

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

Title: ACRS US EPR Subcommittee

Docket Number: n/a

Location: Rockville, Maryland

Date: November 15, 2011

Work Order No.: NRC-1280

Pages 1-362

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

1 UNITED STATES OF AMERICA

2 NUCLEAR REGULATORY COMMISSION

3 + + + + +

4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

5 + + + + +

6 US EPR SUBCOMMITTEE

7 + + + + +

8 TUESDAY

9 NOVEMBER 15, 2011

10 + + + + +

11 ROCKVILLE, MARYLAND

12 + + + + +

13 The Subcommittee met at the Nuclear
14 Regulatory Commission, Two White Flint North, Room
15 T2B1, 11545 Rockville Pike, at 8:30 a.m., Dana A.
16 Powers, Chairman, presiding.

17 SUBCOMMITTEE MEMBERS PRESENT:

18 ***DANA A. POWERS, Chairman***

19 ***SANJOY BANERJEE***

20 CHARLES H. BROWN, JR.

21 GORDON R. SKILLMAN

22 JOHN W. STETKAR

23 NRC STAFF PRESENT:

24 DEREK WIDMAYER, Designated Federal

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Official
2 GETACHEW TESFAYE
3 TERRY JACKSON
4 MICHAEL CANOVA
5 JACK ZHAO
6 TUNG TRUONG
7 DEANNA ZHANG
8 KENNETH MOTT
9 DIERDRE SPAULDING-YEOMAN
10 WENDELL MORTON
11 SURINDER ARORA
12 ALSO PRESENT:
13 DARRELL GARDNER
14 JEREMY SHOOK
15 CHRIS DOYEL
16 DUC PHAN
17 SANDRA SLOAN
18 TIM STACK
19 VIC FREGONESE
20 MARK ROYAL
21 MARK FINLEY
22 CYRIL RODEN
23
24

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

4 (8:30 a.m.)

5 CHAIR POWERS: Let's come back in order.

6 This is the second day of the meeting of the
7 Advisory

8 Committee on Reactor Safeguards US EPR Subcommittee.

9 I'm Dana Powers, Chairman of the Subcommittee.

10 ACRS members in attendance are John
11 Stetkar, Dick Skillman, Charles Brown. Derek
12 Widmayer is still the Designated Federal Official
13 for the meeting.

14 All the constraints that I talked about
15 yesterday still apply. Everybody speak with
16 sufficient clarity and volume. And if you are on
17 the phone line, mute the phone line when you are not
18 talking.

19 After yesterday's intense discussions on
20 Auxiliary Systems, we are going to move to a less
21 controversial area. So we should have a much
22 quieter day today dealing with digital I&C.

23 Do members have any opening comments
24 they would like to make? You 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 MEMBER BROWN: Do you really want me to
2 make an opening --

3 CHAIR POWERS: No.

4 MEMBER BROWN: Okay.

5 CHAIR POWERS: Okay.

6 MEMBER BROWN: Why did you ask?

7 CHAIR POWERS: This is just being
8 polite. I have to get along with you guys.

9 MEMBER BROWN: You're being polite?

10 CHAIR POWERS: Yes.

11 MEMBER BROWN: Let me get that on the
12 record.

13 (Laughter.)

14 CHAIR POWERS: In that case I will turn
15 to Getachew Tesfaye to begin our discussions.

16 MR. TESFAYE: Good morning. I guess my
17 remarks from yesterday, they apply for today also.
18 So I don't have anything more to add.

19 CHAIR POWERS: Nothing more to add?

20 MR. TESFAYE: Nothing more to add.

21 CHAIR POWERS: Yes, I know it because
22 digital I&C is such a noncontroversial issue.

23 MR. WIDMAYER: You don't want to go over
24 those reactors that we have completed again?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. TESFAYE: No.

2 MR. WIDMAYER: Oh, okay.

3 CHAIR POWERS: We need to get his list
4 to make sure we agree. I think he can sneak a
5 couple in there, honestly, so look out.

6 MEMBER BROWN: I have one administrative
7 issue. I have got a pencil without lead. That is
8 absolutely unsatisfactory. Thank you very much.

9 CHAIR POWERS: You are definitely
10 getting us off on a good foot here, Brown.

11 In that case, I will turn to Darrell
12 Gardner of AREVA and let you begin the discussion.

13 MR. GARDNER: Well I think I would just
14 like to reiterate how excited we are to be here
15 again today.

16 CHAIR POWERS: Darrell, you have got to
17 quit lying to us.

18 (Laughter.)

19 CHAIR POWERS: You're just being polite.
20 Right?

21 MR. GARDNER: Yes, that's it.

22 Just a quick opening comment. That is,
23 that today's presentation on Chapter 7 is going to
24 provide an overview of that Chapter of the US EPR

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 FSAR. This session is open. However, I would point
2 out that our design is based a series of technical
3 and topical reports, portions of which are
4 proprietary. So if we get into areas where members'
5 questions would result in a discussion of
6 proprietary material, we would ask that that portion
7 may be closed or deferred until a point where we
8 could close the session.

9 With that said, I would say with I&C, as
10 with many of our systems there are plenty of
11 acronyms at the back of the presentation. There is
12 an acronym list in case you need a decoder ring.

13 And with that, I will turn it over to
14 Jeremy Shook, who is going to be our lead presenter
15 today.

16 MR. SHOOK: Good morning. My name is
17 Jeremy Shook. I am the I&C Engineering Discipline
18 Lead for AREVA for the US EPR Design Certification
19 project.

20 Just a quick background on my
21 professional experience. I started off after a
22 bachelor's degree at Villanova University, I went
23 into the Navy for six years as a submarine officer.

24 I served onboard the USS Tucson for two and a half

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 years in roles of rad controls assistant, electrical
2 division officer, main propulsion assistant,
3 communications officer, and I got qualified as an
4 engineering officer by a naval reactor, which is Mr.
5 Brown's former organization, which that is always a
6 fun experience to go to naval reactors for two days.

7 I then spent two years at the prototype
8 in Upstate New York as a shift engineer and
9 production training officer responsible for
10 operations and training of over 400 students going
11 through the prototype program.

12 After leaving the Navy in 2001, I went
13 to graduate school at Rensselaer Polytechnic
14 Institute. I received a master's of science in
15 mechanical engineering with a focus on control
16 systems. Also during that time I received a
17 professional engineer license from the State of New
18 York in the mechanical area.

19 Coming out of graduate school, I went to
20 work for General Electric in Schenectady. I worked
21 for two and a half years in design of combustion
22 turbines, steam turbine, wind turbine designs,
23 mostly advance controls in areas of model predicted
24 control and model base control, at which point my

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 wife told me she was tired of living in Upstate New
2 York.

3 (Laughter.)

4 MR. SHOOK: So I managed to find a job -
5 - Yes?

6 MEMBER STETKAR: I grew up just south of
7 Albany. Be careful.

8 (Laughter.)

9 MR. SHOOK: I enjoyed it up there.

10 CHAIR POWERS: Who says he grew up?

11 MEMBER STETKAR: I'm sorry, I was young.

12 CHAIR POWERS: Yes, more accurate.

13 MEMBER STETKAR: I'm sorry. Go ahead.

14 MR. SHOOK: And so we came to AREVA in
15 2005, we moved to Charlotte. And I have been
16 working on the US EPR project in various stages of
17 licensing and detail design for the Calvert Cliffs 3
18 project ever since.

19 And let's see. I think that's about a
20 pretty decent summary. I have a couple of patents
21 and three of four publications that have published
22 papers.

23 CHAIR POWERS: Good.

24 MR. SHOOK: So with that, I will go

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 ahead and get started on the presentation.

2 So the way we sort of arranged this is
3 we are just going to step through the various
4 sections of Chapter 7 and we will be starting with
5 the introduction, going through the reactor trip
6 system, engineered safety features, safe shutdown
7 systems, information systems important to safety,
8 interlock systems important to safety, control
9 systems not required for safety and diverse I&C
10 systems.

11 One note. There is section 7.9 which
12 you will see later as part of the staff's review.
13 We didn't put any information specifically in there.

14 We included the data communications descriptions as
15 part of 7.1 with a description of all the other
16 systems. So you will see that.

17 Just to kind of have an understanding of
18 the way that we kind of laid this out, in the
19 introduction we are just going to kind of give you a
20 brief overview of the systems that are included
21 within the scope of Chapter 7. And then as we go
22 through the different sections, we will talk about
23 more the functions. For example, in 7.2, we will
24 talk about reactor trip functions and then how they

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 implemented within the various systems that make
2 up the design.

3 So you won't see a "dedicated reactor
4 trip system." This is just following the format of
5 the SRP. But we are going to talk about how those
6 functions are then implemented within the various
7 systems of the design.

8 CHAIR POWERS: This, Stetkar, is a
9 diagram that I can understand.

10 MEMBER STETKAR: They are finished.
11 That's it.

12 MEMBER BROWN: It seemed like a pretty
13 thin slide package. We should be finished by noon
14 if the slide package is any estimation of what we
15 are going through.

16 You have asked me not to make comments
17 so I just thought I would step in now.

18 CHAIR POWERS: And we are happy that you
19 did. Please continue.

20 MR. SHOOK: So this is, albeit a very
21 simplified drawing but one to sort of frame the rest
22 of the discussion we will be having today.

23 You know when you look at I&C and you
24 are kind of looking at the totality of I&C, as far

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 as the plant is concerned, you know, you are really
2 looking at basically four different elements. You
3 know, the first element you start off with is the
4 instrumentation. That is the means with which we
5 measure the process parameters that we are trying to
6 control and monitor in the plant.

7 For the most part, most of the
8 instruments come in the plant directly into what we
9 call the Distributed Control System or DCS. And
10 those variables are then processed and are sent to
11 the operator either for display or used in the
12 automated control loop with which the commands are
13 then sent to the actuators.

14 Also from the operator, work stations.
15 The operator can manually control the plant as
16 defined by the system design. The operating
17 procedures can affect manual commands through the
18 DCS down to the final actuated elements.

19 So again, I would say most, a good
20 majority of the controls in the plant are
21 implemented in this manner. There are certainly
22 dedicated black box systems that don't interact
23 directly with the operator through this path or
24 potentially manual actions just with not going

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 through any control system at all. But I would say
2 the vast majority of the controls in the plant are
3 implemented through this type of design. Next
4 slide.

5 And so basically we are going to do here
6 in this section is just basically lay out the
7 systems that are involved in those different pieces.

8 Starting with the instrumentation, you now
9 basically most of the instrumentation in the plant
10 is part of, from a formal system boundary
11 perspective, part of the various process systems.
12 For example, Reactor Coolant System, Main Steam,
13 Feedwater, all contain instruments that are a part
14 of those systems.

15 We do have also some dedicated
16 instrumentation systems which are listed in Chapter
17 section 7.1 which are listed here as well. For
18 instance, Incore and Excore Instrumentation Systems
19 are stand-alone instrumentation systems that monitor
20 various parameters. In these cases, neutron flux
21 parameters within the core and external to the core,
22 in the case of Excore.

23 And so these systems will typically
24 include sensors and some signal conditioning

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 equipment, and then providing a signal to the DCS
2 for further processing, either whether it is just
3 for monitoring, for the operator, or used in closed-
4 loop functions.

5 So coming to slide six, now we are
6 getting to that second piece of that overall
7 drawing, which is what we call the Distributed
8 Control System or DCS. This is what we call a
9 functional architecture so a functional block
10 diagram. I'm not going to go through and detail at
11 this point all the interfaces. I just didn't want
12 to redraw this picture. I just wanted to use the
13 same one out of the FSAR.

14 I will speak generally to the systems
15 now and then as we walk through the various
16 sections, 2, 3, 7, 8, we will be showing you how
17 those various functions are implemented within this
18 design and speak in more detail to how those
19 functions interconnect.

20 The architecture in general is organized
21 in basically three levels. We have the top level,
22 which is the operator interface. And there we have
23 two main systems. The first is on the right, which
24 is the Process Information and Control System or the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 PICS is designed to be the primary operator
2 interface, which with the operator will be used
3 during all playing conditions, as long as it is
4 available.

5 The PICS is basically a modern DCS type
6 of operator interface. It is a collection of
7 operator workstations using flat screen monitors.
8 Operator inputs is by use of a mouse. And various
9 graphic type of displays allow information to be
10 displayed to the operator, as well as features such
11 as alarm display and filtering. For example, we can
12 prioritize the alarms and filter them based on that
13 priority. So it helps the operator during
14 significant events, whether we are trying to
15 diagnose what is going on with the plant.

16 MEMBER STETKAR: Jeremy, are you going
17 to talk later, I was kind of thumbing through your
18 slides here and see whether you were, about
19 interactions between PICS and SICS? I had some
20 questions and I don't know exactly where in the flow
21 of things it is best to ask those questions.

22 MR. SHOOK: In terms of interactions, I
23 don't think we discussed that specifically.

24 MEMBER STETKAR: Okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: You know, we will discuss,
2 in 7.5 we will talk about how like for example PAM
3 variables are displayed on one system versus the
4 other.

5 MEMBER STETKAR: Let's wait. I'll let
6 you get through --

7 MR. SHOOK: Okay.

8 MEMBER STETKAR: -- the introduction and
9 I will bring it up later sometime then.

10 MR. SHOOK: Okay.

11 MEMBER STETKAR: Thanks.

12 MR. SHOOK: As you can see, the PICS,
13 the majority of the equipment is located in the Main
14 Control Room, as the primary location for plant
15 operations. We also provide some equipment done in
16 the Remote Shutdown Station or the RSS. And that is
17 in case of evacuation from the Control Room; we can
18 go and shut the plant down from that location.

19 And we also have some equipment located
20 in the Technical Support Center to support emergency
21 operations. That equipment is configured to be
22 basically a monitoring only so there is not control
23 available but the emergency response personnel at
24 that location can pull up all the data available to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the operator and it will just, you know, provide a
2 lot of benefit in terms of looking at the overall
3 plant response.

4 Going over to the SICS, or the Safety
5 Information Control Room -- or I'm sorry, the Safety
6 Information and Control System. The SICS are
7 basically our safety or HMI. It is primarily is a
8 backup to the PICS although there are some controls
9 that are only available on SICS and we will try to
10 discuss those as we go through the various pieces of
11 the design.

12 Most of the controls for the SICS are
13 located in the Main Control Room. There is actually
14 a mix of both safety-related and non-safety-related
15 controls. The majority of the controls -- The
16 majority of the non-safety controls are related to I
17 would call it beyond design basis events, whether it
18 is controls related to a common-cause failure
19 protection system, so it controls associated with
20 the DAS or there are also some controls associated
21 with severe accident mitigation. So it is, I call
22 it the big S. It is not real narrow to be safety
23 related but it is overall safety HMI.

24 And then we have also a small inventory

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 of just controls in the Remote Shutdown Station and
2 essentially those are the controls that are not
3 available in PICS that are needed to reach or
4 maintain safe shutdown. So we are not designing the
5 SICS and they are assessed for actually accident
6 mitigation. But just so those controls and
7 permissives needed to reach and maintain safe
8 shutdown from the Remote Shutdown Station.

9 MEMBER STETKAR: PICS is non-safety
10 related.

11 MR. SHOOK: PICS is non-safety. That is
12 correct.

13 MEMBER STETKAR: So if you have some
14 sort of fire that affects non-safety-related
15 equipment and the operators need to abandon the
16 Control Room, what control capability do they have
17 at the Remote Shutdown Station, if they only have a
18 limited amount of SICS functions?

19 MR. SHOOK: Well the PICS is designed
20 for that event, for fire. And if you look, first of
21 all we have the MCR and RSS are in different fire
22 zones. And so the operator work stations in the RSS
23 aren't affected by the fire in the Main Control
24 Room.

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 you look in the servers, the servers
2 are also physically separated in the two different
3 buildings. So if I have a fire in Safeguards
4 Building 2 that takes out a Main Control Room in
5 that server, I still have a redundant server in
6 Safeguards Building 3 that allows me to interface
7 with all the equipment down in the I&C electrical
8 rooms.

9 MEMBER STETKAR: There is no credible
10 Main Control Room fire that can affect the PICS
11 panels that would indeed take out all of the PICS
12 systems, because they all come together? You know,
13 what servers come together in the Main Control Room?

14 MR. SHOOK: No, the servers are actually
15 not located in the Main Control Room.

16 MEMBER STETKAR: No, no, no. Signals
17 from them, though, do.

18 MR. SHOOK: Oh, signals. Well I mean
19 when you transfer to the remote shutdown station,
20 you will be disabling the signals coming from the
21 Main Control Room.

22 MEMBER STETKAR: Okay, so you have an
23 active transfer.

24 MR. SHOOK: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Okay.

2 MR. SHOOK: You can see here there is a
3 hardwired signal going from transfer switches at the
4 RSS which actually physically disable the network
5 equipment in the Main Control Room.

6 MEMBER STETKAR: And the little drawing
7 over there in the RSS box receives independent
8 signals from the servers. They don't come through.

9 MR. SHOOK: Well what you don't see
10 there is the two redundant servers. One is in
11 Safeguards Building 2 and the other is in Safeguards
12 Building 3.

13 MEMBER STETKAR: So the one over in
14 Safeguards Building 3 will take care of it.

15 MR. SHOOK: Will take care of it and
16 maintain operation.

17 MEMBER STETKAR: Okay. Thank you.

18 MEMBER BROWN: The lines going to the
19 RSS, are those -- You don't show the server networks
20 going over towards to the RSS in the SICS
21 arrangement, relative to Protection System controls
22 limited. So are those dedicated lines or are they
23 still coming off the servers or the ability to
24 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 From what I read, I didn't think any of
2 your protection system remote stuff went through the
3 PICS server network system. They go direct but I
4 couldn't figure that out based on -- I was hoping
5 that would be the case but it wasn't very explicit.

6 MR. SHOOK: That's correct. We'll get
7 into more in the further sections. But the PICS
8 cannot send signals to the protection system in SAS.

9 We physically limit the communication to be
10 unidirectional from the safety systems out to PICS.

11 So in order to perform any controls associated with
12 the protection system, we have to hard-wire directly
13 from the SICS panels, whether it is in the MCR or
14 Remote Shutdown Station directly to the protection
15 system.

16 MEMBER BROWN: Yes, well I was assuming
17 that part of the dotted box, if you have a fire in
18 the Main Control Room, as John postulated, it kind
19 of removes your ability. You would be in the Remote
20 Shutdown Station. So that is why my interest was in
21 the ability to operate or shutdown with dedicated
22 signals, not dependent on any of the network server
23 lines or anything else. Are they direct connections
24 or are you still relying on the servers?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: When we operate from the
2 Remote Shutdown Station, essentially we are relying
3 primarily on the PICS to control the plant to reach
4 and maintain shutdown. The only controls that we
5 provide in the Remote Shutdown Station that aren't
6 on PICS are those controls that you would need to
7 operate the protection system to the point to reach
8 and maintain safe shutdown. So we limit the
9 controls in the Remote Shutdown station to only
10 those that aren't available on PICS that you would
11 need to reach and maintain safe shutdown.

12 So I guess the key point is you can't go
13 to the Remote Shutdown Station and shut down the
14 plant just with hardwired control on SICS.

15 MEMBER BROWN: You can't -- You can
16 scram the plant.

17 MR. SHOOK: We can scram the plant.

18 MEMBER BROWN: But you can't take the
19 rest of the plant down to a safe shutdown. All the
20 other systems --

21 MR. SHOOK: That's correct.

22 MEMBER BROWN: -- you can't cool it
23 down. You can't do anything.

24 MR. SHOOK: That's correct.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: So you are still relying
2 on a location that may not be available then in the
3 Main Control Room.

4 MR. SHOOK: No. I mean, we are relying
5 primarily on the PICS if we lose the Main Control
6 Room, relying on the PICS.

7 MEMBER BROWN: But the PICS is in the --
8 I mean, the Main Control Room, all those signals go
9 into the Main Control Room.

10 Are there other stations that have PICS
11 signals?

12 MR. SHOOK: Yes. Yes, what we are
13 showing here is that the PICS is located primarily
14 in the Main Control Room but also in the Remote
15 Shutdown Station.

16 MEMBER BROWN: Still I couldn't do
17 anything. So I have to -- Okay, so these monitors,
18 or these control stations, or computer workstations,
19 whatever the heck they are, are in the RSS. I got
20 that. But from those can you then complete the rest
21 of the plant operation that you need --

22 MR. SHOOK: Yes.

23 MEMBER BROWN: -- via whatever servers
24 remain; one of the two.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: That's correct.

2 MEMBER BROWN: As long as you have one
3 of the two.

4 MR. SHOOK: That's correct, yes.

5 MEMBER BROWN: If you lose both servers,
6 what do you do?

7 MR. SHOOK: In that case, I mean, if we
8 lost both servers, you wouldn't be able to perform
9 safe shutdown from the Remote Shutdown Station. The
10 design wouldn't support that. So we would have to
11 look at --

12 MEMBER BROWN: Could you do it from any
13 place?

14 MR. SHOOK: You may be able to do it
15 locally, you know, with --

16 MEMBER BROWN: May?

17 MR. SHOOK: I don't know off the top of
18 my head as far as our capability of providing like
19 local switchgear controls or things like that.

20 I don't know if we know.

21 MR. GARDNER: Well, I'm not sure. Are
22 you postulating multiple failures --

23 MEMBER BROWN: No.

24 MR. GARDNER: -- beyond the fire in some

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 area?

2 MEMBER BROWN: I have no idea what I am
3 postulating.

4 MR. GARDNER: Okay.

5 MEMBER BROWN: I just see two servers --

6 MR. GARDNER: Well I think what --

7 MEMBER BROWN: -- and I have got network
8 lines running all over the place to send signals to
9 places. So even if you don't take out a server, a
10 fire or whatever that took out one place can burn
11 your tables, do whatever it is. And there is no
12 definition at this stage of the separation of the
13 various trunk lines that are going to carry those to
14 such a server signal in various places.

15 So my point, and I'm just springing from
16 fires take out a lot of stuff. They burn cables.
17 They burn walls. They burn people. They burn the
18 whole shenanigans. So you know, just having two
19 servers is not necessarily good enough if the roads
20 where you have got to go send signals aren't
21 available.

22 It is kind of constrained, the ability
23 to shut down the plant. If those wires are burned,
24 you are toast. And so that is why I was curious

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 because when you said may, maybe you can go to the
2 local stuff. It seems to me you ought to be able to
3 take care of stuff locally, as well as not having to
4 depend on the Distributed Control System.

5 That is a very centralized system is
6 what you have designed. That is not typical of most
7 of the earlier plants. At least, it is certainly
8 not typical of any of the plants that I have ever
9 been involved with on the detailed design. They
10 were extremely segregated, lots of baskets,
11 separated all over the place, and very difficult to
12 take out all of the baskets. And here, you have got
13 all the eggs in two baskets.

14 MR. SHOOK: Yes, I would say that the
15 PICS is specifically designed to deal with a fire in
16 the Main Control Room. So again, the servers are
17 physically separated in different fire zones. And
18 we have redundant networks that are physically
19 separated so a fire in the one area will not affect
20 a fire.

21 MEMBER BROWN: They still come into the
22 Main Control Room, both server outputs.

23 MR. SHOOK: That is correct. But they
24 are network signals. So the server outputs are, 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 know, you have both servers sending signals to all
2 the different clients up on that top level bus.

3 You know, so again in the case of a
4 fire, -- And the other thing is the interconnects
5 between the two buildings are implemented with fiber
6 optic networks. So the --

7 MEMBER BROWN: They melt with fire.

8 MR. SHOOK: That's true. That's true.
9 But in terms of they will provide an adequate
10 independence from affecting, having like a voltage
11 spike or something like that transmitted to the
12 other are --

13 MEMBER BROWN: Okay. John, I was going
14 to pass unless you wanted --

15 MEMBER STETKAR: I have one more. Are
16 the panels in the RSS normally live? I mean, if you
17 walk from the Control Room to the RSS, can you
18 operate equipment from the RSS without transferring,
19 actively transferring control there?

20 MR. SHOOK: They are set up that you can
21 see but in order to control, you actually have to
22 log in. The operator has to log in to those
23 workstations.

24 MEMBER STETKAR: That is for the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 operators to actually manually take control. But
2 all of the signals then are there. I mean,
3 essentially in the background, everything is live.

4 MR. SHOOK: That's correct, yes.

5 MEMBER STETKAR: Okay. Then the
6 question is, we talked a little bit about fires in
7 the Main Control Room. This comes from doing fire
8 analysis. Can a fire in the Remote Shutdown System
9 room disable all of PICS? Because it is talking
10 back to the Control Room. If the fire is in the
11 RSS, I'm not going to run in there and open up
12 disconnect switches.

13 MR. DOYEL: This is Chris Doyel. The
14 fire design basis is that if you do get a fire in
15 the remote shutdown, the Main Control Room would
16 still be available to shut the plant down.

17 MEMBER STETKAR: I understand in terms
18 of habitability. I am asking whether or not the
19 PICS information system and signals will still be
20 functional.

21 MR. SHOOK: Yes, they would be. From an
22 effect on, when you look at the design, from an
23 effect on just the servers themselves, you know,
24 like I have a fire in Safeguards Building 3 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 Remote Shutdown Station -- MEMBER

2 STETKAR: I understand that fire isn't going to burn
3 the Safeguards Building server.

4 MR. SHOOK: Right. So from that aspect,
5 you are not going to have any impact on the PICS.
6 The only potential impact and you would have to look
7 at from a hot short and for the most part we don't
8 have any really high-voltage information, you could
9 potentially a short of your transfer switches in the
10 RSS come and turn off the PIC servers in the Main
11 Control Room.

12 MEMBER STETKAR: Everybody these days,
13 because of the term of hot shorts and because of
14 copper conductors, becomes wire-centric in terms of
15 spurious signals. I tend to all them spurious
16 signals.

17 The question is, can fire damage in the
18 Remote Shutdown Room call spurious signals that will
19 effectively disable PICS? Not hot shorts in fiber
20 optic cables because they pretty much don't occur
21 but spurious signals because I don't know how those
22 signals are processed. I don't know where the buses
23 are.

24 The question is, I heard a very positive

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 statement that no, absolutely this cannot happen.
2 And that is a good confidence builder. What I am
3 trying to challenge a bit is how carefully have
4 people looked at that possibility to draw that
5 conclusion?

6 MR. SHOOK: I would say that in terms of
7 we can't sit here today and say that there is no
8 possibility of a spurious signal being able to go
9 and disable those PICS servers. Because as you can
10 see, there is clearly a hardwired connection from
11 the RSS to the PICS that is designed to disable
12 those servers or the equipment in the case of an
13 evacuation.

14 But I would say in this case, even if we
15 did lose the PICS, you can still go and shut down
16 the plant from the SICS in that scenario.

17 MEMBER STETKAR: From the SICS in the
18 Main Control Room, you still have power.

19 MR. SHOOK: From the Main Control Room.
20 You have all the capabilities and controls that you
21 need to --

22 MEMBER STETKAR: Okay.

23 MR. SHOOK: You could isolate all the
24 non-safety and shut the plant down.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Okay, that is what I
2 was hoping you were going to tell me. Thanks.

3 MR. SHOOK: Yes.

4 MEMBER STETKAR: Thanks. That helps.

5 MR. SHOOK: You know, we would have to
6 look in detail. The probability of that spurious
7 signal I would say is generally fairly low but I
8 can't sit here and say that it is impossible.

9 MEMBER STETKAR: You don't want to use
10 the word probability with me.

11 (Laughter.)

12 MR. SHOOK: Okay, so if there no other
13 questions on the HMI systems, I will go down to the
14 automation --

15 MEMBER SKILLMAN: I do have a question,
16 please.

17 MR. SHOOK: Okay.

18 MEMBER SKILLMAN: In the image that is
19 on the screen, I see that for each division --
20 excuse me. I see at the image for each division
21 there is a Division 1 and then three underlying
22 layers. I am assuming that what you are really
23 showing is four divisions and what you are
24 presenting here is just one example of Division 1.

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. SHOOK: That's correct.

2 MEMBER SKILLMAN: Thank you. Got it.

3 MR. SHOOK: That's correct. And you
4 will see on the next slide how those divisions are
5 physically allocated within the plant.

6 MEMBER SKILLMAN: Thank you, Jeremy.

7 MR. SHOOK: Okay. So as you can see the
8 next level down we have is what we would call the
9 automation level. And starting at the right-hand
10 side, we have our two non-safety control systems.
11 We have the Process Automation System or the PAS,
12 which is the primary control system within the
13 plant. It is going to control everything from steam
14 generator water level, to main steam, to condensate
15 feedwater, circ water systems. It is your general
16 control system for the plant.

17 For the RCSL, we have, it is essentially
18 our control system for anything that can affect
19 reactivities or rods and boron are controlled
20 through RCSL, as well as some limitation functions
21 that we will talk about more in detail in Section
22 7.7.

23 The PAS, I forgot to mention, is
24 implemented in an industrial type of control 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 We intend to use for our first project the Siemens
2 T3000 system. I will say that is not specified in
3 the FSAR but in terms of our design, that is what we
4 currently intend to use. The RCSL is, while a non-
5 safety system, utilizes the TELEPERM XS platform,
6 which is qualified for safety in the U.S.

7 Going to the next two systems, we have
8 the Protection System or the PS and the Safety
9 Automation System. The easy way to think about
10 these two systems is that the Protection System
11 actuates the safety systems when demanded by the
12 process conditions. And then the Safety Automation
13 System provides controls for the safety plant
14 systems either continuous controls in the case of
15 support systems like HVAC or cooling water that
16 don't change state prior to an event and then after
17 an event. Or in the case of safety systems that do
18 change state following an event, they are initiated
19 by the Protection System and then provide follow-on
20 controls for that.

21 MEMBER BROWN: I was writing and missed
22 your transition from PAS. Were you just talking
23 about SAS?

24 MR. SHOOK: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: Okay. I guess that was a
2 question that I wanted to ask that I had on my list
3 from the reading. While SAS is Safety Automation,
4 what I thought I heard at the end of your discussion
5 since I picked it up, was it doesn't actually do the
6 actuation of the ESFS or the safety systems, it is
7 for post-actuation control.

8 MR. SHOOK: That is correct.

9 MEMBER STETKAR: Okay. All right and
10 that is stated in the text. But I just wanted to
11 make sure I understood it was totally from that
12 standpoint.

13 MR. SHOOK: That is correct. And just
14 to kind of put a little bit more picture on that,
15 there is actually when you look at SAS in total,
16 there is really sort of three different categories
17 of functions. One is if I have a control loop,
18 again, that is always in operation and doesn't
19 necessarily change state on an ESFS. And that is
20 typical for some support systems like HVAC or
21 cooling water. The SAS performs those types of
22 functions.

23 The second is any controls that are
24 needed upon actuation and ESFS signal, for example,

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 emergency feedwater. When we actuate emergency
2 feedwater, we then initiate some closed-loop
3 controls to maintain water level automatically and
4 also the flow rate through the emergency feedwater
5 system. So those controls are actually started as a
6 result of the ESFS function being initiated by the
7 protection system.

