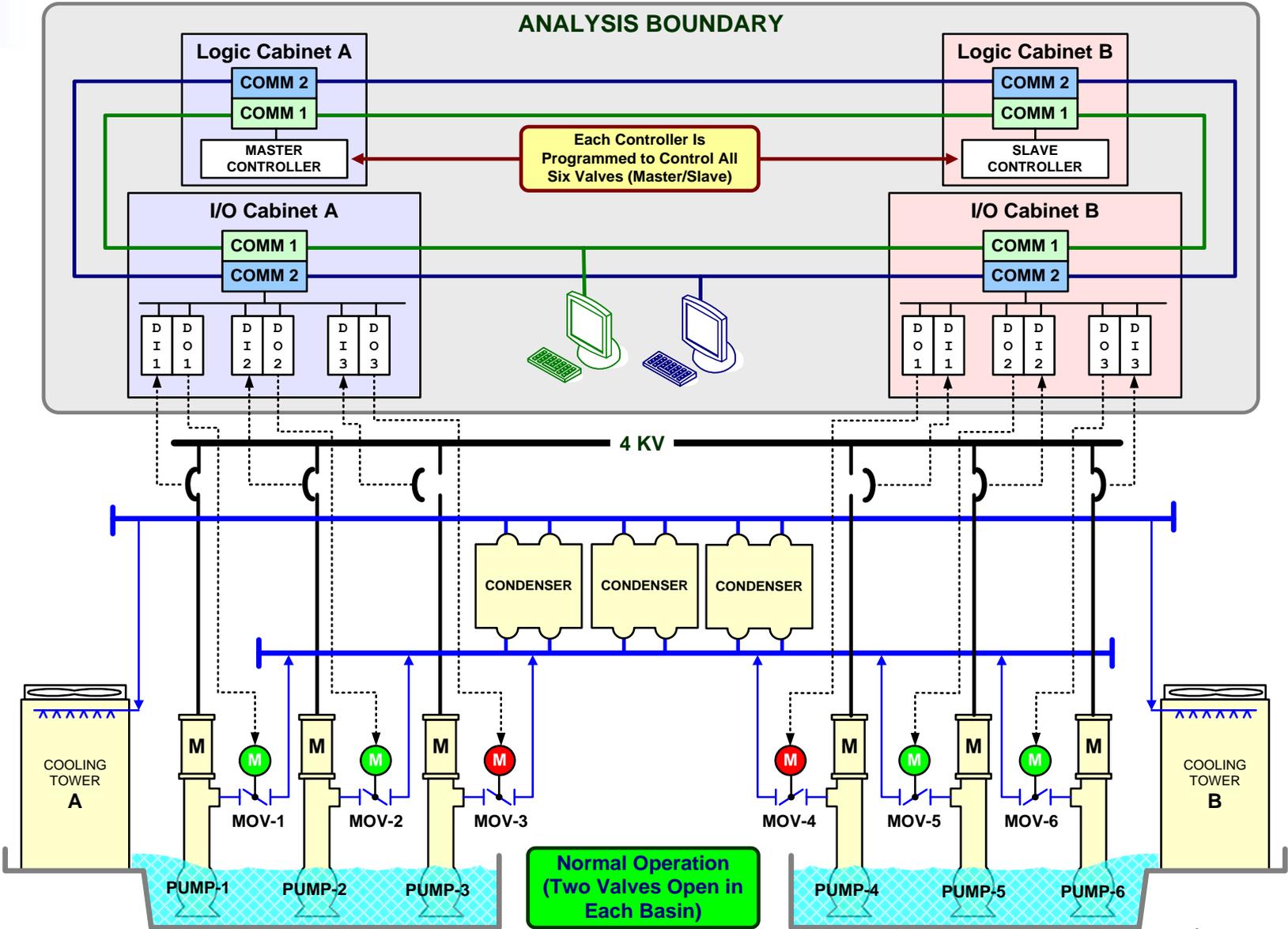
Top Down (Fault Tree Analysis) Method Applied to HPCI Example, cont'd

| Component | Failure Modes | PRA Basic Event(s) | Normal Config. | Accident Config. | Auto | Comment |
|---|---|--|----------------|------------------|---|--|
| Steam supply | | | | | | |
| Isolation valve (inboard) MO-014, 055 | <ul style="list-style-type: none"> Fail to remain open Spurious close | <ul style="list-style-type: none"> HPI-MOV-OC-MO-014 RCI-MOV-OC-MO-055 | Open | Open | Close on Gr5 Isol. | Not required to change position to provide steam supply function |
| Isolation valve (outboard) MO-015, 056 | <ul style="list-style-type: none"> Fail to remain open Spurious close | <ul style="list-style-type: none"> HPI-MOV-OC-MO-015 RCI-MOV-OC-MO-056 | Open | Open | Close on Gr5 Isol. | Not required to change position to provide steam supply function |
| Actuation valve MO-016, 058 | <ul style="list-style-type: none"> Fail to open Fail to remain open | <ul style="list-style-type: none"> HPI-MOV-OC-MO-016 HPI-MOV-CC-MO-016 RCI-MOV-OC-MO-058 RCI-MOV-CC-MO-058 | Closed | Open | Open on low-low Rx level | The HPCI actuation valve also opens on high drywell pressure |
| Trip/Throttle valve HO-007 MO-060 | <ul style="list-style-type: none"> Fail to remain open Spurious close | <ul style="list-style-type: none"> HPI-HOV-OC-HO-007 RCI-MOV-OC-MO-060 | Open | Open | Close on: <ul style="list-style-type: none"> Over-speed Lo suction Hi Exhaust Gr5 Isol. | Not required to change position to provide steam supply function |
| Governor valve HO-008, 009 | <ul style="list-style-type: none"> Fail to throttle Fail to remain open | <ul style="list-style-type: none"> HPI-HOV-OC-HO-008 RCI-HOV-OC-HO-009 | Open | Throttle | Throttle | Too much throttling may result in insufficient flow to the reactor. Too little throttling may result in turbine trip on overspeed. |

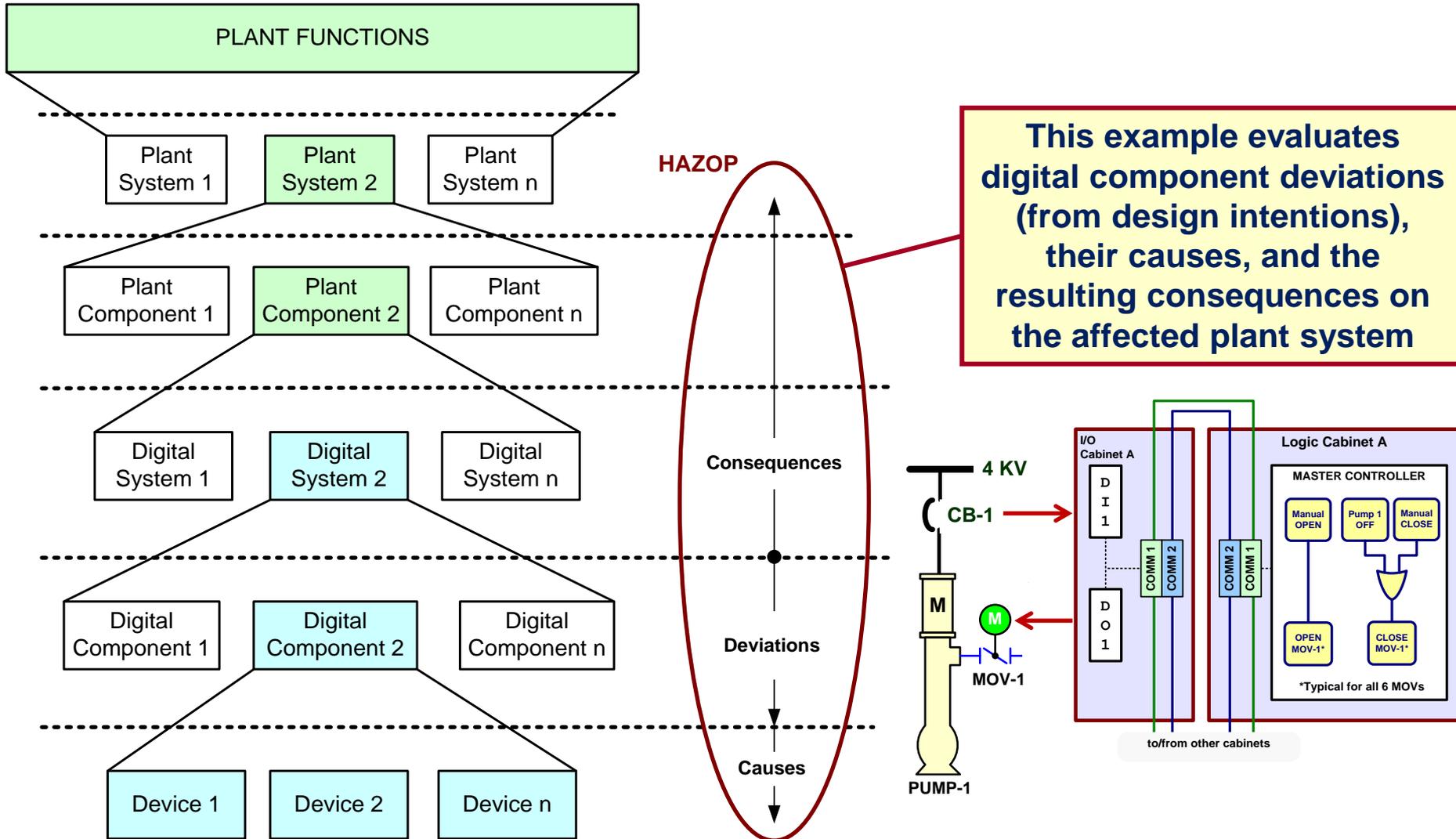
Top Down FTA method narrows the search for critical failure modes



Example - Circ Water Control System (CWS)



HAZOP Method Applied to CWS Example



HAZOP Worksheet on CWS Example

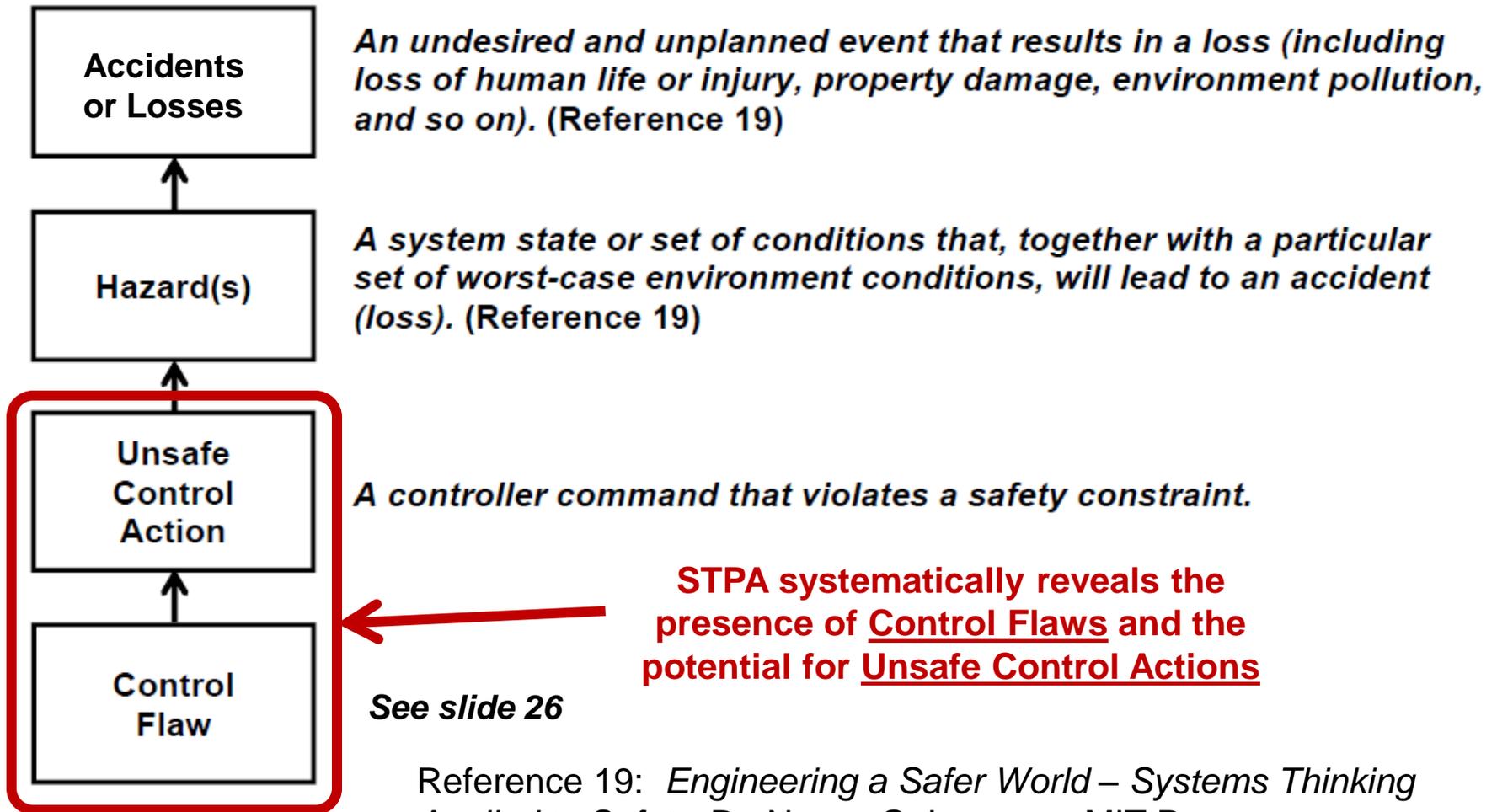
| Team: | PM, RT, BG, TN, DB | | Success Criteria: | No data errors, or losses of the data link to other cabinets | | | | |
|-------|-------------------------------|---|---------------------------------------|--|---|--------------------------------|--|------------|
| Part: | COMM1 or COMM2 in I/O Cabinet | | Intent: | Pass data addressed to/from I/O modules | | | | |
| No. | Guide Word | Element/Attribute | Deviation | Possible Causes | Consequences | Safeguards | Comments | Action |
| 1 | No | Signalling Voltage on Physical Interface (indicating the presence of a modulated carrier) | No carrier signal | broken wire | None. Other COMM maintains communication | Wiring standards | Confirm wiring standards cover this item | TN |
| | | | | Dead Module | | Testing | Confirm periodic test procedures | DB |
| | | | | Failed Backplane | Loss of both COMM modules, Loss of three CWS pumps | None | Revisit fundamental architecture of CWS control system and propose a design change to prevent loss of CWS pumps | RT, |
| 2 | More | | Carrier Voltage Too High | Degraded Circuit | None. Other COMM maintains | Carrier validation diagnostics | Confirm data communication diagnostic features detect and mitigate this item | PM |
| 3 | Less | | Carrier Voltage Too Low | | COMM | Carrier validation diagnostics | Confirm data communication diagnostic features detect and mitigate this item | PM |
| 4 | As Well As | | Two or more carriers at the same time | Failed collision detection | Degraded communications on one COMM loop; other COMM loop available | Carrier validation diagnostics | Confirm data communication diagnostic features detect and mitigate this item | PM |
| 5 | Part Of | | N/A | --- | --- | --- | --- | --- |
| 6 | Reverse | | Reverse carrier voltage | Degraded Circuit | None. Other COMM maintains communication | Carrier validation diagnostics | Confirm data communication diagnostic features detect and mitigate this item | PM |
| 7 | Other Than | | N/A | --- | --- | --- | --- | --- |
| 8 | Early, Before, Late, After | | Carrier Jitter | Degraded Circuit | None. Other COMM maintains communication | Carrier validation diagnostics | Confirm data communication diagnostic features detect and mitigate this item | PM |

Guide Words

HAZOP found the failure reported in the OE

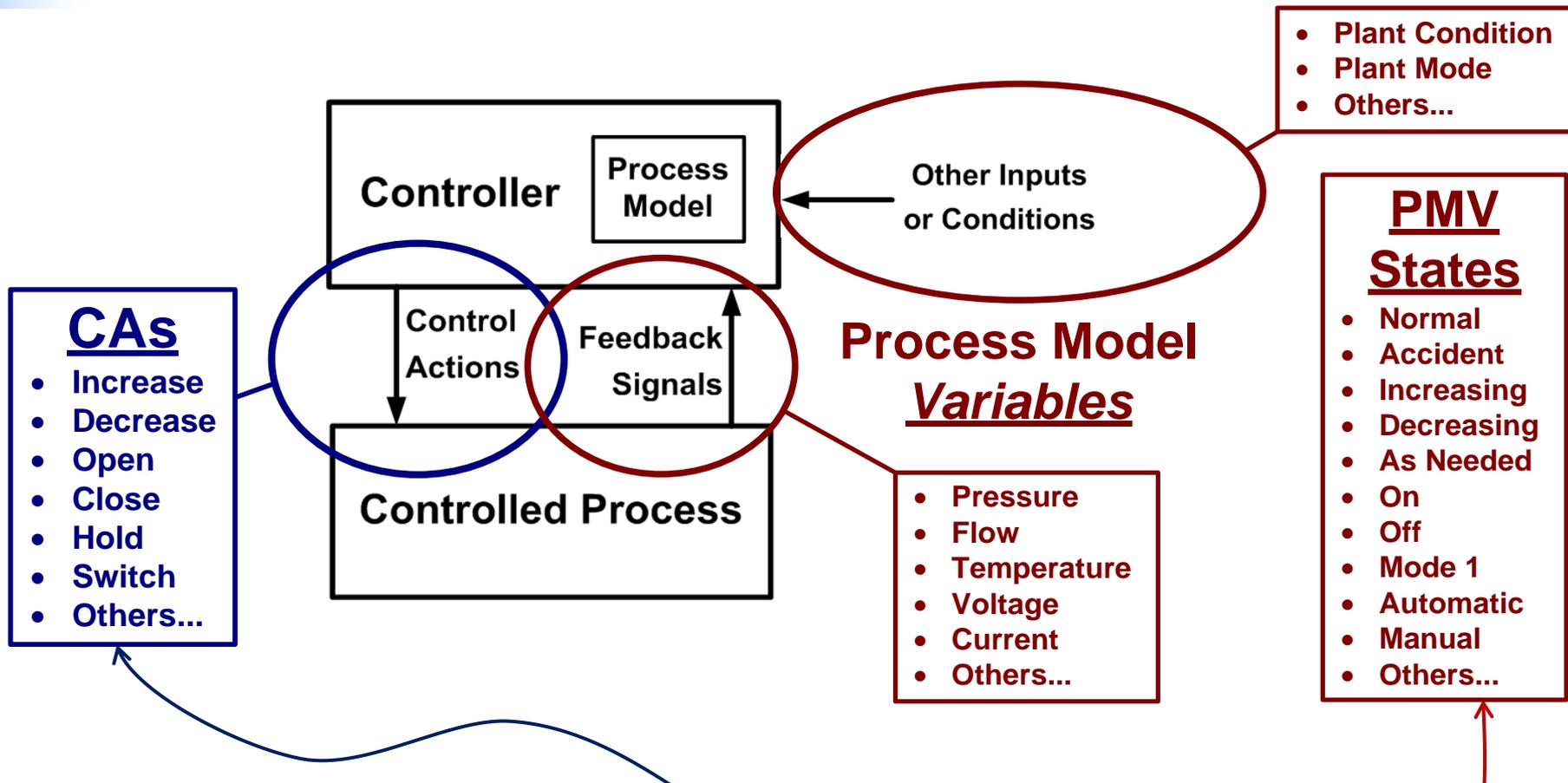
Systems Theoretic Process Analysis (STPA)

Overview



Reference 19: *Engineering a Safer World – Systems Thinking Applied to Safety*, Dr. Nancy G. Leveson; MIT Press

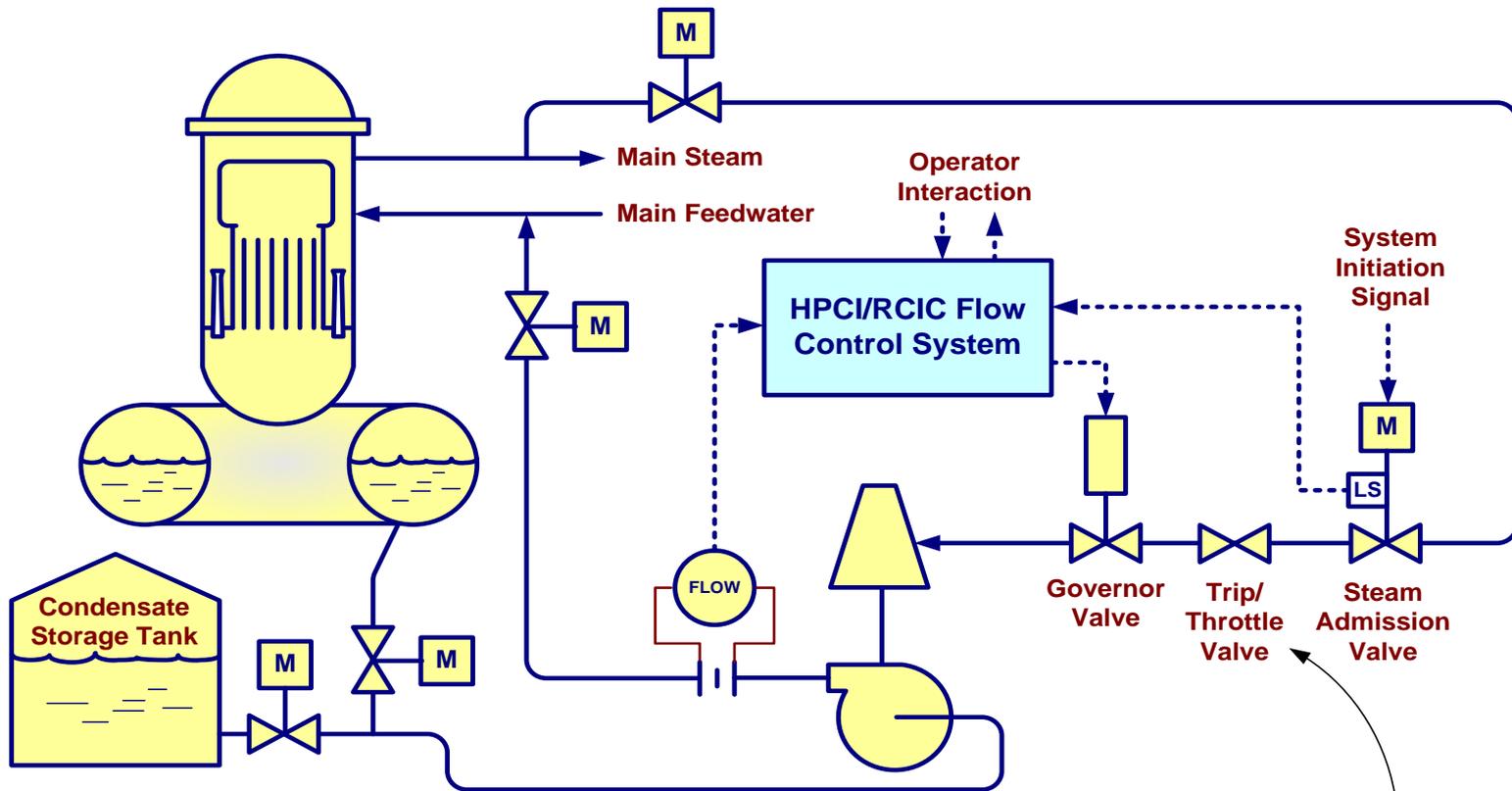
Control Actions in the Context of the Process Model



STPA determines if any **Control Actions** (including lack thereof) are unsafe (i.e., hazardous) under a wide range of **Process Model** conditions

(See step-by-step procedure in 3002000509)

STPA Applied to HPCI Example



System Initiation Signals

(Open Steam Admission Valve & Process Valves)

1. Low Reactor Level (-48")
2. High Drywell Pressure (HPCI only; +2 psig)

System Isolation Signals

(Trip Turbine & Close Process Valves)