8 The third category is --

9 MEMBER BROWN: Does that come down
10 through PACS?

11 MR. SHOOK: It does.

12 MEMBER BROWN: For the initiation?

13 MR. SHOOK: Yes. You have got the
14 Protection System and the SAS. The Protection
15 System will send a signal to actuate. And that is
16 the highest priority.

17 MEMBER BROWN: I don't want to get into
18 priorities now.

19 MR. SHOOK: Okay.

20 MEMBER BROWN: My point being is that
21 when you trigger the ESFS functions, based on a
22 couple of your figures in here, that is Protection
23 System to the Priority Actuation and Control System
24 or something, whatever that is, the little Priority

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 Module. It doesn't go via SAS or anything like
2 that. It just goes directly --

3 MR. SHOOK: That's correct.

4 MEMBER BROWN: -- to go and collection
5 \$200 as it is heading down to turn some stuff on.
6 Right?

7 MR. SHOOK: That's correct.

8 MEMBER BROWN: Okay.

9 MR. SHOOK: I will give you sort of a
10 functional example to give the sense of how this all
11 kind of fits together. So if you are looking at
12 emergency feedwater, levels in steam generator
13 drops. Once you go below the minimum setpoint,
14 emergency feedwater is actuated. Okay? And then
15 the pumps will start, the valves will open, and then
16 the level will start to recover.

17 Once the level clears some setpoint, the
18 actuation signal is removed and the -- Actually at
19 the same time as the actuation, the closed-loop
20 control is initiated within the SAS. Once the level
21 clears the setpoint, the actuation signal is removed
22 from the PACS and then the control loop, which is a
23 PID step controller within the SAS will then
24 modulate the control valve to maintain levels on

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 band.

2 If for some --

3 MEMBER BROWN: You need the emergency
4 feedwater system to do that.

5 MR. SHOOK: Yes, that's correct.

6 MEMBER BROWN: Okay, it is not the
7 normal control system that comes via the PAS.

8 MR. SHOOK: That's correct. And then if
9 we have a control system failure within the SAS if
10 level goes high or low, the Protection System will
11 either actuate if it goes or low or isolate if it
12 goes high. And that order takes priority over the
13 control loop. So you can see here how the
14 actuation, the high or low level is sort of the
15 actuation taking ultimate priority. And then the
16 control is in the middle to maintain level within a
17 tighter band, so the operator doesn't have to do
18 that manual, which is typically done.

19 MEMBER BROWN: Once the emergency feed
20 system is operating and controlling and if the level
21 goes back down, you get another actuation signal?

22 MR. SHOOK: That's correct.

23 MEMBER BROWN: But you've already
24 triggered the system that is supposed to bring it

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 back up and it's already not doing its job. So why
2 does it matter?

3 MR. SHOOK: Well, depending on the type
4 of failure it may or may not make a difference.
5 You're right.

6 MEMBER BROWN: Well, it's already
7 running.

8 MR. SHOOK: Right.

9 MEMBER BROWN: If the control loop can't
10 keep it up, then --

11 MR. SHOOK: Well the difference is that
12 in terms of depending -- Again, it depends on the
13 failure. But if it is a failure let's say the SAS
14 to properly provide a signal, the actuation signal,
15 what happens is there is an isolation valve and a
16 control valve. And if you get to the low level
17 point and needing actuation again, that actuation
18 signal will open those valves fully. So if the
19 failure mode is such that that type of signal will
20 then provide benefit, it will provide benefit.

21 But you are right. To your point, if
22 the control valve just fails shut, if I actuate it,
23 it is not going to make any difference, you know, if
24 it is mechanically stuck. So depending 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 failure mode that may or not make a difference.

2 I mean the system wasn't necessarily --
3 that's how the system will operate. It wasn't
4 necessarily designed to always do that. It's just
5 that as the way the logic works, as it goes low, it
6 will restart or it will re-actuate the system, even
7 though it is already running.

8 MEMBER BROWN: Please go ahead.

9 MR. SHOOK: Okay.

10 MEMBER BROWN: Thank you.

11 MR. SHOOK: Okay, moving over to the DAS
12 or the Diverse Actuation System. So the DAS is
13 designed as a diverse means of implementing reactor
14 trip and ESF actuation functions in the case of a
15 common cause failure of the protection system. So
16 this is designed to satisfy both the ATWS rule, 10
17 CFR 50.62 as well as BTP 19 guidance on software
18 common cause failures.

19 As we get into more in 7.8, the DAS is
20 in a diverse technology from the Protection System
21 and implements a lot of the same functions as you
22 see in the Protection System.

23 Again --

24 MEMBER SKILLMAN: Jeremy, just in my

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 flow of conscious in listening to you and listening
2 to Charlie over there, has AREVA taken any
3 departures in Chapter 7?

4 MR. SHOOK: With regards to?

5 MEMBER SKILLMAN: The base design for
6 the Design Certification. Are there any departures?
7 Are there differences between this, what you are
8 presenting, and the US EPR Design Cert?

9 MR. GARDNER: This is the EPR Design
10 Certification. I'm not sure, maybe you are talking
11 about for a COLA application for an individual
12 plant. I mean, we are presenting what the US EPR
13 Design Certification -- this is the US EPR Design
14 Certification.

15 MEMBER SKILLMAN: My question is off-
16 base. Thank you. I'm in two different places at
17 one time. Excuse me. I apologize.

18 MR. SHOOK: Okay. Going down to the
19 bottom level, we have two systems that are used to
20 interface with those sensors and actuators within
21 the plant. We have what is called the Signal
22 Conditioning and Distribution System or the SCDS.
23 And that is used to acquire all safety-related
24 sensors, as well as non-safety-related sensors 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 have to go to multiple systems within the DCS. So,
2 typically these signals are related to either SBO or
3 severe accident but the majority of non-safety
4 sensors are wired directly to the PAS because they
5 are just provided for control. There is no other
6 auxiliary safety type of input.

7 And then going over the PACS, we have a
8 system where we get all the signals coming down from
9 the various systems within the DCS and the PACS
10 prioritizes those signals in accordance with the
11 functional requirements for that logic and then
12 sends a final prioritized signal out to the actuator
13 for control. And again, all safety-related
14 actuators are controlled through the PACS, as well
15 as any non-safety-related actuators that have
16 received signals from various multiple different I&C
17 systems. So for example, the severe accident heat
18 removal pump, we can control that from SICS. So we
19 are going to -- as well as PICS -- so we can provide
20 a PACS module for that particular pump. So even
21 though it is non-safety, it is still provided for
22 the PACS.

23 But like let's say in the case of a
24 condensate pump, there is no real other safety

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 features associated with that. That is controlled
2 directly from PACS to the switch gear.

3 And then at the very --

4 MEMBER BROWN: To get back to the PACS
5 on the priority issue, so if you request -- all this
6 stuff has to be done in series. I mean, the way I
7 gathered the priority system works, the PACS system
8 gets all kinds of requests to do something and says
9 I'm not going to do this one, this one, this one,
10 and this one, right now. I'm going to do this one
11 first because I have got a priority assigned. So it
12 may decide not to do something.

13 MR. SHOOK: That's correct.

14 MEMBER BROWN: And it will come back
15 later and say okay, it is time to do it now because
16 I have already done all the other things that come
17 out ahead of it. Why in the world wouldn't you
18 allow an operation say I do from the SICS or from
19 wherever you want to do it, to go ahead and take
20 action instead of saying I'm going to figure out --
21 I mean, because you are sending all this data in
22 there, it has got to wait to figure out whether it
23 is going to actuate or not? The only one that takes
24 priority over everything is the protection 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 from what I have gathered. It goes direct, and no
2 matter what else is going on, it will override and
3 stop everything else.

4 So if you have energized something else
5 to try to do something and then go to scram the
6 reactor, it will stop that and go back and do the
7 other thing.

8 MR. SHOOK: I don't think that is a
9 quite accurate representation of how it works.

10 MEMBER BROWN: I'm just talking about
11 what I read.

12 MR. SHOOK: Right. The PACS is
13 essentially you can think of it as it is nothing
14 more than relay logic shrunken down on a card. So
15 there is not sequencing. There is no time-based
16 behavior. It is basically just looking at the
17 various signals and in accordance with a priority
18 scheme if it says well this signal has priority over
19 this one and they are competing, then I am going to
20 go with the higher priority signal.

21 So it is not a matter of like a schedule
22 or a sequence.

23 MEMBER BROWN: -- it ought to do the
24 other one. Does it come back? I mean, the PACS is

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 not a microprocessor-based system, isn't it?

2 MR. SHOOK: That's correct.

3 MEMBER BROWN: It is a combinational
4 logic.

5 MR. SHOOK: That's correct.

6 MEMBER BROWN: So it is like Or gates
7 and And gates all wired together, integrated
8 circuit.

9 MR. SHOOK: That's correct.

10 MEMBER BROWN: It's all estate type
11 stuff.

12 MR. SHOOK: It uses, the Priority Module
13 itself, uses what is called a Programmable Logic
14 Device. So, it is a PLD is essentially a very
15 simple programmable chip that you program using --
16 It is essentially firmware. You know you can think
17 of it in that way. So there is no operating system.
18 There is no application software or system
19 software. You are just basically configuring the
20 logic of various gates by setting different switches
21 to find that logic.

22 MEMBER BROWN: So it is defined by the
23 software that you use to program the gates --

24 MR. SHOOK: That's correct.

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 BROWN: -- for the order in which
2 they are supposed to do stuff, like the FPGA or
3 whatever, PLDs, whatever.

4 MR. SHOOK: Yes. Yes, it is a PLD. And
5 PLD is -- FPGA is a little bit more complicated.
6 PLD is typically simpler.

7 MEMBER BROWN: But fundamentally, they
8 operate the same, similarly.

9 MR. SHOOK: At some level, yes.

10 MEMBER BROWN: Well I mean, you know,
11 they have got on/off gates and they progress to a
12 set of logic functions that you program into them.

13 MR. SHOOK: Yes, they --

14 MEMBER BROWN: There are other things in
15 FPGAs that you don't have in PLDs.

16 MR. SHOOK: Yes, I think between the
17 two, and PLD is essentially the combinatorial logic.
18 I mean, it is just Ands and Ors and truth gates.
19 Whereas, an FPGA, you implement logic using look-up
20 tables, truth tables. So it provides more
21 flexibility but I would say it is a more complicated
22 device than a PLD.

23 A PLD is essentially like an integrated
24 circuit just done with like a prompt.

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 back to your original point, just
2 again to give a functional example, let's say I
3 have, going back to the emergency feedwater, let's
4 say I have a control system failure that is always
5 demanding the level control valve. And just to give
6 a sense, you have got -- in emergency feedwater you
7 have got the pump, then you have got a level control
8 valve, and then an isolation valve in series. So in
9 actuation, the pump starts and the two valves open
10 and get open signals. Once the actuation resets,
11 the signals are removed and then the control valve
12 that modulates with the SAS.

13 So let's say that I have a control
14 system failure that drives the level control valve
15 closed. Okay? So I have got a close order from the
16 SAS driving the valve closed. That is going to
17 result in the steam generator water level dropping
18 and at some point I will re-actuate emergency
19 feedwater. When I do that, the protection system
20 then resends those actuation signals to the PACS to
21 open those valves.

22 So now I have got a close order from the
23 SAS and I have got an open order from the PS and all
24 the PACS does is it says this one wins and then

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 changes the output from a closed to an open. And so
2 basically you know, so as long as the PS is saying
3 open, it will open. And then once the PS signal is
4 removed, then it goes back to, it will go back to
5 closed. So there is no time, history, or sequence
6 involved. It is just which one, which signal is
7 present at that particular point in time.

8 MEMBER STETKAR: Jeremy, I think I
9 understand how that works. And I certainly don't
10 understand every valve in the entire plant but I
11 have seen plant designs in the past where a single
12 valve performs two different safety functions. One
13 safety function might be to close the valve to
14 isolate the line. Another safety function might be
15 to open the valve to bribe closed through the line.

16 As I said, I can't mention specific valves in this
17 design but that is kind of a moot point. MSRTs come
18 to mind.

19 The example you just mentioned where
20 signal B, let's call it, from the protection system
21 always has priority over the control system so that
22 that valve, the PACS knows that the valve shall
23 always be open because that is the most important
24 position for that valve to be. How does PACS 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 which signal is the correct signal if I have two
2 safety signals? How do those priorities set? Who
3 sets those priorities?

4 MR. SHOOK: Those priorities are
5 established and actually two examples, emergency
6 feedwater and MSRT are two examples where you
7 essentially have competing priorities. And those
8 priorities are established in accordance with the
9 functional requirements for those systems. And I
10 will say in both these cases, the closing will have
11 priority over the opening. So for example, it kind
12 of takes a little bit of the walk-through.

13 Well I'll tell you what. Let me walk
14 through how we do that within the PACS and then I
15 will get back to --

16 MEMBER STETKAR: Let me ask you, rather
17 than gory details about individual control signals,
18 is it possible for the operators to somehow manually
19 override those control signals in PACS?

20 MR. SHOOK: Yes.

21 MEMBER STETKAR: Okay. So manual
22 control always comes in downstream of the PACS
23 output.

24 MR. SHOOK: No, the manual control from

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 either PICS or SICS comes to the PACS. So those
2 signals get prioritized with all the other signals.

3 What the operator has to do -- So let's say for
4 example we have this case of emergency feedwater and
5 I want to take manual control. What the operator
6 would have to do is go and first re-set EFW
7 actuation signal and if you look at the drawing, you
8 can think of it as you have got an active signal
9 coming in for a protection system. You are
10 essentially just removing that signal. But in
11 accordance with IEEE 603 requirements, the system
12 doesn't reset once you just reset the signal. The
13 system continues to stay in the same state. Then
14 once you have cleared that signal, then the operator
15 can then come in and take manual action as they see
16 fit dictated by the EOPs.

17 So the capability is in the ability to
18 reset the safety actuation signals or, in the case
19 of the control system, to take the loop to manual
20 and then the operator can take those actions.

21 MEMBER STETKAR: When are -- Are those
22 priorities already defined in the design on a
23 compliment by compliment, system-by-system basis? I
24 mean, today.

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. SHOOK: We have general rules today
2 but those -- The way we have it set up is in the
3 detailed design, we were going to draw logics for
4 every single PACS, every single actuator that would
5 then show clearly how the --

6 MEMBER STETKAR: I mean if you have
7 general rules, if I go to a particular valve, let's
8 say the EFW control valve, I could know today which
9 is the higher priority signal for that valve?

10 MR. SHOOK: That's correct.

11 MEMBER STETKAR: Because you know that
12 is a rule. That is not implementation of the actual
13 --

14 MR. SHOOK: Yes.

15 MEMBER STETKAR: Okay.

16 MR. SHOOK: And actually, I mean the
17 basic rules are actuation always has prior over
18 safety controls.

19 MEMBER STETKAR: Yes.

20 MR. SHOOK: And then in the cases where
21 there is competing priorities, those have to be
22 defined on a case-by-case basis.

23 MEMBER STETKAR: Yes, those are the
24 things that I am interested in. Is that information

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 available for the staff to review as part of the
2 design?

3 MR. SHOOK: It is not. Is it? Do we
4 have that in 7.3 in terms of --

5 MR. PHAN: The logic is shown in our 100
6 percent testing, combinatorial testing document.

7 MR. SHOOK: No, in terms of the
8 priority, like showing that EFW isolation has
9 priority over actuation.

10 MEMBER BROWN: I don't remember seeing
11 it.

12 MR. PHAN: No, we don't.

13 MR. SHOOK: Okay.

14 MR. PHAN: We don't discuss that.

15 MR. SHOOK: It is not in Chapter 7. I
16 don't know if it is available in the other chapters.

17 MR. GARDNER: Is there a specific
18 example you are trying to get to?

19 MEMBER STETKAR: No, there isn't. The
20 problem is there isn't. I mean, the two that
21 immediately come to mind are the ones Jeremy
22 mentioned in terms of EFW and MSRT where I know
23 there are -- just because of the functions of those
24 systems, I know that there must be some sort of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 competing priority. I don't know whether there are
2 others.

3 What I am trying to search out is number
4 one, I heard already the basic priorities are set.

5 MR. SHOOK: Right.

6 MEMBER STETKAR: So it is not something
7 that is still nebulous in terms of at least at a
8 functional level. That's good news.

9 The second part of the question was to
10 determine whether that information is available for
11 staff review or principle for our review. But in
12 practice, it is staff review because some of those
13 priorities might not necessarily -- I have seen
14 designs in the past where it is not at all clear
15 that the priorities that are established by design-
16 based accident sort of linear through process may
17 necessarily be appropriate. And that is especially
18 true if the operator input essentially comes through
19 the same prioritization logic, unless they actively
20 reset or block a signal or something like that that
21 they can't circumvent it some other way.

22 So I can't give you a specific example
23 where I have very well defined black and white
24 concern because I don't know enough to be able 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 ask that level of question.

2 MR. GARDNER: Right. I think I was
3 trying to separate out are you asking do we
4 understanding sort of the mechanical requirements of
5 the function is out of the system. I think the
6 answer is yes.

7 MEMBER STETKAR: Yes. Yes, I mean --

8 MR. GARDNER: And that is detailed --

9 MEMBER STETKAR: Yes, that's what I
10 mean.

11 MR. GARDNER: -- directions the answer
12 would be that would be something that would be part
13 of the detailed design.

14 MEMBER STETKAR: Yes, but how the
15 individual signals are wired together, I'm less
16 interested in that than knowing for example what
17 Jeremy said that it sounds like the closed signal
18 for the EFW control valves always has priority over
19 the open signal.

20 MR. GARDNER: That's correct.

21 MEMBER STETKAR: Because for some
22 reason, you know, somebody made the decision that
23 you would only have a broken steam -- broken line in
24 one steam generator and that is the only situation.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And obviously, you have the other three trains that
2 can feed the other three steam generators. So
3 therefore closed for that particular valve shall
4 have higher priority than open.

5 MR. GARDNER: You know, I think --

6 MEMBER STETKAR: And that is sort of the
7 thought process that I am kind of delving into. And
8 I don't want to do it in this forum here. I'm just
9 trying to find out whether that basic priority
10 information is available. And from what Jeremy
11 said, I think the answer to that is yes.

12 And then the second part of the question
13 is more toward the staff is has the staff looked at
14 that and made a determination that indeed those
15 priorities seem adequate or acceptable for the
16 integrated design of the whole plant, over the whole
17 spectrum of things that can occur.

18 MR. GARDNER: Okay.

19 MEMBER STETKAR: And the answer to the
20 second part of the question, from what I am hearing,
21 is no, that hasn't been done yet. I don't know. I
22 would let the staff answer that one.

23 MR. GARDNER: I guess I can say to try
24 to address a piece of that is those two functions

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 are the only functions where there this competing
2 actuation signals from the Protection System. And
3 in both cases, the closing or the isolation function
4 takes priority over the actuation function. And if
5 you would like, I can go into the details why that
6 is.

7 MEMBER STETKAR: RCP thermal barrier
8 cooling?

9 MR. GARDNER: RCP thermal barrier
10 cooling?

11 MEMBER STETKAR: I don't actually know
12 how the signals come out. You will get asked about
13 that later.

14 MR. GARDNER: Okay.

15 MEMBER STETKAR: I mean there are a few
16 that I can think of that could have competing
17 priorities. But I don't want to necessarily raise
18 those to an inordinate level of importance. It I
19 just things that I can think about because we talked
20 about those particular systems yesterday.

21 EFWS and MSRTs are more obvious from the
22 bigger picture safety functions. But I think we
23 have said enough.

24 Essentially what I am probing is if the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 priorities are set, does somebody from the staff
2 have the opportunity to look at them and essentially
3 understand how they work and why a certain signal
4 has priority one and why another signal has not
5 priority one.

6 MR. JACKSON: This is Terry Jackson with
7 the staff. And I think we will address your
8 question a little bit more in our presentation.

9 MEMBER STETKAR: Okay.

10 MR. JACKSON: But overall, I think as
11 AREVA has said, there was some priority discussion
12 in previous documents but we understand the
13 priorities game is changing some, even with Revision
14 3.

15 MEMBER STETKAR: Okay.

16 MR. JACKSON: So the staff is still
17 looking at that part.

18 MEMBER STETKAR: Okay. So it is still -
19 - Thanks.

20 MEMBER SKILLMAN: I would like to ask
21 another question. It is kind of built on what I
22 asked before. And let me tell you where I am coming
23 from. I spent almost three years importing a
24 foreign design into Design Certification under 10

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 CFR 52. So I saw this design that was not a US
2 design being brought into our country. You have
3 kind of done the same thing here.

4 What my real question is is under 10 CFR
5 52 you include OE. So at a high level, could you
6 identify perhaps some key elements of operating
7 experience that are in the AREVA design that weren't
8 in the European design that you imported?

9 That is my real question. What is
10 different? What have you added here that was not in
11 your early underlying design that you brought into
12 the country?

13 MS. SLOAN: Jeremy, let me comment.
14 This is Sandra Sloan from AREVA. I don't think that
15 is part of the staff's review process. I think what
16 we are presenting today is simply the design that we
17 are proposing for US EPR. I would propose that if
18 there is an interest in those kind of differences,
19 that should be addressed off the record. They are
20 not part of this Design Certification review.

21 MEMBER STETKAR: Well, Sandra, I
22 understand the concern but I will give you a good
23 example. I mean, I hate to bring this stuff up
24 because it is a bit -- I'm aware for example of, in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 my opinion, quite a good design based on operating
2 experience that uses N16 signals for automatic
3 mitigation if a steam generator tube rupture. This
4 particular design doesn't do that.

5 MR. SHOOK: Well --

6 MEMBER STETKAR: That is, in my mind, a
7 difference that merits questioning. That is
8 operating experience. That is design experience
9 from international application of this type of
10 design that is not being proposed for the United
11 States and I am curious why.

12 MR. SHOOK: Just for that particular
13 case --

14 MEMBER STETKAR: That is something that
15 we can ask. Perhaps the staff can't but we can.

16 MS. SLOAN: I think it is fair to ask us
17 to defend the design that we have proposed.

18 MEMBER STETKAR: Okay.

19 MS. SLOAN: And if you think there is a
20 deficiency to ask it in those terms, but to ask
21 Jeremy to justify or enumerate and articulate the
22 differences compared to the European design, we are
23 not prepared to do that.

24 MEMBER STETKAR: Okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: I will say just that that
2 particular case isn't quite as you represented. It
3 is true that the accident analysis credits manual
4 action but we still do have an automated tube
5 rupture function and I can go into the bloody
6 history of why that is, if you care.

7 MEMBER STETKAR: I'll let you get
8 through on some of this stuff.

9 MR. SHOOK: Okay. But that is also in
10 the history as well.

11 MEMBER STETKAR: It is.

12 MEMBER SKILLMAN: Let me ask, perhaps
13 Getachew, is the NRO staff comfortable that
14 operating experience has been appropriately
15 incorporated into the AREVA design?

16 MR. TESFAYE: We've been in
17 international forums. In fact, the I&C branch,
18 Terry Jackson he is the chairman of the I&C
19 committee of MDEP so he may have something to say
20 about the staff's --

21 MEMBER BROWN: Putting him on the spot.

22 MR. TESFAYE: That's my job.

23 MR. JACKSON: Terry Jackson again. With
24 regards to the question you have, if somebody with

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 operating experience I think are what Getachew is
2 talking about, the staff is involved in
3 Multinational Design Evaluation Program or MDEP
4 where the regulators who are involved with reviewing
5 the EPR design is, right now, I think, five
6 countries, we routinely meet and we discuss design
7 aspects about the EPR and what kinds of things that
8 the various regulators have picked up.

9 So we have been able to gather
10 information from the other regulators, from their
11 review, and we have also been able to share some
12 information with them as well.

13 MEMBER SKILLMAN: Thank you, Terry, but
14 my question is, is it incorporated in the AREVA
15 design.

16 10 CFR 52, if you look at the list,
17 requires the applicant to include OE. The work
18 international OE is not in there. It is just OE.
19 And I am presuming the answer to the question is yes
20 but I am just exploring --

21 MR. JACKSON: From the staff's
22 perspective, we did review operating experience for
23 the US EPR I&C design and I don't believe we have
24 any open items on that. So we haven't found 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 issues with operating experience with regards to the
2 EPR design, EPR I&C design.

3 MEMBER SKILLMAN: Thank you. And I
4 accept Susan's comment that this is not the forum --

5 MR. SHOOK: Okay.

6 MEMBER STETKAR: -- to try to explain
7 that and I certainly was not expecting that you
8 could say, yes here is a list. But the larger
9 question is how 10 CFR 52 regarding operating
10 experience incorporation has been incorporated into
11 the AREVA design. I think you are saying hey, yes,
12 it is in there.

13 I think that is what you are saying.

14 MR. SHOOK: I think I can maybe just
15 speak to it generically. I mean, the base design
16 that we inherited from Europe had a lot of operating
17 experience behind it. And I can say all the changes
18 that we have made were based on trying to make the
19 design conform to US NRC's specific requirements,
20 where we had to make changes that kind of deviate
21 from the base OE. We tried to incorporate OE as
22 much as we could but the driving force the changes
23 were all regulatory based, not necessarily US-
24 specific OE.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER SKILLMAN: Thank you.

2 MR. SHOOK: Okay.

3 MEMBER BROWN: Can I step up a level? A
4 response to an earlier question -- no. In your
5 earlier presentation, you talked about the PAS is a
6 normal mode of plan automation controls. So steam
7 generator control, main feed control -- I presume
8 you are controlling main feed pumps separately in a
9 normal manner. Is that correct? You have variable
10 speed -- I don't know the design of that part of it.

11 I haven't looked at. Are they variable speed main
12 feed pumps so that you have a control system for the
13 pumps themselves?

14 MR. SHOOK: I believe so. I don't know.

15 MR. STACK: This is Tim Stack from
16 AREVA. They are constant speed motor-driven pumps.

17 MEMBER BROWN: Okay. So, all right. So
18 emergency feed control consists of what, opening an
19 alternate path valve?

20 MR. SHOOK: That's correct. Yes, so you
21 have --

22 MEMBER BROWN: In case your normal
23 control valve goes closed or what have you?

24 MR. SHOOK: That is correct. The main

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 feedwater system is providing your normal flow of
2 feedwater during normal operation. In case you lose
3 main feedwater, for whatever reason whether it is a
4 loss of outside power or a failure of the system,
5 you have an independent flow path with separate
6 pump, separate pump and control valves, and its own
7 water supply to provide water to the steam
8 generator.

9 MEMBER BROWN: All right. The net part
10 of the question then. So if the PAS is normally
11 controlling the water level with the flow control
12 valve, now for some reason you get this signal to
13 actuate via the PACS. It says actuate the emergency
14 feedwater control system. You start the new pumps,
15 the feed pumps, the emergency feed pumps. You open
16 and you have another valve with which you control it
17 and the SAS now takes over control?

18 MR. SHOOK: Well again, they are two
19 different --

20 MEMBER BROWN: Is there another control
21 system?

22 MR. SHOOK: Again, there is two
23 different flow paths here. The main feedwater
24 controlled normally through the PAS, and then

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 emergency feedwater the automated control is through
2 the safety automation system.

3 MEMBER BROWN: That is what I was
4 asking.

5 MR. SHOOK: Yes.

6 MEMBER BROWN: So there are two
7 different control systems with the two different
8 valves.

9 MR. SHOOK: That is correct.

10 MEMBER BROWN: Would it turn off the one
11 from PAS?

12 MR. SHOOK: No.

13 MEMBER BROWN: That was just a side
14 question.

15 MR. SHOOK: No, it doesn't.

16 MEMBER BROWN: I don't need that detail.
17 I'm just trying to understand.

18 So you transfer control from one control
19 systems to another for both the valve, the control
20 functionality itself, the electronics sensing, and
21 all that kind of stuff, and the pumps. Those are
22 all shifted to another set of the component.

23 MR. SHOOK: That's correct. There is
24 two different flow paths and each flow path has its

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 own controls.

2 And I will say that upon a reactor trip,
3 we isolate main feedwater so I don't have to worry
4 about feeding from this flow path. I have basically
5 shifted over my backup flow paths for decay heat
6 removal to the emergency feedwater system.

7 MEMBER BROWN: Okay. Now once you go
8 above the actuation point again, you are now up in
9 the -- Where -- Is it still the emergency feed
10 system that is modulating? You don't shift over
11 back to the original?

12 MR. SHOOK: No.

13 MEMBER BROWN: Okay. That's all I
14 wanted to know.

15 MR. SHOOK: No, once you have
16 essentially the way the logic is set up, once you
17 "lose" your main feedwater system, you shift over to
18 the emergency feedwater system. You don't go back
19 unsecured from the event.

20 MEMBER BROWN: Okay, thank you.

21 MEMBER STETKAR: That's a good thing to
22 do to isolate main feedwater every time you tip the
23 plant?

24 MR. SHOOK: Well, you can --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: That just comes back to
2 my priority scheme, in terms of looking at risks
3 from different types of transients versus design-
4 basis events for which you might want to isolate
5 main feedwater. I don't need an answer right now.
6 It is rhetorical.

7 MR. STACK: That's okay. John, this is
8 Tim Stack from AREVA. In general, you isolate the
9 majority of pathways from main feedwater into the
10 steam generators to minimize the overfill. And then
11 you have, you continue to run main feedwater through
12 a small path. If you lose the main feedwater and
13 that will be sensed by low level in the generator,
14 you start emergency feedwater.

15 So there is an overlap in functionality.

16 MEMBER STETKAR: Okay, thanks.

17 MR. SHOOK: Okay?

18 MEMBER STETKAR: What you are saying is
19 it is not a complete isolation.

20 MR. STACK: That's correct.

21 MEMBER STETKAR: Some plants to have
22 that. Okay, thanks.

23 MR. SHOOK: Okay, I guess just based on
24 the time, I would like to move on to the next slide.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 This is just pictures merely just to show a
2 physical layout of those various systems within the
3 plant.

4 MEMBER BROWN: Have you got that SCDS?

5 MR. SHOOK: I did, just very briefly.
6 It is just a Signal Conditioning and Distribution
7 System.

8 MEMBER BROWN: It's the only independent
9 system you have got in the whole plant. So, it's
10 really nice.

11 MR. SHOOK: Well I will show you more
12 detail on that here in the following sections.

13 So this drawing here is what we call the
14 physical architecture. And this just showing a
15 physical representation of the layout of the --

16 MEMBER BROWN: Oh, I did have one
17 question, I'm sorry, I meant to ask.

18 Do all sensing, all measurement,
19 everything comes through SCDS. Is that correct?

20 MR. SHOOK: No.

21 MEMBER BROWN: So you have got separate
22 sensors for -- I notice you have got some of these
23 spread around with black boxes and sensors in some
24 other places. So there are other sensing devices,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 measurement devices that don't function or come
2 through what you big-picture envelope as the SCDS.

3 MR. SHOOK: That's correct. So when we
4 look at allocating the PAS sensor signal pathway,
5 you look at two things. Actually, why don't you go
6 back to the previous slide so we can talk to that.

7 MEMBER BROWN: Keep trying, right?

8 MR. SHOOK: First of all, if the sensor
9 is safety-related, it goes through SCDS, because
10 SCDS is my primary means of acquiring and isolating
11 and distributing safety-related signals.

12 And then the other criteria is if the
13 sensor is non-safety-related but I need it in
14 multiple DCS subsystems, whether that is the SICS or
15 the DAS or RCSL, then I will send it also through
16 the SCDS to provide the same sort of distribution
17 function.

18 If the only, once I allocate all the
19 functionality associated with that sensor, if it is
20 only needed in PAS, I just route it directly to PAS.

21 That minimizes the amount of cabinets that we need
22 for SCDS.

23 So SCDS is essentially it is a
24 distribution system, so if I need it in more than

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 one place, I will send it through there first to
2 take advantage of that capability.

3 MEMBER BROWN: How come you don't
4 provide those criteria in the DCD so somebody would
5 understand that from reading it?

6 MR. SHOOK: It has been provided in Rev.
7 3 of the DCD.

8 MEMBER BROWN: I read that and I don't
9 remember seeing that nice definition of all the
10 sensors and other stuff. I don't remember that.

11 MR. SHOOK: Okay.

12 MEMBER BROWN: I'll have to go back and
13 look.

14 MR. SHOOK: Okay.

15 MEMBER BROWN: No, you don't have to do
16 anything. I'll go back and look, --

17 MR. SHOOK: Okay.

18 MEMBER BROWN: -- now that you have told
19 me.

20 MR. SHOOK: Okay. Okay, here just
21 looking at the physical layout, essentially within
22 the nuclear island which consists of the safeguards
23 buildings, the emergency power generating buildings,
24 the Essential Service Water Pump Structures and then

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the main -- those are sort of the main buildings in
2 the nuclear island.

3 You have got all your safety systems
4 segregated in the four divisions to go along with
5 the building layouts. And in addition, in those
6 buildings you also have non-safety systems. RCSL is
7 only located in the four safeguards buildings
8 because it is primarily doing rod control. But when
9 I go out to the emergency power generating buildings
10 and essential water pump structures, we also have
11 paths out there as well. And the primary reason for
12 that, which we didn't really talk about it in the
13 previous too much is because the PICS is designed to
14 be our primary operating station, I can control
15 manually at a minimum all the equipment in the
16 plant, whether it is safety related or not. And I
17 provide that through that PACS pathway and that is
18 based on operating experience that we inherited from
19 Europe as far as trying to provide a consistent HMI
20 for the operator.

21 So you can see that even though the
22 majority of the equipment in those buildings is
23 safety, I am still providing PAS for that pathway to
24 PICS to allow control, at least component level for

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 those equipment.

2 Also in the nuclear island you can see
3 the Fuel Building. There is no systems there. What
4 we decided to do, this is basically just based on a
5 cable routing decision, we just will run the control
6 cable from Safeguards Building 1 of 4 into the fuel
7 building to control that equipment.

8 And then when you get in the aux
9 building and rad waste, the only cabinets we have
10 out there are process automation system cabinets.

11 Outside the nuclear island in the
12 turbine building, we have got --

13 MEMBER STETKAR: Jeremy, is that -- a
14 light just lit. Is that why the stuff out in the
15 fuel building is Division 1 core stuff?

16 MR. SHOOK: Yes.

17 MEMBER STETKAR: Oh, okay. Thanks.

18 MR. SHOOK: Just a survey.

19 MEMBER STETKAR: Thank you.

20 MR. SHOOK: In the turbine island, we
21 look at all of the PAS equipment is, we have trains.
22 In the nuclear island we call it division. In the
23 turbine island we call it trains. And I can give
24 you again a long bloodied story history as far as

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 why that is but you can see the PAS. We have trains
2 one and two in the switchgear building and also out
3 in the circ water structure as well.

4 And then finally the HMI systems you can
5 see, as we discussed earlier, I have SICS and PICS
6 both located in Safeguards Building 2 and 3, with
7 the control capability we previously discussed.

8 Okay and then lastly, that last box of
9 going back to our DCS drawing is we have actuator
10 systems. Again, the majority of the actuators in
11 the plant are included within the various plant
12 systems, whether Process, or HVAC or Electrical
13 Systems.

14 We do have two have two dedicated
15 actuator systems that we talk about in Chapter 7.
16 So those are the Control Rod Drive Control System
17 and the Turbine Generator I&C.

18 MEMBER BROWN: Process, that includes
19 all of your like Safety Injection System and
20 everything else?

21 MR. SHOOK: That's correct, yes.

22 MEMBER BROWN: All the miscellaneous
23 safeguard systems would fall under process.

24 MR. SHOOK: That's correct, yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: Thank you.

2 MR. SHOOK: Okay, before going on to
3 Reactor Trip System, could we take just a quick
4 five-minute break to use the rest room? Is that
5 possible?

6 CHAIR POWERS: We can.

7 MR. SHOOK: Okay.

8 CHAIR POWERS: Would you like to take a
9 break at this time?

10 MR. SHOOK: Short break.

11 CHAIR POWERS: Well there is a
12 fundamental rule that there is no such thing as a
13 short break.

14 (Laughter.)

15 CHAIR POWERS: If we take a break, we
16 will take a break. And then we will take a break
17 until five of.

18 (Whereupon, the foregoing proceeding went off the
19 record at 9:42 a.m. and went back on the
20 record at 9:56 a.m.)

21 CHAIR POWERS: Let's continue our
22 discussion. I think we are on trips.

23 MR. GARDNER: I just had wanted to --
24 Dr. Powers wanted to revisit a question 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 earlier had on the operating experience Mr. Skillman
2 had. And just to say on the record that we
3 understood the question. It was the larger question
4 of all the operating experience considered, I would
5 say that AREVA certainly has a program that
6 considers our international operating experience as
7 well as operating experience here as part of our
8 design efforts. And operating experience obviously
9 is an ongoing program within our design
10 organization. So, I think the larger, you know, the
11 details of all the possible operating experiences
12 that have been considered would be certainly
13 something larger, bigger than we could go into in
14 this meeting but I wanted to set the record
15 straight. It has been considered.

16 MEMBER SKILLMAN: Thank you, Darrell.

17 MR. SHOOK: Okay. So we are going to be
18 talking about reactor trip functions here in this
19 section and we are going to be focusing on some key
20 points. We are first talking about the functions in
21 general. And my intention is we are not going to
22 spend too much time talking about the functions in
23 terms of the specific logic, but just kind of show
24 what they are. Then we will talk about how

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 specifically we implement those functions within the
2 design. And then we will focus on some key areas,
3 specifically redundancy, independence, deterministic
4 response time behavior, fail-safe behavior, and how
5 we test those functions.

6 CHAIR POWERS: That sure looks like a
7 very familiar litany.

8 MR. SHOOK: I will say we greatly
9 appreciated the feedback we got from Member Brown in
10 September to help structure this presentation. So
11 hopefully this will --

12 CHAIR POWERS: You realize I have to
13 live with him now.

14 MEMBER BROWN: What getting a
15 compliment?

16 CHAIR POWERS: Yes.

17 MEMBER BROWN: I was going to say, it
18 may not help.

19 CHAIR POWERS: Please continue.

20 MR. SHOOK: So we go on to slide 11.

21 Here is a list of all the reactor trip
22 functions that are listed in part of our design and
23 are represented in 7.2 in the FSAR. I am not going
24 to go through these in detail again and 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 the logic. I will say that the majority of these I
2 would say fairly typical of what you find in
3 operating plants, at least in my experience in
4 looking at operating plants.

5 There are a few trips though that are
6 unique to the EPR design that we will be talking
7 about in a little bit more detail. The first two,
8 the low departure from nucleate boiling trip and
9 high linear power density trip utilized the 72 SPNDs
10 to measure Incore flux conditions. And we will be
11 talking about how that is implemented specifically
12 in the design.

13 And the other two trips that are a bit
14 unique are the high core power level and low
15 saturation margin trips. Those are trips that you
16 typically don't see in an operating plant.

17 But other than that, most of the trips
18 are basically the same as what you would see in an
19 operating plant today. Let's go to the next slide.

20 So here we are showing --

21 MEMBER BROWN: Just one question on
22 that. When you talk about high neutron flux rated
23 changes, is that all ranges? Is all three of the
24 major ranges source intermediate, as you described

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 them under the nuclear function? Are those
2 generated with the Excore or are they done with the
3 SPDS -- excuse me -- SPNDs or whatever?

4 MR. SHOOK: Those are generated with the
5 Excore power range detectors.

6 MEMBER BROWN: And is it all ranges?

7 MR. SHOOK: Just power range.

8 MEMBER BROWN: Just power range.

9 MR. SHOOK: Yes. Okay?

10 So just as Member Brown notices, there
11 is significantly more reactor trips in this design
12 than you might see in a submarine but it is just a
13 difference in the plant design.

14 Going on to slide 12, we will see
15 basically, you know, we talked about the slide as
16 the overall DCS and the various systems within it.
17 And now we are showing how the reactor trip
18 functions are allocated within the DCS.

19 You can see that all those sensors are
20 safety-related and those are all acquired via the
21 SCDS. Those signals are then sent to the Protection
22 System for processing. You know basic processing
23 includes any calculations that may need to be
24 performed, sub-point comparison, two out of four

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 voting, and then any subsequent logic, for example,
2 permissive logic.

3 And then the actuation signal is sent
4 from the Protection System to the reactor trip
5 breakers. As you can see on the bottom right,
6 specifically to those, the Protection System
7 actuates the UV coil and the reactor trip breakers
8 and those we will talk about later when we talk
9 about DAS. The DAS implements the shun trip coil
10 on the trip breakers for a diverse actuation
11 mechanism.

12 We also have within the Protection
13 System trip we also trip the trip contactors. Those
14 are part of specifically the CRDCS system but they
15 are safety-related and provide a diverse means from
16 the trip breakers to trip the reactor.

17 We also show on SICS the --

18 MEMBER BROWN: Say that again. Which
19 one are the diverse names, the trip contactors?

20 MR. SHOOK: The trip contactors, yes.
21 So they are safety-related 1-E qualified diverse --

22 MEMBER BROWN: I guess I understand it
23 but those are considered the diverse?

24 MR. SHOOK: Yes, so there is within the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 trip mechanism cells, there is for the reactor
2 trips, for the Primary Reactor Trip Signal
3 Protection System, you will trip both the trip
4 breakers and the trip contactors. But separately
5 for DAS, we also trip the trip breakers through a
6 different mechanism, the shun trip coils, and we
7 also trip the control logic within the CRDCS. So
8 both between the primary trips and the backup trips
9 in the DAS, we have diverse mechanisms to trip the
10 reactor.

11 MEMBER BROWN: Okay, that part I
12 understand. But I -- Well I'll wait until you get
13 to slide 15.

14 MR. SHOOK: Okay. And you can see here
15 on the SICS, we have manual capability of tripping
16 the reactor from the Main Control Room. And I just
17 noticed and I apologize for this, we didn't shade
18 the box in the RSS but we also do provide the
19 ability to mainly trip the reactor from the Remote
20 Shutdown Station.

21 So slide 13, we are going to talk about
22 a little bit more. So we are going to kind of blow
23 up those boxes we just saw in the previous slide and
24 show a little bit more detail as far as 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 components are inside those boxes and how we
2 implement these trips.

3 This slide is titled Standard Reactor
4 Trips. What I mean by that is these are reactor
5 trips that utilize forward measurements per process
6 variable. The next slide will be talking about the
7 SPNDs specifically. So this is for all the trips
8 except for low DNBR and high linear power density.

9 So we start with the instrumentation --

10 MEMBER BROWN: Wait. Sorry. These, if
11 I go back to your list of functions, they all come
12 under this four-division architecture.

13 MR. SHOOK: Except for --

14 MEMBER BROWN: Except for the SPNDs.

15 MR. SHOOK: Except for the first two
16 trips --

17 MEMBER BROWN: Yes, I got that.

18 MR. SHOOK: -- listed in the table.
19 That's correct.

20 MEMBER BROWN: Okay.

21 MR. SHOOK: Okay, so we start with the
22 instrumentation. Again we have four redundant
23 process measurements of each process variable that
24 is being monitored. That signal comes into 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 SCDS, is conditioned, and then distributed primarily
2 to the Protection System but if the signal is also
3 used in other systems, we will send that signal out
4 to other systems, whether it be safety-related or
5 non-safety-related.

6 Coming out of the distribution module,
7 we then enter the protection system into the APU.
8 The APU is essentially, the easiest way to think
9 about it is it is a sub-rack within a cabinet. It
10 consists of IO modules and processor modules and
11 communication modules.

12 So the signal will come in to the APU
13 through the A-to-B converter card, get converted to
14 digital and then sends signal over the back playing
15 to the processor module where the logic is then
16 implemented. Again, any calculations that need to
17 be done to calculate a process variable are done and
18 then comparing that value to a set point threshold
19 comparison.

20 MEMBER BROWN: So the APU generates a
21 trip?

22 MR. SHOOK: A trip signal. That's
23 correct.

24 MEMBER BROWN: Particularly relative to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 your figure in the DCD and in your technical report.

2 MR. SHOOK: That's correct.

3 MEMBER BROWN: Is that trip an on/off
4 signal or is it a serial data stream? In other
5 words, it is like a dry contact only it is
6 electronic. A solid-state switch type dry contact.

7 MR. SHOOK: The signal itself is a one
8 or a zero. It is a digital --

9 MEMBER BROWN: Okay, let me go back.
10 Does it come on and stay on or is it a data stream?

11 MR. SHOOK: It comes on and stays on.

12 MEMBER BROWN: Okay, so just like a
13 relay contact, the thing says trip, contact closes,
14 it stays closed unless it is reset by some other
15 mechanism.

16 MR. SHOOK: That's correct. That's
17 correct.

18 MEMBER BROWN: Okay.

19 MR. SHOOK: So each division -- So again
20 you have four redundant process measurements. So
21 each division is going to be independently looking
22 at those redundant process measurements and
23 performing its own setpoint comparison. So out of
24 the APU, you get essentially a vote to trip out 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 each APU.

2 That vote to trip, then is then
3 distributed to all the other divisions to the ALUs.

4 And that is distributed over a network, a digital
5 communication network and we will talk more about
6 the means mechanisms, how that works, in the
7 appendix and some subsequent slides.

8 Each ALU then gets that vote to trip and
9 then does two out of four voting. And then again if
10 there is any subsequent logic downstream of that,
11 like for example a permissive logic that is done
12 downstream of the voting is implemented at that
13 point.

14 And so coming out of the ALUs -- and
15 ETLU is redundant within that division. And you
16 need both ALUs within that division to get a reactor
17 trip signal out of the protection system.

18 So you can see that coming out of that
19 And gate. The ALUs are also TXS sub-racks, as I
20 mentioned before. And you can see that the And gate
21 is a discrete electronic circuit.

22 One thing to note, I apologize. I
23 didn't mention this earlier is the first slide, we
24 are using this convention.

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 Most of the pictures in this
2 presentation are done using the figure legend that
3 is in the back. I think it is right in back of the
4 acronyms. It is actually the last slide, number 81.

5 And what the figure legend shows is the blue color
6 indicates that it is either electrical or electronic
7 equipment, discrete electronics where you actually
8 have dedicated circuits to configure the
9 functionality. You actually have to solder the
10 circuits together.

11 The red indicates that it is a
12 microprocessor-based programmable electronic
13 technology. And then what is not shown in this
14 slide but when you see the PACS, green indicates
15 non-microprocessor-based programmable electronic
16 technology.

17 So those terms, electric, electronic,
18 and programmable electronic are derived from there
19 is an IEC standard that defines those terms. In one
20 of the staff's questions, we had to sort of try to
21 define the technology and that was the basis of
22 using that terminology.

23 MEMBER BROWN: Okay, so the green could
24 be anything like PLDs or FPGAs --

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. SHOOK: That's correct.

2 MEMBER BROWN: -- if you wanted to. It
3 could be any of that family --

4 MR. SHOOK: That's correct.

5 MEMBER BROWN: -- of stuff.

6 MR. SHOOK: That's correct.

7 MEMBER BROWN: And you said earlier what
8 you all are using as PLD-based.

9 MR. SHOOK: That's correct.

10 MEMBER BROWN: Is that dictated in --I'm
11 trying to remember whether that was written down in
12 the DCD or the topical report. It just said, my
13 memory was it just says electronic something. I
14 forget what the word is. I have to go look it up.

15 MR. SHOOK: Electronic technology or --

16 MEMBER BROWN: Yes, electronic
17 technology or something like that. It didn't say
18 that you wanted to use something as simple as the
19 PLDs relative to the more complex or logic tables --

20 MR. SHOOK: Right.

21 MEMBER BROWN: -- PGAs.

22 MR. SHOOK: This level, I mean, you can
23 -- When you start to try classifying this different
24 technology, it is almost a fool's errand. But 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 we are trying to show at this level is that I have
2 got either a programmable technology and then there
3 is two different main flavors that it is either
4 microprocessor-based where I have this --

5 MEMBER BROWN: I understand that.

6 MR. SHOOK: Okay.

7 And then also the figure legend. The
8 skinny lines indicate hardwired signals and then the
9 thick black lines indicate a data bus connection.

10 MEMBER BROWN: You said the ALUs -- Gee,
11 I'm going to have to go back and look at that, too.

12 I thought they were non-microprocessor-based. They
13 were the -- They should have been green. That's
14 what I understood from reading the other stuff.

15 MR. SHOOK: No, they are implemented
16 using TXS microprocessors.

17 MEMBER BROWN: Oh, okay. I'm going to
18 take your word for it. You know. I don't. I'm
19 just reading.

20 MR. SHOOK: Okay.

21 MEMBER BROWN: My brain was ready to
22 explode anyway.

23 MR. SHOOK: So coming out of the And
24 gate, then we have an Or gate within each cabinet.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And you can see that there is three signals coming
2 in. One is the manual trip coming from the SICS.
3 Then you have the signal from Subsystem A. One of
4 the things I didn't show in this picture but you can
5 see in the Chapter 7 figures, in each division, the
6 protection system there is actually two subsystems.

7 And that is implemented for defense in depth and
8 diversity. So, what we do is we look at trips that
9 implement, that are designed to mitigate the same
10 type of event but utilize different diverse process
11 variables.

12 For example, we might have one trip on
13 pressurizer pressure and another trip on hot leg
14 pressure. And so we will implement those in the
15 different subsystems within the protection system.
16 So I am not showing Subsystem B here just because it
17 made the figure a little bit too complicated but you
18 can see that I showed the signal coming from the
19 other subsystem. And that gets Or-ed along with
20 Subsystem A, B and then the manual trip Or-ed at the
21 bottom coming out.

22 And then you can see also the manual
23 trip from the SICS goes to both the ALUs and also
24 bypasses the ALUs to the hard-wire Or-ed. 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 reason for that is there is some, 603 has a
2 requirement that says any, when you have a manual
3 initiation that you have to perform the same
4 functions that are performed with the automation.
5 And so for example we talked about isolating main
6 feedwater reactor trip. When I trip the reactor
7 manually, I still want it, I am required by 603 to
8 have it perform the same functions as the automatic
9 trip. So that is why we have to wire that signal
10 into the ALU. But we also bypass the ALUs from a
11 defense in depth and diversity perspective so we
12 have a hardwired means of bypassing all the
13 computers. That way, we can manually initiate that
14 trip to perform the function.

15 MEMBER BROWN: You said Subsystem B was
16 to do the purpose was to do what?

17 MR. SHOOK: The purpose of the two
18 subsystems is for functional diversity. So we have
19 a number of --

20 MEMBER BROWN: Well they are both TXS.

21 MR. SHOOK: They are both TXS.

22 MEMBER BROWN: And they are both
23 microprocessor-based.

24 MR. SHOOK: That's correct.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: They are both the same
2 hard-wire.

3 MR. SHOOK: That's correct. What we are
4 trying -- You know when you look at --

5 MEMBER BROWN: I would not, let me
6 characterize it another way, instead of letting you
7 beat around the bush.

8 When I looked at your figure in the DCD
9 and in the I think it is replicated in the topical
10 report also, I viewed more not as a diversity issue
11 but more as an independence issue. In other words,
12 you have got a network feeding all the ALUs from
13 ATUs A1 and A2, Division 1 to A1 and A2, in Division
14 2, etcetera. You have got another network shown for
15 B1 and B2 and its ALUs separated so that you have
16 functionally you are feeding all your measurement
17 information which I guess goes to all the APUs, I'm
18 hoping that is the case, that the SCDC feeds their
19 one-fourth of the plant measurement data as it is
20 stated in the DCD, it goes to all the APUs in that
21 division.

22 MR. SHOOK: No, that is not quite --

23 MEMBER BROWN: Well, it is not broken
24 out. It just says each division gets one-fourth of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 all the measurement signals.

2 MR. SHOOK: That is correct, yes.

3 MEMBER BROWN: Okay. And there is no
4 definition of what goes where or how they are broken
5 out inside at the division level. I kind of assumed
6 they all went to all of them if you were going to
7 maintain an independence approach to this. Because
8 otherwise you have gotten one bus feeding across
9 everything. And so having the two subsystems
10 actually, either one of those subsystems can provide
11 the logical Or -- is that what it is -- yes, down
12 here for the final trip signal.

13 I don't understand the diversity issue
14 and that functional diversity is not explained in
15 the DCD as to what you are trying to achieve.

16 MR. SHOOK: Right.

17 MEMBER BROWN: That's missing right now.

18 MR. SHOOK: Well I think it is -- we do
19 talk about it in the topical report, the
20 protectional --

21 MEMBER BROWN: You say functional
22 diversity. That's it.

23 MR. SHOOK: Yes.

24 MEMBER BROWN: Two words and you don't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 explain what it means.

2 MR. SHOOK: Okay. We inherited --

3 MEMBER BROWN: The topical report --

4 MR. SHOOK: When we inherited the design
5 from European, the Europeans refer to this as
6 functional diversity but NUREG-6303 refers to it as
7 signal diversity. So in the U.S. connotation, in
8 the D3 Technical Report and the Protection System
9 Technical Report refer to it specifically as signal
10 diversity.

11 But the general idea -- I mean, you are
12 right to an extent. So let's start with the
13 subsystems themselves.

14 MEMBER BROWN: Well you don't have to go
15 through that.

16 MR. SHOOK: Okay.

17 MEMBER BROWN: My point being is that if
18 you want to achieve that functional diversity, you
19 have got to define what you mean by it and you have
20 got to write it down in the DCD so that people who
21 go off to design it can know what they are doing,
22 what you are trying to achieve. If you don't define
23 it, well it is just like the SCDS. If you don't
24 define what the criteria are for which ones are

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 under the safety and which ones are not, and which
2 ones have their own PAS, then who knows? They can
3 start combining this stuff.

4 MR. JACKSON: This is Terry Jackson. It
5 may be helpful and I think AREVA may be getting to
6 the discussion on the diversity a little bit later
7 on. But I don't think that this functional
8 diversity is actually credited for defense in depth
9 diversity between, for a common cause failure of the
10 protection system.

11 MEMBER BROWN: Well that's okay. What I
12 am trying to do is ensure when I look at this system
13 that number one, we have got an independent set of
14 systems such that based on without having a great
15 knowledge of the network you have got feeding across
16 A1s and -- You know, A1s and A2s have two different
17 networks at least in the DCD. That is the only
18 means of achieving independence. Otherwise, you
19 have got everything coupled when you are sending it
20 off to the voting level.

21 MR. SHOOK: I will say that the
22 subsystems are not relied upon to achieve
23 independence between divisions.

24 MEMBER BROWN: Oh, okay. Well that is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 going to be interesting. I couldn't figure it out
2 otherwise.

3 MR. SHOOK: Okay. The reason for the
4 subsystems is to implement a measure of diversity
5 and functionality that is within the design but is
6 not credited to meet BTP-19.

7 MEMBER BROWN: Okay. I guess I
8 misunderstood and other than when I read the words,
9 I interpreted something more extensive to it. And
10 in reality, that is not defined anywhere as to how
11 much --

12 MR. SHOOK: It is defined. It is within
13 the technical report and we can get you to the
14 specific section where it talks about that. But
15 there are rules associated with how we allocate
16 functions between the different subsystems.

17 MEMBER BROWN: I would like to know
18 where those are.

19 MR. SHOOK: Yes, we can get that to you.
20 Okay, so let's go to the next slide then, looking
21 at the SPND-based reactor trips. So the main
22 difference with the SPND versus all the other
23 process parameters is that in this case the process
24 variable being neutron flux within the core is not 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 homogenous process variable, meaning that it is
2 spatially dependent upon which location you are at.

3 So what we do here is we have 72 SPNDs located
4 axially and radially throughout the core, measuring
5 flux at those various locations.

6 And for the way that the DNBR and HLPD
7 functions are constructed is that you need all 72
8 measurements within each of the four divisions in
9 order to recreate that neutron flux. You can kind
10 of think about you are essentially sampling the flux
11 at different locations and you need to get all the
12 measurements in each division to meet your
13 redundancy requirements.

14 So it is different than the standard
15 process variable to the trip. So the way that we do
16 this, the way we accomplish the routing of all 72
17 signals to all four divisions of Protection System,
18 we first acquire 18 signals, 18 of each of the SPND
19 signals into the four divisions of the SCDS. So you
20 can see here that I have got 18 coming into Div 1,
21 18 coming into Div 2, 3 and 4 and so forth.

22 And then those signals are then
23 distributed via hard-wire connections to all four
24 divisions of the protection system. So we are just

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 sending those signals.

2 So you can see here that Div 1 of the
3 Protection System is receiving 18 signals from Div 1
4 of the SCDS, 18 from Div 2 of the SCDS, Div 3, and
5 Div 4. And that's how we get all 72 signals within
6 the Protection System.

7 MEMBER SKILLMAN: Question, please.
8 Jeremy, I'm presuming that the 18 are quadrant-
9 symmetrical. Is that accurate?

10 MR. SHOOK: I don't know off the top of
11 my head.

12 MEMBER SKILLMAN: So there are 72 during
13 the which?

14 MR. SHOOK: They are not -- No, they are
15 not quadrant-symmetrical.

16 MR. DOYEL: This is Chris Doyel from
17 AREVA. Each 18 is spread over all four quadrants.
18 Okay?

19 MEMBER SKILLMAN: Okay.

20 MR. DOYEL: So that it is not quadrant-
21 specific like ES.

22 MEMBER SKILLMAN: Is it quadrant-
23 symmetrical.

24 MR. DOYEL: Symmetrical.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER SKILLMAN: I would think the
2 answer is yes.

3 MR. DOYEL: No.

4 MEMBER SKILLMAN: It's not?

5 MR. DOYEL: No, there are symmetrical
6 pairs. Okay? In other words, but what you are
7 asking is not true for our design.

8 MEMBER SKILLMAN: It's not accurate.

9 MR. DOYEL: It is not accurate.

10 MEMBER SKILLMAN: Okay, let me go a
11 little bit further.

12 What is the basis for using an SPND for
13 an RPS function? Are the SPNDs qualified for safety
14 function?

15 MR. SHOOK: They are.

16 MEMBER SKILLMAN: Oh, they are?

17 MR. SHOOK: Yes.

18 MEMBER SKILLMAN: And for each of the
19 strings, for each of the 72 strings, is there a
20 planar count for the 18?

21 MR. SHOOK: There are 12 strings and
22 there are six SPNDs per string. And so those
23 strings are located --

24 MEMBER SKILLMAN: Twelve or 18?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: What's that? There is 12
2 strings and then there is six SPNDs within that
3 string, for a total of 72.

4 MR. PHAN: Just a clarification. The
5 string he is referring to, we call those fingers --

6 MR. SHOOK: I'm sorry, finger. Yes.

7 MR. PHAN: -- in our documentation.

8 MEMBER BROWN: They go straight, I mean,
9 they are in one line.

10 MR. SHOOK: That's right.

11 MEMBER BROWN: It's not like one string
12 or finger has one in this quadrant and one 60
13 degrees away and another one. That would be a
14 nightmare. So this is just like one big detector
15 line, thimble that you feed through and they are all
16 in there.

17 MR. SHOOK: Right.

18 MEMBER BROWN: One string.

19 MR. SHOOK: But you have different
20 detectors. They are sort of stacked.

21 MEMBER BROWN: I understand that. You
22 have got six detectors within that one finger of
23 stuff that you stuff in.

24 MR. SHOOK: That's correct.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: And then you have got 12
2 of those located circumferentially around the core.

3 MR. SHOOK: That's correct.

4 MEMBER STETKAR: There is a figure 4.4-8
5 in the FSAR that shows the distribution, if I
6 remember right. There is a couple of figures I
7 remember when we were going through Chapter 4. It
8 sort of makes sense when you stare at it
9 geometrically. It is difficult to describe it
10 without those pictures in front of you.

11 MEMBER SKILLMAN: You have answered my
12 question. Thank you.

13 MR. SHOOK: Okay. Okay and then once we
14 get all 72 signals in the Protection System, it is
15 basically the same design on out. Go to the next
16 slide.

17 So here we are down at the reactor trip
18 device level. So you can see once the Protection
19 Systems sends, each division sends a signal out, you
20 can see here this is the actuation device during the
21 trip.

22 Up at the top you have the reactor trip
23 breakers. There is four breakers and each breaker
24 gets a signal from its own division. And those are

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 implemented in one out of two, taken twice logic.

2 Down below, we have the trip contactors.

3 Those again those are located within the CRDCS
4 system and those are implemented in a two out four,
5 straight two out of four logic.

6 So you can see we have voting at the ALU
7 level. We also have voting down here. And the
8 result of that is, is basically we get the trip when
9 we need the trip and we reduce the probability of
10 spurious actuations.

11 MEMBER BROWN: If only for the -- Well,
12 with the circuit breakers, you can trip one and two
13 and it won't scram. Is that correct?

14 MR. SHOOK: Yes, that is correct. So it
15 has to be the right pair.

16 MEMBER BROWN: Whereas if I trip two
17 contactors, you will always scram.

18 MR. SHOOK: That is correct.

19 MEMBER BROWN: That was the best I could
20 do walking through.

21 So in reality, the trip breakers are not
22 really a full scram protection mode similar to the -
23 - In other words, if I get two out of four channels
24 tripping, I won't trip, if they are the wrong

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 channels for the breakers the contactors will.

2 MR. SHOOK: That's correct.

3 MEMBER BROWN: That is why I asked the
4 question about you talked about they were the
5 diverse means. They looked to me like they were the
6 primary means and the other ones are just kind of
7 there. That's my own personal opinion.