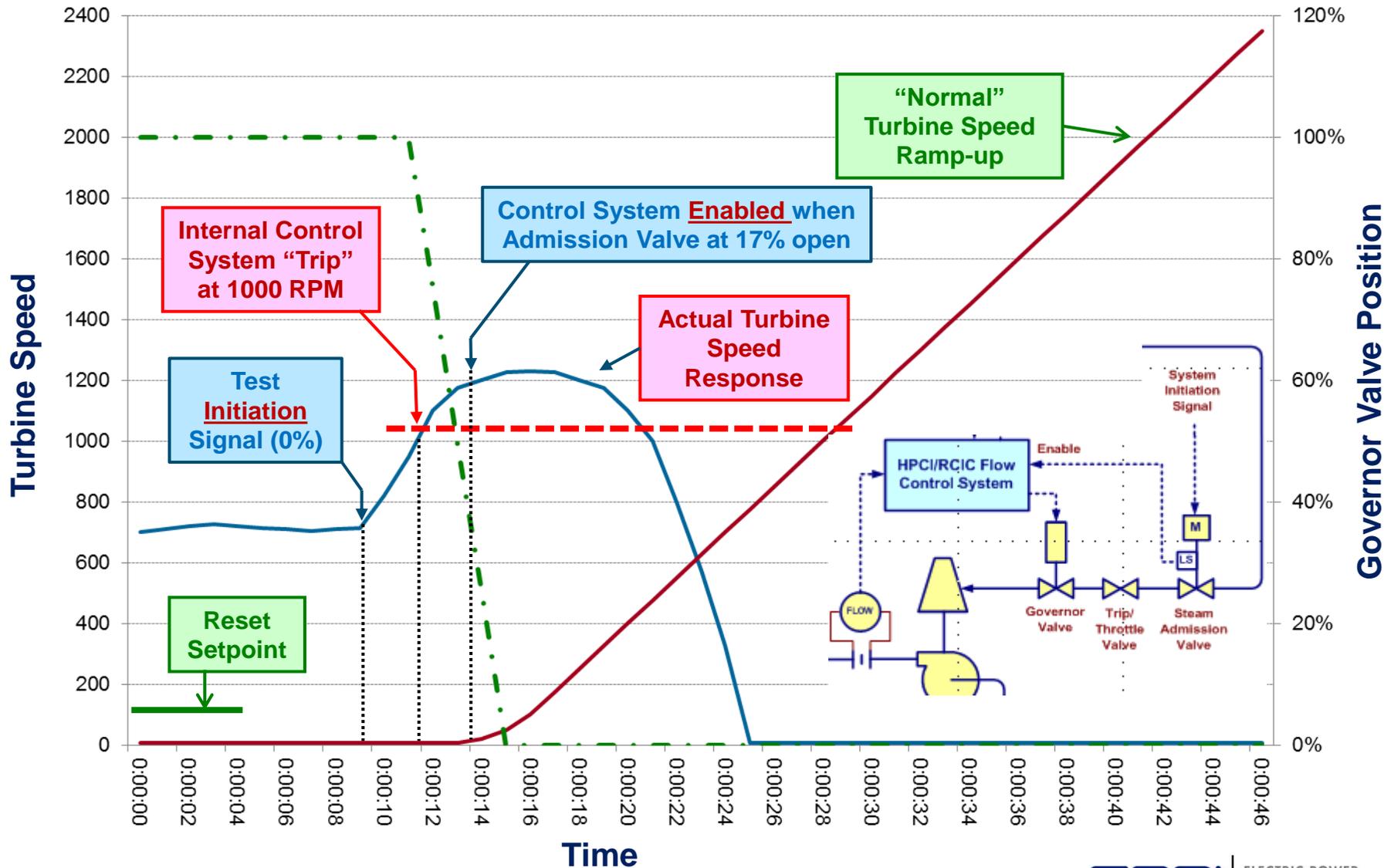
1. High Steam Line Flow
2. High Area Temperature
3. Low Steam Line Pressure (HPCI only)
4. Low Reactor Pressure (RCIC only)
5. Manual

Turbine Trip Signals

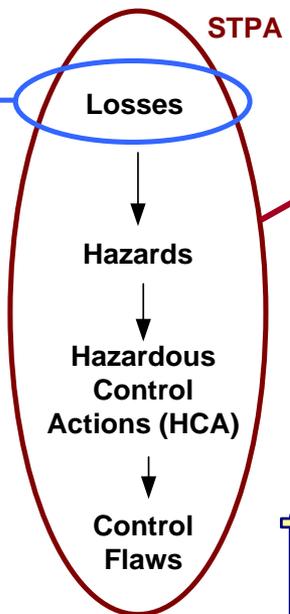
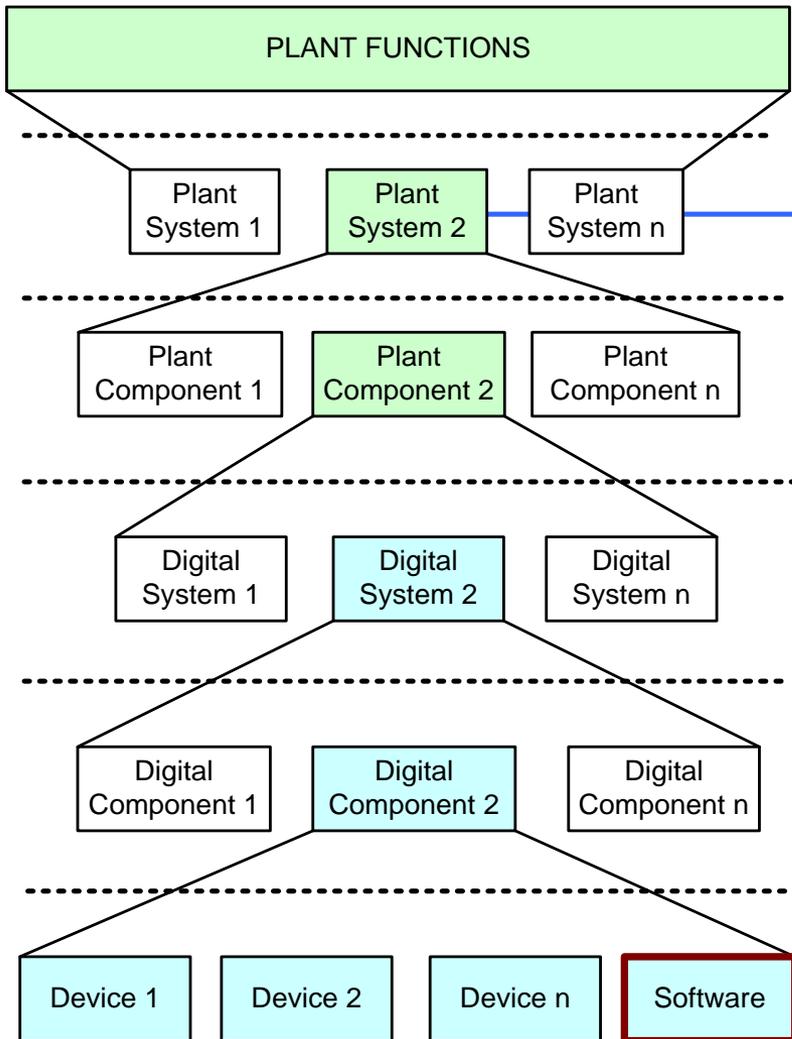
(Close Trip/Throttle Valve)

1. Any system isolation signal
2. High Steam Exhaust Pressure (150 psi)
3. High Reactor Level (+46")
4. Low pump suction pressure (15" Hg)
5. Turbine overspeed
6. Manual (local or remote)

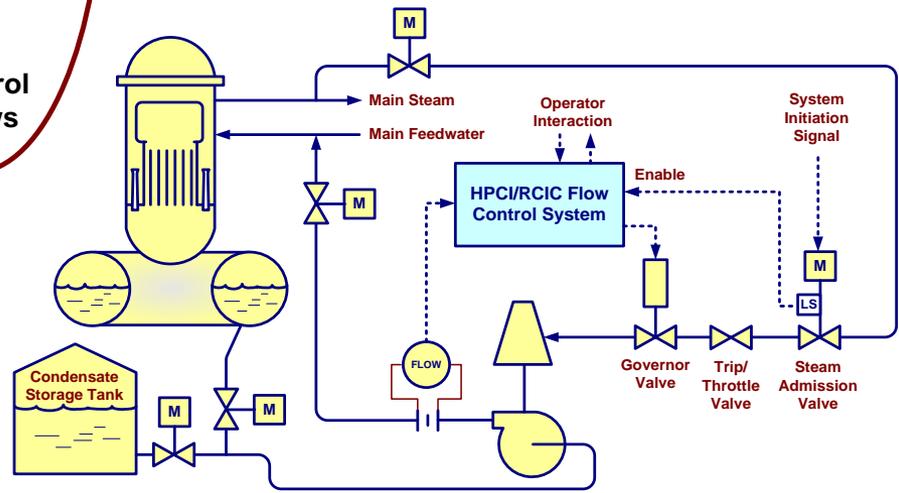
Operating Experience Event (No Component Failures)



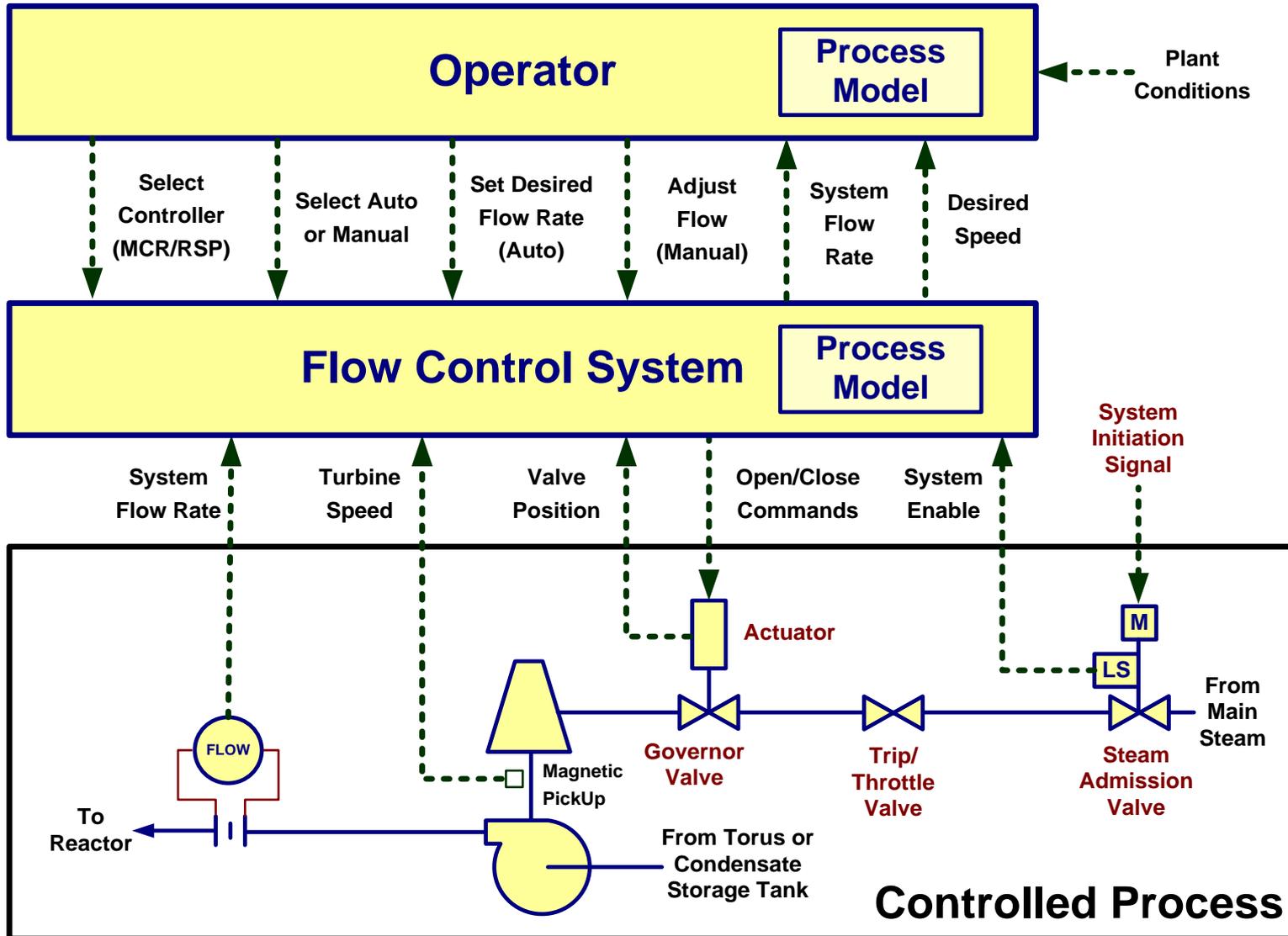
STPA Method Applied to HPCI Example



This example evaluates losses at the plant system level by identifying hazardous control actions that can lead to those losses, and any control flaws that cause them



STPA Control Structure for HPCI Example



STPA Process Model for HPCI

STPA evaluates each control action for each combination of PMV states

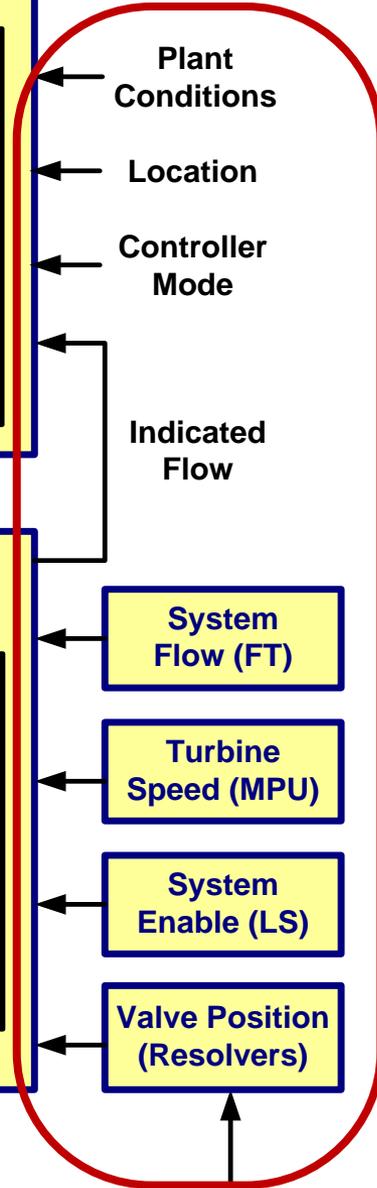
Control Actions

CA1: Increase Desired Flow
CA2: Decrease Desired Flow

CA3: Increase Actual Position
CA4: Decrease Actual Position

| Operator | |
|---------------------------------|-----------------------|
| Process Model Variables | Process Model States |
| Plant Conditions | Normal |
| | Accident |
| Selected Controller | Main Control Room |
| | Remote Shutdown Panel |
| Flow Indicating Controller Mode | Manual |
| | Automatic |
| System Flow | Too Low |
| | At Desired Flow |
| | Too High |

| Flow Control System | |
|-------------------------|----------------------|
| Process Model Variables | Process Model States |
| System Flow | Too Low |
| | At Desired Flow |
| | Too High |
| Turbine Speed | Too Low |
| | At Desired Speed |
| | Too High |
| System Enable | Yes |
| | No |
| Valve Position | Too Closed |
| | At Desired Position |
| | Too Open |



Process Model Variables (PMV)

Governor Valve Actuator

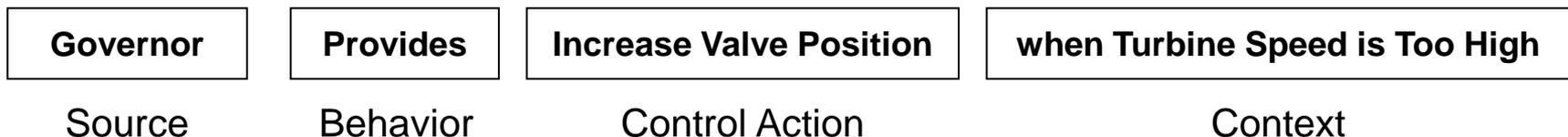
Governor Valve

STPA Evaluates each Control Action for all Combinations of PMV States

Postulated Control Action Behaviors

1. Control Action Is *Provided*
2. Control Action Is *Not Provided*
3. Control Action Is *Provided Too Early*
4. Control Action Is *Provided Too Late*
5. Control Action Is *Stopped Too Soon*

Structure of a Hazardous Control Action (HCA):

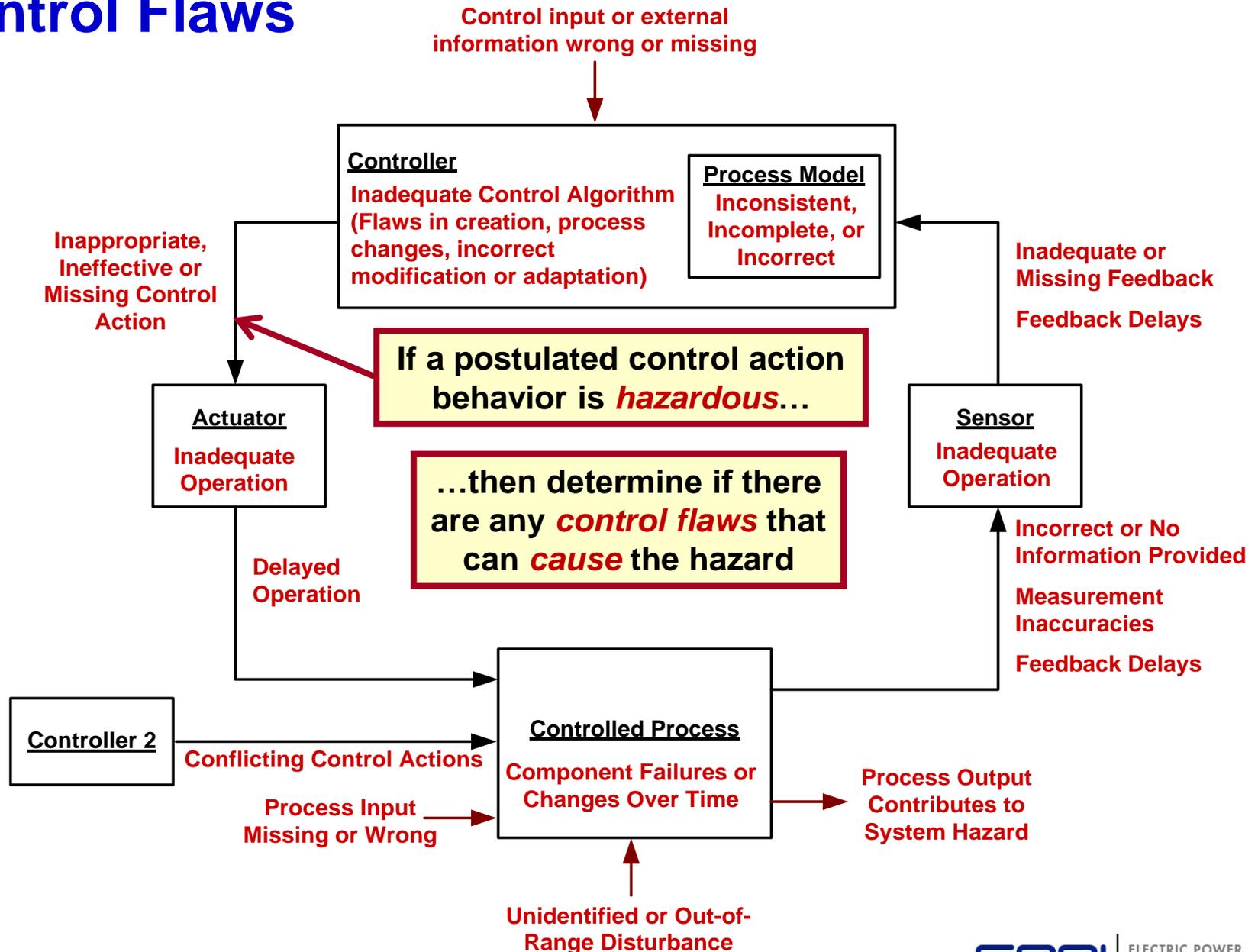


Identify Hazardous Control Actions (HCAs)

| | | | | |
|----------------------|---|----------------------------------|----|---------------------------|
| Controller: | HPCI-RCIC Flow Control System | | H1 | Reactor Exceeds Limits |
| Control Action: | CA3 | Increase Governor Valve Position | H2 | Radioactive Release |
| | | | H3 | Equipment Damage |
| Postulated Behavior: | <u>Providing</u> (the increase valve position command) (Is CA Behavior Hazardous?) | | H4 | Personnel Injury or Death |
| | | | H5 | Reactor Shutdown |

| Row | Process Model Variables | | | | | Analysis Results | | | |
|-----|-----------------------------|---------------------------|--------------------------|------------------------|--------------------------|---------------------------------------|---------------------------------|--------------------|-----------------------------------|
| | PMV1 Plant Conditions | PMV2 Valve Position | PMV3 Turbine Speed | PMV4 System Flow | PMV5 System Enable | Is Situation Already Hazardous? | Is CA Behavior Hazardous? | Related Hazards | Comments (Situational Context) |
| | | | | | | | | | |
| 1 | Accident | Too open | Too high | Too high | Yes | Yes | Yes | H3 | Leads to Rx overfill |
| 2 | | | | | No | Yes | No Response | H1, H2 | Accident and no enable |
| 3 | | | | Too low | Yes | Yes | Maybe | H3 | Increase flow, but overspeed? |
| 4 | | | | | No | Yes | No Response | H1, H2 | Accident and no enable |
| 5 | | | | As needed | Yes | No | Yes | H3 | Leads to Rx overfill |
| 6 | | | | | No | Yes | No Response | H1, H2 | Accident and no enable |
| 7 | | | Too low | Too high | Yes | Yes | Yes | H3 | Leads to Rx overfill |
| 8 | | | | | No | Yes | No Response | H1, H2 | Accident and no enable |
| 9 | | | | Too low | Yes | Yes | Maybe | H3 | Increase flow, but valve damage? |
| 10 | | | | | No | Yes | No Response | H1, H2 | Accident and no enable |
| 11 | | | | As needed | Yes | No | Yes | H3 | Leads to Rx overfill |
| 12 | | | | | No | Yes | No Response | H1, H2 | Accident and no enable |
| 13 | | | | Too high | Yes | Yes | Yes | H3 | Leads to Rx overfill |
| 14 | | | | | No | Yes | No Response | H1, H2 | Accident and no enable |

Control Flaws



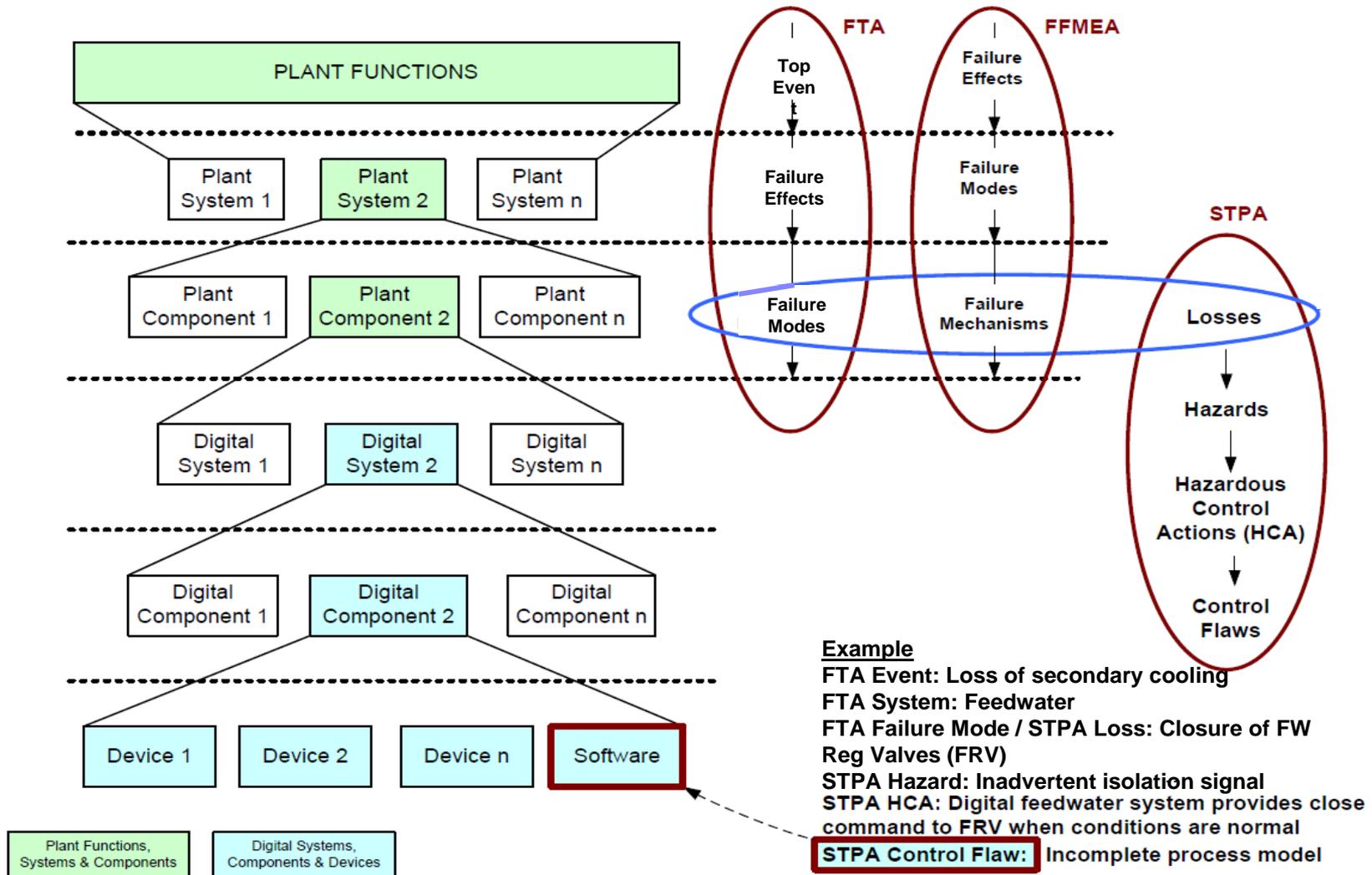
Identify Potential Causes of HCAs

| |
|--|
| Hazard: Equipment Operated Beyond Limits (H3) |
| Controller: HPCI-RCIC Flow Control System |
| Hazardous Control Action No. 2: “Increase governor valve position” command is <u>provided</u> when: there is an accident and turbine speed is too high, regardless of system flow |
| Inadequate, Missing or Delayed Feedback |
| Enable signal sent to controller before there is a valid demand on HPCI/RCIC |
| enable provided when steam admission valve is not open (broken or misaligned LS) |
| steam admission valve commanded open when there is no demand on HPCI/RCIC (spurious ESFAS signal) |
| Enable signal sent to controller when there is a demand on HPCI/RCIC, but delayed |
| enable provided when steam admission valve is opened, but too late (misaligned LS or LS setpoint too high) |
| steam admission valve opens too slowly when commanded by ESFAS Initiation Signal (excessive stem thrust) |
| steam admission valve commanded open too late when there is a demand on HPCI/RCIC (ESFAS delay) |
| HPCI/RCIC pump flow rate signal to controller is missing, delayed, incorrect, too infrequent, or has inadequate resolution |
| Signal corrupted during transmission |
| sensor failure |
| sensor design flaw |
| sensor operates correctly but actual flow rate is outside sensor’s operating range |
| fluid type is not as expected (water vs. steam?) |
| Governor valve position signal to controller is missing, delayed, incorrect, too infrequent, or has inadequate resolution |
| Problems with communication path |
| actual position is beyond sensor’s range |
| sensor reports actuator position and it doesn’t match valve position |
| sensor correctly reports valve position but position doesn’t match assumed area/shape |

Blended Approaches May Combine Strengths of Multiple Methods

- Objectives: I&C hazard analysis methods that:
 - are as complete as practical
 - can be performed with a reasonable level of effort
- Six approaches
 - each has strengths and limitations
 - not clear that any one method can achieve both objectives
- Consider blended approaches to take advantage of the strengths and minimize the effects of the limitations

Blending FTA or FFMEA with STPA (One Possibility)



Next Steps

- EPRI Product 3002000509 published June 2013
- Further development of hazard analysis methods for practical application to nuclear plant problems
 - Software tools to address management of large intermediate data sets produced in STPA
 - MIT researchers
 - Set Equation Transformation System (SETS)
 - Plant demonstration projects
 - Computer-based training modules
 - Case studies
 - Industry workshop
 - ...