8 MR. SHOOK: Yes. I mean, what I meant
9 to say, the point I was trying to make is that they
10 are, from the Protection System you have
11 fundamentally diverse means of tripping the reactor
12 and both are safety related and both meet single
13 failure criteria. But you are correct that in terms
14 of different combinations may not get you the trip
15 for the trip breakers, where you always get two out
16 of four in the trip contactors.

17 MEMBER BROWN: So the true safety grade
18 stuff is the trip contactors.

19 MR. SHOOK: They are both safety grade.

20 MEMBER BROWN: I'm just saying the only
21 ones that are really reliable are the trip
22 contactors. If you trip two divisions, you will get
23 them to scram. If you trip two circuit breakers
24 that is the wrong ones, they won't scram. So those

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 are the ones I would look at. I don't -- I just --
2 It is what it is. It meets the requirements.

3 MR. SHOOK: Okay, yes.

4 MEMBER BROWN: So you can go on.

5 MR. SHOOK: Okay. So let's go to the
6 next slide, 16. Okay, so now we are going to start
7 talking about some of the key points. The first one
8 we look at, redundancy. For the standard reactor
9 trips, as I already mentioned, we have four-fold
10 redundancy for measurements, signal condition at the
11 APU level for setpoint comparison. For the manual
12 actuation, we also have four trip buttons in the
13 Control Room and RSS.

14 At the ALU level, we actually are eight-
15 fold redundant and kind it is two points. First is
16 at the division level we have four divisions and
17 that is where we are taking credit for single
18 failure. The fact that we have redundant ALUs
19 within each division that you have to get an And for
20 both to get a trip, is to reduce potential for
21 spurious actuation to improve plant availability.
22 So there is two different reasons there.

23 The other piece is that if I only have
24 one ALU per division, if I took that out of service,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I would be fairly limited in terms of the
2 operability from a tech spec perspective. So having
3 the two ALUs allowed me to take one out of service.

4 The other one is still operating in much more
5 greater operational flexibility from that
6 perspective. And all your voting is two out of
7 four.

8 And as we just talked about, we have
9 four-fold redundancy for the trip breakers. Again,
10 one out of two taken twice logic and then the trip
11 contactors for two out of four.

12 Okay, moving on to slide 17, the
13 redundancy for the SPND-based trips. As I mentioned
14 earlier, the SPNDs are not redundant in the typical
15 sense of having four redundant measurements of a
16 homogenous process variable, such as pressurizer
17 pressure or pressurizer level.

18 In this case, we were monitoring a
19 spatially-dependent variable neutron flux inside the
20 core. You know, the benefits of doing this design
21 are that anytime you can measure more closely the
22 parameter of interest that you are interested in is
23 better, both from a safety and an operational
24 perspective. And one of the things 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 specifically Clause 6.4 of IEEE 603 says that you
2 should do that because again, that is just good
3 design practice. And also from a margin standpoint
4 and a safety standpoint allows you to move a lot of
5 the uncertainties and assumptions that are baked
6 into a traditional safety analysis when you only can
7 look at Excore instrumentation.

8 MEMBER BROWN: So it allows you to
9 operate at a higher power.

10 MR. SHOOK: That's correct.

11 MEMBER BROWN: For whatever flow
12 condition, configuration you have.

13 MR. SHOOK: That's correct.

14 MEMBER BROWN: Even though you don't
15 theoretically meet the strict interpretations of
16 independence.

17 MR. SHOOK: That's correct.

18 MEMBER BROWN: And that's the only
19 protection function that will take care of you under
20 those circumstances.

21 MR. SHOOK: No.

22 MEMBER BROWN: If that is the basis for
23 you allowing yourself to operate at a higher power,
24 then those two functions that you have identified

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 are the basis for ensuring that you can operate
2 those safely.

3 MR. SHOOK: Yes, that's correct.

4 MEMBER BROWN: I just wanted to rephrase
5 it. That's the way I understood it.

6 MR. SHOOK: That's correct.

7 MEMBER BROWN: And they are not strictly
8 independent, based on the strictest interpretation.

9 MR. SHOOK: Yes, I think you know, we
10 spent a lot of time discussing with the staff as far
11 as how to interpret this. I think from our
12 perspective I think the ultimate goal in what you
13 are trying to accomplish in designing the function
14 is high reliability. And so when you look at the
15 way the commercial nuclear industry typically does
16 that, is through single failure criterion and then
17 redundancy and independence typically fall out of
18 that.

19 So what we are saying here is the basis
20 of our argument is okay, we don't have redundant
21 measurements because it is not a homogenous process
22 variable like pressurizer pressure. So I can't just
23 put four and say they are all the same because they
24 are not.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So what we are saying is well even
2 though we don't technically meet redundancy
3 independence, we still meet single failure criteria
4 and that is the basis for our -- I'm sorry --
5 alternative request.

6 MEMBER BROWN: So as long as a single
7 failure can't common cause the problem with all your
8 all four divisions.

9 MR. SHOOK: That's correct, which we
10 demonstrate. Yes.

11 MEMBER BROWN: How did you demonstrate
12 that?

13 MR. SHOOK: Well, through -- So there is
14 a couple of things we have to look at. One is
15 single failures in instrumentation itself, the SPND,
16 which we account for that not through again
17 redundancy but for detectible failures, the
18 algorithm actually goes through and selects more
19 conservative setpoints up until six and then after
20 six failed SPNDs we actually automatically trip the
21 reactor.

22 And then for a non-detectable failure of
23 an SPND, if it is an in-range failure, that is
24 assumed in the safety analysis, which is currently

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 an open item, which our safety analysis folks have
2 to go back and reanalyze those events, assuming a
3 single undetected failure.

4 MEMBER BROWN: Since every detector goes
5 to every division, how do you ensure that no single
6 detector failure can compromise the performance of
7 all four divisions at the same time?

8 MR. SHOOK: Oh, I'll get to that when we
9 talk about independence.

10 MEMBER BROWN: All right. Fire away.

11 MR. SHOOK: Okay. So I think I actually
12 covered most of the points in this slide. If there
13 isn't any other questions, I'll move on.

14 Okay, so now we are going to go through
15 independence. And what I would ask you to do is if
16 you go back to slide 13, and I am going to be
17 talking about every point on this slide where either
18 we go safety to non-safety or between the redundant
19 divisions in the Protection Systems and I will just
20 point these out.

21 So the first point we are going to talk
22 about is the signal coming out of the signal
23 distribution module going to other I&C systems. In
24 some cases, those are going to safety systems within

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 same division so there is no strict independence
2 needed. In other cases --

3 MEMBER BROWN: What signal are you
4 talking about right now, from an APU?

5 MR. SHOOK: No. So the first signal I'm
6 talking about is this one.

7 MEMBER BROWN: Oh, out of the SCDS.

8 MR. SHOOK: Right. So coming out of the
9 SCDS, we will send signals to other systems, either
10 safety or non-safety. And those non-safety
11 interfaces, we have to demonstrate independence for.

12 The second point is to the service unit
13 from the MSI. The third point is to the QDS from
14 the MSI.

15 MEMBER BROWN: But it gets to the
16 service unit through the APU.

17 MR. SHOOK: That is correct. Yes.
18 Basically the APU or ALUs send all this information
19 to the MSI. And then from there, you are
20 essentially sending it to three non-safety places.

21 MEMBER BROWN: Okay.

22 MR. SHOOK: So we have to demonstrate
23 how we make that independence.

24 MEMBER BROWN: And then you are going to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 division to division.

2 MR. SHOOK: And then we will talk about
3 the interdivisional communications, yes.

4 MEMBER BROWN: Go ahead.

5 MR. SHOOK: And then on the next slide,
6 14, we will talk about how the sharing of these
7 signals to the hardwired signals to all four
8 divisions, how that demonstrates independence as
9 well.

10 Okay, so the first point on slide 18,
11 this is on the SCDS output to other I&C systems, the
12 purpose for this safety to non-safety interface is
13 basically if I need to send that sensor signal to
14 another non-safety system to implement another
15 function, so for example, pressurizer level, I need
16 to send that to the PAS to perform automated
17 pressurizer level control. I also send that to the
18 Protection System for a reactor trip.

19 So in this case, sending the signal to
20 the PAS is, we do that via hardwired interface
21 because again at this point everything is hardwired
22 four to 20 outputs. And to provide for
23 independence, we implement physical separation. So
24 the PAS cabinets are physically separated from 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 Protection System cabinets. The non-safety cable is
2 separated from the safety-related cable. And for
3 electrical isolation, the distribution module itself
4 has up to four isolated qualified outputs. So a
5 failure of the non-safety system from an electrical
6 perspective can't come back into the SCDS and impact
7 its operation.

8 MEMBER BROWN: Those are analogue
9 outputs?

10 MR. SHOOK: That's correct.

11 MEMBER BROWN: This is all analogue at
12 this point.

13 MR. SHOOK: This is all analogue.

14 MEMBER BROWN: It doesn't get converted
15 until you get into the APUs --

16 MR. SHOOK: That's correct.

17 MEMBER BROWN: -- and wherever they go.

18 MR. SHOOK: That's correct. These are
19 all four to 20 signals, four to 20 milliamp signals.

20 Okay?

21 MEMBER BROWN: Do you put any criteria
22 on the qualified, what did you call them, qualified
23 isolation devices?

24 MR. SHOOK: We committed in the FSAR to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 meet the requirements at IEEE 384, which defines the
2 separation and independence requirements for
3 specific, the details of the electrical, you now,
4 how much separation you need in voltage
5 qualification and so forth.

6 MEMBER BROWN: That is a somewhat
7 generic answer. I mean, these are simple, you said
8 four to 20 milliamp signals.

9 MR. SHOOK: Right.

10 MEMBER BROWN: Those are easy to
11 isolate.

12 MR. SHOOK: Yes. I mean, on the
13 distribution module, there is isolation. You know,
14 each circuit is electrically isolated. And the
15 criteria for how that, the specific criteria as far
16 as how far apart they need to be and the specific
17 testing that gets done, that is all in accordance
18 with IEEE 384.

19 MEMBER BROWN: From a physical
20 separation?

21 MR. SHOOK: Yes.

22 MEMBER BROWN: I'm talking about
23 electrical isolation, not necessarily physical
24 separation.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So you don't provide any other, just
2 meet whatever the 384 says for the electrical
3 isolations?

4 MR. SHOOK: Well again, the distribution
5 module itself includes isolators on the module. So
6 when we split out the four signals coming in from
7 the one, those outputs are all isolated from each
8 other.

9 CHAIR POWERS: Chris has some comments.

10 MR. DOYEL: This is Chris Doyel from
11 AREVA. The isolation outputs coming out of an SND
12 module in TXS are qualified to Reg Guide 1.75
13 criteria.

14 MR. SHOOK: Which is 384.

15 MR. DOYEL: Which is, yes, it is
16 essentially 384.

17 MEMBER BROWN: That is kind of
18 meaningless. What is in there? If it is in the TXS
19 device, what the hell are they? Are they diodes or
20 are they microprocessor-based controlled things that
21 are getting -- I thought these were in the SCDS and
22 didn't have anything to do with the TXS system.

23 MR. SHOOK: Yes, these are all discrete
24 electronics.

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 BROWN: That's what I thought.

2 MR. SHOOK: Yes.

3 MR. DOYEL: And TXS has discrete
4 electronics. These modules are an SAA1 module and
5 an SMD1 module --

6 MEMBER BROWN: I have no idea what those
7 are.

8 MR. DOYEL: I understand. But basically
9 what they are is analogue signal processing modules.
10 And within the SND module, they create isolated
11 output signals that you could send to another
12 safety-related division or to a non-safety system.

13 MR. SHOOK: I guess the short answer is
14 we don't have the specifics, the actual circuit
15 design to go through that today but that is
16 something we can get to you if you need it.

17 MEMBER BROWN: I would like to have some
18 idea of what this -- how it is defined so that you
19 don't get a spectrum. Or do you get stuff that, you
20 know, somebody else interprets that this is okay and
21 it doesn't necessarily meet everybody else's
22 interpretation.

23 I mean, you ought to have some idea of
24 what these -- if they have got these, you ought 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 know what it is and if you are not going to specify
2 them. If you specify them, then you know what you
3 are getting. If you don't, then you don't.

4 MR. SHOOK: Well again, the details of
5 the specification would be in accordance with IEEE
6 384. I don't know -- I can't recall the specifics
7 of that --

8 MEMBER BROWN: Go on.

9 MR. SHOOK: Okay. Okay, next slide.
10 Okay, this is for the service unit. So, the purpose
11 of this interface is to allow the Service Unit to be
12 able to connect to the Protection System via the MSI
13 for system testing and maintenance. This is a
14 database communication and the means of independence
15 is between the MSI and the Service Unit, we an
16 isolated key switch, which there is no software, no
17 microprocessor as part of this system. It is a
18 straight electrical device. It is we normally
19 operate with the service unit disconnected from the
20 Protection System. And it is disconnected via key
21 locked switch. It is not intended to be
22 continuously connected from an operational point of
23 view.

24 When we do connect it, whether for

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 periodic or corrective maintenance, the switch
2 physically restricts SU, connecting only one
3 division at a time. So you would only -- You would
4 still have the other three divisions to be
5 unaffected by any potential failures coming from the
6 service unit.

7 Okay, moving to slide 20. The next
8 point of safety/non-safety is the QDS interface. So
9 the QDS is a graphical display located on the SICS
10 in the Main Control Room. However, it is
11 technically non-safety-related and as such, we
12 provide independence measures between the Protection
13 System and the QDS.

14 So the purpose is to display information
15 to the operator on SICS when they are operating at
16 that location. It is a data interface. To provide
17 for independence, again, physical separation. We
18 separate the cabinets physically. Electrical
19 isolation is performed via use of a fiber optic
20 cable between the MSI and the QDS. And for
21 communications independence, we physically restrict
22 dataflow to a one-way communication.

23 And what see you here on this drawing on
24 the right, you have got the MSI, the Monitoring

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 Service Interface, and then that is connected to
2 this Electrical Optical Converter. So here I go
3 from an electrical signal to an optical signal.

4 And then between the two Electrical
5 Optical Converters, I physically only connect a
6 unidirectional, you know, your transmit path out
7 from the one converter to the other. For optical,
8 you can't send signals on the same line. You know,
9 you can't transmit and receive in the same line.
10 They actually have to be two separate transmit and
11 receive lines. So when we only connect one, it is
12 physically impossible to get signals back from the
13 other device.

14 So once we get to the other Electrical
15 Optical Converter where they convert back to
16 electrical signal, then we communicate to the QDS.

17 MEMBER BROWN: Is that defined like that
18 as you just stated it in the DCD?

19 MR. SHOOK: Yes. Yes, we can again get
20 you those sections.

21 MEMBER BROWN: I'd like you to show me
22 where that is.

23 MR. SHOOK: Okay. Okay, next slide.

24 So this is our PICS interface. So, you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 know again this is where the operator would be
2 spending most of their time. And here it is again
3 the same basic purpose as the QDS. We want to send
4 information from the Protection System to the PICS
5 for the operators awareness of what is going on in
6 the Protection System. It is a data interface and
7 it is the same basic means of providing independence
8 as we just showed for the QDS. So in this case the
9 only difference is we have gateways in the middle.
10 But the gateways are not credited for independence.

11 It is actually the electrical optical converters
12 with the fiber optic cable and the transmit only
13 path from going out from the MSI to the gateways
14 that is connected and provide for independence.

15 Okay. Slide 22 is the independence
16 between redundant divisions, specifically at the APU
17 to ALU interface. So this is the only point in the
18 design that we share information between divisions.

19 The purpose is to send reactor trip votes from each
20 division's APU to all four divisions' ALUs to allow
21 for voting.

22 This is a data interface and means of
23 independence again we have three main points. We
24 provide for physical separation in the divisions as

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we showed in the Section 7.1 figure. They are
2 physically separated into four different buildings.

3 The electrical isolation, the connections on these
4 networks are done via fiber optic cable. So you
5 know, any electrical fault won't transmit to the
6 other division.

7 And then for communication independence,
8 there is a couple main points as far as the design
9 of the platform that are provided to ensure for
10 communication independence. The first is, and I
11 will be referring to this drawing on the right to
12 kind of help explain some of these concepts.

13 The green box you see at the top it is
14 noted SVE1 and that is the processor module. So that
15 is the function processor performing all your logic
16 associated with that device, whether it is an APU or
17 an ALU.

18 And then the blue box on the bottom is
19 your communications module. That is entitled the
20 SL21. And then you and see the SLLM is essentially
21 your electrical optic converter, just like we showed
22 with the previous drawing.

23 So the main points for which we use to
24 credit communications independence, first of all 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 separate the processing of the safety function
2 versus the communications processing via the
3 network, so you can see that the SL21 is performing
4 all the communications functions; whereas, the SVE1
5 is performing all the actual logic, whether it is
6 the setpoint comparison two out of four voting.

7 We separate coming out of the SVE1, a
8 separate send and receive paths so you don't have to
9 worry about necessarily collisions or lost data on
10 those paths.

11 Both the SVE1 and the communications
12 module operate in a cyclic manner. So that means
13 they are in a fixed cycle time. They operate once
14 you establish what we call the frame rate for the
15 processor, whether it could be 25 milliseconds, 50
16 milliseconds. It always executes at that same rate,
17 once it has been established.

18 And more importantly, the processors are
19 asynchronous. So the operation of the SVE1 is
20 completely independent from the operation of the
21 SL21. So if there is a network failure, the SVE1
22 can continue to perform its operations independently
23 of the network.

24 And then lastly there is the token

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 passing principle. So these networks are
2 implemented using a PROFibus network or protocol.

3 And that token passing principle at
4 essentially kind of a high level the way it works is
5 that each of the communication modules on the
6 network, there is a token that is passed between
7 them and they can only communicate when they have
8 possession of that token. So for example, let's say
9 the APU has the token. It is going to pull to get
10 its messages and then transmit its messages. And
11 when it is completed as operations, the token gets
12 passed then to the next device on the network and it
13 just keeps coming around in that manner.

14 So all those taken together provide for
15 a very deterministic behavior for the networks and
16 that what allows us to demonstrate independence
17 between the divisions for those APU or ALU networks.

18 MEMBER BROWN: I asked you before -- I'm
19 going to conclude or ask the SVE1 would be like an
20 APU. Right?

21 MR. SHOOK: The SVE1 is part of the APU.
22 So if you think of the APUs in the entire sub-rack
23 to include the SVE1, which is this primary, that is
24 the primary card on that sub-rack and then it would

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 include the communication modules as well as
2 any I/O modules that are a part of that sub-rack.

3 MEMBER BROWN: Okay well let me get back
4 to my other question. When I asked about the output
5 that you calculated a trip, is that a constant value
6 on or off?

7 MR. SHOOK: It is constant value on or
8 off.

9 MEMBER BROWN: On or off?

10 MR. SHOOK: Yes.

11 MEMBER BROWN: It's like a dry contact.

12 MR. SHOOK: That's correct.

13 MEMBER BROWN: Okay, which doesn't
14 involve any serial data, I mean, it is just an
15 on/off signal. And then you said you send that to
16 an ALU where it gets voted on.

17 MR. SHOOK: That's correct.

18 MEMBER BROWN: And if I send that same
19 on/off signal to another division, do you change its
20 character when you send it to another division?

21 MR. SHOOK: No. It's the same value.

22 MEMBER BROWN: Well this implies that --
23 It says constant busload, designated messages, which
24 imply I have got a front-end address, and I have got

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 a back-end address, and I got all other garbage that
2 is floating along and I am sending this as a serial
3 data stream, as opposed to if I am talking constant
4 busload as opposed to a dry contact, tells the next
5 division I am on or off. That's very clean.

6 If I am sending a structured set of
7 data, then I have just set myself up for corrupting
8 every other microprocessor I have got in each
9 division. Whereas, if I have got a nice dry
10 contact, which is very clean isolable piece of
11 signal, you know an optical coupling, as you showed
12 in the pictures, your optical logic OLMs or
13 something like that. You almost had me convinced
14 that you didn't have any difficulty, until I saw
15 this pictures, which makes it sound like now I have
16 got this nice bus that is being controlled with all
17 this nice data on it that has flown over with
18 headers and footers, and little pieces in-between,
19 and cyclic redundancy checks and all kinds of
20 checks. So as soon as you do that, you have to
21 figure out some way to say okay, I can corrupt every
22 other one, and once they, if all those other
23 processors lock up, how do you scram?

24 So I dropped that thought process based

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 reading the DCD and the Technical Report and now
2 it is back on the table again.

3 MR. SHOOK: Let me address that.

4 MEMBER BROWN: So this same issue rises
5 on more than just your project.

6 MR. SHOOK: Right. I may not have quite
7 understood --

8 MEMBER BROWN: It doesn't matter whether
9 it is optical or not. That is electrical isolation.

10 MR. SHOOK: Right.

11 MEMBER BROWN: It's not data isolation.

12 MR. SHOOK: Right.

13 MEMBER BROWN: It's not corrupt data
14 isolation in any way, shape, or form.

15 MR. SHOOK: Right.

16 MEMBER BROWN: You are postulating that
17 there is no way I will ever get corrupt data that
18 can go from Division 1 APU to all the other ALUs.
19 It is sent to all four of the division voting units.

20 MR. SHOOK: No, we are not saying that.

21 What we are saying is that the mechanisms that are
22 inherent in the platform allow for compensation,
23 compensatory measures that will handle that type of
24 --

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 BROWN: That's what I just said.

2 MR. SHOOK: Right.

3 MEMBER BROWN: And you are depending on
4 software to protect you from your software.

5 MR. SHOOK: Well I mean --

6 MEMBER BROWN: Your data transmission.

7 MR. SHOOK: Yes.

8 MEMBER BROWN: Your software to figure
9 out whether it works or not.

10 MR. SHOOK: That's correct.

11 MEMBER BROWN: And that's a hard spot.

12 MR. SHOOK: Well you know, let me kind
13 of walk through how this works. I mean from a --
14 Let's say for example Division 1 sends data out,
15 sends its vote to trip to all four divisions and
16 that message gets corrupted through that process.
17 The other processors receiving that data perform
18 checks on the data.

19 MEMBER BROWN: I understand that.

20 MR. SHOOK: So and once -- And if they
21 detect an error, you know, the system -- We are
22 required to design the system to be fail-safe. So
23 if we detect an error in that data packet, that data
24 is flagged by the software and then the voting logic

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 is then --

2 MEMBER BROWN: I understand that. Okay?

3 I understand that but you can't guarantee that it
4 will not be corrupted and not be detected. You
5 can't guarantee that it can be detected.

6 And as soon as you do that, I mean, if
7 it corrupts Division 1, then it will corrupt
8 Divisions 2, 3, and 4.

9 MR. SHOOK: Can't guarantee that it
10 won't be detected. I'm not sure I agree with that.

11 MEMBER BROWN: Well, other people have
12 not agreed either but they have been able to
13 demonstrate that if all the function processors lock
14 up in the voting units, that they scram.

15 MR. SHOOK: Well again, you know if we
16 do have -- Again, there is a number of different
17 mechanisms. There are two pieces. First of all,
18 the primary protection system is designed to fail-
19 safe, based on detectible faults. Okay?

20 So, based on all the faults that we
21 analyzed the system for, the system will fail to
22 trip the reactor --

23 MEMBER BROWN: I understand. You are
24 assuming you can identify all the faults and all the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 corrupt data packages.

2 MR. SHOOK: Right. And so in case we
3 haven't figured out that there is a fault after we
4 have analyzed the system, okay, there might be a
5 fault. Because you are right. You probably can
6 never postulate every single potential fault but
7 that is why we have a DAS, so the DAS is there for
8 that backup purpose.

9 MEMBER BROWN: The DAS doesn't take care
10 of every function. You don't have a DAS for every
11 one of your protection functions.

12 MR. SHOOK: No, but the DAS to meet the
13 guidance of BTP 719, the DAS meets Part 100 limits
14 for all the design-based events enumerated in
15 Chapter 15.

16 So while we don't necessarily have a
17 one-for-one function comparison between the two
18 systems, we have demonstrated for all the events
19 that are enumerated in Chapter 15 that we provide
20 adequate backup protection within the DAS to meet
21 Part 100 elements that have been specified in BTP
22 19.

23 MEMBER BROWN: You have a single packet
24 of corrupted data that gets through to your defenses

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 on all four processors, all four voting units. You
2 don't have a DAS that will cover that. I mean, you
3 have locked them all up.

4 MR. SHOOK: No, that's not true.

5 MEMBER BROWN: Sure it is.

6 MR. SHOOK: The DAS is completely
7 independent from the protection system.

8 MEMBER BROWN: I understand that. I'm
9 not saying it will lock up the DAS. I know you can
10 manually go back and do that but you are automatic
11 system is toast.

12 MR. SHOOK: Well the DAS is not an
13 automated system.

14 MEMBER BROWN: It can be but it is not
15 getting the same data.

16 MR. SHOOK: It is getting the same
17 process variables.

18 MEMBER BROWN: That's the input.

19 MR. SHOOK: Right.

20 MEMBER BROWN: I mean, it is not taking
21 the outputs of these APUs.

22 MR. SHOOK: No, no.

23 MEMBER BROWN: And I'm just saying your
24 normal protection system right now is set up such

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 a single packet of corrupted data can lock up
2 all four of your voting units.

3 MR. SHOOK: Again, the system is
4 designed such that all detectable failures, the
5 system is designed to fail to a safe state based on
6 all the technical failures.

7 MEMBER BROWN: If you can find all the
8 data packages that could possibly do anything, that
9 would be one thing, but you can't.

10 MR. SHOOK: Well, I mean that is --

11 MEMBER BROWN: We are going around in
12 circles right now.

13 MR. SHOOK: Right.

14 MEMBER BROWN: So all I'm telling you
15 right now, I'm looking for some way that says if all
16 four of those processors lock up, how do you scram
17 automatically?

18 MR. SHOOK: Okay. Well, that's a
19 different question. If all four processors lock up,
20 each processor has a hardware-based watchdog timer
21 that will look at --

22 MEMBER BROWN: That's not discussed in
23 the DCD.

24 MR. SHOOK: It's discussed in the PS

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Technical Report.

2 MEMBER BROWN: It's not in the technical
3 report. I have keyworded watchdog timer and WDT and
4 didn't find it.

5 MR. SHOOK: Okay.

6 MEMBER BROWN: So either that or I
7 keyworded the wrong thing.

8 Now it is in the -- It does respond in
9 the TELEPERM Technical Report, which I have not
10 looked at.

11 MR. SHOOK: Right.

12 MEMBER BROWN: But I have no idea how
13 that works. I don't know -- if there is no
14 description of how the watchdog timer is going to
15 protect you in the ALU if all those ALUs lock up.
16 But if it does, then there is a method for
17 understanding why this would be okay.

18 MS. SLOAN: Jeremy, this is Sandra.
19 What I would suggest is we take the follow-up action
20 to identify --

21 MEMBER BROWN: That's all I am looking
22 for.

23 MS. SLOAN: -- so we can move on with
24 the discussion. So we will take a look.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: If you just look at if
2 they all lock up, how do you scam automatically.

3 MR. SHOOK: What I would say is I can
4 describe how that works here and then we can --

5 MEMBER BROWN: Don't do it right now
6 because I won't understand you.

7 MR. SHOOK: Okay, fair enough.

8 MS. SLOAN: Let's follow-up.

9 MR. SHOOK: I'll just say that the
10 design accommodates for that.

11 MEMBER BROWN: And I'm looking for that
12 detail somehow that was similar to what we have done
13 in other places to get expressed in either the
14 Protection System Technical Report or in the DCD,
15 one of the two.

16 MR. SHOOK: Okay.

17 MEMBER BROWN: To describe how that
18 process would go if you had that likelihood of
19 corrupted data locking them all up.

20 MR. SHOOK: Okay.

21 MEMBER BROWN: And it shuts it down, if
22 it automatically scrams them in that circumstance,
23 then we can walk away from that. If it doesn't and
24 if it just locks everything, it just stops, that is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 a different issue.

2 MR. BRIXEY: I think the current
3 description that is in one of the topical reports --

4 MR. SHOOK: Yes, we'll take the action.

5 MEMBER BROWN: And if I missed it, that
6 is fine also. I have to admit I did not read all
7 188 pages.

8 MR. SHOOK: Okay.

9 MEMBER BROWN: I probably did and didn't
10 remember most of it. That is probably the
11 circumstance.

12 MR. SHOOK: I empathize with you. It is
13 a lot of material to go through in a short period of
14 time. So but we will take the action to get you
15 those passages.

16 MEMBER BROWN: It is a fundamental
17 point.

18 MR. SHOOK: Okay. But I will say
19 generally that the design will accommodate that and
20 trip the reactor to the safe state. Okay?

21 MEMBER BROWN: The other point that I
22 tried to make earlier, you do have the two
23 subsystems, A and B in each division. And what I
24 didn't know what was the division of the four, one-

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 fourth of the signals coming in. In other words,
2 how much stuff is unique to each of the
3 subdivisions, subsystems, excuse me. It looked like
4 your buses, whatever you did in here with these
5 communication modules were independent of each other
6 between the two subsystems. At least you said that.

7 MR. SHOOK: And that's true.

8 MEMBER BROWN: I think you said that in
9 there.

10 MR. SHOOK: Yes. Yes, the only point
11 between the two subsystems that is common is at the
12 MSI. So the APUs --

13 MEMBER BROWN: Yes, I understood. I got
14 that out of reviewing the reports and the DCD.

15 MR. SHOOK: In terms of --

16 MEMBER BROWN: Two parts of that.

17 MR. SHOOK: Okay.

18 MEMBER BROWN: So I am just trying to
19 identify another pathway of thinking about this.

20 MR. SHOOK: Okay.

21 MEMBER BROWN: Of course, if you don't
22 cover all the functions, you still need to be able
23 to figure out if everything locks up. It ought to
24 automatically scramble them.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: Right. Yes --

2 MEMBER BROWN: Without waiting.

3 MR. SHOOK: Okay, let's move on now.

4 MEMBER BROWN: Okay. You can go on now.

5 Thank you.

6 MR. SHOOK: Yes, we can address that.

7 MEMBER BROWN: But thank you for making
8 it clear. I appreciate that.

9 MR. SHOOK: Okay. So, okay good.

10 Going to the next slide, 23, we have
11 independents. And again so this point is going back
12 to slide 14 where we showed specifically the SPNDs
13 being shared between the SCDS and all four divisions
14 of the Protection System.

15 So as you can see here, we have the
16 purpose again is to send 18 SPND signals from one
17 division of SCDS to all four divisions of the PS.
18 It is a hardwired interface. The input coming in
19 and going out are both four to 20 milliamp signals.

20 So there is no data communications here at this
21 level.

22 The means of independence, again, we
23 have to provide for physical separation from the
24 cabinets and cable perspective and we also provide

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 for an electrical isolation on the output of the
2 distribution module.