Another EPRI Report on Failure Analysis

Protecting Against Digital Common Cause Failure - Combining Defensive Measures and Diversity Attributes (EPRI 1019182)

- Issue - No consensus on best way to protect against CCF
 - Diversity often assumed effective
 - Other factors may be more important
- Report takes holistic approach, considers all types of defensive measures:
 - Development practices effective in avoiding or eliminating errors
 - Hardware architecture and software design features that preclude or mitigate certain types of failures
 - Various types of diversity to prevent or mitigate CCF

Provides guidance on ways to eliminate or mitigate hazards

Topic 2 –

Operating Experience (OE) Update

Focus of research - actual and potential software common-cause failure (CCF) in safety and non-safety applications

Key Points From 2009 Presentation

- Software has been no more problematic than other CCF contributors
- Need to capture and promote process and design characteristics that have been effective in protecting against CCFs

EPRI reports

- *Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems* (EPRI 1016731, 2008)

(Provided to ACRS and NRC January 2009)

- *Digital Instrumentation and Control Operating Experience Lessons Learned: Volume II - Case Studies 6-10* (EPRI 1022247, 2010)
- *Digital Operating Experience in the Republic of Korea* (EPRI 1022986, 2011)

Ongoing and future work

- Lessons learned from plant-wide upgrade (Czech Republic)
- Additional digital OE – from non-U.S. plants

OE Update – Summary of U.S. and Korean Data

| Categories | KHNP 1984 – 2010 (EPRI 1022986) | U.S. 1987 – 2007 (EPRI 1016731) |
|---|------------------------------------|------------------------------------|
| Digital Events | 97 | 322 |
| Safety-related | 19 (20%) | 49 (15%) |
| Actual or potential CCFs - system or subsystem level | 0 | 11 |
| Software | 0 | 1 |
| Non-software | 0 | 10 |
| Non-safety related | 78 (80%) | 273 (85%) |
| Actual or potential CCFs - system or subsystem level | 17 | 56 |
| Software | 4 (5%) | 14 (5%) |
| Non-software | 13 | 42 |

In both the Korean and U.S. data, software was not a dominant contributor to actual or potential CCF

Topic 3 – PRA Insights

Focus of research - applying risk methods to digital

- Use current PRA methods
- Sensitivity studies to address uncertainties
- Modeling level of detail
- Methods to estimate digital reliability

Key Points From 2009 Presentation

- Risk insights are possible today using existing techniques
- Should encourage use of PRA given its capabilities and current state of the art

PRA Insights, cont'd

EPRI Reports

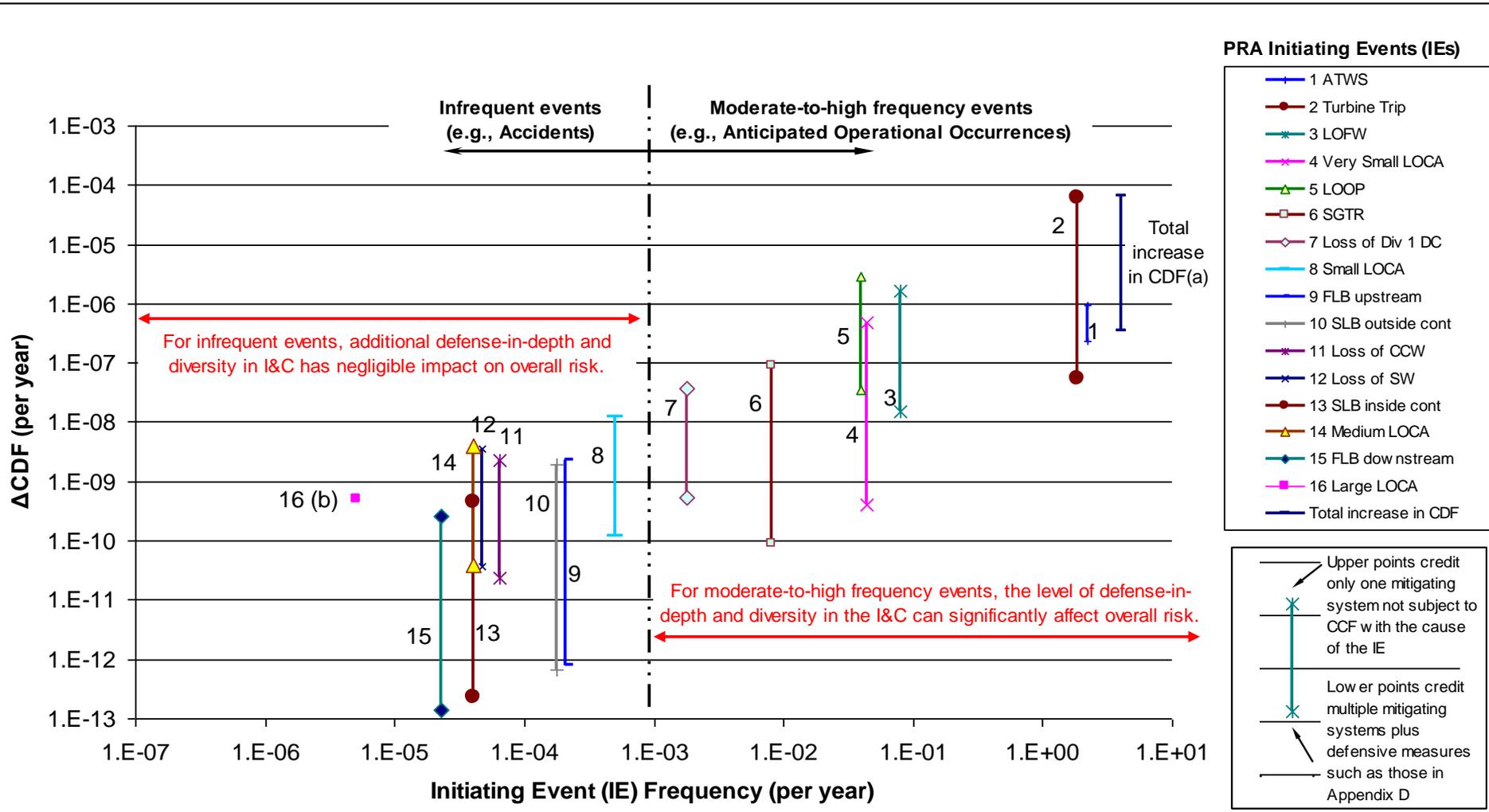
- *Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions* (EPRI 1016721, Dec 2008)
- *Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants* (EPRI 1019183, 2009)
- *Estimating Failure Rates in Highly Reliable Digital Systems* (EPRI 1021077, 2010)
- *Modeling of Digital Instrumentation & Control in Nuclear Power Plant Probabilistic Risk Assessments* (EPRI 1025278, 2012)

PRA Update

Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants (EPRI 1019183)

- Traditional deterministic approach for defense-in-depth and diversity (D3) ignores risk insights
 - Can overlook important accident sequences
 - Can divert resources to sequences that do not drive risk
- Report looks at importance of defense-in-depth and diversity in I&C of mitigating systems for various accident sequences
 - Diversity is most important for high frequency events with multiple mitigating systems (e.g., turbine trip, loss of feedwater)
 - Diversity least important for low frequency events with a single mitigating system (e.g., large break LOCA)

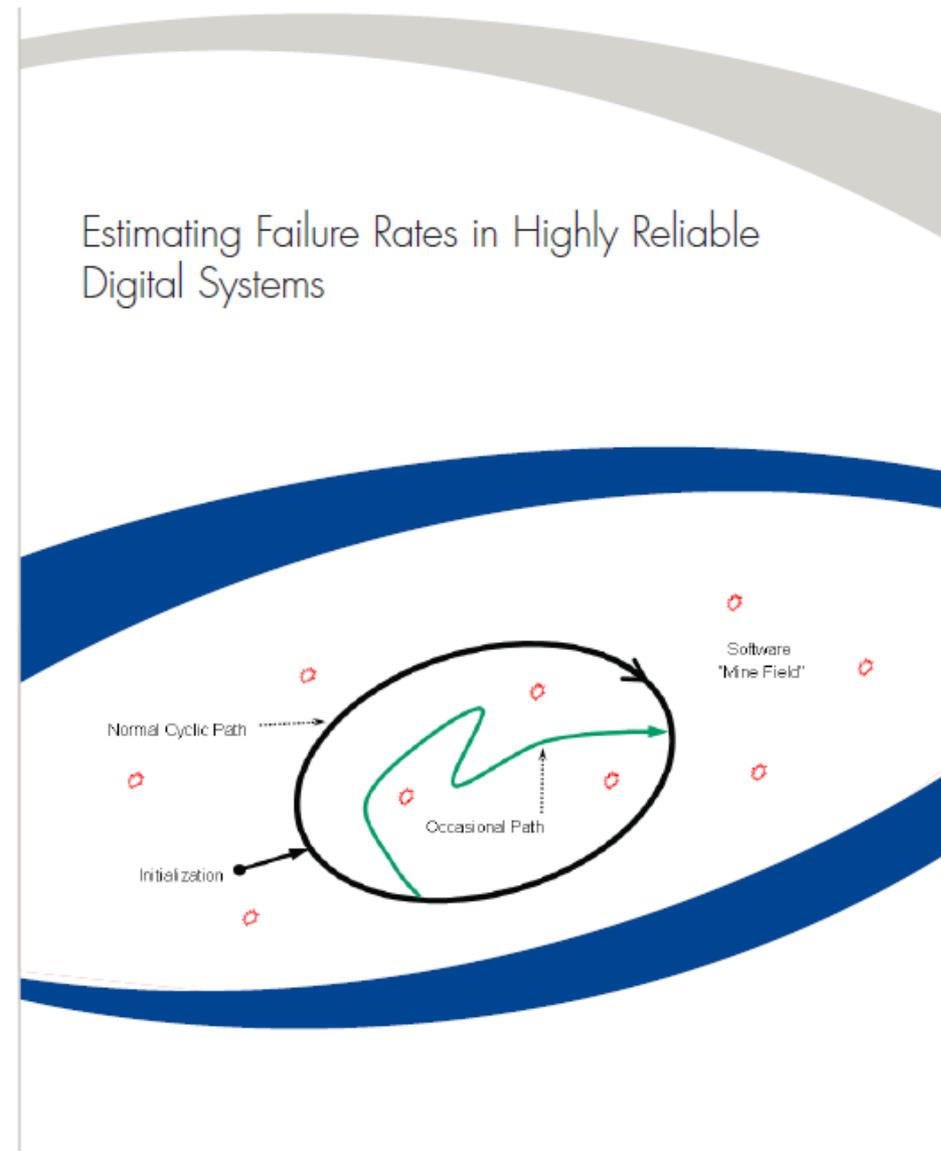
Calculated Increases in Core Damage Frequency (CDF) Due to Digital Common-Cause Failure (Figure 4-1 in 1019183)



PRA Update, cont'd

Estimating Failure Rates in Highly Reliable Digital Systems (EPRI 1021077)

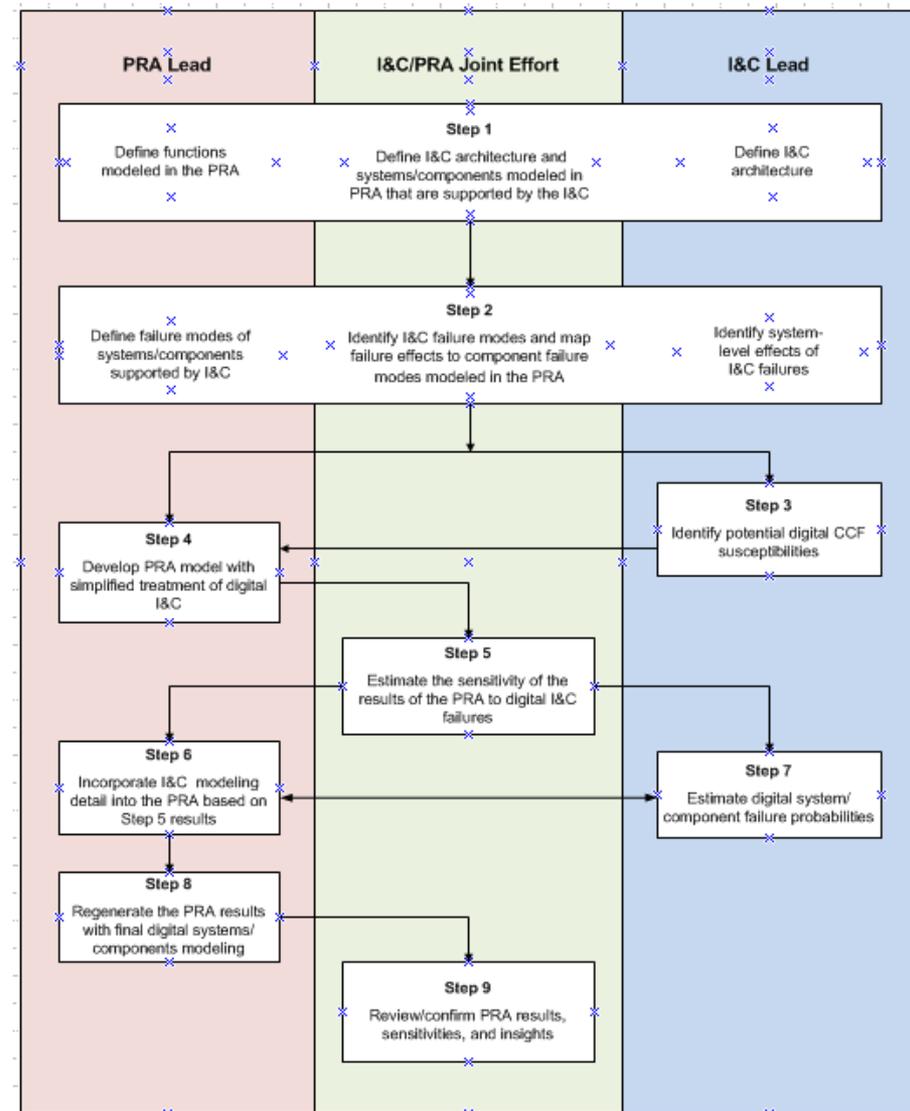
- Hardware methods not well-suited to digital
 - Systematic (non-random) failure mechanisms cause same behavior **every time**
 - Manage 'triggers' to improve dependability
- Report approach:
 - Use PRA to focus analysis on significant failure modes (context)
 - Engineering judgment to assess design features that affect dependability
 - Failure rates not precise, but adequate for PRA insights



PRA Update, cont'd

Modeling of Digital Instrumentation & Control in Nuclear Power Plant Probabilistic Risk Assessments (EPRI 1025278)

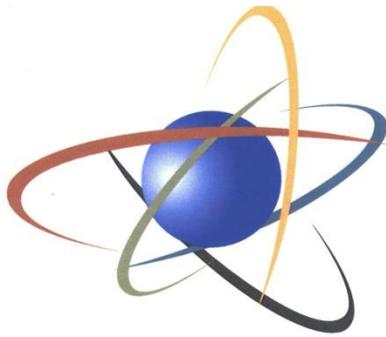
- Presents a nine-step process
 - Uses current PRA methods
 - Focus on recognizing role of I&C within the plant (context)
 - Considers failure modes of controlled electrical and mechanical equipment
 - Credits design practices and features that affect reliability (defensive measures)
 - Addresses level-of-detail, failure probability estimation
 - Stresses joint effort between PRA analysts and I&C experts



Acronyms

- CCF Common Cause Failure
- D3 Diversity & Defense-in-Depth
- DI&C Digital Instrumentation and Control
- DFMEA Design FMEA
- EMC Electromagnetic Compatibility
- EPRI Electric Power Research Institute
- FFMEA Functional FMEA
- FMEA Failure Modes and Effects Analysis
- FPGA Field Programmable Gate Array
- HAZOP HAZard and OPerability Analysis
- HFE Human Factors Engineering
- HPCI High Pressure Coolant Injection
- KHNP Korea Hydro & Nuclear Power
- LOCA Loss of Coolant Accident
- OE Operating Experience
- PRA Probabilistic Risk Assessment
- RCIC Reactor Core Isolation Cooling
- STPA Systems Theoretic Process Analysis

Together...Shaping the Future of Electricity



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

NRC DIGITAL SYSTEM RESEARCH

Digital System Failure Modes, Hazard Analysis and Operational Experience

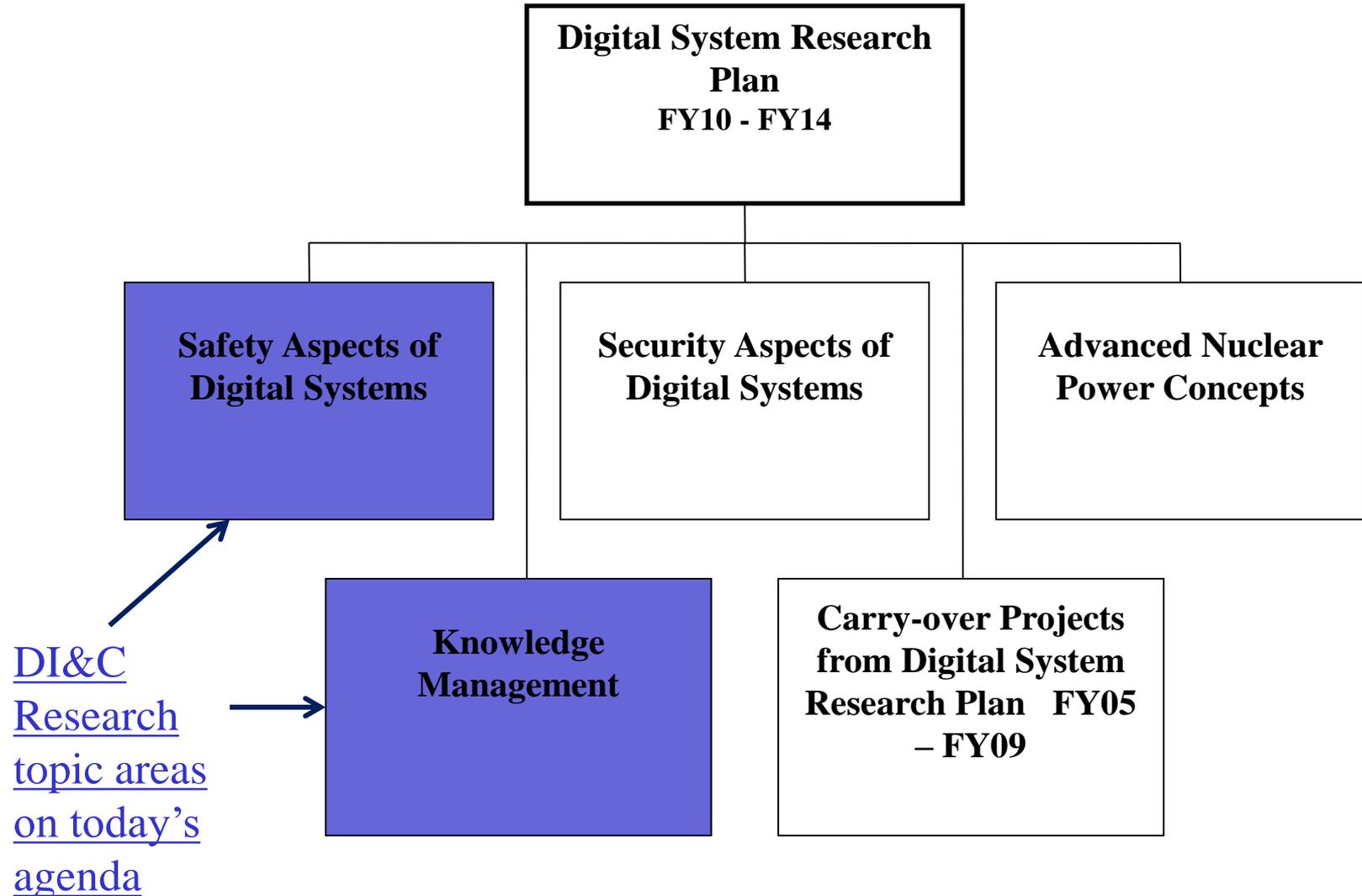
**Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee
September 19, 2013**

Russell Sydnor

**Division of Engineering
Office of Nuclear Regulatory Research
(301-251-7405, russell.sydnor@nrc.gov)**

- **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**
- **No letter is requested**

DI&C Research Program



Background –

- **February 2010 - issued FY10-14 DI&C Research Plan**
 - **Previous research plan/results**
 - **License Office input**
 - **ACRS input and letters**
 - **Digital System Failure Modes and Operational Experience**
 - **Commission SRM M0806058B**
 - **Flexible/iterative research approach**

Background continued -

- **ACRS June 2011 – DI&C research results and status update**
 - **Expert Clinic, RIL-1001 on Software Uncertainties**
 - **NUREG/IA-0254 on SFMEA**
 - **Operational Experience – Scope and plans**
- **Refocused research when needed based on:**
 - **Expert input**
 - **License Office Experience**
 - **License Office User Needs**
 - **ACRS Feedback**

Today's presentations will address ACRS recommendations & concerns (NUREG-1635)

- User need driven research
 - **Concern:** Premature termination precluding in-depth understanding.
- Provide sound technical basis to resolve foreseeable safety issues.
- Develop and maintain NRC-internal expertise.
- Understand sources of uncertainties.
- Seek external collaborations:
 - Other federal agencies.
 - International, esp. areas requiring data.
- **Concern:** Design review for safety & security not integrated.
- **Concern:** Preserving Independence; D3; Deterministic behavior.

Today's topics

- **RIL-1002, Identification of Failure Modes in Digital Systems**
 - **2nd of 3 RILs that will answer SRM M0806058B**
- **RIL-1101, Technical Basis to review Hazard Analysis of Digital Systems**
 - **Research Plan - Analytical Assessment of Digital Systems**
 - **NRO User Need Request (SMR DSRS)**
- **Operational Experience – Analysis methods**
 - + **Learning from Nuclear DI&C OpE**
 - **Use of non-nuclear and international data**

- **ACRS – Advisory Committee on Reactor Safeguards**
- **DI&C – Digital Instrumentation and Controls**
- **DSRS – Design Specific Review Standard**
- **FY – Fiscal Year**
- **I&C – Instrumentation and Controls**
- **NRC- Nuclear Regulatory Commission**
- **NRO – Office of New Reactors**
- **OpE – Operational Experience**
- **RIL – Research Information Letter**
- **SMR – Small Modular Reactor**
- **SRM – Staff Requirements Memorandum**

Backup Slides

- **Analytical Assessment of DI&C Systems**
 - **Identification of credible systematic failure and fault modes typical of software-intensive DI&C systems**
 - **Gain a better understanding of DI&C failure modes and of the feasibility of applying failure analysis in risk quantification**
 - **Develop an inventory, classification, and characterization of DI&C systems for use in nuclear safety applications**

Learning From Digital System Experience

"Every event is a learning opportunity" – Sushil Birla



Learning Experience

- Mining existing data sources such as licensee event reports and Equipment Performance and Information Exchange System (EPIX) is difficult.
- Software and interconnection information is not available from existing data sources.
- Direct contact with the plants is needed to obtain information on system configuration, software, and interconnections.
- NRC and industry should work together to enhance digital inventory data structure and information.

Next Steps

Work with the Institute of Nuclear Power Operations (INPO) and industry to develop enhanced methods for collecting and extracting digital information.

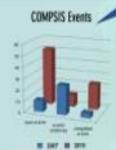
EPRI ELECTRIC POWER RESEARCH INSTITUTE

Improve digital instrumentation and control methods, tools, data, and technical information useful to the U.S. nuclear industry and the U.S. Nuclear Regulatory Commission (NRC).



Learning Experience

- Well-defined requirements can improve system safety and reliability.
- Main root causes are design defects, problems with configuration management, and hardware failures.



COMPSIS

Computer-based Systems Important to Safety

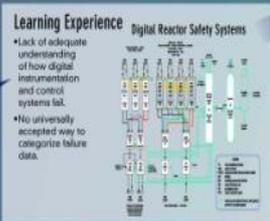
International participation in collecting information on fault experiences with computer-based safety systems at nuclear power plants.



Next Steps

- Continue adding research-grade events.
- Add new lower-severity events to the database.
- Compare data structure with other databases, e.g., Working Group on Risk Assessment (WGRisk).

Other Collaborative Activities

Next Steps

- Support a consistent structure for categorizing failure data.
- Research methods for data mining and learning.
- Develop a framework for organizing information.

IRSN Institut de Radioprotection et de Sûreté Nucléaire

NASA National Aeronautics and Space Administration

The NETS Nuclear Reactor Project

Methods and Tools

Develop methods and tools for data mining and learning from digital systems.

Non-Nuclear

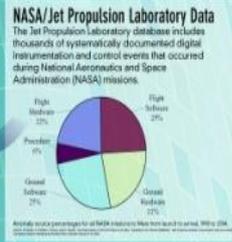


Learning Experience

- More careful and consistent documentation of minor incidents correlates with fewer major incidents.
- While incident frequency drops over time, it will increase whenever new conditions are encountered.

Next Steps

- Gain insight into diagnostics and prognostics.
- Investigate whether the root causes of minor and major events differ.
- Evaluate emerging technologies.
- Investigate NASA software rigor at different quality categories and compare to NPP software rigor.





Research Information Letter (RIL)-1002

Identification of Failure Modes in Digital Safety Systems – Expert Clinic Findings, Part 2

Mauricio Gutierrez
RES/DE/ICEEB

Sushil Birla
RES/DE

September 19, 2013

Outline

- RIL-1002 Background and Objectives
- Research Method
- Findings
- Results
- Next Steps

Background – ACRS Interest

- Advisory Committee for Reactor Safeguards (ACRS) has a long standing concern that software based DI&C system failure modes are not well understood.
- 2008 - ACRS formally brought concerns about failure modes to Commission attention when ACRS reviewed DI&C Interim Staff Guidance-03, “Interim Staff Guidance on Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments”.
- 2010 - Recommended that “software Failure Modes and Effects Analysis (FMEA) methods should be investigated and evaluated to examine their suitability for identifying critical software failures that could impair reliable and predictable Digital I&C performance.”

Background – Commission Direction

Staff Requirements Memorandum (SRM) M080605B dated June 2008 (ML081780761) “At the next Commission briefing on digital I&C, the staff should

...report the progress made with respect to identifying & analyzing DI&C failure modes

RIL-1001

IRSN-NRC NUREG/IA

RIL-1002

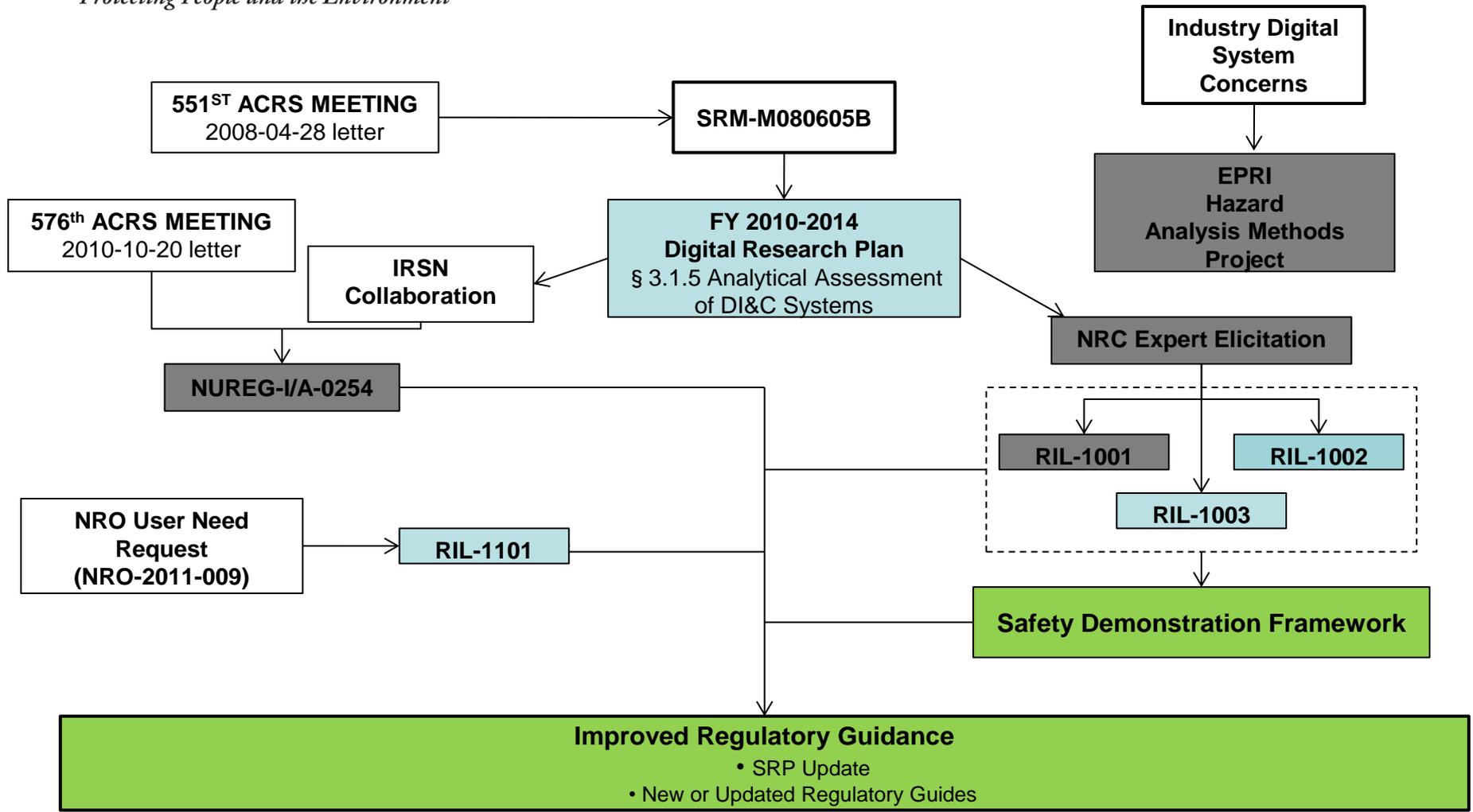
and discuss the feasibility of applying failure mode analysis to quantification of risk associated with DI&C...”

RIL - 1003

■
Completed Work

■
Ongoing Work

Failure Mode Research



Work Drivers
 Ongoing Work
 Completed Work
 Future Work

Objectives of RIL-1002

1. Report the progress made with respect to identifying and analyzing Digital I&C failure* modes.
2. Report the findings resulting from the staff investigation on the efficacy of Software Fault* Modes and Effects Analysis (SFMEA) as a method for identifying faults leading to system failures impairing a safety function.

Research Method

- **Elicited Information from Subject Matter Experts**
 - Individual Expert Interviews
 - Expert Clinic held in 2010
 - Follow up references suggested by experts consulted
- **Performed Supplemental Research Activities**
 - Reviewed over 150 public and non-public articles and reports from journals, conferences, technical meetings, and technical organizations.
 - Institut De Radioprotection Et De Sûreté Nucléaire (IRSN) Collaboration – NUREG/IA-0254
 - Interviewed additional experts not part of Elicitation Activities

Digital System Failure Modes Found

- RIL-1002 reports 10 sets of system level digital failure modes
 - NRC Collaboration Efforts (Set A with IRSN, 4 failure modes; Set J via OECD technical exchange, 7 failure modes)
 - ACRS (Set B, 6 failure modes)
 - Automotive Industry Experts (Set C, 6 failure modes; Set D, 6 failure modes)
 - Cross Industry-Surveys of Failure Modes, US National Lab and PRA Experts (Set E, 9 failure modes; Set I, 6 failure modes)
 - Aerospace Industry Experts (Set F, 5 failure modes)
 - Academic Researchers (Set G, 4 failure modes; Set H, 2 failure modes)

Staff Synthesized Digital System Failure Mode Set

- Technical community does not consider any set found as standard or complete.
- The staff identified the failure modes that were repeated in the 10 sets and synthesized them to eliminate duplicates and to summarize the learning that resulted from this project (Set K^{**}, 8 failure modes).
- Set K may be missing possible failure modes.
- Other characterizations of distinct failure modes in set K are possible.

Efficacy of SFMEA

- Not main focus of RIL-1002.
- Information relevant to efficacy of SFMEA was in the resources reviewed.
- Appendix B reports 10 large sets of Software Faults and Fault Modes found.
- Appendix C describes 6 techniques that could be called SFMEA (a few others were found but were very similar to the 6 described).

Results

- **Objective 1:** Report the progress made with respect to identifying and analyzing digital I&C failure modes.
 - The failure modes found are not applicable to all digital safety systems.
 - There are many ways of characterizing digital system failure modes.
 - Failure Mode Set K does not constitute a set of digital system failure modes suitable for assurance of a moderately complex system.
 - Expansion of Failure Mode Set K is unlikely to provide assurance
 - A safety function can be impaired without any failures
 - It is unknown how many other system specific digital system failure modes exist.

Results

- **Objective 2:** Report the findings resulting from the staff investigation on the efficacy SFMEA as a method for identifying faults leading to system failures impairing a safety function.
 - The fault space is large for digital systems.
 - No standard or widely accepted set of fault modes found.
 - No assurance of a complete set of fault modes for software in digital safety systems was found.

Conclusions

- **Objective 1**
 - Completeness (of a set of failure modes) is not assurable at this time.
 - There are major obstacles to identifying all critical failure modes for a moderately complex digital safety system.
- **Objective 2**
 - No sound technical basis to require any SFMEA technique from NRC applicants and licensees.
 - No changes in DI&C regulations or guidance for SFMEA is suggested.

Next Steps

- Track external research on identification of DI&C system failure modes.
- No further work on SFMEA techniques.
- Complete work on RIL-1003 (Feb 2014).
- Focus on Hazard Analysis Techniques and Safety Demonstration Framework for Regulatory Reviews of Digital Safety Systems. [*](#)



Questions
?????

Acronyms

- **ACRS** Advisory Committee for Reactors and Safeguards
- **DI&C** Digital Instrumentation and Control
- **EPRI** Electrical Power Research Institute
- **FMEA** Failure Modes and Effects Analysis
- **I&C** Instrumentation and Control
- **IRSN** Institut De Radioprotection Et De Sûreté Nucléaire
- **NRC** Nuclear Regulatory Commission
- **NRO** NRC Office of New Reactors
- **PRA** Probabilistic Risk Assessment
- **RES** NRC Office of Nuclear Regulatory Research
- **RIL** Research Information Letter
- **SFMEA** Software Fault Modes and Effects Analysis
- **SRM** Staff Requirements Memorandum



Backup Slides

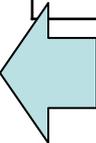
**Identification of Failure Modes in Digital
Safety Systems – Expert Clinic Findings,
Part 2**

Staff Synthesized FM Set

| ID | Failure Mode | Elaboration |
|-----|---------------------------------------|---|
| K.1 | No output upon demand | Includes no change in output or no response for any input. |
| K.2 | Output without demand | e.g.: Unwanted response. |
| K.3 | Output value incorrect | Incorrect response to input or set of inputs. Includes: Value too high or too low; Value stuck at previous value, e.g. ON, OFF |
| K.4 | Output at incorrect time | Too early; Too late. |
| K.5 | Output duration too short or too long | This mode is specific to continuous functions. |
| K.5 | Output intermittent | Functions correctly intermittently Example: Loose connection |
| K.6 | Output flutters | Unwanted oscillation; output fluctuates rapidly Example: Unstable servo-loop. Could damage equipment. |
| K.7 | Interference | Affects another system, often resulting from unwanted, unintended interactions, coupling, or side effects. |
| K.8 | Byzantine behavior | <ul style="list-style-type: none"> • Possible in a distributed system. • Could affect redundant elements of a system. • Could be caused by software, e.g. propagating and worsening effect of round-off error. • Could be caused by hardware, e.g. single-bit hardware fault caused Amazon S3 system failure in 2008. |

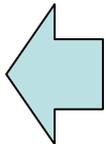
Staff Failure Mode Synthesis Example

| ID | Failure Mode | Synthesized from: |
|-----|-----------------------|---|
| K.1 | No output upon demand | A.2 Failure to perform the module function with correct value B.1 Task Crash B.5 Task Incorrect Response C.4 Erroneous Execution C.5 Failure to return D.1 Input value incorrect D.2 Output value corrupted E.1 Zero or maximum output E.2 No change of output with change of input E.4 No function with signal E.6 High output E.7 Low output F.1 Continuous control failure F.2 Failure to activate F.5 Failure to run correctly J.1 Failure to actuate J.5 Loss of function J.6 No actuation signal when demanded |



Definitions

- **Failure**
 - The termination of the ability of an item to perform a required function.
- **Failure Mode:**
 - The effect by which a failure is observed to occur.
 - The manner in which a failure occurs.
- **Fault**
 - 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.
- **Fault Mode**
 - One of the possible states of a faulty item.





U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Research Information Letter (RIL)-1101:

**Technical Basis to Review Hazard Analysis of
Digital Safety Systems**

Luis Betancourt / Sushil Birla

Division of Engineering

Office of Nuclear Regulatory Research

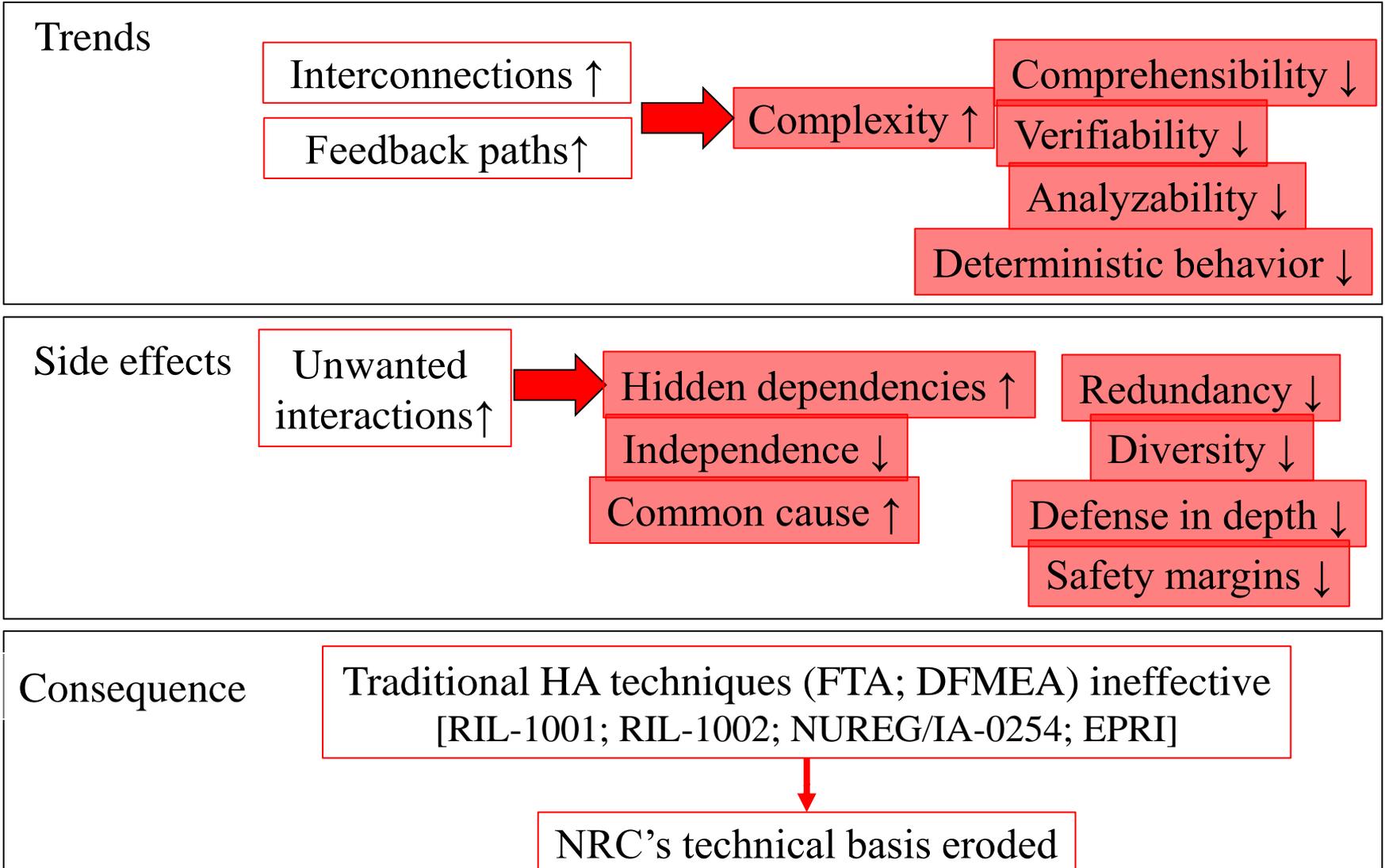
September 19, 2013

Outline

- **Background**
 - Current State & Trends
 - Motivation for RIL-1101
- **Hazard Analysis: What it means**
 - Hazard – definition
 - HA explained in terms of IEEE Std 603
 - HA is part of safety analysis
 - Organizational & analytical framework
 - RIL-1101: Relationship with Plant HA
- **Dependencies**
 - Types of dependencies: Examples
 - Dependency example: System architecture dimension
 - Product-process dependency over lifecycle
 - Dependency on a process activity
- **Research Method**
- **Scope**
 - RIL-1101 scope
 - Contributory hazard space in focus
 - Contributory hazard scenario 1/2
 - Contributory hazard scenario 2/2
- **Evaluation of Hazard Analysis**
 - Factors affecting quality of HA
 - Reasoning Model
- **Envisioned Roadmap**

- **Background**
 - Current State & Trends
 - Motivation for RIL-1101
- **Hazard Analysis: What it means**
 - Hazard – definition
 - HA explained in terms of IEEE Std 603
 - HA is part of safety analysis
 - Organizational & analytical framework
 - RIL-1101: Relationship with Plant HA
- **Dependencies**
 - Types of dependencies: Examples
 - Dependency example: System architecture dimension
 - Product-process dependency over lifecycle
 - Dependency on a process activity
- **Research Method**
- **Scope**
 - RIL-1101 scope
 - Contributory hazard space in focus
 - Contributory hazard scenario 1/2
 - Contributory hazard scenario 2/2
- **Evaluation of Hazard Analysis**
 - Factors affecting quality of HA
 - Reasoning Model
- **Envisioned Roadmap**

Current State & Trends



Motivation for RIL-1101

User need

- Technical basis to review HA of a digital safety system
- Support mPower DSRS Chapter 7 Appendix A
 - Support reviewer in judgment

Value to others

- Organization & Analytical framework
- Technical reference

- **Background**
 - Current State & Trends
 - Motivation for RIL-1101
- **Hazard Analysis: What it means**
 - Hazard – definition
 - HA explained in terms of IEEE Std 603
 - HA is part of safety analysis
 - Organizational & analytical framework
 - RIL-1101: Relationship with Plant HA
- **Dependencies**
 - Types of dependencies: Examples
 - Dependency example: System architecture dimension
 - Product-process dependency over lifecycle
 - Dependency on a process activity
- **Research Method**
- **Scope**
 - RIL-1101 scope
 - Contributory hazard space in focus
 - Contributory hazard scenario 1/2
 - Contributory hazard scenario 2/2
- **Evaluation of Hazard Analysis**
 - Factors affecting quality of HA
 - Reasoning Model
- **Envisioned Roadmap**

Hazard: Definition

- (IEC Vocab) **Potential for harm**
 - **Condition.** Circumstance. Scenario.
 - Scope boundary: System to be analyzed.
- (ISO/IEC/IEEE 24765 3.1283-1) An intrinsic property or **condition** that has the **potential** to cause **harm** or damage.
 - {Harm OR damage} = Loss

HA explained in terms of IEEE Std 603 criterion 4h

A specific basis shall be established
for the design of each safety system
of the nuclear power generating station;
the design basis shall document as a minimum ...

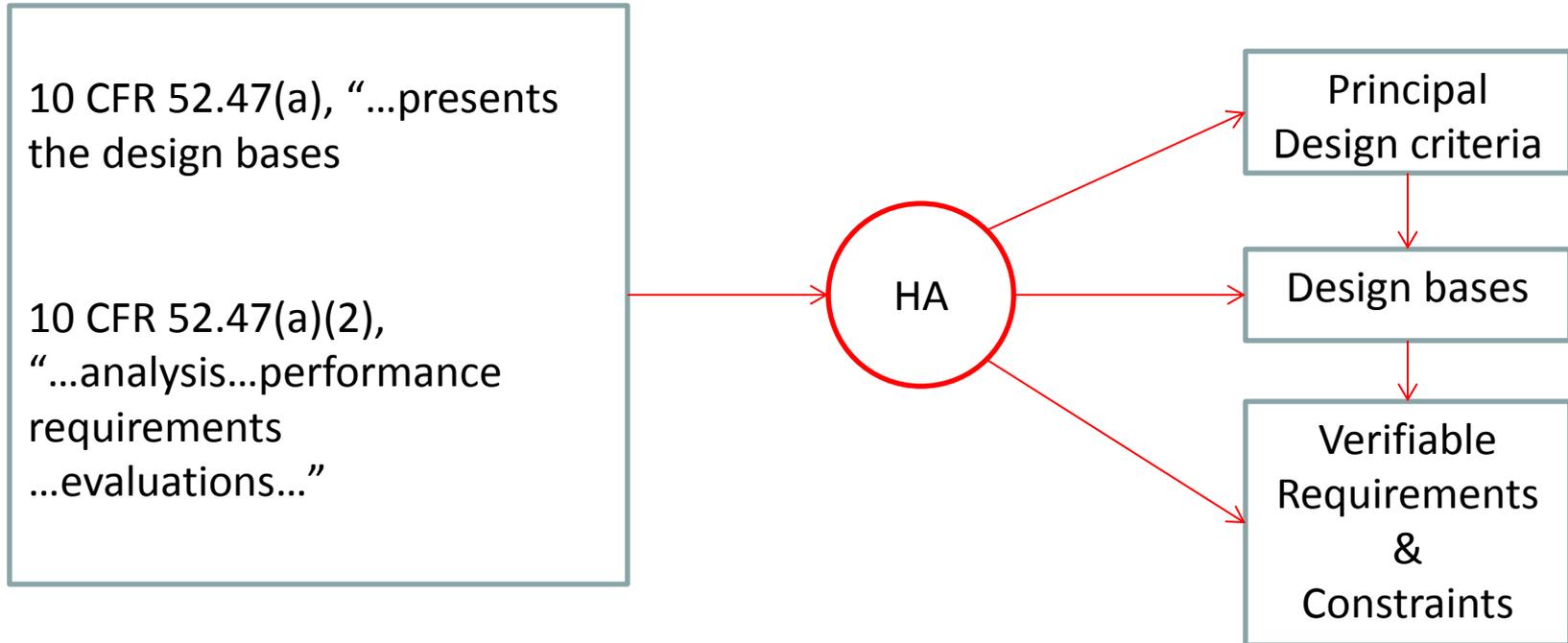
the conditions having the potential for functional
degradation of safety system performance

Hazards

and for which provisions shall be incorporated
to retain the capability of performing the safety
functions.