3 So an electrical fault wouldn't be able
4 to spread to all four Protection System Divisions.

5 MEMBER BROWN: I take it this is
6 identical to the isolation you talked about before.
7 Right?

8 MR. SHOOK: Yes, the same module. Just
9 used in a little bit different manner.

10 Okay, slide 24. Okay, so when we look
11 at, you know, we talked about redundancy. We talked
12 about independence. Now we need to look at the
13 response time. So each function is specified with a
14 certain overall loop time and then that gets
15 allocated down to the different elements of the
16 system.

17 So when we look at demonstrating how the
18 system as designed will always make sure that we
19 meet that overall response time requirement, we have
20 to look at the technology that we are using.

21 So when we first look at the sensors,
22 the signal conditioning and distribution that is
23 implemented with electronic technology and based on
24 that technology it provides for inherent predictable

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 response time characteristics that are just using
2 electrical signals. So there is no potential for
3 latencies or anything like that. You know, that is
4 no different from protection systems today.

5 Looking at the APU and ALU, those are
6 microprocessor-based programmable electronic
7 technologies. And so we have to look at those
8 pieces a little bit differently.

9 Based on the TELEPERM XS platform
10 design, there are two key aspects that allow us to
11 demonstrate a deterministic response time behavior.

12 The first is that the application software operates
13 on fixed cycle intervals. Like I said, once you
14 establish that frame rate, whether it is 25
15 milliseconds or 15 milliseconds, the processor will
16 always operate at that cycle speed. It is not like
17 your Windows computer which is an event-based system
18 which it will start executing something based on a
19 trigger, an external trigger.

20 In the case of the application software,
21 let's say the frame is 25 milliseconds, you will
22 always take a sample of whatever your inputs are at
23 that point in time, execute the logic, send the
24 outputs, and then it will go idle for the remainder

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 the frame while during that time there is self-
2 testing. We have a slide that kind of goes into
3 more detail on that coming up. So I won't spend too
4 much time on that.

5 But the key point is that the actuation,
6 you know the logic itself is always being processed
7 on a cyclic time basis. It is not event-driven. So
8 that allows for a measure of determinism.

9 The other key point to that is that the
10 system software operation which controls the
11 operation of the application software is completely
12 independent of all input signals. Now in some
13 systems, again like your Windows computer, it is
14 going to be, its processing loading may vary with
15 what you are doing on the internet or what you are
16 doing with applications or how much input you are
17 having; whereas in this case, the TXS operating
18 system design that its system software operates
19 independently of all system inputs, specifically
20 process system inputs. So if the pressurizer level
21 is not changing or changing very rapidly, it is not
22 going to affect at all the operation of the system
23 software. The system software is going to continue
24 to do, execute its tasks independent of the inputs.

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 BROWN: Is the execution of the
2 system software always on a fixed time basis?

3 MR. SHOOK: Yes.

4 MEMBER BROWN: A fixed cycle -- It's
5 cyclic.

6 MR. SHOOK: Yes. It's cyclic. That's
7 correct.

8 MEMBER BROWN: And it performs a
9 complete system software process with everything it
10 wants to do within the system --

11 MR. SHOOK: That's correct.

12 MEMBER BROWN: -- within some
13 predetermined time period.

14 MR. SHOOK: That's correct. And I have
15 a slide that shows a little bit more in how the
16 details, how that works.

17 MEMBER BROWN: Okay, I was looking at --

18 MR. SHOOK: It's actually the next
19 slide.

20 MEMBER BROWN: Well I was looking at
21 that more as application. Is this actually the
22 application software processing methodology or is
23 this the systems software?

24 MR. SHOOK: This is actually showing

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 sort of both. And I'll tell you what, I will just
2 kind of get --

3 MEMBER BROWN: Let me -- Okay, system
4 software doesn't do what system software does in
5 what we see in typical computers, where it says hey
6 I want to go off and check this sector of my hard
7 drive and figure out something. You move your mouse
8 and nothing happens. And then all of a sudden your
9 little pointer starts moving and you say oh, I'm
10 happy now. It doesn't do that. It runs through a
11 fixed set of system evolutions and operations
12 without change and doesn't vector off to do
13 something else. It is always in a series. Is that
14 correct?

15 MR. SHOOK: That's correct, yes.

16 MEMBER BROWN: Okay, that's --

17 MR. SHOOK: So actually, why don't we
18 just go to the next slide?

19 I will just say that this slide, the
20 bottom there, the output logic circuits are all
21 electronic, so they provide for a predictable
22 response time.

23 So if we look at the next slide, this is
24 showing a complete cycle. In this case, a frame is

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 to 50 milliseconds. So this is showing complete
2 cycle of the system software operation.

3 So when we start at the frame, it goes
4 through step one. And you can also, if you want to
5 see from sort of a graphical perspective, you can
6 tell back the number steps to the drawing on page
7 22, or slide 22. It shows it a little bit different
8 way.

9 But looking at the picture on slide 25,
10 you start off the frame, you read your input data so
11 you activate your received channels and then
12 activate the input drivers.

13 The second step is then you do your
14 checks, your CRC checks, and sequence checks on the
15 incoming data, whether that is the hardwired or the
16 communication information.

17 Then step three is essentially then
18 activating your activation software. Okay? So now
19 that I have got my input data for that frame, then I
20 go through and execute the application logic with
21 that input. So all that input data is put in the
22 memory and I execute the various functions, you
23 know, the comparing inputs, the step points, the so
24 forth on step three and 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 And the output of step five is that all
2 the outputs of my function diagram so then are put
3 back into memory and then are available for sending
4 the output through a hardwired I/O card or a
5 communication module.

6 Step six then we are going to do our CRC
7 computation for the outgoing data messages and
8 adding a sequence counter onto those messages. And
9 then again, this is done to allow for error checking
10 based on transmission faults between the
11 transmitting computer and the receiving computer.

12 And then we activate the send channels
13 for data transfer and output, activate the outputs
14 for hardwired outputs.

15 And then essentially after the end of
16 step seven, that is the completion of the primary
17 thread, if you want to think about it that way. My
18 former employer would call it that is your
19 foreground thread of performing. That is your
20 primary safety function task. At that point, that
21 releases and then goes to your again what I call, I
22 forget the TXS terminology, but a background thread
23 where you are doing your self-monitoring activities.

24 So the self-monitoring is a lower priority in the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 real-time operating system than the other
2 application software. And the system will then go
3 through and perform self-monitoring checks.

4 What happens is then at the end of that
5 frame, whatever self-monitoring, basically the self-
6 monitoring task will then get suspended and then you
7 will restart the application processing again up at
8 the top of the frame.

9 Typically it will take about an hour to
10 go through all the different self-monitoring tests
11 on the processor because you are only getting maybe
12 a few milliseconds at end of each cycle to perform
13 those tasks. So at the end of that frame, it gets
14 interrupted and then you go back and do your
15 function processing again. So I guess to answer
16 your question yes, it does, the system software does
17 operate on a fixed time cycle basis and that is
18 configured on an application level, whatever frame
19 rate you set the processor to operate on.

20 MEMBER BROWN: Okay, so two questions.
21 Maybe more than two. I take it section five would
22 be where I would generate my trip point. Right?
23 I've done my self-point trip comparison in here or
24 is that done in four? It can be either place. I

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 don't really --

2 MR. SHOOK: I'm not sure.

3 MEMBER BROWN: I mean you do all your
4 functions. You say you do all your function groups
5 within frame four or step four. And so I presume
6 your finish your computation and you determine
7 whether you have had a trip or not for each of the
8 functions that you have gone through. Is that
9 correct?

10 MR. BRIXEY: My understanding is that
11 section five is a collection and putting the results
12 of section four into a grouping, then six and seven,
13 you will be preparing it to be a message. So five is
14 where the output has been generated and is being
15 collected and being put into a message.

16 MEMBER BROWN: Okay, so that is where we
17 come back to this. Is it a dry contact that you
18 send to a driver that says hey this is on and
19 tripped or whether it's not or whether it is into
20 this data-packet routines where you have data
21 messages going back and forth, which we discussed
22 earlier.

23 MR. BRIXEY: Yes.

24 MEMBER BROWN: Okay, so that's fine. I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 don't want to go back. I just wanted to make sure I
2 understood that point.

3 The next question was on page -- I don't
4 know. Where's that table of functions, 13, 12?
5 Shoot. I didn't count them all.

6 MR. WIDMAYER: Eleven.

7 MEMBER BROWN: There was number of
8 functions you talked about. Page 11, yes, thank
9 you. There is a pot full of these in here. Probably
10 close to 15 or 20. Can I transpose -- take these
11 and I will look at your diagram here that says A, B,
12 C, D, E, F, G, H and you say individual I&C
13 functions perform the safety tasks A through H. I
14 would think that that is really A through M or P, or
15 Q, or R, or something like that.

16 MR. SHOOK: Yes.

17 MEMBER BROWN: My point being is is
18 every one of these done in series in each 50-
19 millisecond program cycle?

20 MR. SHOOK: Not necessarily.

21 MEMBER BROWN: Okay.

22 MR. SHOOK: So the way that works is so
23 during the engineering process we start with this
24 list of functions and what happens is there is a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 series of diagrams that are done at different levels
2 in the design process. What will happen is at a
3 certain point in the design process we start carving
4 up different pieces of the logic to be performed,
5 different modules, processing modules.

6 MEMBER BROWN: Functions, not logic.
7 You mean functions to be performed.

8 MR. SHOOK: Yes, but it is not
9 necessarily a one-to-one correlation to these
10 functions. For example, I might like take
11 pressurizer pressure will use that sensor for both
12 reactor trip and ESFS. Okay? So here you are just
13 seeing at the top level function I have a reactor
14 trip on low pressurizer pressure and then in 7.3,
15 you will see an SI actuation on low pressurizer
16 pressure.

17 So at the top level there are two
18 separate functions. Now once we get down in the
19 logic, what you will end up having is okay I'm going
20 to have when I acquire that sensor and bring it in
21 through my A to D card, I am going to have one, you
22 know scaling block set of logic that converts up
23 from a four to 20 to zero to 3,000 pounds of
24 pressure range. Okay?

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 that signal conversion would be
2 assigned as a sub-processing module within the logic
3 software. And then the portion of the logic that
4 does the reactor trip maybe gets its own assignment
5 within a different function processing module. Then
6 the ESFS gets its own processing module. So
7 essentially what happens is as you go through the
8 design process, as these functions utilize the same
9 set of logic, you end up kind of carving out
10 different pieces of the processing. And once that
11 gets down to the space software, each of that
12 processing gets assigned to its own function diagram
13 group. And the grouping of how that ends up is that
14 that is what get processed in a time series.

15 So these functions don't necessarily get
16 processed in time series. It is more of how you
17 translated that into specific software diagram
18 logic. That is what gets processed in time series.

19 By the look on your face, I don't think
20 I adequately captured your question.

21 MR. WIDMAYER: You locked up.

22 MEMBER BROWN: No. Yes, right. My
23 functional processor locked up all over the place.

24 MR. BRIXEY: These don't all exist on

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 one processor. So every 50 milliseconds, it is not
2 that we run an order through these through a single
3 processor but they are broken up across the
4 different ones. So, --

5 MEMBER BROWN: Let me translate my
6 question. Thank you. Now good way to jog my memory
7 as to what question I wanted to ask before my memory
8 bank collapsed.

9 We've got multiple APUs.

10 MR. SHOOK: That's correct.

11 MEMBER BROWN: Like there is three APUs
12 in the A group, two in the B group. So I am
13 presuming, based on your earlier whatever one-fourth
14 of the measurements that come into division one, is
15 divided up between the APUs, as opposed to all being
16 performed by --

17 MR. SHOOK: That's correct.

18 MEMBER BROWN: Each APU.

19 MR. SHOOK: Yes.

20 MEMBER BROWN: Okay, got that. I'm not
21 judging it one way or the other. I just got it.

22 MR. SHOOK: Okay. Let me just address
23 that real quick.

24 MEMBER BROWN: No.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: I'm sorry.

2 MEMBER BROWN: You're going to confuse
3 me.

4 MR. SHOOK: Okay.

5 MEMBER BROWN: If you do that, we could
6 go off into la-la land. Be very careful. Okay? I
7 only work in -- My brain works linearly sometimes.

8 MR. SHOOK: Okay. Go ahead.

9 MEMBER BROWN: My point being is that if
10 you have divided them up, does each of those
11 functions get processed every time within each 50-
12 millisecond cycle?

13 MR. SHOOK: Yes.

14 MEMBER BROWN: Okay. In other words, if
15 you are going to have separation, you put them in
16 another processor.

17 MR. SHOOK: That's correct.

18 MEMBER BROWN: And that is how you cover
19 them but each 50, it covers all that they are
20 supposed to do. You don't hit a certain point you
21 jump off and you grab this routine and sometimes you
22 ignore it and sometimes you don't, other than in
23 your modules to do the calculation and then to do
24 the setpoint calculation and all the other type

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 stuff.

2 MR. SHOOK: That is correct. Whatever
3 functions have been allocated to that APU, it does
4 all those functions, every scan.

5 MEMBER BROWN: Every time.

6 MR. SHOOK: Yes, that's correct.

7 MEMBER BROWN: Okay. And I was just
8 interested because I don't like personal preference.
9 Jumps are dangerous. Once you jump out of a linear
10 program, you never return.

11 MR. SHOOK: No.

12 MEMBER BROWN: That generally generates
13 an interrupt and I'm not talking about an interrupt-
14 driven system but you have to have something to move
15 it out of the main line to get it out of there and
16 then make it come back.

17 MR. SHOOK: No, no.

18 MEMBER BROWN: And that's always
19 dangerous because it may not come back.

20 MR. SHOOK: Yes, it's just a linear
21 scan.

22 MEMBER BROWN: Okay. All right. You
23 answered my question then.

24 MR. SHOOK: And just to make a point,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the reason for -- Between the subsystems, the reason
2 for allocation is for functional versatility.
3 Within the subsystems, the number of APUs is driven
4 just primarily on sizing.

5 So if I had an APU that was fast enough,
6 I just have one or had enough capacity to bring in
7 all that I/O. I just have one. But it is basically
8 driven off of I/O capacity and processor loading
9 that you end up having multiple APUs per subsystem,
10 per division.

11 MEMBER BROWN: Why is there three and
12 two subsystem?

13 MR. SHOOK: It is just again how you
14 have allocated the I/O and how much processing
15 capability.

16 MR. PHAN: Yes, I can answer. And this
17 might be going too far but like one of our functions
18 in DMBR function specifically is very, very, very
19 complicated. So that loads down your processor
20 quite a lot. So that is one of the reasons why you
21 have three in one division and two in another
22 because that one function takes a lot of processing.

23 MEMBER BROWN: Okay. Now, I can
24 understand that. So the reality Subsystem B does

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 not replicate Subsystem A relative to. So that is
2 an argument against my independent thought that I
3 thought was being incorporated in A3 with some other
4 miscellaneous processor that was doing other stuff
5 because it didn't look like it was feeding the ALUs
6 the same way.

7 MR. SHOOK: No. Essentially what you
8 will have is when you take this whole list of
9 functions here, you will first allocate these to A
10 and B, depending on the functional diversity aspect.

11 Again like so for example high core power level is
12 a diverse trip to load DMBR. So I am going to put
13 one on one subsystem and one on the other.

14 MEMBER BROWN: You are kind of looking
15 at 6303 and --

16 MR. SHOOK: Exactly.

17 MEMBER BROWN: -- kind of dividing up by
18 functional things to get it in a different system.
19 Okay, I got the picture now.

20 MR. SHOOK: So that is the separation
21 between A and B. And then once you are within the
22 subsystem, then it is just a matter of sizing. How
23 much can I fit in a sub-rack. And then that
24 determines what to use.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: Okay, I got it. And that
2 makes your watchdog timer more important now.

3 MR. SHOOK: Yes, I mean each APU will
4 have a watchdog timer.

5 MEMBER BROWN: Scramming the plan in the
6 ALU -- I'm looking at the ALUs.

7 MR. SHOOK: Yes.

8 MEMBER BROWN: Okay, thank you.

9 CHAIR POWERS: Mr. Stetkar can't help
10 but know that this system is only partly American.

11 MEMBER BROWN: Only partly what?

12 CHAIR POWERS: It's kind of like a
13 behaviour. It reflects its European origins.

14 MEMBER BROWN: Oh, yes.

15 MR. SHOOK: This is actually a test to
16 see if you noticed.

17 CHAIR POWERS: We also noticed that CRC
18 is not in your list of acronyms.

19 MR. SHOOK: Oh.

20 CHAIR POWERS: Got you!

21 MEMBER BROWN: Dana, everybody knows
22 what that is.

23 CHAIR POWERS: Two out of four logic
24 shows that not everyone knows it.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: Okay, so moving to slide 26.
2 Here we are talking about the fail-safe behavior.
3 And we have already kind of talked about a piece of
4 this but we will just kind of walk through the whole
5 system.

6 You know, basically we started with a
7 sensor, signal conditioning and distribution
8 failures. If we have an out of range failure, that
9 is detected by -- that will be detected by the APU.

10 And the reasons for that is for generally most of
11 the inputs are four to 20 milliamp signal input so
12 we use the live zero failure detection mechanism.
13 So if I have a short circuit of zero current. I'm
14 sorry -- A short circuit will be greater than 20
15 milliamps. An open circle will be a zero. That
16 gets configured within the APU. When I bring that
17 signal in, in terms of defining an out-of-scale high
18 or low range. And if the system detects and out of
19 scale high or low, the system flags that message and
20 when that message is then used in all the subsequent
21 downstream logic, particularly when it gets to the
22 voting, it modifies the voting logic. So if I
23 detect the single sensor failure, I actually modify
24 the voting logic to two out of three, which this is

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 improvement over analogue systems because I am still
2 satisfying my single priority criteria but in an
3 analogue system, I would be one further sensor
4 failure away from reactor trip. Whereas here, I am
5 at two out of three. So I have reduced the
6 probability of a spurious actuation.

7 If I have two sensor failures, we modify
8 to a one out of two logic and then three or more
9 sensor failures, we fail to the safe state. In this
10 case, the reactor trip.

11 In range failures are not detected but
12 obviously those are covered by your single failure
13 analysis.

14 MEMBER BROWN: So if a pressurizer
15 pressure sensor fails low, it would go to zero and
16 you all would ignore it.

17 MR. SHOOK: Well, we would modify the
18 voting logic in accordance with these rules. So we
19 wouldn't ignore it. I mean, we would ignore it but
20 modifying the voting logic.

21 MEMBER BROWN: If one sensor goes, you
22 are requiring -- You still are then two out of three
23 buys two out of four logic.

24 MR. SHOOK: That's correct.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: So you are effectively
2 ignoring it then, as opposed to generating a trip
3 with it.

4 MR. SHOOK: That's true. That's
5 correct.

6 MEMBER BROWN: Okay.

7 MR. SHOOK: Okay. When look at going
8 down to ALU failures, the ALU outputs are designed
9 to fail low. And a low, a zero signal out of the
10 APU results in a reactor trip signal to be actuated.
11 And then the same with output logic circuit
12 failures. So failures anywhere downstream of the
13 ALU or APU result in a fail low reactor trip
14 actuating signal.

15 Slide 27. So a little bit more kind of
16 meat on the fail-safe behavior with regards to the
17 APUs and ALUs. There are four main features that
18 allow us for fail-safe fault detection. Then you
19 can configure the system to fail to a safe state.
20 In this case, reactor trip is actuated.

21 First of all we have the self-monitoring
22 of the function processors. As we talked about
23 before, once I finish all the function diagram
24 processing and I release that primary thread, I will

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 do self-monitoring to do different memory checks and
2 so forth.

3 We also have a CRC check sub-monitoring
4 of the software. This is actually more -- This is
5 done during the extended self-test when we reboot
6 the processor. It checks to make sure it is the
7 same software version.

8 Here we also have the hardware-based
9 watchdog timer, which we have already discussed and
10 we will get you some information on the details of
11 how that operates.

12 And then lastly, we talked about already
13 the data messages going between the APUs and the
14 ALUs utilize a checksum as well as a sequence
15 number. So the receiving processor will look at the
16 checksum of the sequence to make sure it is a valid
17 message before processing. If it detects it, it is
18 an invalid message and will then modify the building
19 logic.

20 MEMBER BROWN: A question I didn't ask
21 on your processing of the --

22 (Simultaneous speakers.)

23 MEMBER BROWN: -- cycle. Do you have a
24 monitor, independent monitor that looks for short

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 cycle, like in other words if a sample period
2 doesn't go for its full 50 milliseconds or if it
3 goes in overtime?

4 MR. SHOOK: I don't know that.

5 MEMBER BROWN: Probably the short cycle
6 is of more interest. I was just curious as to
7 whether you do that or not. In other words, if it
8 goes short cycle, you may not do some stuff that you
9 may have -- In other words, you have skipped
10 something.

11 For some reason, you know, your software
12 has skipped through. Don't ask me how. It was a
13 concern of ours years ago and we typically look at
14 that.

15 MR. SHOOK: Okay.

16 MR. BRIXEY: So the watchdog is what we
17 use for watching the long cycle. The short cycle I
18 can't think of anything off the top of my head that
19 we are using to monitor for short cycles or how it
20 would happen. So I will look for an answer for
21 that.

22 MEMBER BROWN: I mean, the watchdog has
23 to get triggered by the end of function cycle. I
24 mean, this trip is it supposed to trigger it and 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 don't pay any attention. I'm going back to start
2 over again.

3 MR. BRIXEY: Yes.

4 MEMBER BROWN: Okay.

5 MR. SHOOK: Depending on the particular
6 failure mode, there could be some mechanism that
7 will detect that. For example, if you didn't
8 complete all the function diagram processing and
9 that message didn't get updated with the next
10 sequence counter, the receiving processor will then
11 detect that and then modify its logic.

12 MEMBER BROWN: That update is not based
13 on a change of the output but it just didn't get
14 updated.

15 MR. SHOOK: Right.

16 MEMBER BROWN: That's what you are
17 talking about.

18 MR. SHOOK: Right. So again, that is
19 one potential failure mode where it would get
20 detected. But without kind of going through all the
21 details, it is hard to say exactly how that would
22 operate.

23 MEMBER BROWN: Okay, thank you.

24 MR. SHOOK: Okay, then the last slide

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 for reactor trip, next slide is 28.

2 And this is just showing the various
3 surveillances on how we test the various pieces of
4 the entire string of the reactor trip function. We
5 start with the calibration. We calibrate the
6 detector. We essentially do a calibration check of
7 the detector and then make sure that the scaling
8 factor in the APU matches the calibration. We have
9 sensor operational tests that will basically check
10 the input circuitry starting with the SCDS into the
11 APU. We have the continuous self-test. It is shown
12 to go up to the sensor. The continuous self-test is
13 only being performed on the TXS processing units,
14 the ALUs and APUs. The reason why we show it all
15 going over these sensors that the self-testing will
16 detect failures, upstream failures coming into the
17 system, based on whether it is out of range high or
18 low.

19 Once we get within the APU and ALU, we
20 rely on the continuous self-test, as well as the
21 extended self-test. The extended self-test
22 basically is once every 24 months you have to reboot
23 the processors and it will check certain things
24 about the processor operation that can't be tested

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 continuous self-test.

2 Then we have the ADOT which checks the
3 outputs from the ALU all the way through the trip
4 device. And then we also have setpoint verification
5 on the APUs, as well as the calibration. It is not
6 quite shown very clearly but really that other
7 calibration on the other side is to check the manual
8 trip, the operation of the manual trip switches from
9 the Main Control Room and RSS into the ALUs to the
10 hardwired Or gates.

11 And then lastly, we have a response time
12 check to check the response time of the whole loop.

13 Okay. So moving on to ESFS. For the
14 topics, we are going to discuss the same topics. In
15 the cases where the topics are the same as the
16 protection system, I will just note that or as for
17 the reactor trip, I will just note that and then we
18 will move on and not spend too much time rehashing
19 the same information.

20 Starting with Slide 31, we have a
21 listing of all your ESFS functions. And where is
22 the -- Mr. Stetkar, one thing I wanted to point out
23 here is we do have an automated steam generator
24 isolation function for the tube rupture event. I

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 will just give you --

2 MEMBER STETKAR: Yes, okay.

3 MR. SHOOK: -- a quick background. The
4 reason is in Europe they analyze multiple tube
5 ruptures as part of their design basis. So the
6 event progressed quickly enough that they automated
7 the function because they needed action within 30
8 minutes. And we analyzed it for the U.S. We
9 analyzed the single tube rupture as part of the
10 design basis and the event didn't progress quickly
11 enough. So that is why there is not manual operator
12 action, Chapter 15. However, we did retain the
13 automated function because in reality you may have
14 more than one tube rupture. So the automated is
15 still there. It is just not credited.

16 MEMBER STETKAR: But it is only the
17 isolation. It is not the cooldown and
18 depressurization that is implemented in Europe.

19 MR. SHOOK: No, we still have that as
20 well, the partial cooldown.

21 MEMBER STETKAR: Well you have the
22 partial cooldown for any --

23 MR. SHOOK: Right. Right. So the steam
24 generator isolation, that function is the same as

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 is in Europe.

2 MEMBER STETKAR: Okay.

3 MR. SHOOK: And I guess my point is it
4 does use the N16 detectors as an input to help
5 detect that.

6 MEMBER STETKAR: Oh, okay.

7 MR. SHOOK: Yes.

8 MEMBER STETKAR: I must have missed
9 that. So, thanks.

10 MR. SHOOK: Okay. Other than that,
11 these are the functions. And I'm going to guess
12 that the differences that I have already been talked
13 about in various different chapters. So I'm not
14 going to spend too much time on these. These are
15 the ESFS functions.

16 Moving to slide 32, these are the ESF
17 control functions. And I will say these are what is
18 currently listed in the FSAR. We have an ongoing
19 open item with the staff that will be modifying this
20 list but this is what is being presented here today
21 as far as the current design.

22 We have the emergency feedwater level
23 and control and flow control, which we discussed and
24 then also the MSRT control.

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 Okay, slide 33. We are showing here
2 again the allocation of these functions within the
3 DCS. The signal input path is the same. We have
4 safety related sensors coming in through the SCDS to
5 be distributed out. And those signals are
6 distributed either to the Protection System, if it
7 is an actuation function or to the SAS if it is a
8 control function. Both the PS and SAS send outputs
9 out to the PACS. As a general rule, actuation
10 always has priority over controls so the Protection
11 System outputs without priority over the safety
12 automation system.

13 And then you see on SICS in the Main
14 Control Room, we also have system level means of
15 actuating the actuation functions as well.

16 And again I apologize, I missed the
17 shading but we also have controls for the SAS for
18 the control function as well on SICS in the Main
19 Control Room.

20 MEMBER STETKAR: Jeremy, just before,
21 because I am more linear and worse than Charlie is
22 in terms of being able to hold a thought. Do you
23 remember where in the DCD that N16 signal for steam
24 generator isolation is described?

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. SHOOK: We talk about it in Section
2 7.3. We show the logic for that.

3 MEMBER STETKAR: Okay, 7.3.

4 MR. SHOOK: Yes.

5 MEMBER STETKAR: Okay. I just did a
6 quick word scan and I didn't see it. I will look
7 for it. Thanks.

8 MR. SHOOK: Okay. And then we also show
9 here at the bottom we have safety-related actuators
10 which are sent signals from the PACS as well as also
11 the turbine generator I&C which is a turbine trip
12 signal from the protection system.

13 Okay, going to slide 24 for the design
14 ESF actuation. Basically the SCDS and Protection
15 System implementation of these functions is the
16 same, as for reactor trip. So there is really no
17 need -- Well actually, so let me, there is one
18 difference.

19 We only implement functional diversity
20 for reactor trips. We don't implement functional
21 diversity for ESFS. So the ESFS essentially gets
22 assigned to whatever subsystem is most convenient
23 from the sizing or the signal routing perspective.
24 And the other key difference here is the output of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the ALUs are Or-ed instead of And-ed.

2 And let's see what else we have here.
3 And then the main difference is at the bottom. With
4 the reactor trip there is no PACS associated with
5 reactor trip but here we have signals coming from
6 the Protection System into the PACS, as well as
7 prioritizing with other signals coming from other
8 systems. So you can see there that we have
9 hardwired signals coming into the diversity module -
10 - sorry. Excuse me -- the Priority Module from the
11 SICS. Those would be your manual commands.
12 Component level commands go into the PACS, as well
13 as automated ESFS actuations from DAS and automated
14 control functions from SAS.

15 Also SAS, if we threw the EOP
16 development and task analysis and so forth, if we
17 find that there is a post-accident manual action
18 that we want to -- we use the term manual boot
19 command. So if there is a manually initiated
20 sequence, that would be performed in SAS and then
21 come through that path as well. An example of that
22 would be going to hot leg recirc and following the
23 LOCA.

24 So then we come down to the PACS. And

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you can see there that the Priority Module is
2 implemented.

3 MEMBER BROWN: Before you get to the
4 PACS, okay, you come down -- I understand what you
5 are doing as you go through the cycle here. You
6 come down, the Or goes off and hits the Priority
7 Module and does something. But you were just
8 talking about there is another arrow that goes off
9 the SAS, PAS, TG, I&C, and such and such.

10 MR. SHOOK: Okay.

11 MEMBER BROWN: Are those -- SAS you have
12 already said. Once you actuate something then the
13 SAS takes over for the control, if it has got an
14 automated control function.

15 MR. SHOOK: That's correct.

16 MEMBER BROWN: Under the ESFS function,
17 it does the control work.

18 You send a signal to PAS. Does that
19 turn off the other system? I mean, what is the --
20 Is there a reason for that to go over there?

21 MR. SHOOK: There is --

22 MEMBER BROWN: I mean I take it this is
23 just an electronic signal like an on/off switch.

24 MR. SHOOK: Yes. It is just, basically

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you are going to send that signal to PAS. There is
2 a couple of -- I would say there are two main
3 categories of why I would send that to PAS. One is
4 specific to the partial cooldown function. So with
5 the partial cooldown, the basic idea is there is no
6 high-head safety injection in the plant. So I need
7 to cool down and depressurize the primary to the
8 point where I can get medium head safety injection
9 pumps to come down below the shutoff head so I can
10 provide water into the primary.

11 There is two ways that is done. There
12 is the preferred way and then the safety credited
13 way. So the preferred way is to use the turbine
14 bypass valve to actually perform that cooldown
15 function. And so to initiate that, --

16 MEMBER BROWN: You use bleed steam.

17 MR. SHOOK: -- we just bleed steam
18 around the turbine to the condenser. And so now it
19 is important to note that is preferred but it is not
20 credited in the safety analysis. Okay?

21 So the PAS, we send a signal to the PAS
22 to initiate that close of control for the turbine
23 bypass valve. Now for some reason if that fails to
24 operate properly because it is non-safety, 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 MSRTs are your safety grade credited means of
2 performing partial cooldown.

3 MEMBER BROWN: And that is the RT?

4 MR. SHOOK: The Main Steam Relief Train.

5 MEMBER BROWN: Oh, train. Okay.

6 MR. SHOOK: Right. You relief.

7 Essentially it is your relief valve of the steam
8 generators. And then that control is done within
9 the SAS.

10 So that is sort of a unique function in
11 the EPR.

12 The other more general category is if
13 there is operational systems that need to know that
14 an ESFS has occurred to put them in a state that is
15 more amenable to sort of post-accident. You know,
16 once you remove your ESFS signal. For example, and
17 we haven't done a lot of the detailed design yet to
18 give every single list of specific examples but for
19 one example would be isolate main feedwater. Okay?

20 And normally I have got the control valve in an
21 automated loop. I am probably going to want to just
22 kick that loop to manual, once I have the feedwater
23 isolation signal sent. Because when I restore main
24 feedwater, I don't want to start coming back in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 automated mode. So that is one example of why you
2 would send those type of ESFS signals. But is
3 basically just so that non-safety, any non-safety
4 controls associated with that actuated equipment
5 knows that an ESFS has occurred and you can do --
6 You can then do whatever logic you need to do to
7 make the plant recover make a little bit more sense
8 for the operator.

9 Does that answer your question?

10 MEMBER BROWN: Yes, I think it does.

11 MR. SHOOK: And then turbine generator -

12 -

13 MEMBER BROWN: I liked the example you
14 gave.

15 MR. SHOOK: Okay. And then the turbine
16 generator I&C is for turbine trip.

17 Okay, and then we come down to the PACS.

18 So again we have the signals from the Protection
19 System as well as the other systems. And then we
20 have the Priority Module. The Priority Module is,
21 as we discussed before, it is a Programmable Logic
22 Device, PLD, that is subject to 100 percent
23 combinatorial testing to basically preclude
24 consideration for common cause failure for that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 device. And we will talk a little bit more about
2 that in the 7.8 when we talk about D3.

3 We also have a Communication Module,
4 which allows us to interface the PAS because we want
5 all the nice features and functions for the operator
6 using on the PICS as a modern type of HMI. So we
7 provide that pathway as well.

8 And then we have the output of the
9 Priority Module interface to the switchgear in the
10 actuators themselves.

11 And in general, the general priority
12 which is established in the FSAR, the Protection
13 System and DAS are implemented essentially at the
14 same level priority. Okay? And the reason for the
15 DAS being at the same level of priority is because
16 the DAS is essentially a functional substitute for
17 the protection system. So while the DAS is
18 technically not a safety-related system, I can't
19 have the DAS be a lower order of priority than the
20 SAS or the SICS because it just functionally
21 wouldn't work properly. You know, that would mean
22 that your EFW closed-loop control would have a
23 higher priority over the non-safety DAS, EFW
24 actuation, which just doesn't make any sense.

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 the PS and DAS have the same level of
2 priority and we provide for independence measures
3 coming from the DAS to make sure a failure doesn't
4 affect the PACS.

5 And then so the PS and the DAS are
6 basically equivalent and then we have SAS for
7 control, being the next level of priority. Then we
8 have the SICS being the next level of priority. And
9 then lastly the inputs from the PAS are the bottom
10 priority, coming from the communication module.

11 Okay, any more questions on this before
12 we move to the next slide?

13 MEMBER BROWN: Yes. I'm still puzzled
14 on the priority circumstance. I mean, if you want
15 two or three to actuate or to be responded at the
16 same time, why can't you do that? I mean, that is -
17 - We did that. I don't remember seeing Priority
18 Modules or priority methodologies in some of the
19 more conventional plants. I mean, we had time-
20 delayed relays that trigger certain things starting
21 on the switchgear so you didn't unload it or
22 overload it but that was about it. I mean, if you
23 were -- I mean, I could trigger the fill system and
24 I could trigger the scram and I could trigger a feed

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 operation. I could trigger every one of them
2 simultaneously and I didn't worry about they would
3 all operate. They didn't wait for somebody else to
4 tell them it was okay or finish some other operation
5 first.

6 So is there a plant basis for doing
7 this? I mean, is there some -- or is just because
8 you have only got -- Are all these Priority Modules
9 -- Is there only one Priority Module for the whole
10 first division that deals with every one of the
11 systems that is covered by Division 1?

12 MR. SHOOK: No. Each actuator gets its
13 own pair of priority and communication modules. So
14 like let's take the EFW pump, for example. It has
15 the pump itself has a Priority Module and
16 Communication Module. And so each actuator gets its
17 own pair.

18 You know, I would say two main reasons
19 why you have -- Actually, Shaun if you could go back
20 to slide 33. The two main reasons why you have to
21 do priority as opposed to some of the naval plant
22 designs, first of all is I am providing two manual
23 control stations in both of our control locations,
24 Control Room and RSS, so the operator can manually

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 control the plant either from PICS or SICS. So as a
2 first basis, I have got two manual paths I have to
3 prioritize, I have to deal with. And then the
4 second piece is --

5 MEMBER BROWN: Why? Somebody operated
6 something from the SICS? Why can't you just
7 operate?

8 MR. SHOOK: Well you know, again --

9 MEMBER BROWN: I've got two -- Just a
10 simple example. I've got a switch over here that
11 will start a pump and I've got a switch over here
12 that will start the pump. They are in parallel.
13 Turn one, it start. Turn the other one, it starts.
14 As opposed to well, gee, I haven't figured out
15 whether I want to allow this one to do it or not.
16 Is there a reason for not wanting to allow the SICS
17 not to do it if you can do it from the PICS?

18 MR. SHOOK: I would say the main -- Well
19 at some point you have to choose because the
20 operator can turn the pump on or off from both
21 locations. Right?

22 MEMBER BROWN: Yes.

23 MR. SHOOK: So at some point once you
24 get to the switchgear, there is only two signals

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 going to the switch gear on or off. Right? So you
2 have to have some -- If you provide on/off
3 capability from two locations, there has got to be
4 some gatekeeping because going to the switchgear I
5 only have two signals.

6 MEMBER BROWN: I can turn it off and
7 turn it on from both places.

8 MEMBER STETKAR: Let me interject. One
9 of the things that I mentioned about three hours ago
10 was that some of the things that I came across in
11 terms of human factors engineering and just design
12 of the system that sort of relates to the
13 conversation is statements in the FSAR that say if
14 an operator begins using SICS, it has priority for
15 safety-related components, which means that this
16 Priority Module says that if I push a button in
17 SICS, the Priority Module knows that that is the
18 right thing that is supposed to happen. Is that
19 true?

20 MR. SHOOK: That's true.

21 MEMBER STETKAR: Even though that might
22 not be the right thing?

23 MR. SHOOK: Well, you know, again --

24 MEMBER STETKAR: It always knows that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 SICS is perfect and PICS is not.

2 MR. SHOOK: I mean within the design,
3 because we have provided the capability to control
4 safety-related equipment from PICS, we want the
5 safety systems to take priority -- SICS priority to
6 take over that.

7 MEMBER STETKAR: The safety systems are
8 always perfect and non-safety systems are never
9 perfect.

10 MR. SHOOK: Exactly.

11 MEMBER STETKAR: Okay.

12 MR. SHOOK: So I mean for example, we
13 could postulate. You could postulate control system
14 failure. That would be sending an antagonistic
15 signal to the PACS, at which point you want to be
16 able to make sure you can deal with that situation.
17 Okay?

18 MEMBER STETKAR: If you have a faulty
19 signal from SICS, there is no way that PACS -- that
20 PICS --

21 MEMBER BROWN: That's right.

22 MR. SHOOK: That's correct.

23 MEMBER STETKAR: -- can compensate for
24 that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: That's correct.

2 MEMBER STETKAR: The thing is going not
3 block.

4 MR. SHOOK: That's correct but again, in
5 that case, the Protection System is going to win
6 over anybody else. So --

7 MEMBER BROWN: What do you mean? Which
8 Protection System? If the SICS blocks something but
9 it is not actuating it --

10 MR. SHOOK: Well again, the SICS is just
11 a hardwired panel. So if the operator goes to SICS
12 and says you know, to give you an example, emergency
13 feedwater, if the operator says okay I want to go
14 close those valves, if I close the valves and then
15 the level starts to drop, the Protection System is
16 going to say well I don't care what you want to do
17 operator. I am going to go and re-actuate and open
18 these valves back up.

19 Now, ultimately the operator can still
20 reset the signal, in which case you have then
21 defeated the automation. But then that is
22 controlled through EOPs and operator training and so
23 forth.

24 So at the end of the day, we still give

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the operator the capability to do what they need to
2 do but we have built in some measures of checks and
3 balances so that it is not necessarily, you know,
4 you have to -- there is a thought process that has
5 to be involved with those actions.

6 MEMBER STETKAR: Resets of hardware or
7 software?

8 MR. SHOOK: The actual --

9 MEMBER STETKAR: I understand the button
10 is --

11 MR. SHOOK: The reset is done within the
12 ALUs.

13 MEMBER STETKAR: Okay. So you could get
14 software faults that would spuriously reset signals
15 on you.

16 MR. SHOOK: I mean, we don't think that
17 is likely but yes.

18 MEMBER STETKAR: Don't use the word
19 lightly with me.

20 MR. SHOOK: I'm sorry.

21 MEMBER STETKAR: Two words you don't
22 want to use here are likely and probability.

23 MR. SHOOK: And so that is the first
24 thing we have is manual control from two locations

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 we also have control of if we have
2 actuators that have what I call shared functions.
3 So let's take the main feedwater control valve for
4 steam generator level. That has both an operational
5 and safety function. So the operational function is
6 to maintain level during normal operations, during
7 control some band during normal operation. And then
8 there is a safety function that says to isolate main
9 feedwater. So that valve has to go close.

10 Because I could have a feedwater control
11 system failure that leads to me needing to isolate
12 main feedwater, that safety function has to have
13 priority over the control function.

14 So generally any actuators that have
15 shared purposes, and there is not a lot in the plant
16 but there is some and that is an example, then I
17 have to make sure that that safety function always
18 has priority over the control function.

19 MEMBER STETKAR: Let me ask you a
20 question that came up yesterday and since we are
21 kind of delving into this area of priorities,
22 emergency service water system has a flooding
23 protection logic that isolates emergency service
24 water and trips the pumps on high level 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 safeguards building sumps. Does that signal
2 override the safeguard signal to start the pumps and
3 open the valves?

4 MR. SHOOK: So the answer is the ESF
5 actuation would override that signal.

6 MEMBER STETKAR: It will.

7 MR. SHOOK: Yes.

8 MEMBER STETKAR: Definitely?

9 MR. SHOOK: Yes.

10 MEMBER STETKAR: Okay, thank you.

11 MR. SHOOK: Based on the criteria that
12 we currently have laid out in the FSAR.

13 MEMBER STETKAR: No, that's -- It was
14 either going to be yes or no or I don't know.

15 MR. SHOOK: Okay.

16 MEMBER STETKAR: Thanks. Thank you.

17 MR. SHOOK: Okay, so --

18 MEMBER STETKAR: That's the type of
19 question, by the way when we are talking about these
20 priorities that the reason earlier I said that if
21 that information is available, and obviously it is,
22 I think it is very useful information, at least for
23 the staff to have in their hands.

24 When I asked yesterday, everybody failed

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 open. They said well I have to ask the I&C folks
2 because the people who know the pumps and pipes and
3 valves don't understand all of this signal stuff.

4 MR. SHOOK: Right.

5 MEMBER STETKAR: So I figured well I'll
6 ask the I&C folks today but that's why I am sort of
7 interested in that integrated priority.

8 MR. SHOOK: Right.

9 MEMBER STETKAR: It demonstrates sort of
10 a philosophy, if you will, of the design.

11 MR. SHOOK: Yes, I mean we basically,
12 with an I&C we have established this overall
13 philosophy and I would say all of the functions we
14 have today follow that. But with the detailed
15 design, there is a particular case where there is a
16 --

17 MEMBER STETKAR: The problem is
18 yesterday people were focused on my god you don't
19 want flooding in the safeguards building because if
20 it is high enough it could potentially affect two
21 redundant divisions and that is really bad so you
22 want to be really, really careful that you get that
23 isolation. Well, okay that is good if you are
24 centricon flooding. On the other hand, if you want

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 keep diesel generators cool or if the flooding
2 has occurred from not ESWS, it might not necessarily
3 be a good thing to such down your Emergency Service
4 Water System. So those are the sort of trade-offs
5 that I, in particular, are interested in seeing.

6 MR. SHOOK: And again, you know, I mean
7 because once you get in the scenarios, it is very
8 specific to what the actual failure --

9 MEMBER STETKAR: Absolutely. There is
10 never a perfect solution.

11 MR. SHOOK: But you know, again with the
12 system design, I can go and reset SI, which is what
13 is going to start your ESW. The system will keep
14 operating but I could go and isolate those
15 particular portions if the operator chose to do
16 that.

17 That's what you are looking for?

18 MEMBER STETKAR: Yes.

19 MR. SHOOK: Okay. Yes, the system is
20 designed with that capability.

21 Okay, so slide 35, we are showing the
22 EFS control. So we have the same top-end input. We
23 have the sensors and SCDS. And then we have the
24 signal input to the SAS. The SAS is designed

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 differently than the protection system is assigned
2 as a control system. So we have essentially
3 redundant control units within teach division. And
4 then again, the number of control units is
5 determined by the sizing of the system in terms of
6 the amount of I/O and function processing that is
7 required.

8 The network design we have got, we do
9 have interdivisional communication. Not all
10 functions with the SAS require interdivisional
11 communication. It is on a function-by-function
12 basis. And actually the control function shown here
13 in 7.3 do not require individual communication.
14 They are all straight up and down -- I'm sorry --
15 except for the partial cooldown MSRT control, we
16 look at four divisions of MSRT position. So there
17 is some interdivisional communication there. But in
18 terms of actual level control and flow control and
19 pressure control loops, those loops themselves are
20 all straight up and down, you know, one sensor to
21 one valve.

22 Yes?

23 MEMBER BROWN: When I look at 34 and 35,
24 34 says I have got a Protection System and there is

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 an ESF actuation system that gets processed pick a
2 division, Division 3, whatever it is. It goes to
3 Priority Module. It says turn this actuator on/off,
4 open and close the valve, whatever it is. That is
5 what it says. To actuator Division 3. That is on
6 slide 34.

7 Slide 35 says now I have got the same
8 data coming to the SAS system.

9 MR. SHOOK: From the SCDS, you mean?

10 MEMBER BROWN: Yes, well it says SCDS
11 Division 3.

12 MR. SHOOK: Sure.

13 MEMBER BROWN: The signal comes into
14 SAS.

15 MR. SHOOK: Yes.

16 MEMBER BROWN: And then the SAS goes to
17 these little things called CUs, control units, and
18 they generate an Or, which I presume open or close
19 the same actuator.

20 MR. SHOOK: That's correct.

21 MEMBER BROWN: So there is two paths
22 here for automatically operating that actuator. Is
23 that correct?

24 MR. SHOOK: Well you know, again -- Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 But the PS is your actuation path. So the
2 Protection System is going to -- Like let's take
3 EFW. When I actuate EFW -- Let's go back to the
4 previous slide, Shaun.

5 So emergency feedwater, I am going to
6 look at I have got four steam generator level
7 sensors per steam generator. Those come into the
8 APUs get paired to sub-point. I share my
9 information between the networks, do two out of four
10 voting and then basically train one, a VFW gets
11 actuated out of Division 1 of the Protection System
12 through the PACS. Okay?

13 Now that is just the actuation. So out
14 of the PS I will essentially get a one, a logical 1
15 and then that starts the pump and opens the
16 isolation valve and the control valve.

17 Now at the same time I send a signal
18 from the PS to SAS to initiate the closed-loop level
19 control. So, --

20 MEMBER BROWN: There is no closed-loop
21 level control. In here it just shows you have on
22 and off operating and actuator or a signal which is
23 kind of a --

24 MR. SHOOK: Right. The control units

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 are doing that control and we use -- because most
2 of the actuators are it is like the main feedwater
3 valve in our previous slide. So it is a --

4 MEMBER BROWN: It is not -- Is this
5 going to be a variable control signal going through
6 the Priority Module?

7 MR. SHOOK: It's an on/off control. No,
8 it is not a variable control signal.

9 MEMBER BROWN: Is it just open the
10 valve?

11 MR. SHOOK: It's open --

12 MEMBER BROWN: If you do the same thing,
13 I am just trying to figure out the difference
14 between the PS and the SAS. They both look like
15 they are doing the same thing, opening a valve.

16 MR. SHOOK: Okay. So level drops in the
17 steam generator. I actuate EFW. And EFW level
18 starts to go back up. Right?

19 MEMBER BROWN: No, before it goes back
20 up. You have got to actuate -- You have got to open
21 the valve and start the pump.

22 MR. SHOOK: Right.

23 MEMBER BROWN: Which one of these starts
24 those?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: The actuation path through
2 the Protection System.

3 MEMBER BROWN: What does the one out at
4 the SAS do?

5 MR. SHOOK: So I am getting to that.

6 So, I get down to the actuation level
7 setpoint and I actuate EFW. So I start the pump and
8 I open the control valve and the isolation valve.
9 When I open the control valve --

10 MEMBER BROWN: The EF system?

11 MR. SHOOK: -- by the PS through the
12 PACS, independent of the SAS.

13 MEMBER BROWN: Uh-huh.

14 MR. SHOOK: Okay? So now I am
15 basically, I am putting in 440 GPM into the steam
16 generator and the level is going to start to
17 recover.

18 MEMBER BROWN: Yes.

19 MR. SHOOK: Okay? Now, if I didn't do
20 anything else, I am just going to overfill the steam
21 generator. So what I do then is I do two things.
22 When I first actuation, I send that signal not only
23 to the PACS but I send it to SAS to initiate the
24 closed-loop level control. So that level control

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 starts. So you can think about it on the PACS I
2 have opened the control valve and then from the SAS
3 I also have the signal that says open the control
4 valve.

5 So even if the SAS said close the
6 control valve, it is not going to do anything. It
7 is going to open. Once level clears its minimum
8 setpoint, the protection system automatically resets
9 EFW and removes the actuation signal off the pump,
10 the isolation valve, and the control valve. So now
11 I have no active signals from the PS. So the pump
12 will keep running and the isolation valve will stay
13 open but now the level control valve, it goes from
14 the closed to control mode and as it reaches its
15 normal control setpoint, it will start modulating
16 back and forth, open/closed to maintain level within
17 its prescribe band.

18 And the valve itself is a motor-operated
19 control valve, again, similar to the feedwater
20 control valves that we used in submarines. So the
21 output is just an on/off. It uses a PID step
22 controller or a PI step controller, to be clear.

23 So the output of the PI is an
24 open/close, not a continuous four to 20 position

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 signal.

2 MEMBER BROWN: Okay. So you just cycle
3 between two bands, then, an upper band and a lower
4 band. You hit an upper band and it tells it to
5 close. And it is closed and it goes down and tells
6 it open and it comes open.

7 MR. SHOOK: Again, it works just like
8 the Steam Generator Water Level Control System on
9 the submarines where it is a PI controller but the
10 output, it is a discrete output. It is either open
11 or closed. It is not an analogue output. You know,
12 so as the PI controller, as you start to deviate
13 your error at some point, --

14 MEMBER BROWN: Our is an analogue
15 output.

16 MR. SHOOK: Not on the 688 --

17 MEMBER BROWN: We don't just close them?

18 MR. SHOOK: The 688s was at least --

19 MEMBER BROWN: Don't talk about it.

20 MR. SHOOK: Okay. All right. See, I
21 told you they warned me.

22 Anyway, the way this -- If I were to
23 trace the output of the -- As it is modulating to
24 maintain level within the band, if I were to look at

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the output, it would say open and then there would
2 be no -- and then once it is back within its error
3 band, there would be no open or closed. And then if
4 it went high, then it would say closed.

5 MEMBER BROWN: Oh, okay. We are just
6 talking different language. That is what I was
7 trying to say.

8 MR. SHOOK: Okay. Okay, so we are
9 aligned.

10 MEMBER BROWN: Yes, we are aligned.

11 MR. SHOOK: Okay, good. So yes, this
12 closed-loop control is going to be operating in SAS
13 to keep the level here. But then the protection
14 system, you have got the actuation and the isolation
15 at the top and bottom to keep it within its --

16 MEMBER BROWN: But that open and closed
17 still goes through the priority module?

18 MR. SHOOK: That's correct, yes. So
19 both the PS --

20 MEMBER BROWN: So if something else
21 takes priority, it will just let the water keep
22 going out or coming in until it is allowed to do
23 something.

24 MR. SHOOK: Yes, if the Protection

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 System -- If the SAS is going to have an open/close
2 signal and the PS has an open/close signal for this
3 particular case. Right? So as long as I am
4 controlling normally with SAS, the PS is not going
5 to do anything. There won't be any active signals
6 on the PACS. So I am happy.

7 But if I have a control system failure
8 that drives level high or low, the protection system
9 will come in and take the appropriate actions
10 whether it is isolate or actuate. You can think of
11 it like this. If my SAS fails, --

12 MEMBER BROWN: The only priority it has
13 to evaluate is between SAS or PS, --

14 MR. SHOOK: Well --

15 MEMBER BROWN: -- in this particular
16 function.

17 MR. SHOOK: In this particular example,
18 right.

19 MEMBER BROWN: Well, for emergency
20 feedwater.

21 MR. SHOOK: Well and DAS because I have
22 -- Below the PS setpoint I have a DAS EFW actuation.
23 I also have a manual control from SICS and a manual
24 control from PICS.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: Okay.

2 MR. SHOOK: Okay? All right. Okay, 36.

3 Okay, we looked at -- Yes, I apologize about the
4 eye test.

5 So when we look at redundancy for the
6 ESF actuation, again we are going to look at the
7 different levels. We look at the sensors, signal
8 conditioning APU level, main actuation ALU and then
9 PACS and actuators.

10 So for the signal sensors and signal
11 conditioning APUs, most ESF actuations are four-fold
12 redundant for each process variable. The same as
13 protection system. Some exceptions for the EDG
14 actuation, we look at three voltage sensors per
15 division. So within each division, I am looking at
16 voltage on that bus and I do a two out of three vote
17 on those values.

18 And then for the RCP trip, we have two
19 D/P sensors per division. So those are the
20 exceptions at this sensor level.

21 For manual actuation, this is, we
22 basically you can think of it as -- And this is all
23 driven by the requirements from IEEE 603.

24 So when you look at the actuation of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 functions, some functions are what I call all four
2 trains and then some functions you do on a per train
3 basis. So when we look at all train functions, we
4 look at safety injection actuation, partial
5 cooldown, main steam isolation, containment
6 isolation, turbine trip, hydrogen mixing dampers
7 opening. And in those cases, I have our switches
8 and I need two out of four of those switches to get
9 the function to actuate. But once I get that two
10 out of four, all the trains of those functions
11 operate.

12 And then for Main Control Room System
13 Isolation and Filtering, I have two switches and
14 that is done on a one out of two voting. And either
15 of those switches will cause both MCR trains to
16 switch into filter and isolate.

17 When I look at the functions that are
18 done on a per train basis, I first look at for the
19 steam generator isolation function, we have four
20 switches per steam generator, and that is
21 implemented in two out of four voting.

22 MEMBER BROWN: Does it isolate all four
23 steam generators?

24 MR. SHOOK: No, that is just per steam

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 generator. So I have got four switches for one
2 steam generator; four for another; four for another;
3 four for another.

4 For the EFW actuation isolation MSR T
5 actuation isolation, main feedwater isolation, EDG
6 actuation, reactor coolant pump trip, I have two
7 switches per train and I just need one of those two
8 to perform the function.

9 And then for PSRV opening, I essentially
10 have enough there in the PSRV design, I have for
11 LTOP, you know, normally there is now power
12 operation but for LTOP we utilize two solenoid valves
13 in series and you essentially need both of those
14 solenoid valves to open to get the PSRV to open. So
15 in this case I have two switches that are two out of
16 two voting.

17 And then the final one is CVCS charging
18 isolation anti-dilution I have got one switch per
19 train. And those are very simple functions. There
20 is essentially a couple of valves, you know, two
21 valves in one division and one valve in a different
22 division.

23 MEMBER STETKAR: Jeremy, just because
24 you mentioned it and I don't know where else to ask

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 question, anti-dilution function during normal
2 power operation, I understand how it works. There
3 is two valves in the letdown line. There is one
4 valve from the VCT that goes closed. When you are
5 in cold shutdown, it is five and six.

6 When you are letting down from the RHR
7 system, does the anti-dilution logic, is the VCT
8 valve the only valve that is preventing you from
9 dilution?

10 MR. SHOOK: I'm going to ask --

11 MEMBER STETKAR: In other words, does
12 the anti-dilution logic close the low pressure
13 letdown flow path from the RHR system? It is a
14 question -- I can't get anybody to answer that
15 question. I have been poked from section four to
16 section nine and now you have got it.

17 (Laughter.)

18 MR. SHOOK: So just to be clear, this is
19 for anti-dilution specifically?

20 MEMBER STETKAR: This is specifically
21 anti-dilution.

22 MR. SHOOK: Okay.

23 MEMBER STETKAR: Because the low
24 pressure letdown line comes into the letdown flow

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 path downstream from the two valves that are
2 normally closed, you know, by the signal during
3 power operation.

4 MR. SHOOK: Okay.

5 MEMBER STETKAR: There is a lot of
6 discussion in the FSAR about redundancy and things
7 like that for anti-dilution protection and that the
8 isolation is the only safety-related function. And
9 it is not clear to me that you would have -- It is
10 not clear to me whether or not you are vulnerable to
11 a single failure to prevent dilution during shutdown
12 when you are on that low pressure letdown flow path.

13 So the basic question is, you know, are
14 the low pressure letdown valves closed automatically
15 by the anti-dilution signal?

16 MR. SHOOK: Okay.

17 MEMBER STETKAR: I probably won't get an
18 answer at the moment. You might have to take it
19 away just to keep the discussion going.

20 MR. SHOOK: Okay.

21 MEMBER STETKAR: I couldn't figure out
22 where else -- since you mentioned it here, I thought
23 I would interject it.

24 MR. SHOOK: All right. You want to take

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 this as an action item?

2 MR. PHAN: Yes, we will take it as an
3 action item.

4 MEMBER STETKAR: Thanks. It's been
5 bouncing around since March 3, 2010. So, I'm hoping
6 that sometime in the next couple of years I can get
7 an answer.

8 MR. SHOOK: Okay. So just to make sure
9 I understand it. So this is anti-dilution and how
10 we deal with it when we are in RHR.

11 MEMBER STETKAR: Exactly. Yes.

12 MR. SHOOK: Okay.

13 MEMBER STETKAR: When you are in that
14 low pressure letdown mode.

15 MR. SHOOK: Okay.

16 MEMBER STETKAR: Because you know, the
17 tech specs require the function to be operable in
18 all six modes.

19 MR. SHOOK: Right. Okay.

20 MEMBER STETKAR: And indeed, there may
21 be situations when you are in shutdown where you are
22 actually vulnerable to dilution.

23 MR. SHOOK: Okay. Yes, we will take a
24 look at 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 Okay, going on to the ALUs, again we are
2 eight-fold redundant on the ALUs. Again, four
3 divisions to meet single failure and two ALUs per
4 division to improve plant availability. In this
5 case, it is specifically if I have an ALU out of
6 service, I don't have to spec for losing that one
7 division.

8 Most voting is two out of four. The
9 exceptions, as we discussed, EDG actuation is two
10 out of three, and RCP trip is one out of two per
11 division per pumps and then two out of four voting
12 for all pumps.

13 The PACS essentially as I mentioned
14 before, I have one pair of priority and
15 communication modules for each actuator. And
16 actually to be more specific per each actuation
17 device. So for example, PSRVs, I actually have two
18 solenoids. So each solenoid gets a pair, a priority
19 and communication module. Sometimes when we say
20 actuator and actuation device we are not always
21 clear on that point. So I just wanted to make sure
22 we are clear.

23 And then actuators themselves, then we
24 are just in the mechanical design of the plant.

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 Most ESF functions are four-fold redundant. You
2 know, for example, we have four EFW trains. We have
3 four safety injection trains but there are a number
4 of functions that are two-fold redundant. And this
5 is kind of counterintuitive. EFW isolation, even
6 though we have four trains for actuation, the
7 isolation function, the safety function is on a per
8 steam generator basis. So you are two-fold
9 redundant there. So you have two valves that can
10 isolate the line. You need control valve and the
11 isolation valve.

12 MSRT actuation and isolation are two-
13 fold redundant systems. Main feedwater isolation,
14 containment isolation, steam generator isolation,
15 and RCP trip, MCR HVAC and CVCS are all essentially
16 two-fold redundant systems.

17 For ESF control it is a little bit more
18 straight forward. Next slide. Basically the
19 control functions just follow straight up and down
20 the redundancy of the mechanical train. And we
21 provide for redundant control units per SAS division
22 and provide for improved availability. Because like
23 I said, if we take one control unit out of service,
24 we still have a fully redundant one in that division

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 perform all the functions needed.

2 CHAIR POWERS: I wonder if this would
3 not be an appropriate time to break for lunch.
4 Independence is a subject of interest.

5 MR. SHOOK: Yes, I think we could get
6 through this section because a lot of the features
7 for independence are the same. So there is only a
8 couple of differences we just have to talk through.

9 I mean, I think we need probably about five to ten
10 minutes and we could probably get through the rest
11 of the slides.

12 And this is about from our dry runs,
13 about halfway through the presentation.

14 CHAIR POWERS: Halfway through the view
15 graphs.

16 MEMBER BROWN: I would note the time for
17 the afternoon session is less than the time for the
18 morning session for you to finish the other half.

19 MR. SHOOK: Okay.

20 MEMBER BROWN: I just thought I would
21 point that out.

22 MR. SHOOK: Okay, well we can
23 accelerate.

24 Slide 38. So the main point here is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that for all these points, it is the same features
2 for independence as we have reactor trip because it
3 is implemented in the same system. So I am not
4 going to go back and speak to those again. So we
5 will just talk about the differences.

6 The first difference is sending signals
7 from the PS to the PAS. Those are hardwired output
8 via an Or and an isolation device from the ALUs over
9 to the PAS. Again, we already talked about why we
10 do that and the means that we do physical
11 separation, electrical isolation. It is non-dated
12 communication so fairly straight forward to provide
13 for independence.

14 The next slide.

15 MEMBER BROWN: Now you have the same
16 issue on independence that you had in the other.

17 MR. SHOOK: For the isolation, the
18 electrical isolation?

19 MEMBER BROWN: Communications isolation.

20 MR. SHOOK: Yes.

21 MEMBER BROWN: So the same issue applies
22 here in how you want it to fail.

23 MR. SHOOK: For the control units, you
24 mean?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: For the actuation ESFS.
2 And I'm just looking at --

3 MR. SHOOK: Yes. Yes.

4 MEMBER STETKAR: But here it is
5 different. If the system hangs, you don't get the
6 ESFS signal.

7 MEMBER BROWN: Well that is a question
8 of how they want the lockup to perform.

9 MR. SHOOK: Yes. We have a slide to
10 speak to that.

11 MEMBER STETKAR: Okay.

12 MR. SHOOK: So we will go through that.

13 For the control units, this is slide 40,
14 we have networks between the control units that
15 require interdivisional communication. We send
16 signals for voting for the ESF control functions,
17 this is the only reason right now per Rev. 3 that we
18 send those signals. It is a data-based means of
19 communication and we provide the same mechanisms for
20 independence are used as what we already talked
21 about between the APUs and the ALUs.