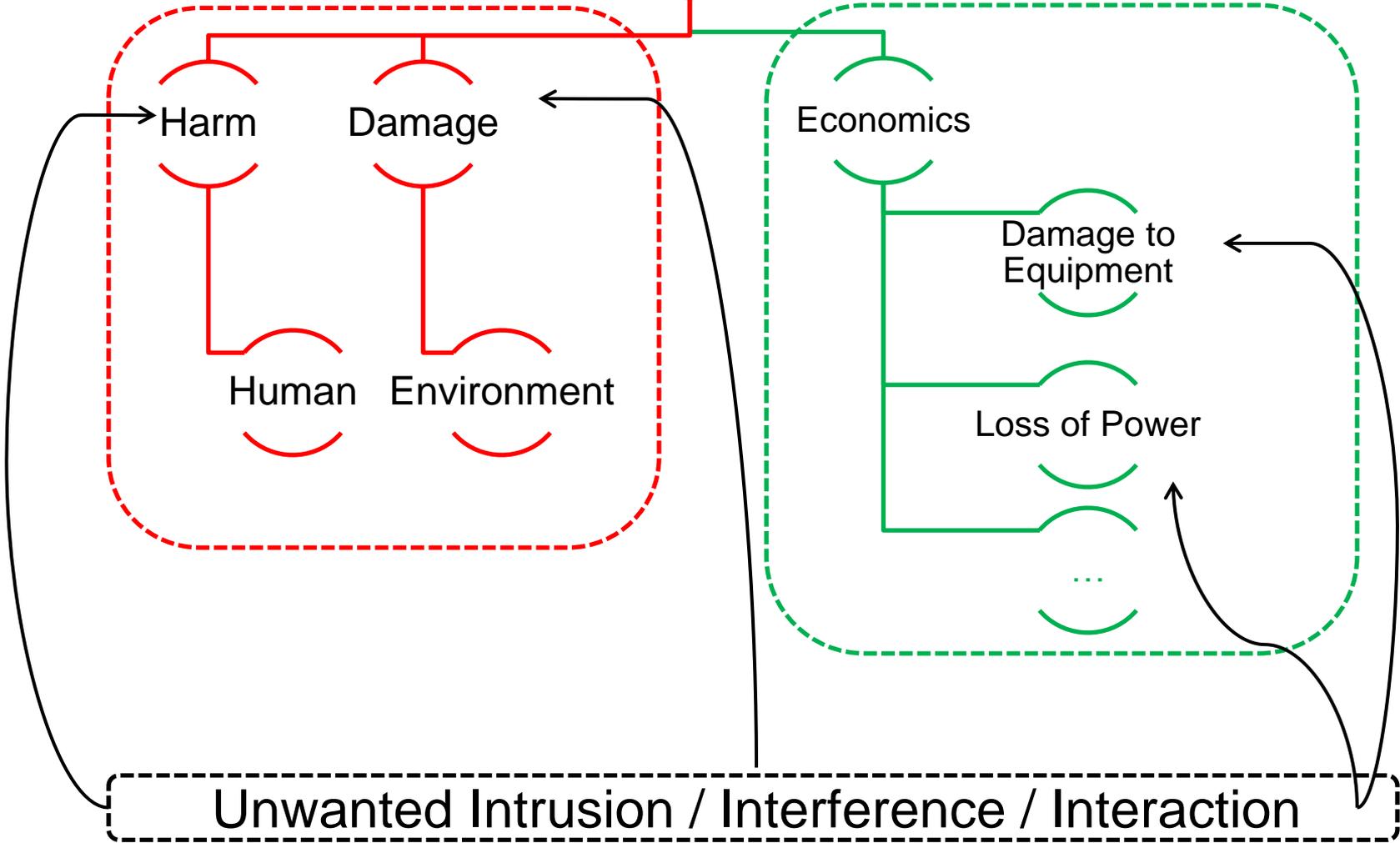
Hazard
Controls

HA is Part of Safety Analysis

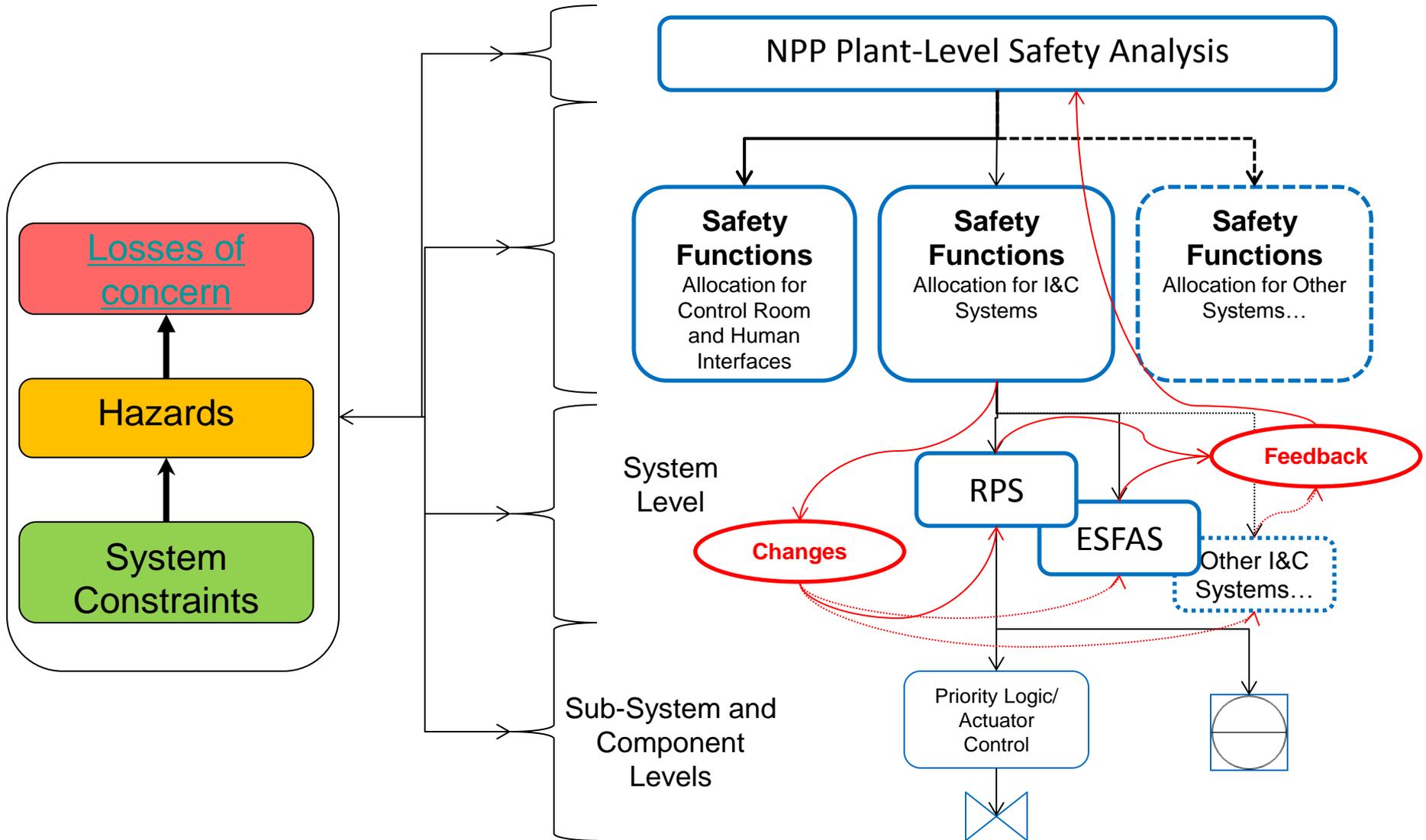


Organizational & Analytical Framework

Loss



RIL-1101: Relationship with Plant HA

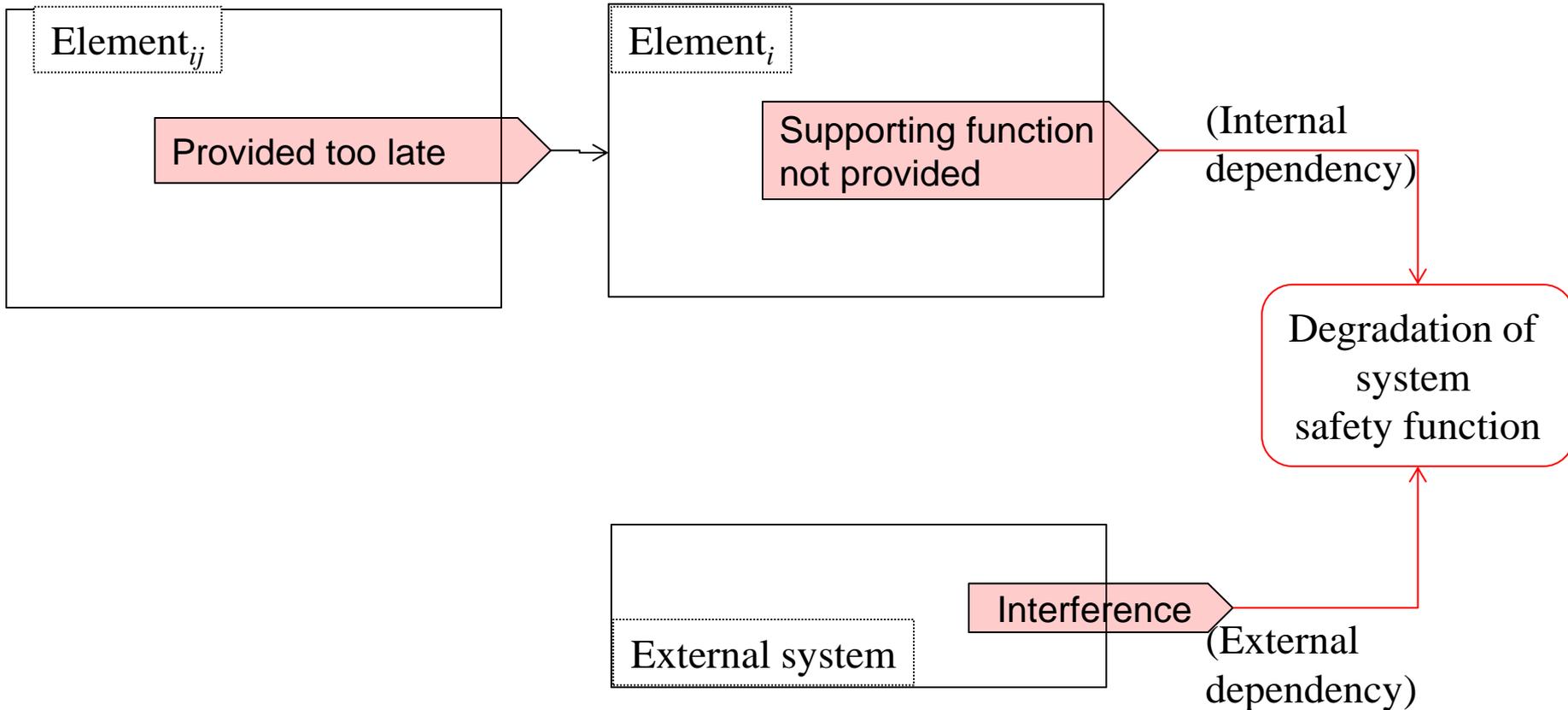


- **Background**
 - Current State & Trends
 - Motivation for RIL-1101
- **Hazard Analysis: What it means**
 - Hazard – definition
 - HA explained in terms of IEEE Std 603
 - HA is part of safety analysis
 - Organizational & analytical framework
 - RIL-1101: Relationship with Plant HA
- **Dependencies**
 - Types of dependencies: Examples
 - Dependency example: System architecture dimension
 - Product-process dependency over lifecycle
 - Dependency on a process activity
- **Research Method**
- **Scope**
 - RIL-1101 scope
 - Contributory hazard space in focus
 - Contributory hazard scenario 1/2
 - Contributory hazard scenario 2/2
- **Evaluation of Hazard Analysis**
 - Factors affecting quality of HA
 - Reasoning Model
- **Envisioned Roadmap**

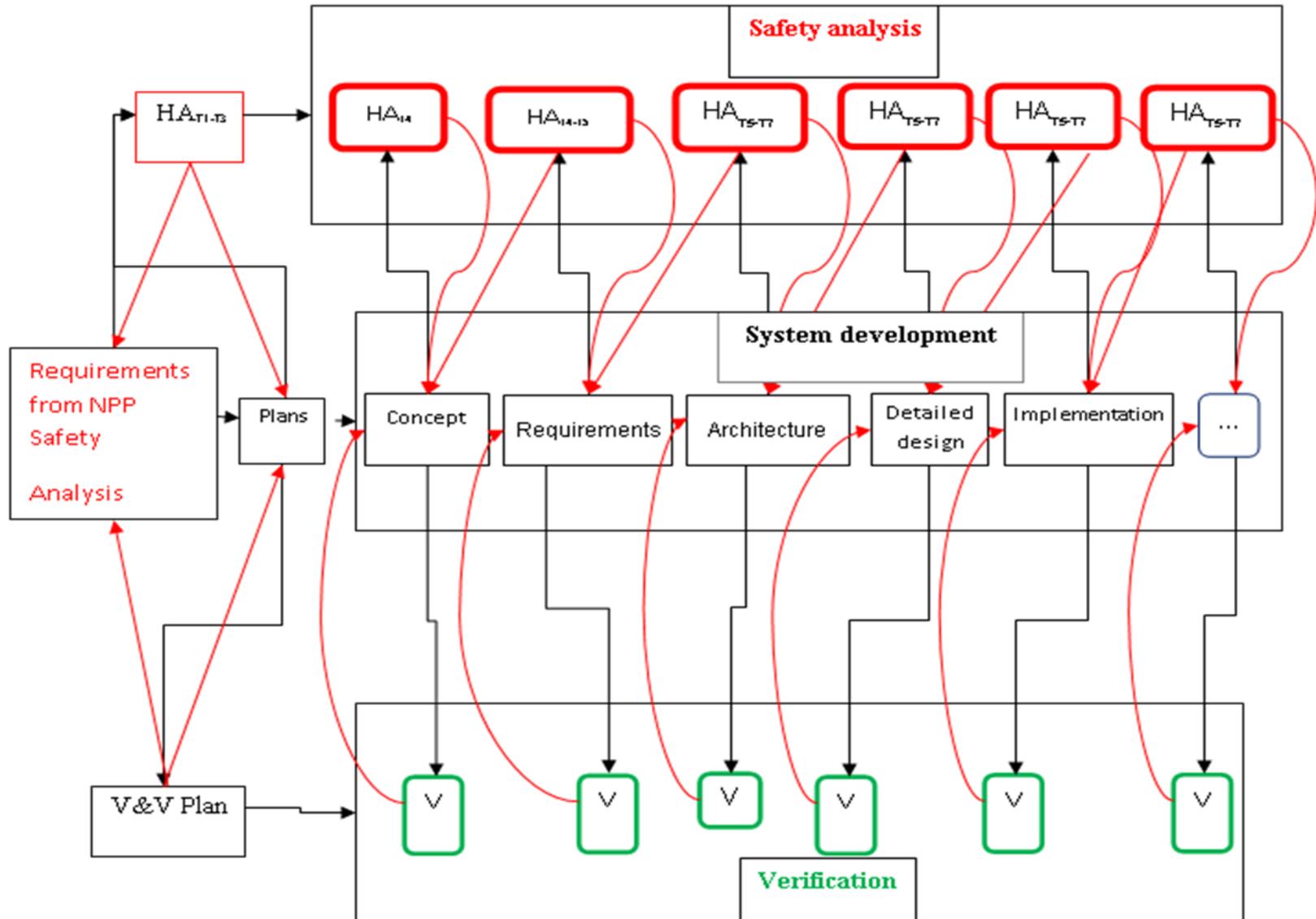
Types of Dependencies: Examples

- Function
- Control flow
- Data; information
- Resource sharing or constraint
- Conflicting goals or losses of concern
- States or conditions in the environment
 - Controlled processes
 - Supporting physical processes
- Concept
- Some unintended, unrecognized form of coupling.

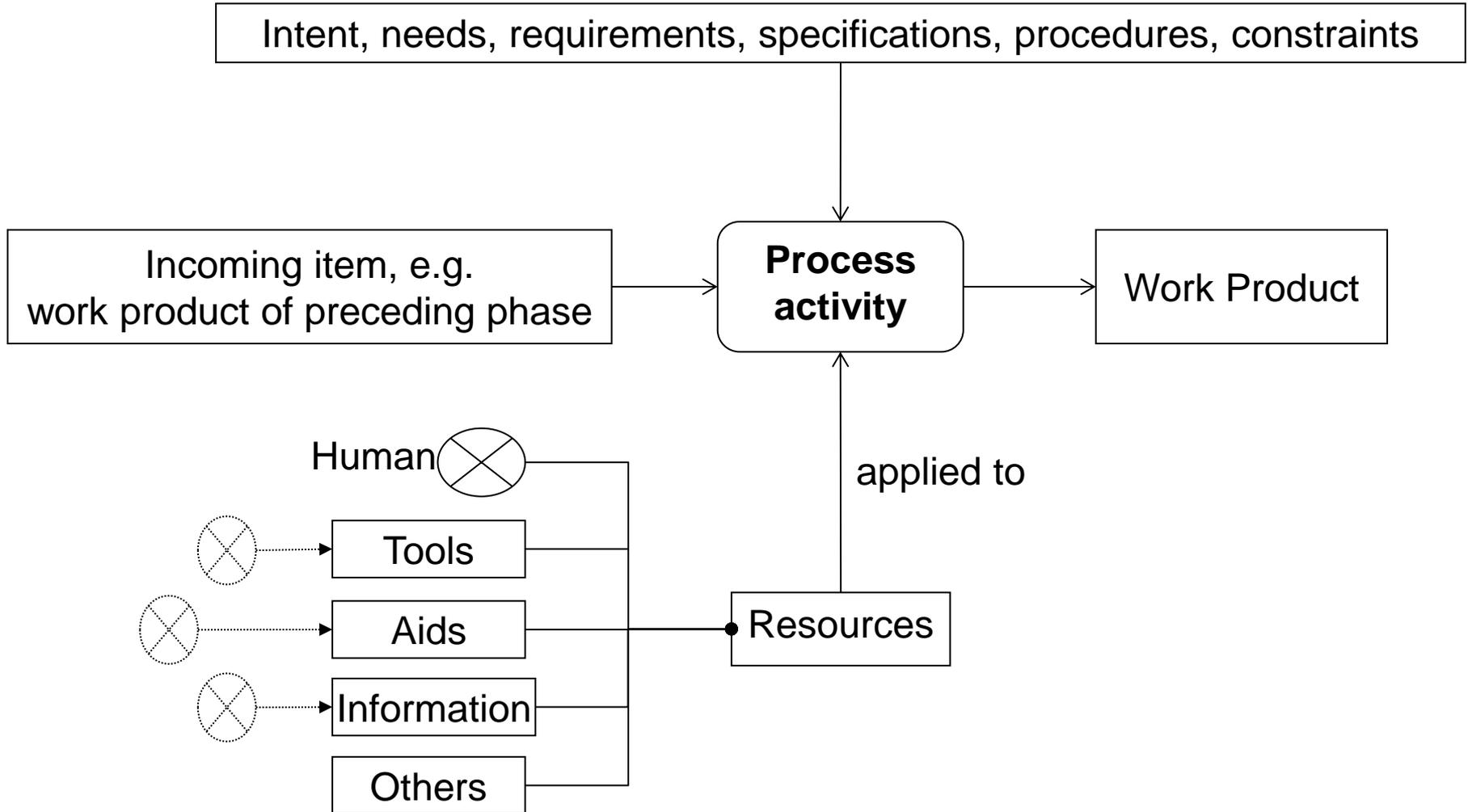
Dependency Example: System Architecture Dimension



Product-Process Dependency Over Lifecycle



Dependency on a Process Activity



- **Background**
 - Current State & Trends
 - Motivation for RIL-1101
- **Hazard Analysis: What it means**
 - Hazard – definition
 - HA explained in terms of IEEE Std 603
 - HA is part of safety analysis
 - Organizational & analytical framework
 - RIL-1101: Relationship with Plant HA
- **Dependencies**
 - Types of dependencies: Examples
 - Dependency example: System architecture dimension
 - Product-process dependency over lifecycle
 - Dependency on a process activity
- **Research Method**
- **Scope**
 - RIL-1101 scope
 - Contributory hazard space in focus
 - Contributory hazard scenario 1/2
 - Contributory hazard scenario 2/2
- **Evaluation of Hazard Analysis**
 - Factors affecting quality of HA
 - Reasoning Model
- **Envisioned Roadmap**

Research Method

Limited to organizing existing knowledge

- Knowledge available in technical literature
 - Reviewed over 150 public and non-public articles and reports from journals, conferences, technical meetings, and technical organizations.
- Knowledge acquired from respective experts
 - Unresolved comments → Need for future research

- **Background**
 - Current State & Trends
 - Motivation for RIL-1101
- **Hazard Analysis: What it means**
 - Hazard – definition
 - HA explained in terms of IEEE Std 603
 - HA is part of safety analysis
 - Organizational & analytical framework
 - RIL-1101: Relationship with Plant HA
- **Dependencies**
 - Types of dependencies: Examples
 - Dependency example: System architecture dimension
 - Product-process dependency over lifecycle
 - Dependency on a process activity
- **Research Method**
- **Scope**
 - RIL-1101 scope
 - Contributory hazard space in focus
 - Contributory hazard scenario 1/2
 - Contributory hazard scenario 2/2
- **Evaluation of Hazard Analysis**
 - Factors affecting quality of HA
 - Reasoning Model
- **Envisioned Roadmap**