22 MEMBER BROWN: But that is in the SAS.

23 MR. SHOOK: This is in the SAS, yes.

24 MEMBER BROWN: And that is not what it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 actuates.

2 MR. SHOOK: That's right. This is for
3 control.

4 Okay, for PACS, basically we have non-
5 safety inputs into the PACS and those are dealt with
6 differently. For the DAS, the hardwired connections
7 are implemented via isolation device within the PACS
8 cabinets. Again, we have physical separation in
9 terms of the cabinet locations and cables. And then
10 our interface to the PAS, a couple of key points.
11 One, we use fiber optic cable to connect between the
12 communication module and the PAS. The communication
13 module itself is qualified as an associated circuit.

14 So even though it is not performing a IE function,
15 it is qualified to that level of specification. And
16 so we can credit the electrical independence point
17 to be the fiber optic connection.

18 And then lastly, communications
19 independence. So the Communication Module
20 implements a microcontroller but the interfaces to
21 the PLD are hardwired, you know, just zero to 24-
22 volt signals. So in this case, there is no data
23 communication going to the priority module. Just
24 on/off signals.

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 Okay, next slide is deterministic
2 response time. Basically, up until the PACS,
3 everything is the same as we have already discussed
4 for the reactor trip. And then the PACS itself, the
5 Priority Module, that technology of the PLD provides
6 for inherent and predictable response time
7 characteristics. Again, there is no operating
8 system, no fixed cycle time. It is just performing
9 combinatorial logic on a signal basis.

10 MEMBER BROWN: Is the PAS the same for
11 all logic processing operations? In other words, is
12 there a discrete -- because I just don't know what
13 it looks like. Is there a discrete max processing
14 time regardless of how you sew in the logic devices
15 internally?

16 MR. SHOOK: Yes, we specify a maximum
17 response time based on -- So again the safety
18 functions specify with an overall loop response time
19 and then we sort of divide that up to, you know,
20 SCDS gets this much, PS gets this much, PACS gets
21 this much. So it will get allocated a certain
22 percentage of that, let's say ten milliseconds or 15
23 milliseconds. And then we will do testing to verify
24 that. But I guess the point is is that based 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 type of technology in terms of demonstrating that
2 the response time will be deterministic that we
3 don't have to worry about time-dependent behavior
4 like you would have to look at a microprocessor
5 system.

6 MEMBER BROWN: So it is fixed once you
7 program it. Once you decide what the logic array
8 is, you want the PLD to reflect.

9 MR. SHOOK: That's correct.

10 MEMBER BROWN: It becomes fixed and --
11 Okay. There has got to be multiple paths depending
12 on -- Because this is not a simple module.

13 MR. SHOOK: I see your point, yes. But
14 --

15 MEMBER BROWN: Some of them go straight
16 through faster, it would seem to me.

17 MR. SHOOK: Right.

18 MEMBER BROWN: And some of them will be
19 longer and you have got to be able to determine
20 which one, which request sequence could result in
21 the longest response time. I assume it is variable.

22 MR. SHOOK: The one that we are --

23 MEMBER BROWN: Not variable. That is
24 the wrong way.

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. SHOOK: No, I understand.

2 MEMBER BROWN: There is three steps.
3 There is a longer term and shorter term.

4 MR. SHOOK: The path that we are
5 interested from a response time perspective is a
6 path that the protection system signals take through
7 the PACS module. Because that is --

8 MEMBER BROWN: That is the credited one?

9 MR. SHOOK: Well, the ESFS functions,
10 your actuation functions are ones that come with
11 very strict response time requirements. And so when
12 we demonstrate that the loop meets the overall
13 response time for the actuation function, we are
14 going to test specifically the path that the
15 protection system signals go through that circuit
16 card.

17 So for example, we don't care
18 necessarily what the response time of the signal
19 path from the PAS through the PACS because that is
20 not -- I mean, we care to some extent but it is not
21 something that is really discretely very specified
22 very clearly and concisely as we do have for the
23 ESFS functions.

24 So from a safety perspective, from an

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 actuation function perspective, the protection
2 system path is the one that we are interested one
3 and that is the one that we will test to make sure
4 that we meet that response time behavior.

5 MEMBER BROWN: Will the controllability
6 thing, since you use the SAS for the automatic
7 control? Isn't there some interest in the time
8 response of the -- because that is where you are
9 telling the valves to open and close or whatever --

10 MR. SHOOK: Right.

11 MEMBER BROWN: -- based on your
12 bandwidth.

13 MR. SHOOK: Yes, there would be, I mean
14 obviously it is, I mean that is something we are
15 interested in but it is not generally, with this
16 type of technology, it is not something that we need
17 to -- I mean, we could specify that but it is
18 typically not something you have to worry about
19 because the technology itself is generally fast
20 enough. You know, it is going to be generally
21 faster than the control units, much faster than the
22 control units. For the control functions, we are
23 not quite as concerned about it.

24 MEMBER BROWN: All right.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: And also the control
2 functions, because it is a closed-loop control, you
3 know, those type of things will generally work
4 themselves out, as long as you know, you are not
5 putting 20 things in series.

6 Okay, 43, fail safe behaviour. So this
7 is addressing Mr. Stetkar's question. Again, for
8 the out of range failures, we have the same
9 detection mechanism with the APU and then flag the
10 signal and modify the voting. Here we do things a
11 little bit differently in reactor trip. For most
12 functions, we modify the logic towards no actuation.

13 So for a signal sensor failure, we go to two out of
14 three. For two sensors, we go to two out of two and
15 then three or more sensors, we go to ESF not
16 actuated.

17 There are two functions that we modify
18 towards actuation for sensor failures, MCR HVAC
19 realignment and hydrogen mixing damper actuation.
20 Those go through the same sensor reconfigurations
21 reactor trips. So we do two out of three, one out
22 of two, and then actuation.

23 And then essentially where it talked
24 about the APU failures, essentially dealt with 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 same as the signal conditioning. And then
2 everything downstream of that, if we design to fail
3 low and that results in no ESF actuation for all
4 functions.

5 MEMBER BROWN: So if the function
6 processors all lock up in this, that is what the
7 ALUs are.

8 MR. SHOOK: Yes, right.

9 MEMBER BROWN: If they all lock up, it
10 will -- Is that a fail low? Does that by definition
11 go in that direction if they lock up?

12 MR. SHOOK: Yes, that is how it is
13 designed. We design it to fail low.

14 MEMBER BROWN: Forget sensors or stuff
15 like that. I'm talking about ALU outputs. You say
16 they are designed to fail low. But you have to
17 consider the failure modes in order to do that.

18 MR. SHOOK: That's correct, yes.

19 MEMBER BROWN: And my concern is that
20 assumes it is processing. And if it is not
21 processing, what tells it to fail low?

22 MR. SHOOK: Well in this case, the
23 hardwired-based watchdog timer will --

24 MEMBER BROWN: Fail it low.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: -- drive the output cards to
2 fail low.

3 MEMBER BROWN: That is going to be
4 acknowledged or explained at some point --

5 MR. SHOOK: Yes.

6 MEMBER BROWN: -- later?

7 MR. SHOOK: We will get to that
8 information.

9 MEMBER BROWN: And how that is done?

10 MR. SHOOK: Yes. Yes, we can give you
11 that detail.

12 MEMBER BROWN: All right, thank you.

13 MR. SHOOK: Okay, slide 44. The control
14 function, typically the safe state for a control
15 function is fail as-is. And so when we look at the
16 sensor signal conditioning and distribution
17 failures, the out of range failures are flagged
18 and the outputs of the PI step controllers are
19 failed low. So there is no control signal set.
20 There is no open or closed signal sent out of the
21 SAS. And again, in range failures aren't detected.

22 Control unit failures, since they
23 operate in a master/hot-standby configuration so if
24 one control unit fails, it will swap over to the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 other control unit. And so the end result is you
2 have no loss in functionality.

3 And then output logic circuit failures
4 and PACS failures --

5 MEMBER BROWN: How fast do they have to
6 transfer?

7 MR. SHOOK: What's that?

8 MEMBER BROWN: How fast do they have to
9 transfer? Have you all done this before?

10 MR. SHOOK: They are using this -- Yes,
11 this has been done before in control systems that
12 use TXS, as well as I believe this is being done in
13 Europe for the Protection System design because it
14 is a little bit different but I will have to double
15 check on that.

16 MEMBER BROWN: Continue.

17 MR. SHOOK: Okay, next slide. And then
18 testing, you know, it essentially follows the same
19 protocol as we had for the reactor trips. The one
20 difference being for the actuation device
21 operational test. That is sort of done in two
22 parts. We do what is called a no-go test, where we
23 send outputs from the ALUs to the priority module
24 and we disable the priority module outputs so 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 we can test the connection between the PS and the
2 PACS but not actually actuate the final end device.

3 And then separately, we will do a go
4 test where we will check the actual actuator
5 configuration. And in that case, we will do that
6 test from PICS and it will just be at a component
7 level through the PICS to the PAS through the
8 Priority Module. So between those two tests, we
9 will be overlapping a section of the circuitry
10 within the PACS to make sure we have complete
11 coverage of the whole test path or the whole
12 actuation path.

13 MEMBER BROWN: Have you got time-
14 response testing down here? Is there a periodicity
15 on doing that?

16 MR. SHOOK: Yes.

17 MEMBER BROWN: Is this just a
18 qualification test and you never do it again?

19 MEMBER STETKAR: It is 24 months.

20 MEMBER BROWN: Oh, okay. I was just
21 curious. Twenty-four months you said?

22 MEMBER STETKAR: Yes, 3.3.1.10 is 24
23 months.

24 MEMBER BROWN: Yes, I saw that there, I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 just didn't -- I hadn't looked at that. That's all.

2 All right.

3 MR. GARDNER: I think, Dr. Powers, we
4 are now at the appointed break point.

5 CHAIR POWERS: Okay. We will recess for
6 lunch until 20 minutes after the hour.

7 (Whereupon, at 12:20 p.m., a lunch recess was
8 taken.)

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

A F T E R N O O N S E S S I O N

1:20 p.m.

CHAIR POWER: On the record. Let's come back into session. We're still involved in Section 7 and in particular 7.4, Systems Required for Safe Shutdown.

MR. GARDNER: Okay. And so you've got two quick things we'd like to go back on, one from yesterday. So the first one from yesterday is a question that we got asked and we'd like to correct our response.

Tim Stack.

MR. STACK: Yes, I am Tim Stack from AREVA. Yesterday we had a question about the risk-significance of the firewater system. And in the original DC supplement and in the original work that was done it was classified as nonrisk-significant.

In a subsequent RAI 268, Supplement 1, there was a further reevaluation and rescreening and it was screened in at that point as risk-significant. That appears in the DC FSAR Table 17.4-2 and that's in the current Rev 3 of the FSAR.

MEMBER STETKAR: It's in Rev 3. So it is screened 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 MR. STACK: It is screened in now.

2 MEMBER STETKAR: Thanks, Tim.

3 MS. SLOAN: By the expert panel?

4 MEMBER STETKAR: Yes. It's not
5 necessarily surprising that it wouldn't meet the
6 numerical goals given the plant design from the fire
7 PRA. But I was surprised. So the expert panel did
8 screen it. Thank you. That's good.

9 MR. GARDNER: Okay. We have one other.
10 We will wait until Mr. Brown returns because it was
11 one of his questions. And we'll proceed along with
12 Section 7.4.

13 CHAIR POWER: All right.

14 MR. SHOOK: Okay. So starting on slide
15 48, actually I'm sorry. We skipped that one. We
16 have three topics with regard to Section 7.4. We're
17 going to talk about the basis for safe shutdown.
18 We'll talk about the design and how we implement
19 safe shutdown functions within the DCS and then talk
20 specifically about transfer from the main control
21 room to the RSS.

22 Slide 48. So when we talk about safe
23 shutdown, there's a number of different scenarios
24 you've look at for safe shutdown. For normal, 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 I call, design-based events, accidents are described
2 in Chapter 15. For fires including loss of MCR it's
3 discussed in Chapter 9. SBOs talked about in
4 Chapter 8.

5 We're not going to get into the
6 specifics of exactly what systems are used to
7 mitigate those particular events. But the key
8 points you have to know for the INC are that
9 depending on the scenario we can use credit either
10 safety related or non-safety related systems to
11 reach and maintain safe shutdown, depending on that
12 particular event.

13 Having said that, going to Slide 49,
14 then talk about how we control those systems from
15 the different locations. Within the DCS, we look at
16 a couple different things. First of all, we have
17 what we call manual group controls. And so we have
18 manual controls overall. And then I'm --

19 MEMBER STETKAR: Before you get into the
20 details here, I'm trying to get spun up after lunch.

21 You said you're not going to go into details for
22 each of the different types of scenarios. Station
23 Blackout, the rated battery life is two hours. Is
24 that correct?

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. SHOOK: For the EUPS, that's
2 correct.

3 MEMBER STETKAR: For the -- I'm sorry.

4 MR. SHOOK: For the EUPS. For the power
5 supply for the safety related --

6 MEMBER STETKAR: Safety related.

7 MR. SHOOK: That's correct.

8 MEMBER STETKAR: So after two hours I'm
9 dark.

10 MR. SHOOK: That's correct.

11 MEMBER STETKAR: Okay. I just wanted to
12 make sure. I sort of remembered that from
13 somewhere.

14 MR. SHOOK: For the non-safety systems -
15 -

16 MR. STACK: Excuse me, Jeremy. Let me
17 interject. Tim Stack from AREVA again. But the
18 battery chargers are powered off the SBO diesels.

19 MEMBER STETKAR: I understand. I tend
20 to think of Station Blackout as no AC power.
21 Thanks.

22 MR. SHOOK: And I would also make the
23 comment that the non-safety systems at least on the
24 nuclear island received power from the 12-hour UPS.

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 SBO power supplies.

2 MEMBER BROWN: Which systems? From the?

3 MR. SHOOK: The non-safety. The PICS,
4 PAS, RCSL and DAS and specifically PS in the nuclear
5 island receive power of the 12-hour UPS.

6 MEMBER BROWN: Twelve-hour?

7 MR. SHOOK: Yes. But I want to be
8 clear. The 12-hour USP, the UPS isn't sized to keep
9 all the systems powered for 12 hours. It's only
10 sized to keep -- It's sized basically to keep all
11 the systems powered for two hours and then from two
12 to 12 only those systems that are needed for
13 basically severe accident monitoring and so forth.

14 MEMBER STETKAR: So with load-shedding
15 you can assimilate that to hold on.

16 MR. SHOOK: That's right.

17 MEMBER STETKAR: Thank you.

18 MR. SHOOK: So if you didn't load shed,
19 there would be somewhere between two and 12.

20 MEMBER STETKAR: Okay. Thank you.

21 MR. SHOOK: Okay. So if we look at the
22 safety shutdown, we have manual controls needed to
23 transition the plant down to safe shutdown. We
24 divide those into two categories. We have what 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 call manual grouped controls and this is defined as
2 a manual action that results in the positioning of
3 two or more actuators. For example, if I'm going to
4 -- Like an example that would be manual actuation of
5 a trade of EFW. So I hit actuate train one. The
6 pump starts and both valves open all at the same
7 time.

8 Contrast that with component level
9 control, I start the pump with one manual action and
10 I open the control valve with another action. I
11 open the isolation valve with a third manual action.

12 That's the difference between grouped in and
13 control level controls. And the reason I highlight
14 that difference is that it affects how we sort of
15 allocate those different functions within the
16 design.

17 We first looked at manual grouped
18 controls related to safety related systems. I
19 allocate that to two paths within the design.
20 Within the MCR we allocate that to two paths. One
21 is from the SICS through the SAC and to the PACS.
22 And then I allocate that to the PICS and PACS and
23 PS.

24 And you're probably asking why I am

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 putting the same function in two places. Again, the
2 reason is because I want to the operate to stay on
3 PICS as long as it's available. So I'm going to
4 provide them all the capability and functionality
5 that I can provide from PICS given the constraints
6 of the design that we currently have.

7 Since we don't allow communication
8 directly from the PICS to the SAS, but we do allow
9 communication from the PS to the PACS, I allocate to
10 this alternate path. And that path is also
11 available in the remote shutdown stations. And
12 since I can credit PICS in the remote shutdown
13 station, I don't need to duplicate that on the SICS
14 in the remote shutdown station.

15 For component level controls, from the
16 main control room I have two paths. I have controls
17 that are credited on SICS and those are directly to
18 the PACS modules. They don't go through a
19 automation system of either the PS or the SAS. And
20 I also have the same path from PICS and PS to PACS
21 through the control safety related equipment. And
22 again that's done so that the operator can stay on
23 PICS as long as it's available. And if it's not
24 available, then they can transition to SICS. So

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 can perform a safe shutdown in the main control
2 room from either control locations.

3 And again in the RSS because I have that
4 capability on the PICS that I can credit PICS for
5 that scenario, I don't need to duplicate those
6 controls on the SICS.

7 For the control non-related safety
8 systems, it's a little bit simpler. We provide
9 controls on PICS through PS directly. So since
10 there are not any safety related systems, I don't
11 need to go through the PACS. And there's not really
12 any overlap between the non-safety systems that we
13 have on SCDS and PACS as those that were during safe
14 shutdown here.

15 I guess the main takeaway is if I'm in
16 the control room I can do safe shutdown either
17 completely from PICS or completely from SICS. And
18 from the MCR -- I'm sorry. From the RSS, I can do
19 -- I need the combination of both PICS and SICS to
20 reach and maintain a safe shutdown. I can't do it
21 from either location by itself. Let's go to the
22 next slide.

23 So we're going to talk about here
24 specifically MCR and RSS transfer. The operators,

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 required to leave the main control room due to an
2 event that required that loss of main control room,
3 for example, like a fire or toxic gas, will leave
4 the main control room, ideally trip the reactor
5 before they leave.

6 But once they get down to the remote
7 shutdown station they'll perform these actions.
8 They will activate the main control room to RSS
9 transfer switches which does the following
10 functions. First of all, it will disable the inputs
11 from the main control room to the Protection System,
12 the SAS and the PACS. All those hard-wired inputs
13 from the MCR will no longer be operable.

14 It also just disables the DAS outputs
15 completely. So this is a little bit different from
16 the first three systems. The reason why we do this
17 is because the DAS there are certain permissives
18 that you would have to implement in order to
19 transition to say shutdown. We decided that it was
20 simpler to do this than it would be to add those
21 permissives in a remote shutdown station and
22 increase cabling and potential for complications
23 with fires and so forth.

24 Since we already had these signals

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 running down into the safeguards buildings, we just
2 decided to go ahead and disable DAS. It's not
3 needed for this scenario and it was a simpler design
4 approach.

5 Then the next thing the operators will
6 do is log into the PICS workstations in the remote
7 shutdown station which we already discussed. And
8 again as we said they'll use the PICS for most
9 actions again with only a limited amount of controls
10 available on SICS.

11 That list is listed in Section 7.4. You
12 can go look at it. Essentially that list consists
13 of a manual reactor trip and then permissives needed
14 to transition the plant down to cold shutdown. For
15 example, P14 to allow going on to RHR.

16 And then we also provided a limited
17 number of ESF resets. And the thinking behind that
18 was what if the operator does something that causes
19 an actuation of safety injection. How am I going to
20 deal with that if I don't have those controls? We
21 decided to put a limited number of ESF resets,
22 basically those that directly affect your ability to
23 control inventory and remove the decay heat from the
24 plant, so SI, EFW, MSRT in the remote shutdown

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 station. And that way in case those systems weren't
2 to automatically actuate, the operator can reset
3 those and then take control back from PICS to go and
4 shut down the plant.

5 And then lastly to demonstrate
6 independence of the RSS from MCR, we already talked
7 about we've got redundant PICS servers physically
8 separated and we've got fiber optic cables. And the
9 six cables from the RSS are physically separated
10 from the main control room cables. That's it for
11 safe shutdown.

12 One of the things we're going to do is
13 address the issue of the hardwired watchdog timer.
14 We went back and looked at our submittals. We do
15 discuss that in two different Technical Reports.
16 One is the self-test report which is ANP 10315.

17 MEMBER BROWN: Let me get the right
18 sheet up.

19 MR. SHOOK: Sure.

20 MEMBER BROWN: Okay. Tell me that
21 again. ANP?

22 MR. SHOOK: It's ANP 10315 and the
23 specific section is 2.2.6.2.

24 MEMBER BROWN: 2.2.6.2?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: That's correct. And the
2 other place where we discuss it is the TXS Topical
3 Report.

4 MEMBER BROWN: Okay. The TELEPERM?

5 MR. SHOOK: That's correct. Yes. And
6 that's EMF 2110.

7 MEMBER BROWN: Yes.

8 MR. SHOOK: And the specific section is
9 2.4.3.4.2.

10 MEMBER BROWN: Okay.

11 MR. SHOOK: Okay. And just a -- I'll
12 just give a 30 second description of how it works
13 and then I'll let you go in detail.

14 MEMBER BROWN: Okay.

15 MR. SHOOK: So it's actually the
16 watchdog timer which is going to look at -- which
17 essentially gets reset every time the processor
18 finishes its fixed cycle operation along with some
19 time delay or it gets reset. If it doesn't reset
20 within the fixed cycle operation plus the time
21 delay, it will essentially put the processor into a
22 safe state and then set the output drivers to a
23 defined fail-safe state. So, in the case of reactor
24 trip, it will trip the reactor. In the case of ESF,

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 it will be the safe states we've already described.

2 MEMBER BROWN: Okay. Does it say what
3 the defined state is for each of those circumstances
4 in either place?

5 MR. SHOOK: In the specific sections, it
6 just says it's going to fail to a predefined safe
7 state. And then in another section's report it
8 talks about what the safe states are for those
9 different functions.

10 MEMBER BROWN: Does it refer to those?
11 Does it reference those in that section?

12 MR. SHOOK: Not specifically. So I'll
13 say it's not completely laid out as I'm describing
14 it here. But you can piece together the information
15 from the different sections.

16 MEMBER BROWN: Which one is 10315?

17 MR. SHOOK: That's the self test and --
18 What's it called?

19 MR. PHAN: Protection System --

20 MEMBER BROWN: Is it referenced in the
21 DCD?

22 MR. SHOOK: Yes.

23 MEMBER BROWN: It's referenced in the
24 DCD as being a source for defining how it's supposed

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 operate.

2 MR. SHOOK: Yes. The Technical Report
3 is used as essentially an extension of the DCD to
4 further incorporate specific technical information.

5 MEMBER BROWN: In other words, my point
6 being is that the designers, whoever gets the
7 contract, would have to comply with that.

8 MR. SHOOK: That's correct.

9 MEMBER BROWN: About regulation or
10 because it's been certified in that.

11 MR. TESFAYE: It is incorporated by
12 reference.

13 MEMBER BROWN: Okay.

14 MR. SHOOK: Okay.

15 MR. PHAN: One more reference section
16 that you wanted was you were asking where we
17 established our design rules for signal diversity in
18 the Protection System and how we allocated it.

19 MEMBER BROWN: Functional diversity
20 thing you were talking about?

21 MR. PHAN: Yes, functional
22 diversity/signal diversity.

23 MR. SHOOK: Right.

24 MR. PHAN: That's in Section 10.2 of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Protected System Technical --

2 MEMBER BROWN: Before you go any
3 further, you made that comment relative to the SCDS
4 I think. The one about which -- I want to make sure
5 we're talking about the same thing.

6 MR. SHOOK: This was the rules that tell
7 you whether it goes to subsystem A or B.

8 MEMBER BROWN: Okay.

9 MR. SHOOK: For the signal -- Or what I
10 was calling function diversity, but what in the
11 report is called signal diversity.

12 MR. BRIXEY: I think that we might have
13 come around to answer on that question because we
14 talked about how we allocate functions back and
15 forth.

16 MR. SHOOK: But he still wanted to see
17 the criteria for that.

18 MR. BRIXEY: Okay.

19 MEMBER BROWN: Okay. You said that was
20 where?

21 MR. PHAN: Section 10.2 of ANP 10309.

22 MEMBER BROWN: That is the Protection
23 System --

24 MR. PHAN: Technical Report.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: -- Technical Report.

2 MR. PHAN: Yes.

3 MEMBER BROWN: No wonder I didn't get to
4 that. It was in section -- It was just so exciting
5 I couldn't hold my eyes open.

6 The one other area I think I asked for
7 criteria you went through a discussion was on what
8 defines what goes through SCDS and what doesn't.
9 And you said there was a bunch of them.

10 MR. SHOOK: That's right. I'll get
11 that. I'll look that up. Can you write that down?

12 I'll get that on the next break.

13 MEMBER BROWN: Okay. Thank you.

14 MR. SHOOK: That's sort of all the look-
15 ups that we had to far. Let's go to slide 52.

16 Now we're discussing Section 7.5 which
17 is Information Systems Important To Safety. The
18 main -- This is sort of a catchall section, but here
19 are the main topics that we'll be discussing:
20 alarms, post-accident monitoring, PAM, safety
21 parameter display system or SPDS, emergency response
22 data systems or ERDS, tech support center, TSC, and
23 then bypassed and inoperable status indication,
24 BISI.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 With alarms, the inventory of alarms is
2 basically -- I'm going to punt to my Chapter 18
3 counterparts and essentially the alarms will be
4 determined via task analysis and alarm criteria
5 developed within the scope of the HFE programs. So
6 I'm not going to go into that detail today.

7 In terms of implementing the alarms
8 within the design, the various alarms are processed
9 within the different automation systems whether they
10 be DAS, PS, SAS, RCSL or PAS. And then they're
11 displayed both PICS and SICS. So PICS is going to
12 show all the alarms that are defined for the plant.

13 And then SICS will have a limited number of
14 hardwired alarms as determined for accident
15 mitigation, safe shutdown and any other potential
16 events like severe accidents or SBO.

17 MEMBER STETKAR: Jeremy, I am trying to
18 tie together a few things from different chapters
19 that we've seen. And this is in Chapter 18 of the
20 FSAR. There are statements of the sort that says,
21 "Alarm signals include logic so that only
22 operationally relevant conditions are alarmed. The
23 overall plant state is considered for the generation
24 of alarms or at least to inhibit alarms that are not

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 relevant for the actual plant state. Pre-alarms are
2 provided before automatic actuation only when an
3 operator has sufficient time to identify and perform
4 mitigative actions."

5 That tells me this isn't a simple alarm
6 system. It's some sort of smart alarm system that
7 contains again this term priorities and logic so
8 that the system knows what I, the operator, must
9 know and provides me only that information that it
10 knows I need. Is that a fair characterization?
11 And, if so, how does it know what I need to know?

12 I hate to be told by a machine that
13 "Don't worry your pretty little head. This isn't
14 something you need to worry about."

15 CHAIR POWER: I can assure you. Not
16 even a machine would say, "Don't worry your pretty
17 head."

18 (Laughter.)

19 They don't make that programming. That
20 is a non computable function.

21 MEMBER STETKAR: You've given them
22 enough time to think now.

23 (Laughter.)

24 MR. SHOOK: I'll say that -- I guess

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I'll answer that question in terms of the general
2 process and capability of the system. When you look
3 at the alarms, the two main ways that we can use to
4 essentially filter alarms to the operator, one is to
5 define the alarm in terms of a plant state. So
6 whether that's mode one through six or some other
7 criterion that we can use to set the alarm and say,
8 "Hey, don't -- " Or even as simple as "Don't give
9 me a low flow alarm if I turn the pump off." Right.

10 You know something as simple as that. And that
11 could range from broad criteria about studying modes
12 one through six and more detailed criteria about the
13 particular pumping sample.

14 The second main way we have to filter
15 alarms is actually by assigning a priority to the
16 alarm. And then the operator can use that to filter
17 based on the priority. So, for example, if I get a
18 reactor trip, I can say "Okay, I just want to look
19 at priority one alarms and I don't care about all
20 the other stuff." And then it lets me look at and
21 say, "Okay. I have low pressurizer pressure. I've
22 got this. I've got that." And then I can very
23 quickly diagnose the event as opposed to having to
24 look at a whole board of red lights lighting up

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 which is not an easy task.

2 So the system I'd say the general
3 process is there. And the system is capable of it.

4 But all that would be defined basically at an
5 alarm-by-alarm basis.

6 But to your point I mean that's all
7 specified with the alarm definition when the alarm
8 is shown in honest. It's just that we don't leave
9 it up to the vendor to make that decision. That's
10 part of the alarm specification.

11 And I want to be clear about that.
12 Those two features are really only available on
13 PICS. You know, SICS, you're not going to have that
14 capability. SICS is just you get what you get.

15 MEMBER STETKAR: You get what you get on
16 SICS.

17 MR. SHOOK: Yes. But again there would
18 be a limited number of alarms on SICS. You're not
19 going to have a complete annunciator like you expect
20 to see --

21 MEMBER STETKAR: Now are all alarms
22 available to the operator to pull up on PICS or?

23 MR. SHOOK: Yes.

24 MEMBER STETKAR: You mentioned there is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 some sort of prioritization or hierarchy. I have to
2 think about that. When are those priorities set?
3 Is that part of the human factors engineering? Is
4 it part of --

5 MR. SHOOK: Yes.

6 MEMBER STETKAR: I mean how does one
7 determine, for example, that the system knows that I
8 have a LOCA rather than overcooling event which can
9 give me a lot of the same types of indications.

10 MR. SHOOK: Right.

11 MEMBER STETKAR: And Alarm X has
12 priority one and because the system knows I have a
13 LOCA rather than Alarm Y that might have told I had
14 an overcooling event, that type.

15 MR. SHOOK: Right.

16 MEMBER STETKAR: Is there a scenario
17 type analysis that's done? Is there -- How is that
18 done and when is that done?

19 MR. SHOOK: It is done through when we
20 develop the logics as part -- You know, the logics
21 are essentially part of the human factors process.
22 And when we define the alarms for the system that
23 all gets worked out at that point in time. And we
24 will have -- I can't say we will have criteria that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 defines all that.

2 MEMBER STETKAR: You don't have a map.

3 MR. SHOOK: We don't have -- To my
4 knowledge, we don't have them. And I think all we
5 have in the HFE program is just implementation plans
6 that state that we will develop that criteria at
7 some point.

8 MEMBER STETKAR: Okay.

9 MR. SHOOK: But I would say it depends.
10 If the alarm is filtered based on what I was
11 saying. Like if I turn the alarm off because I'm
12 turning the pump off and I disable the low flow
13 water --

14 MEMBER STETKAR: That one I have no
15 problem with.

16 MR. SHOOK: Yes.

17 MEMBER STETKAR: It's having been an
18 operator in the old style plant there were a lot of
19 number of high priority alarms that we got used to
20 ignoring because some designer decided that they
21 shall be high priority. And to us they were really
22 more confusing. There were a lot of other lower
23 priority alarms that we paid a lot more attention to
24 because they gave us a lot more indications of 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 was going on in the plant.