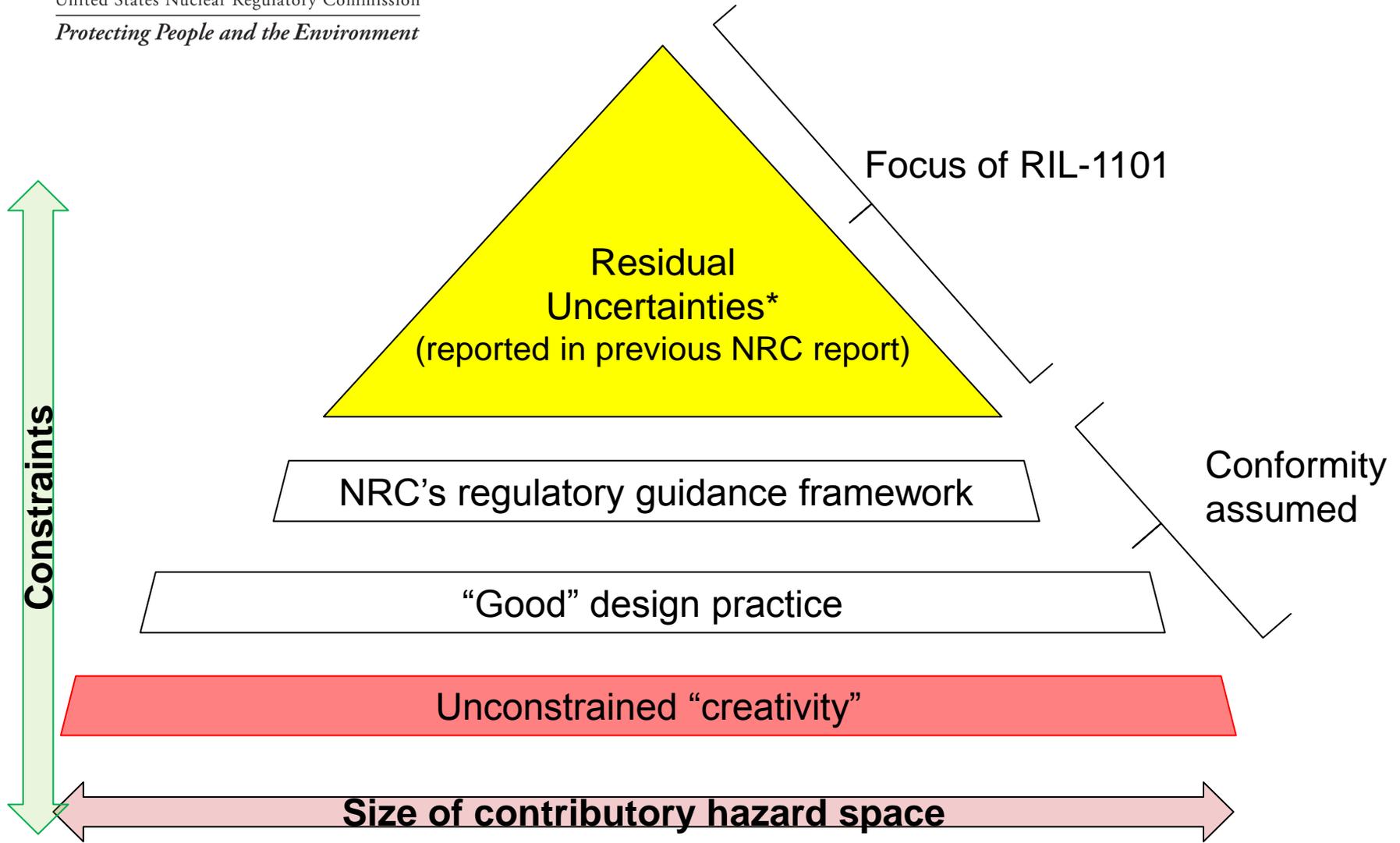
Includes

- Contributory hazards rooted in systemic causes through system development activities
- Focused on evaluation of HA (rather than performance of HA)
- Digital Safety System AND
 - Any system or element interfacing with or affecting digital safety system
 - Any correct timely performance of a safety function is dependent

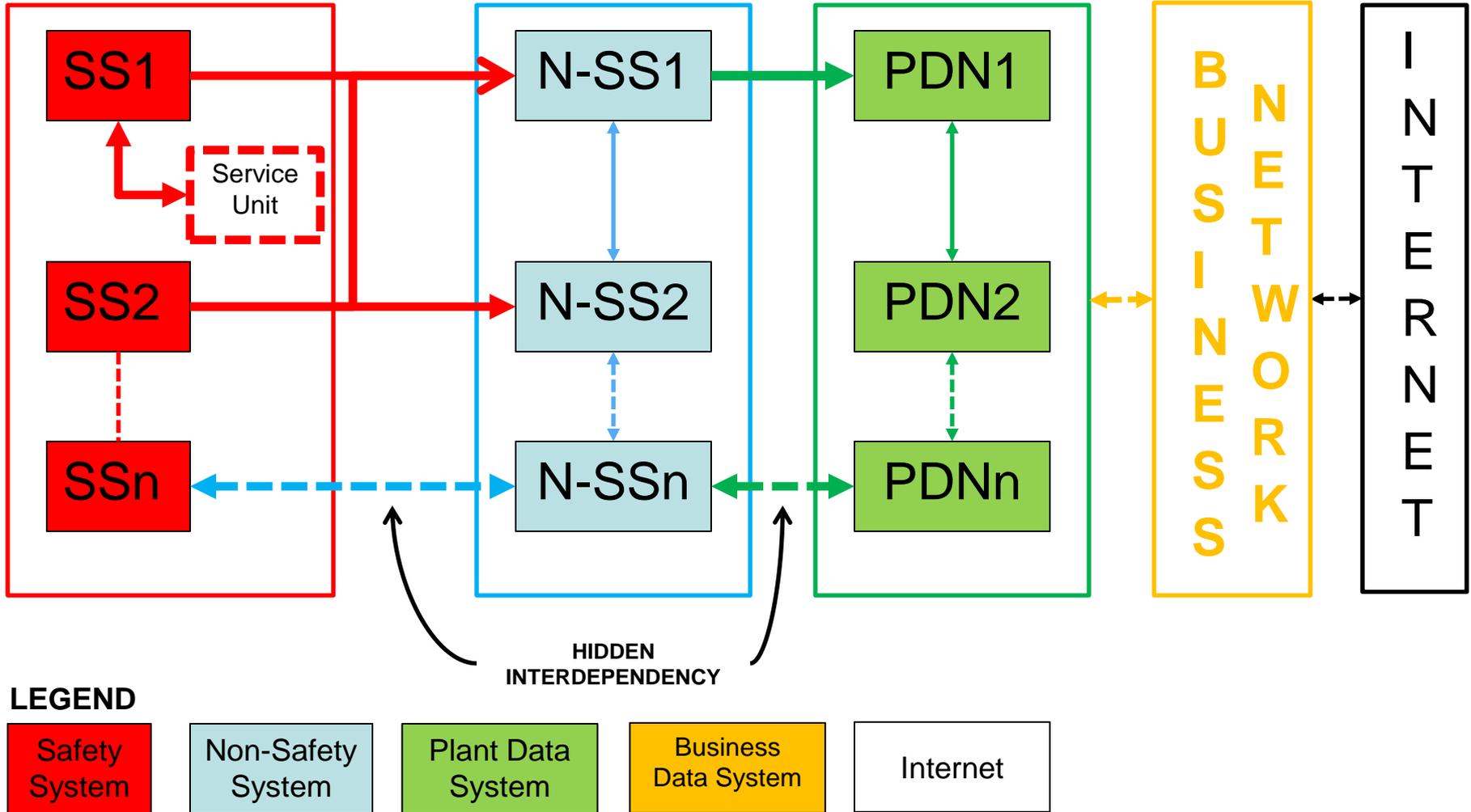
Excludes

- Risk Quantification

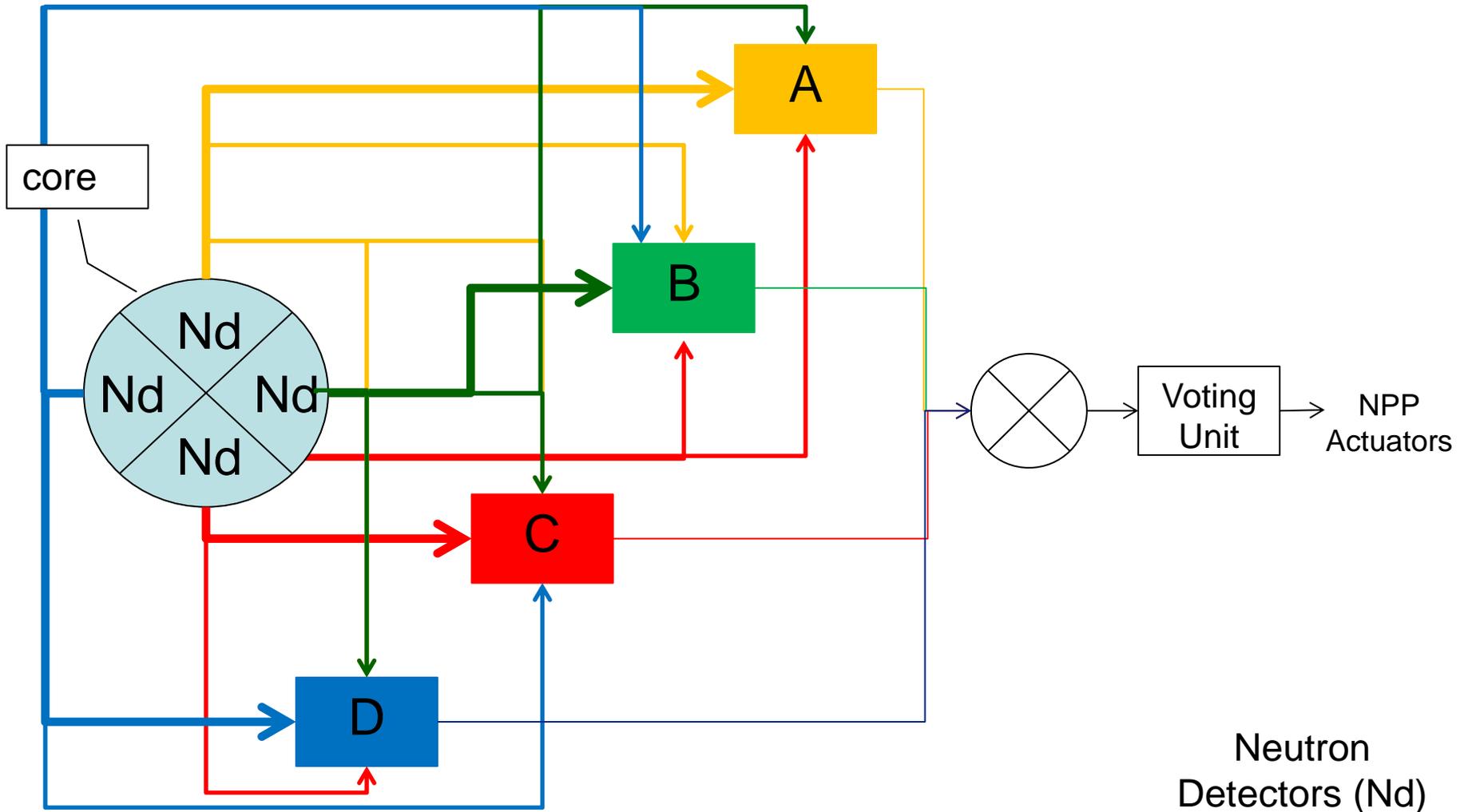
Contributory Hazard Space in Focus



Contributory Hazard Scenario (1/2): S – NS Interconnections

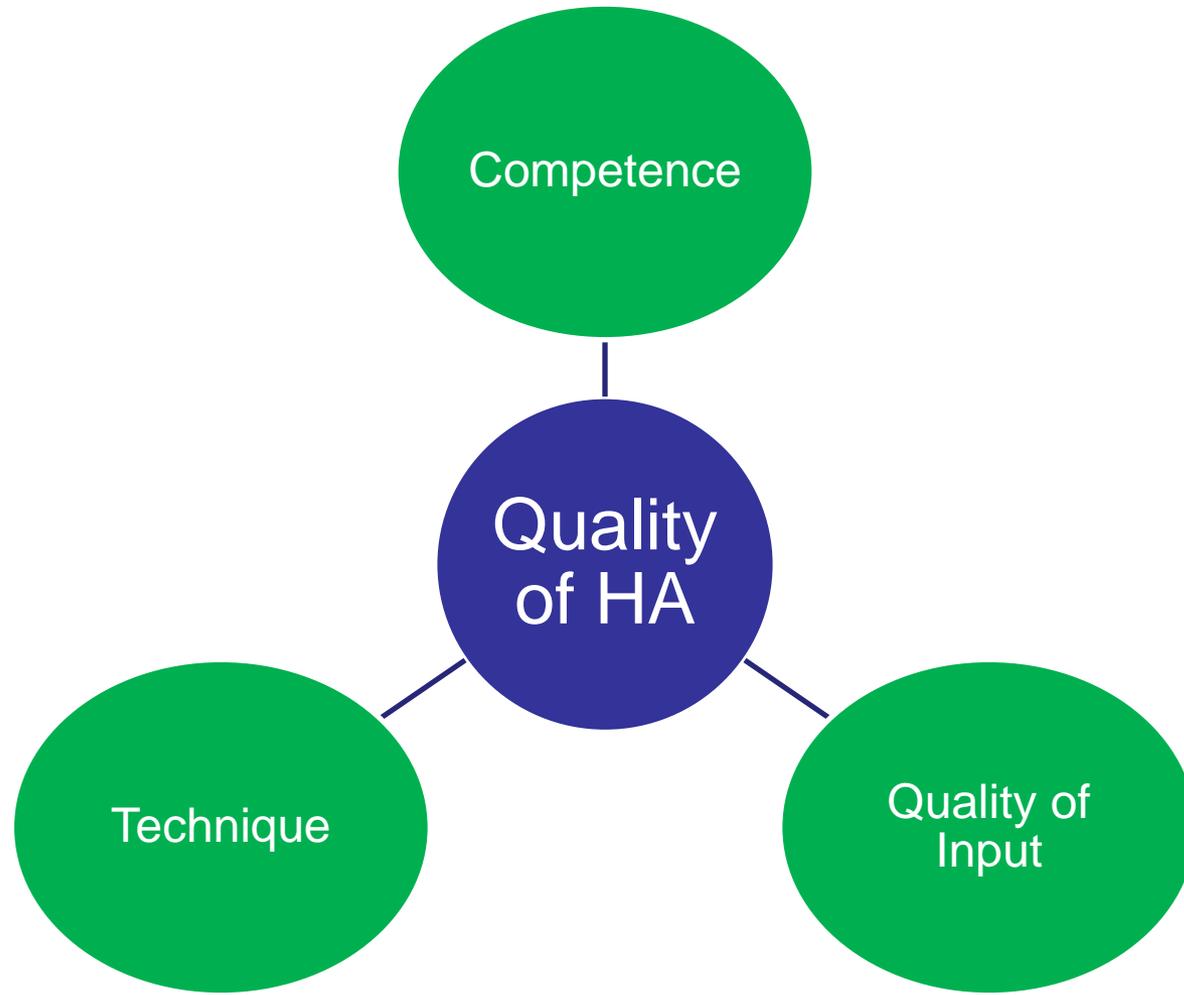


Contributory Hazard Scenario (2/2): Cross-Divisional Interconnections

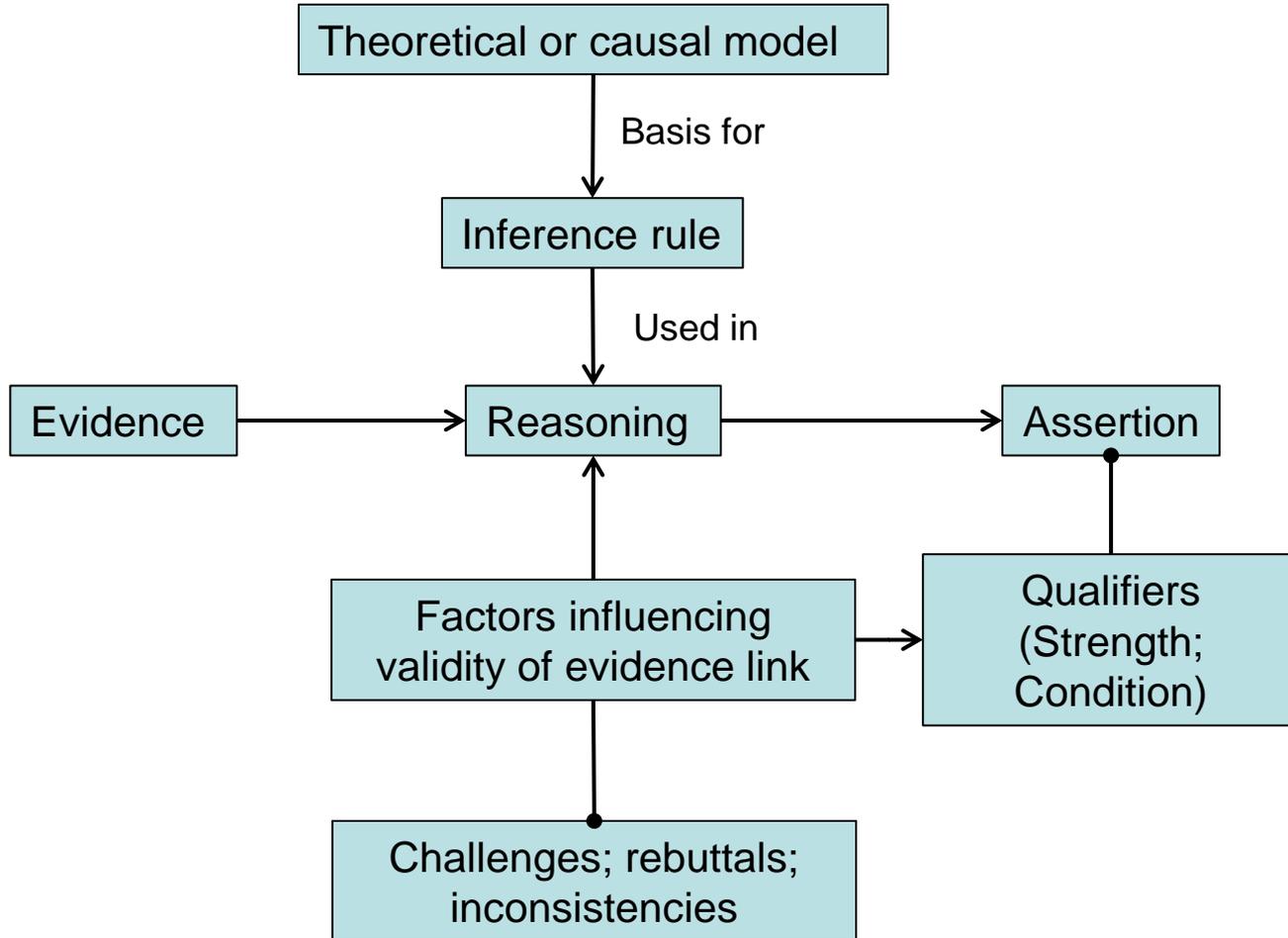


- **Background**
 - Current State & Trends
 - Motivation for RIL-1101
- **Hazard Analysis: What it means**
 - Hazard – definition
 - HA explained in terms of IEEE Std 603
 - HA is part of safety analysis
 - Organizational & analytical framework
 - RIL-1101: Relationship with Plant HA
- **Dependencies**
 - Types of dependencies: Examples
 - Dependency example: System architecture dimension
 - Product-process dependency over lifecycle
 - Dependency on a process activity
- **Research Method**
- **Scope**
 - RIL-1101 scope
 - Contributory hazard space in focus
 - Contributory hazard scenario 1/2
 - Contributory hazard scenario 2/2
- **Evaluation of Hazard Analysis**
 - Factors affecting quality of HA
 - Reasoning Model
- **Envisioned Roadmap**

Factors Affecting Quality of HA



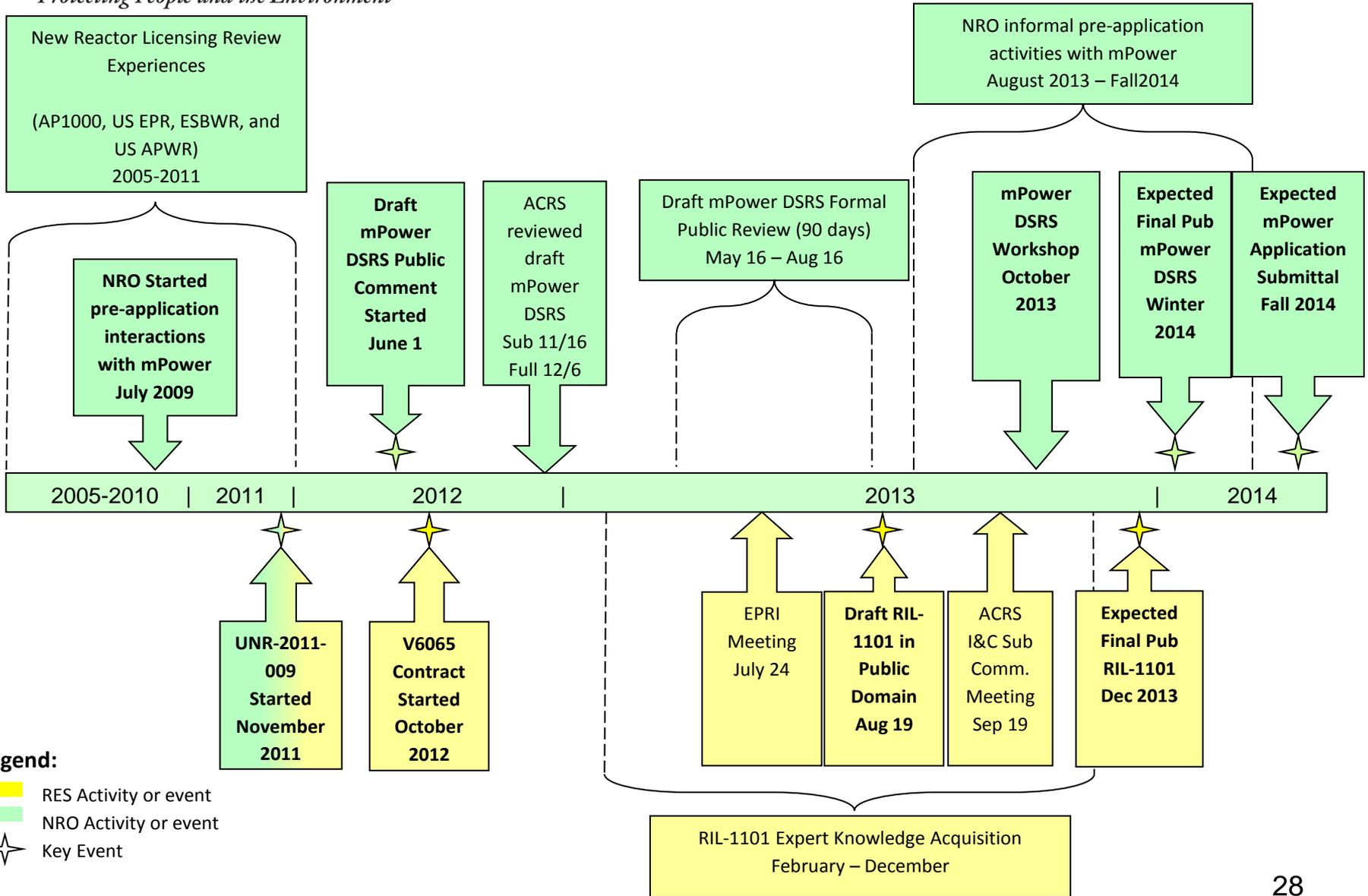
Reasoning Model



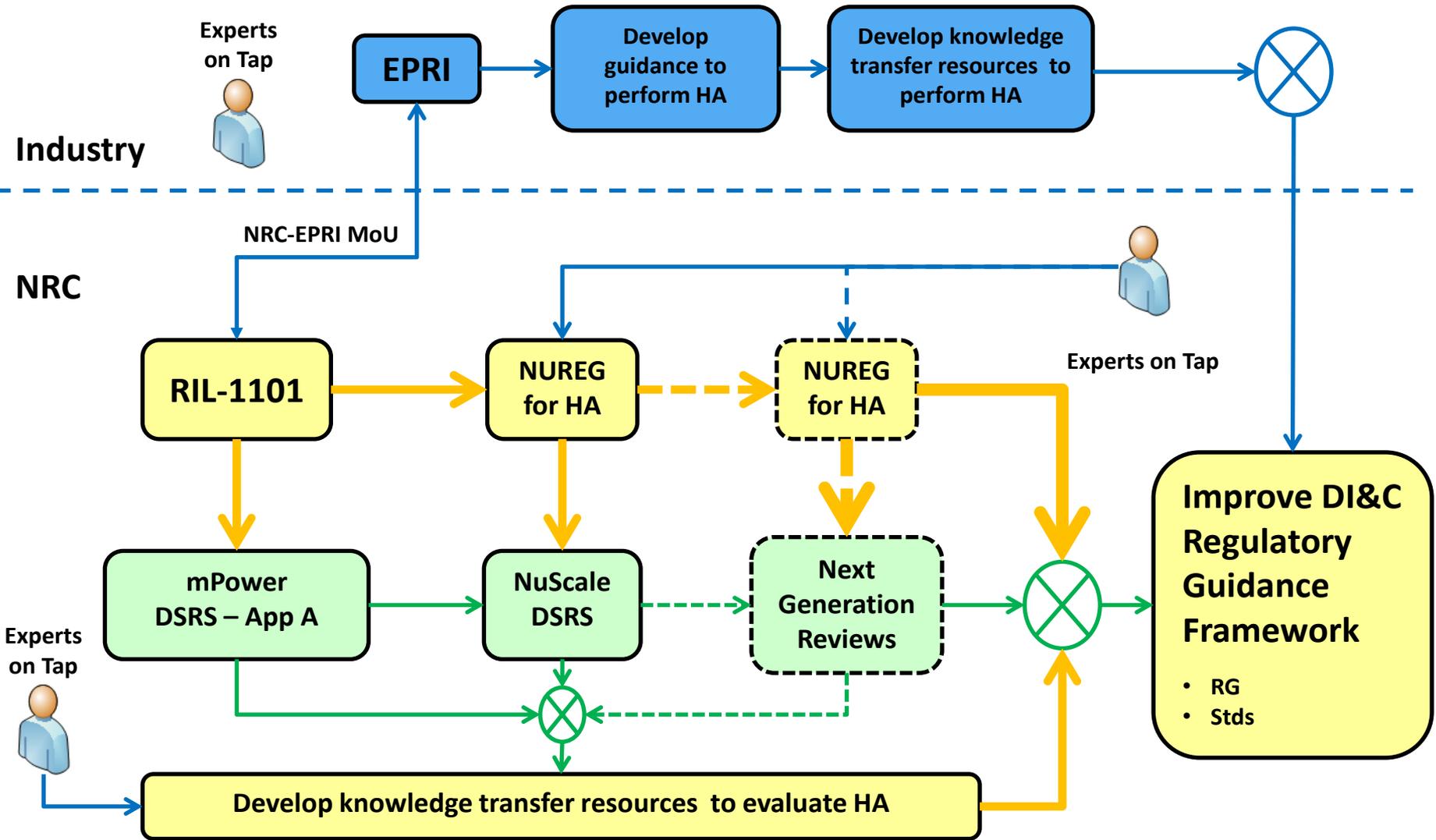
- **Background**
 - Current State & Trends
 - Motivation for RIL-1101
- **Hazard Analysis: What it means**
 - Hazard – definition
 - HA explained in terms of IEEE Std 603
 - HA is part of safety analysis
 - Organizational & analytical framework
 - RIL-1101: Relationship with Plant HA
- **Dependencies**
 - Types of dependencies: Examples
 - Dependency example: System architecture dimension
 - Product-process dependency over lifecycle
 - Dependency on a process activity
- **Research Method**
- **Scope**
 - RIL-1101 scope
 - Contributory hazard space in focus
 - Contributory hazard scenario 1/2
 - Contributory hazard scenario 2/2
- **Evaluation of Hazard Analysis**
 - Factors affecting quality of HA
 - Reasoning Model
- **Envisioned Roadmap**

RIL-1101 Timeline

First of a kind/ Authored in-house



Envisioned DI&C Research Roadmap



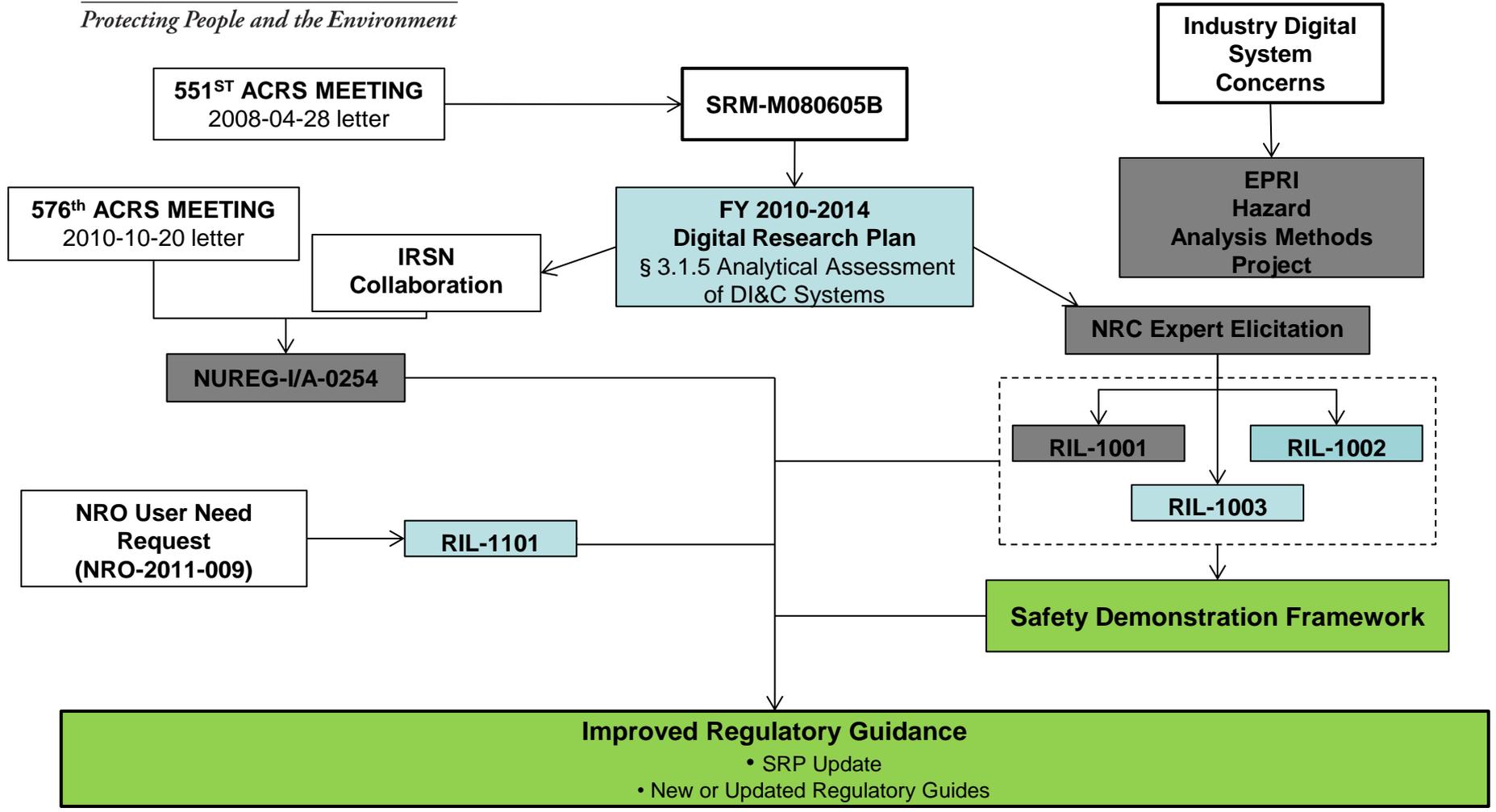
Recap

- **Background**
 - Current State & Trends
 - Motivation for RIL-1101
- **Hazard Analysis: What it means**
 - Hazard – definition
 - HA explained in terms of IEEE Std 603
 - HA is part of safety analysis
 - Organizational & analytical framework
 - RIL-1101: Relationship with Plant HA
- **Dependencies**
 - Types of dependencies: Examples
 - Dependency example: System architecture dimension
 - Product-process dependency over lifecycle
 - Dependency on a process activity
- **Research Method**
- **Scope**
 - RIL-1101 scope
 - Contributory hazard space in focus
 - Contributory hazard scenario 1/2
 - Contributory hazard scenario 2/2
- **Evaluation of Hazard Analysis**
 - Factors affecting quality of HA
 - Reasoning Model
- **Envisioned Roadmap**



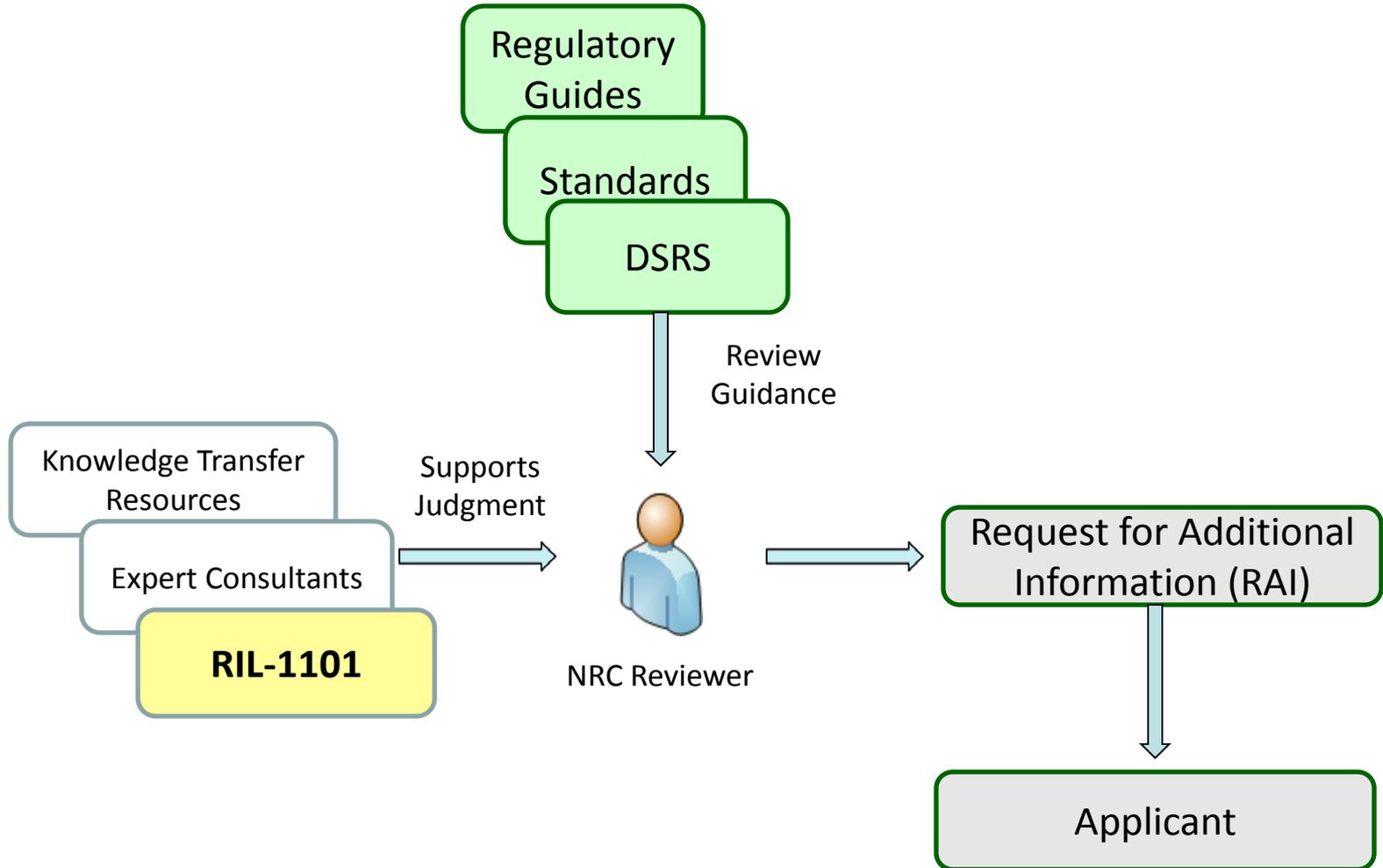
Back-up slides

Related RES/DE Research



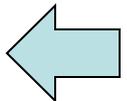
Work Drivers
 Ongoing Work
 Completed Work
 Future Work

Role of RIL-1101 in NRC Review Process



Ways in which things can go wrong

- Not provided; for example:
 - Data sent on a communication bus is not delivered.
- Provided when not needed
- Incorrect state transition
- Incorrect value provided; for example:
 - Invalid data
 - Stale input value is treated inconsistently.
 - Undefined type of data
 - Incorrect message format
 - Incorrect initialization
- Provided at the wrong time or out of sequence
- Provided for too long a duration (e.g., for continuous-control functions).
- Provided for too short a duration; for example:
 - Signal is de-activated too early (e.g., for continuous-control functions).
- Intermittent, when required to be steady; examples:
 - Chatter or flutter
 - Pulse; spike
 - Impairment is erratic
- Interferes with another action; examples:
 - Deprives access to a needed resource; for example:
 - “Babbling idiot”
 - Locking up and not releasing resource
 - Corrupts needed information
- Byzantine behavior



HA Activities and Tasks – Reference Model (1/2)

| HA Task | Input | Output |
|---|---|--|
| T1: Generate Baseline HA Plan | 1. Concept 2. Requirements 3. Premises & Assumptions 4. Plat to validate assumptions 5. Consequences of behavior shortfall 6. Overall V&V Plan 7. Mainstream Development Plan 8. Corresponding information about or from entities in the dependency path | Baseline HA Plan |
| T2: Identify dependencies of HA plan | | Dependencies of Plan |
| T.3 Evaluate other plans, following the dependencies identified above. T3.1. Coordinate information exchanges with HA activities | | Evaluation report. 1. Deficiencies. 2. Changes needed. 3. Request for additional information (RAI). |
| T4. Understand HA-relevant characteristics of the object to be analyzed | Items above + 9. Other requirements allocated to the object. 10 .Non-safety related constraints on the object. 11. Relationship with NPP-wide I&C architecture. 12. Distribution of responsibilities across organizational units/interfaces. 13. Provisions for information exchange across organizational units/interfaces. 14. Lifecycle models; processes; resources; information exchange interfaces. 15. Identification of reused objects and conditions of use. 16. Explicit record of dependencies. 17 Prior HA results, if any | Rejection or Acceptance Revision to HA Plan, as needed 1. Revision to HA plan. 2. Addition to hazard log 3. Change needed; 4. RAI |

HA Activities and Tasks – Reference Model (1/2)

| HA Task | Input | Output |
|--|--|---|
| T5. Analyze object for (contributory) hazards. | Items above + Information specific to object of analysis | 1. Addition to Hazard log 2. Changes Needed 3. Rejection / Acceptance 4. Revision to HA Plan 5. RAI |
| T6. Integrate analyses from lower levels in the integration hierarchy and contribution paths up to the top-level analysis. | Items above + information needed about inter-object dependencies for overall system HA | As in T5. |
| T7. Analyze change proposal (e.g., hazard control proposal). | Change proposal, including information on which it depends (e.g, items listed above). | As in T5. |

Examples of HA Techniques

- Cause Consequence Analysis (CCA)
- Common Cause Failure Analysis (CCFA)
- Design Failure Mode and Effects Analysis (DFMA)
- Dynamic Flowgraph Method (DFM)
- Fault Hazard Analysis (FHA)
- Fault propagation and transformation network/calculus (FPTN/FPTC)
- Fault Tree Analysis (FTA)
- Functional FMEA (FFMEA)
- Functional Hazard Analysis (FuHA)
- Hazard and operability studies (HAZOP)
- Hazard Analysis & Critical Control Points (HACCP)
- Software hazard analysis and resolution (SHARD)
- System-Theoretic Process Approach (STPA)
- What If Analysis (W/I)
- ...

Evaluation of Input in Phase Work Products (1/3)

| Row ID | Work Product of Lifecycle Phase | Common Practice | State of the Practice | State of the Art |
|--------|---|--|--|--|
| 1 | Requirements from next higher level of integration, e.g. from NPP-level safety analysis | Textual narrative. No configuration-controlled vocabulary. “Flat list” organization (i.e., no explicit relationship across requirements is identified). | Restricted natural language with defined vocabulary and structure across elements of a statement. | Use case scenarios |
| | | | SpecTRM-RL | Framework for specification & analysis |
| | | | Requirements engineering support in Naval Research Labs Requirements tables as used for Darlington NPP Models to support mechanized reasoning. | |
| 2 | Plans {Safety plan; V&V plan; HA plan} | Low level of detail; relatively late in the lifecycle. | V&V plan Safety plan | Integrated safety and security plan. |

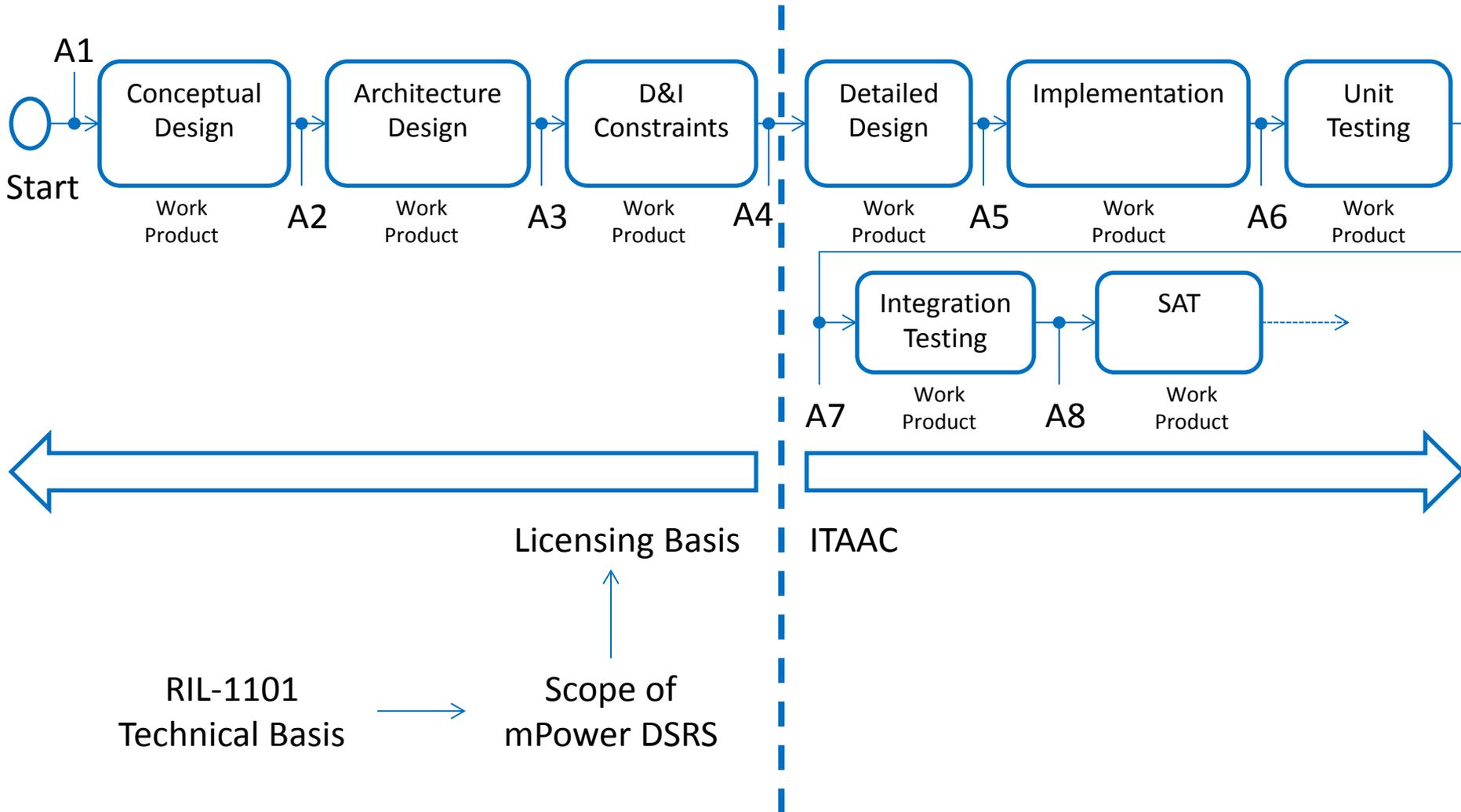
Evaluation of Input in Phase Work Products (2/3)

| Row ID | Work Product of Lifecycle Phase | Common Practice | State of the Practice | State of the Art |
|--------|--|---|--|------------------|
| 3 | Concept | Combination of (a) block diagram without semantics on the symbols and (b) textual narrative | Models to support mechanized reasoning SysML ; AADL Extended EAST-ADL | META |
| 4 | Requirements of digital safety system | See row 1 | See row 1 | See row 1 |
| 5 | Architecture of digital safety system | See row 3 | See row 3 | META |
| 6 | Requirements for software in digital safety system | See row 1 | | See row 1 |
| 7 | Architecture for software in digital safety system | See row 3 | See row 3. MASCOT AADL | META |

Evaluation of Input in Phase Work Products (3/3)

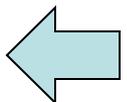
| Row ID | Work Product of Lifecycle Phase | Common Practice | State of the Practice | State of the Art |
|--------|-----------------------------------|---|--|--|
| 8 | Detailed design of software | For application logic: Function block diagram. For platform software: Combination of (a) block diagram without semantics on the symbols and (b) textual narrative. | SPARK | META Refinement from architectural specifications |
| 9 | Implementation of software (code) | For platform software, including communication protocols: C programming language + processor-specific assembler language | Concept of using safe subset of an implementation language: MISRA C Language for programming FPGAs | Auto-generation from detailed design. |

Scope of Licensing Basis



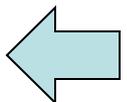
Some Surveyed HA Techniques (1/2)

| HA Technique | Salient Feature |
|--|---|
| Hazard and operability studies | <ul style="list-style-type: none"> • Concept of using teamwork, aided by HAZOP process expert. • Systematizing enquiry through key words. • Systematizing understanding effects through understanding the associated deviations. |
| Fault Tree Analysis | Representation and understanding of fault propagation paths, when the paths are branches of a tree. |
| Design Failure Mode and Effects Analysis | Representation of faulted behavior of a hardware component for understanding its effect, without requiring knowledge of its internals. |
| Functional Failure Mode and Effects Analysis | <ul style="list-style-type: none"> • Understanding effect of unwanted behavior of a function of the system, without requiring knowledge of its internals. • Useful in concept phase. |
| Cause Consequence Analysis | Concept of using causality model to understand fault propagation paths. |
| Hazard Analysis & Critical Control Points | Concept of focusing on critical process variables that affect the outcome. |
| Software hazard analysis and resolution | Adaptation of HAZOP to software, through customization of the key words. |



Some Surveyed HA Techniques (2/2)

| HA Technique | Salient Feature |
|---|---|
| Fault propagation and transformation network/calculus | Representation and analysis of fault propagation, when the faults are transformed during propagation, and when there are feedback paths, supporting mechanized traversal and reasoning. |
| Dynamic Flowgraph Method | Behavior modeling of the system in the finite state machine paradigm facilitates or enables: <ul style="list-style-type: none"> • Mathematical underpinning. • Analysis of its interactions with environment. • Analysis of dynamic behavior across its elements. • Mechanized traversal. • Mechanized reasoning, esp. if directed cyclic graph. |
| System-Theoretic Process Approach | <ul style="list-style-type: none"> • Applicable at concept phase (without a finished design). • Applicable to understanding of organization-culture systems. |



Acronyms

- **ACRS** Advisory Committee for Reactors and Safeguards
- **CFR** Code of Federal Regulations
- **DI&C** Digital Instrumentation and Control
- **DSRS** Design Specific Review Standard
- **ESFAS** Engineered Safety Features Actuation System
- **EPRI** Electrical Power Research Institute
- **HA** Hazard Analysis
- **I&C** Instrumentation and Control
- **I/O** Input/Output
- **INPO** Institute of Nuclear Power Operations
- **ITAAC** Inspections, Tests, Analyses, and Acceptance Criteria
- **NPP** Nuclear Power Plant
- **NRC** Nuclear Regulatory Commission
- **NRO** NRC Office of New Reactors
- **PWR** Pressurized Water Reactor
- **R&D** Research and Development
- **RAI** Request for Additional Information
- **RES** NRC Office of Nuclear Regulatory Research
- **RG:** Regulatory Guides
- **RIL** Research Information Letter
- **RPS** Reactor Protection System
- **SAR** Safety Analysis Report
- **SMR** Small Modular Reactor
- **SRP** Standard Review Plan
- **V&V** Verification and Validation



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Learning From Digital Operating Experience

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee
September 19, 2013

Tom Burton, Doug Eskins, and Derek Halverson
Office of Nuclear Regulatory Research
Division of Engineering
Instrumentation, Controls & Electrical Engineering Branch

The DI&C OpE* Team

- Mr. Thomas Burton
- Dr. Doug Eskins
- Dr. Derek Halverson
- Mr. Luis Betancourt
- Mr. Mauricio Gutierrez
- Mr. Matt Dennis
- Former members
 - Mr. Karl Sturzebecher - to NRR
 - Mr. Louis Dumont – Rotation from RII



Church Street Office Building

Purpose



- Describe DI&C OpE team research approach
- Solicit comment and feedback from Advisory Committee on Reactor Safeguards (ACRS)

Nuclear Regulatory Commission

Digital System Research Plan 2010 - 2014,

Section 3.4.5 Operating Experience Analysis

- Improve the use of DI&C OpE (e.g., regulatory processes)
- Improve DI&C OpE (e.g., event reporting framework)

- **DI&C OpE Research Approach**
 - Sources for DI&C OpE data
 - Uses for DI&C OpE information
 - Exploratory analysis approach

- **Example Event**
 - Illustrate DI&C OpE approach

- **Next Steps**

DI&C OpE Analysis Research Approach

Research Question:

Are there ***digital unique****
aspects in OpE?



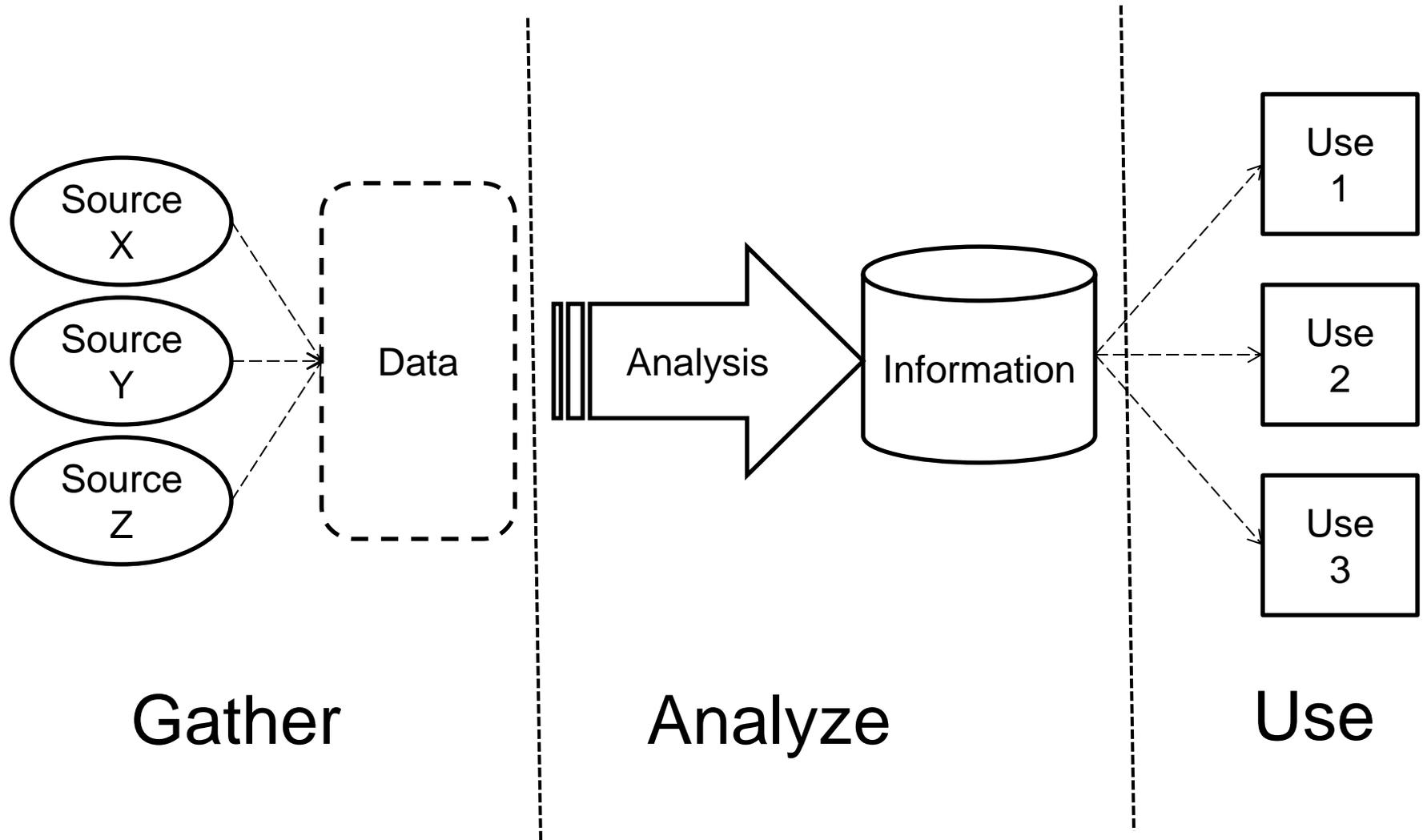
NRC Commissioner
Ostendorff and
inspectors at Oconee

Research Goals:

1. Identify/categorize **important aspects** of DI&C OpE
2. Determine which (if any) of the identified aspects are **digitally unique**
3. Develop a method for identifying, tracking, and using DI&C OpE to **improve regulatory processes**
4. Develop recommendations to **improve DI&C OpE**

* Not captured adequately by existing OpE methods ([list](#))

DI&C OpE Analysis Research Approach



Gather: DI&C OpE Data Sources

- LERs* (reviewed/sorted ~ 7,000 of 20,000)
 - Analog I&C** ~ 1200 (17%)
 - Digital I&C ~ 600 (9%)
 - Non I&C ~ 5200 (74%)
 - Screened/stored in the DI&C OpE database
- Other sources
 - INPO*** Consolidated Event System (ICES) database
 - NRC inspection reports
 - NRC traditional operating experience program
 - NRC safety evaluation reports
 - Vendor notifications

Use: Digital OpE Information

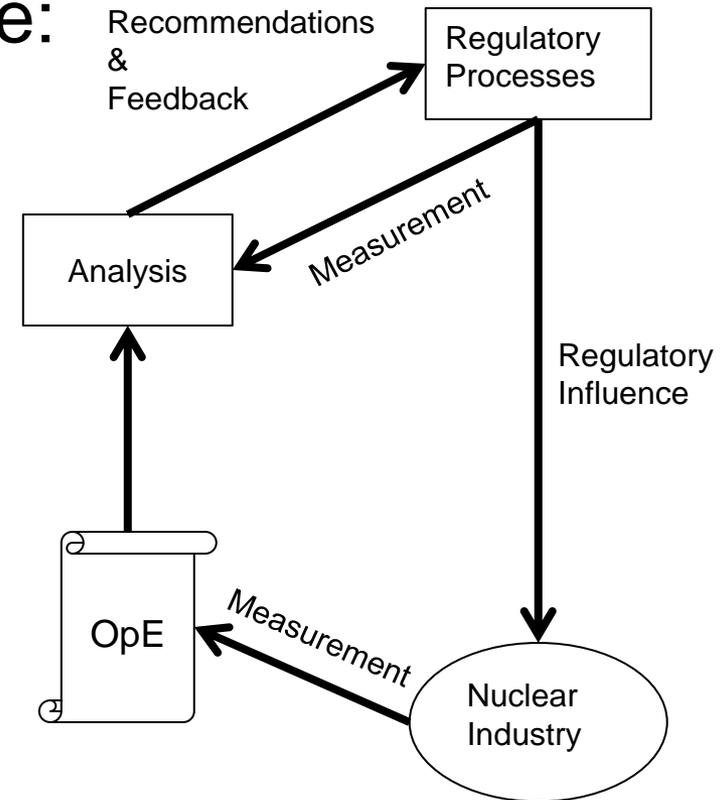
Support research goals to improve:

Regulatory Processes:

- OpE reviews & analysis
- License reviews
- Regulatory guidance
- Lessons learned
- Knowledge transfer/ management
- Inspections

DI&C Operating Experience:

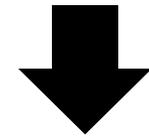
- Enhanced reporting framework (are new/different data sources needed?)
- Data compilation methods (e.g., are there better ways to use the data we already have?)



Analyze: Exploratory Event Analysis Process*

1. Explore ways to sort DI&C OpE data

- Develop useful DI&C OpE keyword sets (e.g., digital unique aspects, hazards, regulatory docs)
- Tag DI&C OpE (metadata) in DI&C OpE database using keyword sets
- Identify useful relationships and structure among the data (basis to generalize, learn, & apply)



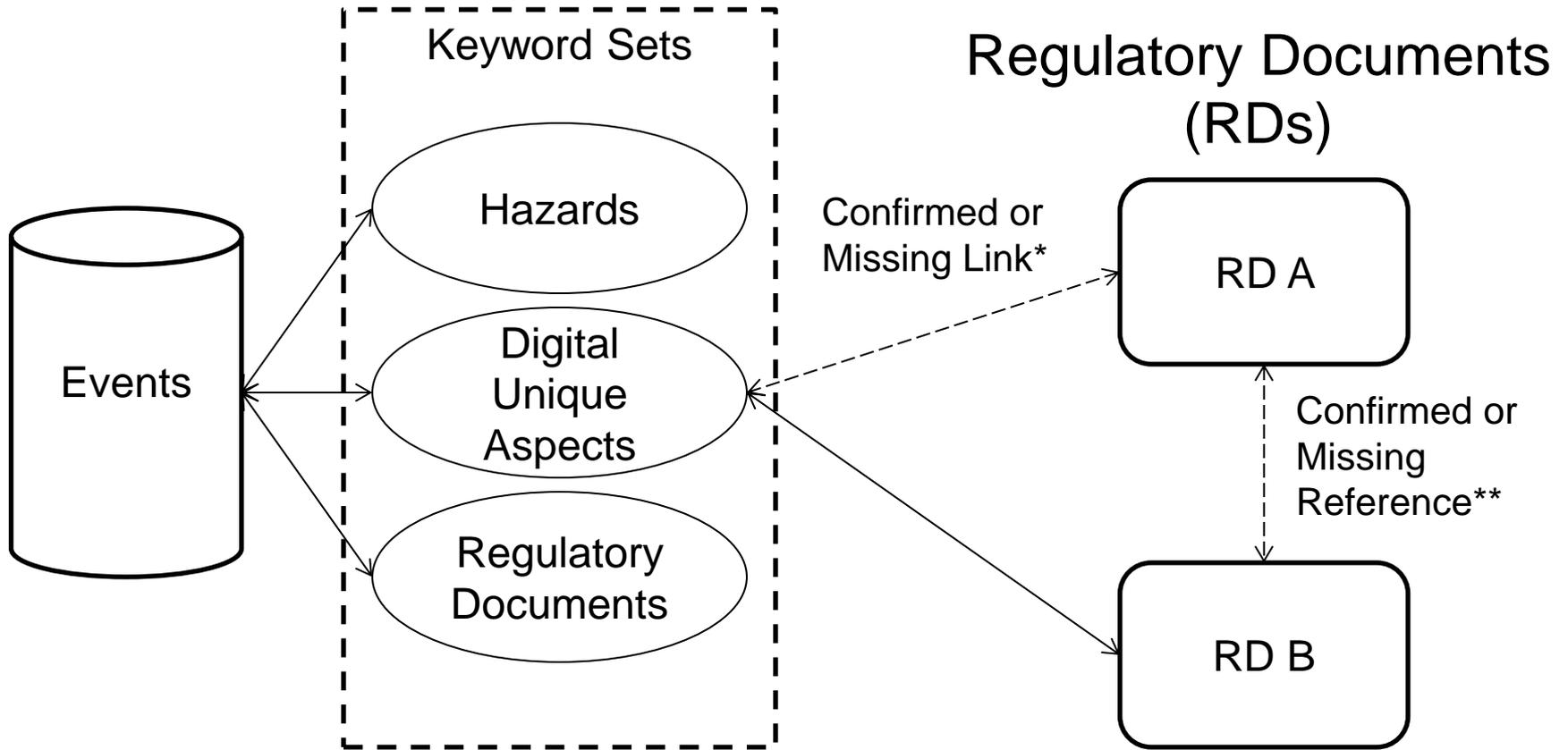
2. Develop techniques to mark useful relationships between DI&C OpE and regulatory documents & processes



3. Develop methods for regulatory confirmation & gap analysis using 1 & 2

* **1st Stage:** learn how to learn

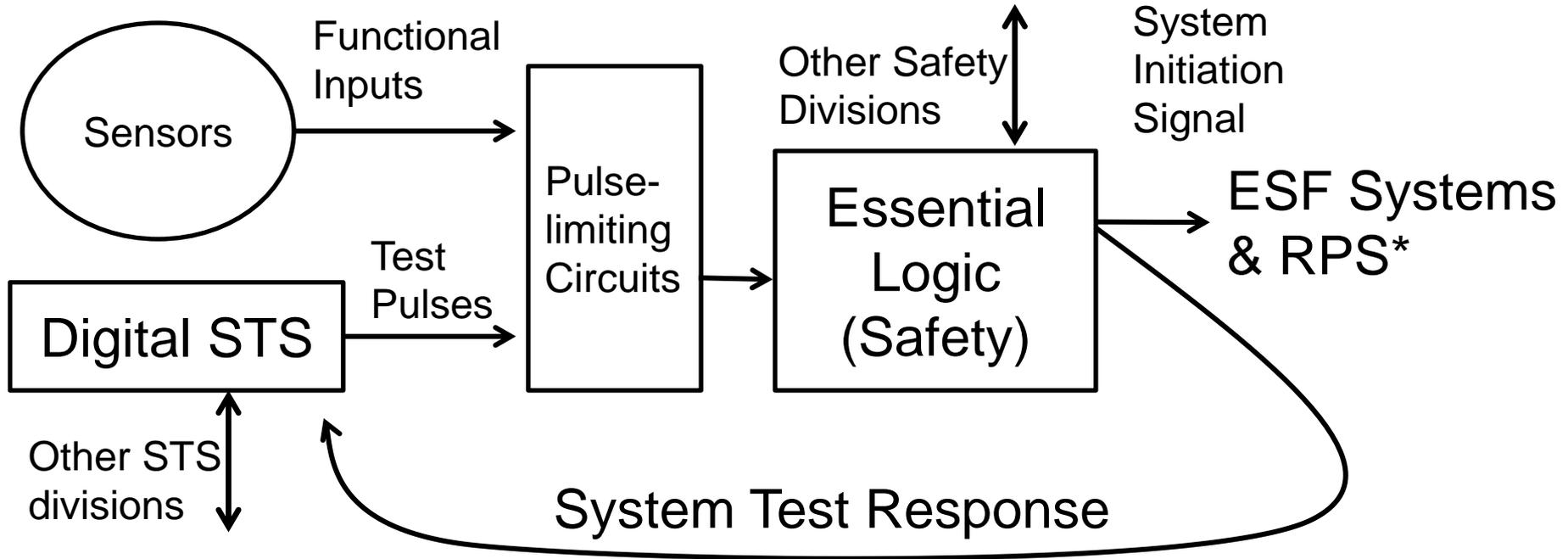
Regulatory Confirmation & Gap Analysis



*Missing Link: keyword without corresponding link to RDs, i.e., potential gap

**Missing Reference: keyword linked parts of RDs do not reference each other

Self-Test Event 2010



Event: **Multiple spurious actuations** of containment isolation and other safety-related valves over three days

Cause: Design defects allowed the Self-Test System (STS), a **digital, non-safety, on-line** self-test system, to cause actuations in the Nuclear Safety Protection System

*Engineered Safety Feature (ESF) & Reactor Protection System (RPS).

Observations:

- **Repeat Event:** Similar event first occurred in division 2. Corrective action only replaced components. Then, several months later, this event occurred in division 1.
- Spurious operation of a safety system

“Practical” Digital Differences:

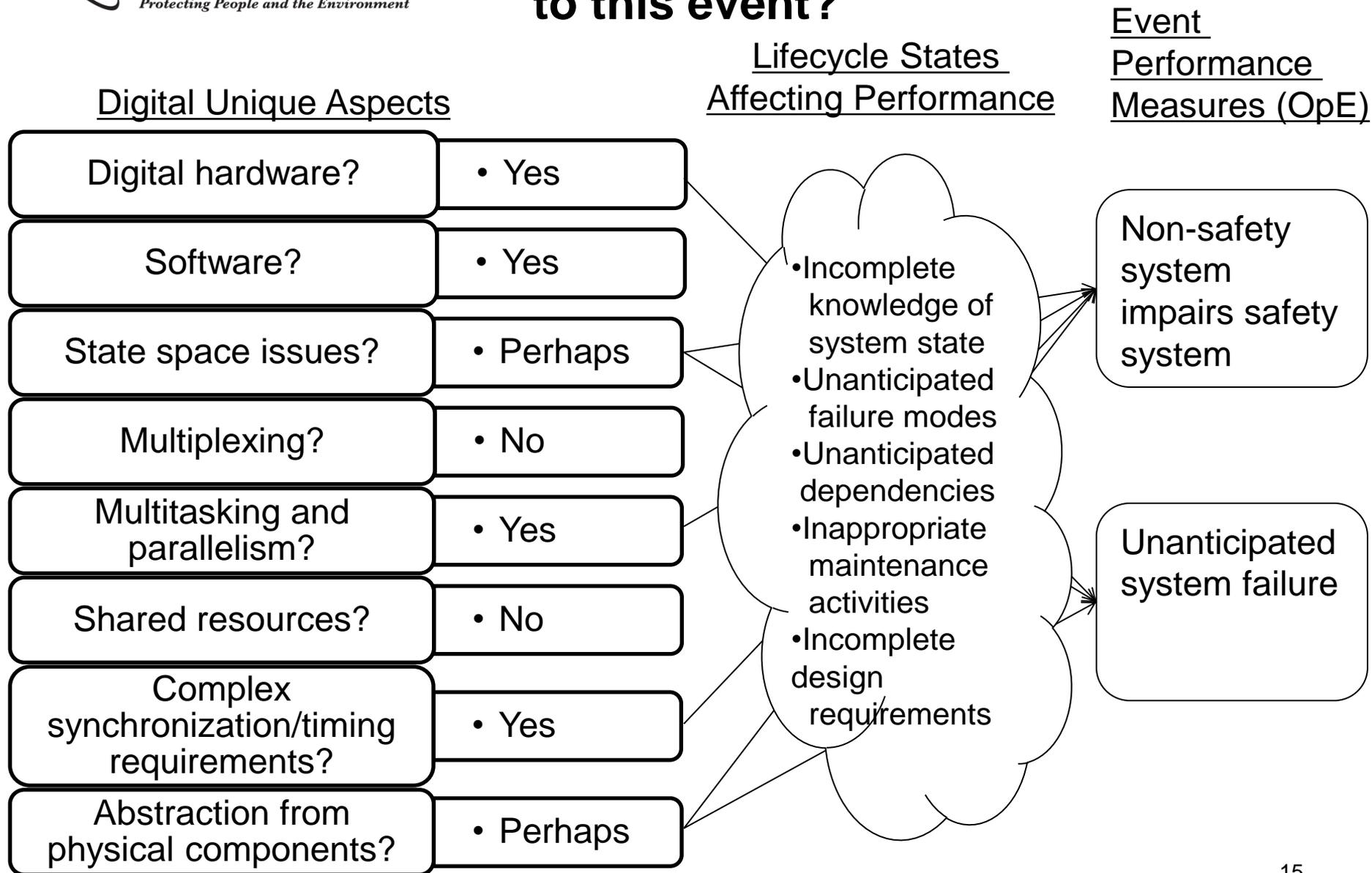
- Complex digital system state space needed to implement these self-test functions
- Testing performed via complex Master/Slave co-ordination of four divisions
- This type of **system level** malfunction may not be practically achievable in older analog systems

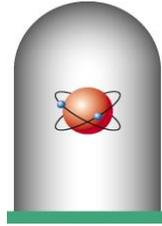
Selected Related Regulatory Documents

| Regulatory Reference Document | Why is the document applicable to the event? | Document (sub)section(s) applicable to event | Comments (e.g., potential use, gap, confirmation) |
|--------------------------------------|---|---|--|
| SRP ¹ Appendix 7.1-D | Safety/non-safety communications | 5.6 | May identify possible need for research support |
| 10 CFR ² 50 Appendix B | Quality requirements, referenced in inspection report | Criterion III Design Control: translate plans/high level requirements into the design. | Reinforces importance of this regulation. May be useful for inspectors and reviewers. |
| RG ³ 1.75 | Independence of electrical safety systems | | Reinforces importance of modern guidance on independence in these sorts of situations. |

¹ Standard Review Plan, ² Code of Federal Regulations, ³Regulatory Guide

Are there Digital Unique Aspects to this event?





Next Steps

- Continue to research event analysis methods
 - Develop draft analysis method
- Continue data gathering/ classification
 - LER screening
- Consider how to integrate
 - Events data
 - Inventory data
 - Regulatory document relationship database

Acronyms

- **ACRS – Advisory Committee on Reactor Safeguards**
- **CFR – Code of Federal Regulations**
- **DI&C – Digital Instrumentation and Control**
- **ESF – Engineered Safety Feature**
- **I&C – Instrumentation and Control**
- **INPO – Institute of Nuclear Power Operations**
- **ICES - INPO Consolidated Event System**
- **LER – Licensee Event Report**
- **NRC – U.S. Nuclear Regulatory Commission**
- **OpE – Operating Experience**
- **RG – Regulatory Guide**
- **RD – Regulatory Document**
- **RIL – Research Information Letter**
- **RPS – Reactor Protection System**
- **SRP – Standard Review Plan**
- **STS – Self-Test System**



Backup Slides

Digital Unique Aspects

Event may involve digital unique aspects* such as:

- Digital hardware
- Software
- State space issues (e.g., system memory, parameters, I/O)
 - Complex/large
 - Time & state dependent
 - Discrete-time, discrete-state
- Multiplexing
- Multitasking and parallelism
- Shared resources, e.g., communication links, clock signals
- Complex synchronization/timing requirements (e.g., internal and networked components)
- Abstraction (more) from physical components

*observable properties at any point in the lifecycle, e.g., requirements, design, implementation

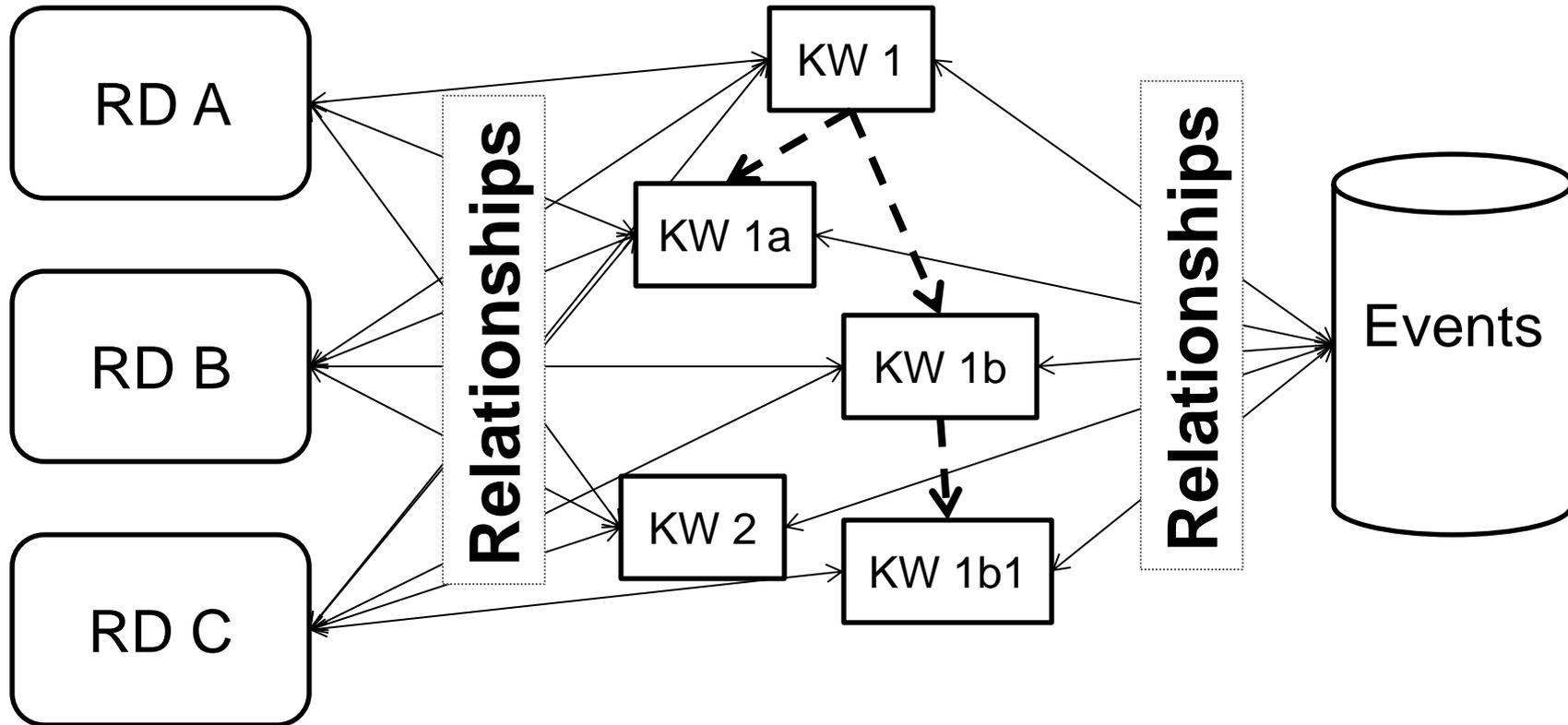
Select Related Hazards from RIL-1101

- H-SR-3: Incomplete requirements
- H-S-1: system is not sufficiently verifiable and understandable.
- H-S-1.1.1: unanalyzed or un-analyzable conditions
- HS-11: Effects of invalid inputs.
- H-S-17: Interference from unintended (including unwanted) functions or side effects.
- H-0-8: The analysis is not propagated to elements on which the system being analyzed depends or the safety functions allocated to it depend

Hierarchical Keywords & Relationship Graphs *

Regulatory Documents (RDs)

Keywords



* A data visualization and analysis tool