2 MR. SHOOK: Right.

3 MEMBER STETKAR: Simply because the
4 designer doing design basis licensing type
5 deterministic analyses hadn't quite thought about
6 how the whole plant works.

7 MR. SHOOK: Right.

8 MEMBER STETKAR: And that's my
9 fundamental concern because it finally comes down to
10 the operator having the information at his hand.

11 MR. SHOOK: Right. Right. And I will
12 say --

13 MEMBER STETKAR: To understand what's
14 evolving in the plant without too much extraneous
15 filtering.

16 MR. SHOOK: And I will say as sort of a
17 general comment I do share your concerns as a former
18 operator and trainer of operators.

19 MEMBER STETKAR: Okay.

20 MR. SHOOK: It's hard as a designer to
21 foresee is this going to be important in this
22 situation or that situation. I will say the modern
23 systems, it's a tool. They offer a lot of
24 capability to improve the operators' performance and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 be able to diagnose situations and respond to that.

2 But you have to be -- When we actually develop that
3 criteria, we'll have to be careful about not trying
4 to over design the scenario.

5 MEMBER STETKAR: And the flip side is
6 the operators after several years and generations
7 become complacent. They know that the system knows
8 more than they do.

9 MR. SHOOK: Right.

10 MEMBER STETKAR: And they've never been
11 challenged unless people running simulator scenarios
12 get pretty doggone clever. They've never been
13 challenged to kind of question whether or not the
14 information they're receiving indeed is the
15 information that they need.

16 MR. SHOOK: Right.

17 MEMBER STETKAR: It's sort of "Well, the
18 system is telling me this and that's the way I
19 should react."

20 MR. SHOOK: Right. I will say I'm not
21 an expert on the NUREG-0711 process or anything like
22 that. But I will say that the part of the process I
23 understand in looking at trying to get operator
24 feedback early on in the process and also the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 verification I think will help out significantly to
2 drive out a lot of those things where before the
3 designers just did what they thought was right. And
4 then the operators get in there and say, "Well, why
5 do I need this?"

6 MEMBER STETKAR: In principle, it works.

7 MR. SHOOK: Yes.

8 MEMBER STETKAR: It's just in many cases
9 it's the selection of the scenarios that you use to
10 sort of test the process that's kind of critical.

11 MR. SHOOK: Right.

12 MEMBER STETKAR: Okay. Thanks. Let's
13 get back to the wires and electrons.

14 MR. SHOOK: Again, at some point we
15 could have a beer and I could talk to you more about
16 philosophical things.

17 MEMBER STETKAR: It would take several
18 beers, but that's okay.

19 MR. SHOOK: Okay. Moving to Slide 54.
20 So we're going to talk about post accident
21 monitoring. I didn't bother to show the list here
22 in the presentation, but it's in Section 7.5, Table
23 7.5-1. And just a couple of bullets here and how
24 that was developed. We thought it was important for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 background information.

2 Essentially we looked at -- We evaluated
3 the B&W owners group EOP technical basis document.
4 AREVA's predecessor company was B&W. So we got
5 access to this information and used that as a
6 starting point essentially. The one important piece
7 to note especially for Member Brown coming from the
8 Navy it's a symptom based approach, not event based
9 which is like different.

10 And again you can have people on either
11 side argue the merits of one or the other. I'm not
12 going to get into that approach. But it is a
13 symptom based approach.

14 And then we looked at the differences
15 obviously in the B&W plant design versus the EPR.
16 Then we also looked at credited operator actions in
17 Chapter 15 specifically for the tube rupture event
18 and a couple other things. And then per IEEE-497,
19 we went and looked at the critical safety functions
20 and fission product barriers functions as discussed
21 in the 497. So it was a process based on
22 information we had access to and then essentially
23 tweaked it from there.

24 MEMBER SKILLMAN: Credited operator

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 action, Chapter 15, is that all of Chapter 15?

2 MR. SHOOK: Yes.

3 MEMBER SKILLMAN: Thank you.

4 MR. SHOOK: Okay.

5 MEMBER STETKAR: A couple questions on
6 procedures. You have redundant procedure -- You
7 have computerized procedures in the design.
8 Correct? Both?

9 MR. SHOOK: Well, let me -- I'll say
10 this because there's some discussion. I can't
11 remember if it's in the Design Certification or COL.
12 The PICS has the capability to implement a
13 computerized base procedure system. And so in that
14 design if you recall we have redundant servers. So
15 the procedures will be loaded on both servers.

16 MEMBER STETKAR: So you do have
17 redundancy.

18 MR. SHOOK: Right. But the SICS would
19 be paper based procedures. There's no computer
20 based procedure system for SICS. It's just open up
21 the boo and --

22 MEMBER STETKAR: Are the computer based
23 procedures point and click to implement actions or
24 are they simply X-files that --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: I don't think we have that
2 level of detail defined yet.

3 MEMBER STETKAR: Because you can control
4 the whole plant from PICS, what sort of functions
5 are not in the computerized procedures?

6 MR. SHOOK: Go back to the --

7 MEMBER STETKAR: That's okay. It's too
8 much detail.

9 MR. SHOOK: No, no. That's fine.

10 MEMBER STETKAR: We need to kinda keep
11 on track with the time here a little bit.

12 MR. SHOOK: Okay. I'll just say if you
13 look at the design. I don't communicate at all
14 directly with DAS.

15 MEMBER STETKAR: Okay.

16 MR. SHOOK: And I can't send signals
17 from PICS to the Protection System or SAS. So I'll
18 have information from those systems flowing up to
19 the PICS so I can see what's going on. But if you
20 get to a point where it says go trip the reactor, I
21 can't do that from PICS. So I have to go to SICS to
22 do that. So there might be some points in there.

23 MEMBER STETKAR: Thanks.

24 MR. SHOOK: Okay, 55. So here you can

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 see the allocation of the PAM variables within the
2 DCS. And it's the same kind of story that we have
3 for Type A through C. It's the same kind of story
4 we have for the safe shutdown control functions.

5 So for Type A through C we have two
6 paths. For a credited path, we go from the SCDS
7 directly to SICS. So this is a key point. All
8 indications needed on SICS are directly hardwired
9 from the SCDS to the SICS. They don't go through
10 any microprocessors or any processing. It's just
11 directly hardware connection.

12 When you see the QDS on SICS, the QDS'
13 purpose is basically only providing those variables
14 that are deemed to be important to show from a
15 graphical display or a trending capability. But
16 that will be in duplicate to the hardwired
17 indicator. And the hardwired indicator is the
18 credited indication as far as meeting all the 1E
19 requirements.

20 MEMBER BROWN: The QDS is the PAM?

21 MR. SHOOK: It is essentially like an
22 SPDS. It's an easy way to think of it.

23 MEMBER BROWN: Yes. But it's what you
24 call the QDS. PAM's not on your big diagram.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: Right. Right.

2 MEMBER BROWN: So is it the QDS displays
3 that you -- Are those where the PAM executed or
4 implemented?

5 MR. SHOOK: Again, all the PAM variables
6 are provided via dedicated indicators. And only
7 those variables as well as all the other variables
8 I've provided on SICS are all provided through
9 dedicated indicators that are hardwired, four to 20
10 loops directly from SCDS to the SICS panel.

11 MEMBER BROWN: I got that.

12 MR. SHOOK: Separate from that, the QDS
13 will provide -- You might say pressurized level I'd
14 like to see a trend of that parameter. I'll provide
15 that parameter on QDS. But it's a duplicate
16 indication of the hardwired and still has the
17 hardwired indicator for the pressurized level
18 indication which is my primary credit.

19 MEMBER BROWN: That's a little more
20 sophisticated post accident monitoring panel.

21 MR. SHOOK: Yes.

22 MEMBER BROWN: That was my whole point.

23 MR. SHOOK: Okay. Yes, it's essentially
24 what it is.

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 BROWN: I understand you had the
2 hardwired stuff which is separate from everything.

3 MR. SHOOK: Right.

4 MEMBER BROWN: Based on your earlier
5 statement. That was it. Thank you.

6 MR. SHOOK: Okay. And then we have a
7 duplicate path where we go from SCDS through the PAS
8 to the PICS and again that's to support the operator
9 being able to continue operation from PICS as long
10 as it's available.

11 And again the PICS is a non-safety
12 system. But we have specified some additional
13 quality requirements for the PICS. And due to the
14 improvement in human factors and a lot of the
15 features with the PICS we want the operator to use
16 that system again as long as it's available. So
17 that's we provide the dual paths for both systems.

18 MEMBER BROWN: Are all the SICS, those
19 indications, switches, controls, whatever you show
20 in here, are all those on a separate panel? Or are
21 they scattered throughout the panels where the
22 operator sits?

23 MR. SHOOK: I'd say that basic concept
24 is that you have the PICS are the primary

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 workstations and they're be essentially a couple of
2 those where operators will sit at. And then the
3 SICS is a separate panel located in a somewhat
4 different location within the control room.

5 MEMBER BROWN: I just questioned that
6 they're segregated separate so that you know what
7 you're operating with.

8 MR. SHOOK: Right. Now we have had some
9 discussions. I will say that with the design change
10 we've made to eliminate communication from the PICS
11 to the Protection System and SAS we have had some
12 preliminary discussions with our HFE folks about
13 either maybe co-locating some of those controls with
14 the PICS or perhaps duplicating some of controls.
15 Those details have yet to be worked out and that
16 will be done as far as the detailed design of the
17 plant.

18 But the basic concept we inherited that
19 we're trying to keep as much as we can is the
20 operator uses PICS as our primary means of control
21 in the plant. And if that fails then they
22 transition to the SICS as a backup HMI.

23 And then Type D through E we just
24 processed through PAS to PICS. We won't display

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Type D and E on SICS.

2 Okay. And the rest of these are fairly
3 straightforward. SPDS, the functionality we don't
4 have a dedicated thing we call the SPDS. But we
5 incorporate that functionality into PICS primarily
6 and also with the QDS on SICS.

7 Emergency Response Data System, we have
8 the PICS. And if you look at the previous picture
9 we show the ability to communicate out from the DCS
10 to external plant networks within the plant. So we
11 can get all the data from the DCS out to business
12 networks. And then ultimately that data can be
13 transferred to the NRC for emergency response.

14 MEMBER BROWN: So your PICS sends data
15 to the TSC as you would expect. Correct?

16 MR. SHOOK: Yes. Well, the TSC, you
17 have to be careful. The system matters. We have
18 PICS equipment actually in the TSC if you look at
19 the previous drawing.

20 MEMBER BROWN: But you just said
21 something about getting from someplace out to the
22 business network.

23 MR. SHOOK: Right. So if you go back
24 and look at slide 55. You can see here that we have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 dedicated, fixed equipment located in the TSC. And
2 then you can also see --

3 MEMBER BROWN: It doesn't say fixed on
4 it. It just says TSC monitoring only.

5 MR. SHOOK: Right. But it's all --

6 MEMBER BROWN: It's in the box.

7 MR. SHOOK: Right. It's all within the
8 fixed --

9 MEMBER BROWN: Yes.

10 MR. SHOOK: But then you can see off the
11 HMI bus we have a pair of redundant firewalls that
12 we send data out from the PICS to external business
13 networks within the plant.

14 MEMBER BROWN: Are those unidirectional
15 firewall?

16 MR. SHOOK: Those are unidirectional
17 firewalls.

18 MEMBER BROWN: And how unidirectional?
19 Are they software determined, unidirectional
20 firewalls?

21 MR. SHOOK: We haven't got to that point
22 in the design yet of actually specifying exactly how
23 that's going to work. Because as you probably know,
24 there's different ways of doing that. We could use

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 a data diode approach like we use with the
2 Protection System to the PICS. Or there is the
3 software based approach. We haven't gotten to that
4 point of specifying that detail yet.

5 MEMBER BROWN: Why would you want a
6 software based system where somebody could come in
7 and hack it and they'll gum up your software and
8 servers?

9 MR. SHOOK: I'm not saying we would want
10 that. I'm just saying that we haven't specified
11 that.

12 MEMBER BROWN: I'm saying why haven't
13 you -- My question is why haven't you specified it
14 to make sure it's secure?

15 MR. GARDNER: I think maybe you're
16 asking questions that would be more in the
17 cybersecurity area.

18 MEMBER BROWN: You picked up on that.

19 MR. GARDNER: And so the cybersecurity I
20 believe is being addressed by the COL Applicant.

21 MEMBER BROWN: About?

22 MR. GARDNER: Outside of design
23 certification.

24 MEMBER BROWN: In other words, we don't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 know.

2 MR. GARDNER: It's just not part of the
3 scope of design certification.

4 MEMBER BROWN: And I've heard that every
5 time which causes me great angst considering the
6 Department of Defense team -- their computer
7 systems. I'm trying to figure out why you all think
8 you can. I haven't gotten a satisfactory answer and
9 I'm sure your licensees don't either.

10 All right. We can address it later.

11 MEMBER SKILLMAN: Question please. What
12 drove you to make the Tech Support Center
13 information important to safety?

14 MR. SHOOK: Tech Support Center. Well,
15 this chapter is entitled Information, Systems,
16 Support and Safety. That's just what the SRP --
17 That's just the title of the chapter. That's all
18 I'm going to say.

19 In terms of the TSC specifically it's
20 non-safety related. It's not relied upon directly
21 to mitigate a design basis event. So it does meet
22 the safety related criteria, 10 CFR --

23 MEMBER SKILLMAN: That's what they all
24 say until you spend a couple weeks in one. Then 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 realize it's one of the most important places in the
2 plant. So I commend you for this, but you've
3 answered my question. It's the SRP.

4 Is there any special quality given to
5 the equipment that's in the TSC so that the people
6 in the TSC know that they've got good stuff?

7 MR. SHOOK: We have specified a number
8 of quality requirements, environmental and some
9 other things that are listed in Section 7.1 of the
10 FSAR to provide some assurance that it will operate
11 during the time when it's needed. So I could get
12 the specific criteria that we've laid out for that
13 to help.

14 MEMBER SKILLMAN: No. You've answered
15 my question.

16 MR. SHOOK: Okay.

17 MEMBER SKILLMAN: Thanks.

18 MR. SHOOK: Well, quite frankly, Dick,
19 if somebody hacks their servers the way it's hooked
20 up the guys in the incident main control room are
21 going to get the same crummy data that the TSC does.
22 If it's corrupted, they won't know what's in the
23 plant in the first place because that's just the way
24 the plant is configured.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So if they come in and corrupt the
2 servers, it's going to go both places. So they'll
3 both have the same information that will both be
4 bad. So that's an interesting way of looking at it.

5 I didn't think about that one when I was looking at
6 it. It's just a side thought that you might keep in
7 mind.

8 MR. SHOOK: Okay. Thank you.

9 And then lastly the Bypassed Inoperable
10 Status. Basically the safety related I&C system are
11 required by IEEE-603 and various reg. guides to
12 provide status indication when the systems are
13 bypassed or inoperable. And that's all provided to
14 the PICS from those systems. Okay.

15 Keep moving onto Section 7.6, Interlock
16 Systems. The topics we have the functions and then
17 we'll just talk briefly about the design.

18 Slide 59, it lists the four functions.
19 And again this is what's currently in Rev 3 of the
20 FSAR. And this is being updated to address some
21 open items from the staff. But this is what it
22 currently reflected in design. We have the RHR
23 Suction Valve Interlocks, the Accumulator
24 Interlocks, and then Interlocks Isolating Redundant

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CCWS Trains and then LTOPP Interlock.

2 Moving to Slide 60, in terms of
3 allocating the interlocks with the new DCS,
4 essentially the sensors come through the same path.

5 They come through the SCDS. And then interlock
6 function itself is either allocated to the
7 Protection System or SAS.

8 Essentially, in terms of the criteria,
9 why you put one in one system versus the other, if
10 the interlock already uses a signal that's in the
11 Protection System, for example, P14 is using some
12 pressure signals and that's already in the
13 Protection System. We'll allocate the interlock
14 there. So we don't end up running additional cable
15 to the SAS for no real benefit.

16 Essentially if we already have the
17 system in the PS, we'll just allocate it to the PS.

18 If we don't have the signal already in the PS,
19 we'll allocate it to the SAS. Both the Protection
20 System and the SAS perform interlock functions.

21 And again the signal out will go back
22 through the PACS. And then if I need to -- If
23 there's a need to manually interact with the
24 interlock function, I'll provide those controls on

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 SICS only. For example, if I want to validate
2 P14 I go do that from SICS. I can see the
3 indication on PICS of the status of it. But I can't
4 actually change the permissive until I go to SICS.

5 Okay. The design, just some inert
6 aspects of interlock functions. We do have inter-
7 divisional communications for interlock functions.
8 There are two main reasons why we do that. One is
9 to provide for voting. And the reason for that is
10 we want to reduce the probability of spurious
11 actuation of that function.

12 The other reason is what we call a
13 cross-train function. An example of this would be
14 your CCWS cross connect interlock.

15 What happens there is if essentially I
16 can't do something with Train 2, for example, open
17 some suction valves, until those same valves on
18 Train 1 are closed, then Train 2 needs to know the
19 status of components in Train 1. In order to
20 actually accomplish the safety function I have to
21 send information from Division 1 to Division 2
22 within the SAS.

23 So this isn't a -- In this case, it's
24 not a nice to have. But it's actually required to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 implement safety function with those communications.

2 And then the futures for independence
3 we've already described in terms of the ESF
4 actuation and control functions in the futures and
5 Protection System in SAS.

6 MEMBER STETKAR: Jeremy, CCWS, you have
7 the unfortunate pleasure of coming the day after we
8 talked an awful lot about pumps and pipes and valves
9 yesterday. And you know about signals. That's not
10 fair.

11 There are a number of CCWS cross connect
12 functions on -- One is the main loops from like you
13 mentioned Train 1 to Train 2 on the common headers.

14 There's also either common header can supply all of
15 the reactor coolant pump thermal barriers.

16 And reading the material at least in
17 Chapter 9 of the FSAR, Rev. 2 of the FSAR anyway, I
18 got really confused about what types of interlocks
19 and functions there are for those thermal barrier
20 supply valves. I read things that say "In the event
21 of an RCP thermal barrier fault such as tube rupture
22 a single RCP thermal barrier is isolated via inlet
23 and outlet isolation valves in the RCS."

24 I couldn't find any valves. But I don't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 have good diagrams of that system to see if there
2 are any valves on the inlet and outlet sides on the
3 primary coolant side of the thermal barrier coolers.

4 I'm not sure where they are if they're there. So
5 I'm not sure whether that statement is correct or
6 not.

7 It also says "Isolation valves at the
8 inlet and outlet of the thermal barrier are used to
9 automatically isolate faulted thermal barrier from
10 the CCWS."

11 And then the one that really got me
12 thinking. It says, "Possibly of diluting the RCS via
13 faulty RCP thermal barrier exists only when the RCS
14 is in a low pressure state. After a predetermined
15 time delay which allows for RCP coast down and when
16 the RCS pressure is low, the CCWS will be
17 automatically isolated from the RCP thermal barrier
18 via CCWS inlet and outlet isolation valves. Now you
19 can't isolate CCW from an individual thermal
20 barrier. You can only allow isolate it from all
21 four."

22 How does all of that work? Do you know
23 how any of that works? I didn't ask the folks
24 yesterday because everybody I asked yesterday 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 anything to do with signals said, "Our I&C people
2 aren't here. You need to ask them."

3 CHAIR POWER: These guys also claim to
4 be your friends.

5 (Laughter.)

6 MEMBER STETKAR: This one was rather
7 complicated. So I didn't even want to bother them
8 yesterday with that.

9 MR. SHOOK: I would first like to make
10 the point that both my degrees are mechanical. So
11 not only knowing signals, I also can dabble in the
12 pumps and pipes and valves piece as well.

13 MEMBER STETKAR: You're doing real good
14 on the signals by the way.

15 MR. SHOOK: Thank you. Thank you. I
16 don't know if I'd be interested in sealing any
17 mechanical drawings at this point.

18 MEMBER STETKAR: You know what I'm
19 talking about. I'm talking about where you can
20 cross tie Common Loop 1 and Common Loop 2 or feed
21 the thermal barriers.

22 MR. SHOOK: What I'll say is we went
23 through an exercise I'd say earlier this year where
24 we went back with the system engineers and we kinda

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 scrubbed the list of all these interlocks and so
2 forth. So the details in that are not currently in
3 the FSAR, but they will be coming with Rev. 4. So
4 you'll have detailed logic diagrams.

5 MEMBER STETKAR: Rev. 4?

6 MR. SHOOK: Yes.

7 MEMBER STETKAR: You're talking to
8 somebody who has seen Rev. 2.

9 MR. SHOOK: Okay.

10 MEMBER STETKAR: Anyway, I'm happy to
11 wait to see the details if it hasn't been worked
12 out.

13 MR. SHOOK: Okay. I mean I can try to
14 go through it now.

15 MEMBER STETKAR: No, that's fine.

16 MR. SHOOK: But it would be a lot easier
17 for you to just look at the logics.

18 MEMBER STETKAR: It will. Thanks.
19 That's all I needed to know for now. Thank you.

20 MR. SHOOK: The material that's going to
21 be in my Rev. 4 should address all the questions you
22 just asked.

23 MEMBER STETKAR: Okay. Thanks. And it
24 is, Sandra, Rev. 4, not Rev. 3.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. SLOAN: The Rev. 3 is the latest.
2 This is Sandra from AREVA. Rev. 3 is the latest
3 docketed revision. But we are working on Rev. 4
4 which incorporates mark-ups in responses to still
5 open RAIs.

6 MEMBER STETKAR: Okay. I'm sure we'll
7 keep that.

8 MR. WIDMAYER: I'll get that and explain
9 it to you later.

10 MEMBER STETKAR: Okay. Fine.

11 CHAIR POWER: The important thing to
12 remember is the SER has been written on Rev. 2.

13 MR. WIDMAYER: Until such time as it
14 isn't.

15 CHAIR POWER: Don't confuse me, Derek.

16 MEMBER STETKAR: Thanks. I'm good.

17 CHAIR POWER: Okay.

18 MEMBER STETKAR: Thanks a lot.

19 MR. SHOOK: Moving onto Section 7.7,
20 this is Control Systems Not Required For Safety. So
21 we're going to talk about again the functions, the
22 basic design and then we'll touch on features in the
23 control systems to reduce probability of failures
24 that would cause an event to occur.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 The functions, we divide things into two
2 categories. We have what we call Process Control
3 Functions. And then those are subdivided in core
4 related and primary related functions. And you can
5 see the list here. And again there's nothing here
6 that's really different from what you see in an
7 operating plant today. The next slide.

8 Here we have process limitation
9 functions. The idea of the limitation function is
10 that if I have a basic control band between two
11 values and my LSSS is up here, the limitation
12 functions is going to be somewhere in between the
13 two to take some initial preventive action or
14 mitigation action to help keep you within your
15 safety battery as well as keep the plant online.

16 In some cases, it either prevents you
17 from getting out of band like, for example, with the
18 reactor power limitation with respect to feedwater
19 flow or generator power would actually in some cases
20 block power increases. And then in other cases it's
21 more of an initial mitigation action. For example,
22 we look at high linear power density and low DNBR.
23 We actually initiate partial trips which drop a
24 certain number of rods into the core.

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 was going to ask you
2 just for my own edification. I haven't looked at
3 this part of the design and I'm not really sure how
4 much it's in there. But is this design fairly
5 similar to the -- I've forgotten what they called it
6 -- but in the Convoy plants the sort of different
7 parameters you look at. You drop selected groups of
8 rods, runback turbines. Take a look at what's
9 happening and run it back a little further.

10 MR. SHOOK: Yes. That's correct.

11 MEMBER STETKAR: Okay.

12 MR. SHOOK: So the idea is it's
13 basically these are all measures to improve plant
14 availability. Right. So I don't just trip the
15 plant which is not necessarily the best either from
16 an operational or a safety perspective. So I can do
17 a little bit and keep the plant operating and
18 keeping it within the safety limit, that's what we
19 like to do.

20 You can see I've noted in there which
21 functions are partial trips. You've got the DMBR,
22 high linear power density as well as the loss of one
23 reactor coolant pump. Go to the next slide.

24 In terms of allocation, there are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 control and limitation functions within the design.

2 If it's a core related control and limitation
3 function if it's only acting on control rods, for
4 example average temperature control, then it's
5 allocated wholly to RCSL with operator interface of
6 PICS.

7 If we implement -- if the control
8 function uses actuators other than just control
9 rods, for example for borating, then we have to
10 involve some components from the CBCS system. We'll
11 utilize RCSL as doing most of the control logic and
12 then send signals for the actuators, you know,
13 specific actuator signals to the PAS.

14 The idea behind that was between the PAS
15 and the PICS there's a lot of integration in terms
16 of tracking actuator position with respect to its
17 demand and signaling and so forth. And so we wanted
18 to keep that integration between the PAS and the
19 PICS because they're the same platform. RCSL is
20 TXS. So we have to manually configure all those
21 interfaces. It's a lot easier to just send the
22 signal over to PAS and that's why we do that.

23 And then if it's just primary related,
24 we just implement those control functions all 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 PAS. And then you can see here obviously if we use
2 safety related sensors or actuators, it will go
3 through SCDS and PAS. If not, it goes directly to
4 those sensors and actuators. Next slide.

5 Some features that are implemented
6 within design to reduce the probability of control
7 system failure. First of all, we have redundant
8 sensors and signal selection algorithms, for
9 example, second min-max. And that helps us prevent
10 a single sensor failure from causing a plant event.

11 For example, an inadvertent rod-withdrawal
12 casualty.

13 And then within the RCSL and PAS you
14 have redundant controllers. If I have a single
15 controller failure, I have a master hot standby. I
16 swap over to the standby. So I continue plant
17 operation and I don't cause an event to occur in the
18 first place. Both of those taken together I've got
19 a decent amount of redundancy at different levels
20 within the control system design to reduce
21 probability of failures in the control systems.

22 MEMBER BROWN: You don't use the signal
23 selection algorithms in the Protection System as
24 PAS.

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. SHOOK: So we just do loading of the
2 Protection System.

3 MEMBER BROWN: And it's the straight
4 signals coming in and whatever are allocated to that
5 division are the ones that are used to make that
6 decision by division.

7 MR. SHOOK: That's correct.

8 MEMBER BROWN: And these are used where?
9 Are they used in the PAS?

10 MR. SHOOK: The signal section, yes.
11 The signal section algorithms are used in PAS or
12 RCSL.

13 MEMBER BROWN: And you say that's for
14 the control purposes?

15 MR. SHOOK: That's correct.

16 MEMBER STETKAR: And typically where you
17 see things like T water control and pressurized
18 level control, that sort of stuff. Right?

19 MR. SHOOK: Right. Like, for example,
20 you look at average coolant temperature control. I
21 have four divisions of T-hot or T-cold. I'm
22 bringing all four of them. And then I'll do a
23 second min to select to get a final one that I use
24 that for my calculation and control logic. Again,

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 can discuss this over a beer sometime if you'd
2 like.

3 (Laughter.)

4 MEMBER STETKAR: Bourbon and branch
5 water would be better.

6 CHAIR POWER: The number of discussions
7 you're going to have over beer leads to cirrhosis of
8 the liver.

9 (Laughter.)

10 MEMBER BROWN: It's interesting. You
11 make a decision for the operator based on what he's
12 going to control with as opposed to letting the
13 operator figure out what he will control with.

14 MR. SHOOK: That's correct. The first,
15 when you look at it, thing you have to do is say
16 "Okay. Am I going to automate the function or I'm
17 going to do it manually. For example, the plant I
18 was on we manually controlled T-ave. So the
19 operator had to go and pick which sensor he's going
20 to look at. Right.

21 When you automate it and you tell the
22 system to run a PID loop to control T-ave and send
23 some band, the control system then has to decide
24 which one they're going to look at. And that's when

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you utilize these signal selection algorithms like a
2 second min-max.

3 Or you can even do -- I mean, there's
4 not within this design, but there's even more
5 sophisticated means of determining what the actual
6 process variable is. Because that's what you're
7 really trying to accomplish. You've got these
8 sensors looking at different specific points. But
9 ultimately you're trying to determine what the
10 process variable actually is and then control that.

11 So the second max algorithm is one way to do that.
12 But there are other ways to do that.

13 MEMBER STETKAR: US EPR, though from
14 what you said, is carte blanche, a second min-max
15 type control.

16 MR. SHOOK: No, not necessarily. I mean
17 it depends on the process framework.

18 MEMBER STETKAR: Do you do any -- I've
19 seen clever algorithms that try to figure out what a
20 mean value might be among a number of unfailed
21 parameters. Do you do any of that sort of stuff?

22 MR. SHOOK: No, we don't. We try to
23 keep it simple.

24 MEMBER STETKAR: Thanks.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: Like I was saying before,
2 with some of my experience with GE, where you can do
3 model based prediction of -- You know, we were
4 predicting a firing temperature of a gas turbine
5 based on measure parameters because you can't
6 measure the firing plane. So there's all sorts of
7 little tricks you can do. But a second min-max --

8 MEMBER STETKAR: You do a basic
9 selection.

10 MR. SHOOK: Yes. It's good enough for
11 our purposes. We don't need to make it more
12 complicated.

13 MEMBER STETKAR: Pretty fault-tolerant.

14 MR. SHOOK: Yes. So we're moving onto
15 Section 7.8. We'll go to Slide 69. I'll kind of
16 touch on the D3 analysis that was performed and the
17 assumptions and basis for the analysis. Then we'll
18 go into the functions that were developed as a
19 result of that analysis, the design and then we'll
20 look at the main diversity attributes of the
21 mitigating systems. Slide 70. Basically what
22 we did was we essentially postulate a software
23 common cause failure of the Protection System that
24 disables the Protection System, like what Member

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 Brown was talking about before. We designed the
2 system such all detectable failures and faults are
3 detected. And we failed to a safe state.

4 In the case that we've missed something
5 and I think when you look at B2B719 it sort of
6 addresses the point and it says in a digital system
7 it may be harder to detect all -- identify all your
8 faults in all our systems. So we go ahead and do
9 this analysis. When we looked at the Protection
10 System, we had to look at what we were going to
11 assume from an analysis perspective as far as the
12 operations of some of the systems in the design.

13 We made a conservative decision to
14 assume -- With a software common cause failure
15 Protection System, basically RCSL we don't credit.
16 We assume that it just doesn't work as well. The
17 reason for that is it's using the same inputs as the
18 Protection System. So your common trigger could be
19 coming from the same sensors.

20 And they are similar functions where I'm
21 doing like -- For example, in the Protection System,
22 I've got the high linear power density full reactor
23 trip. Well, if I'm using the same algorithm in the
24 RCSL to do a partial trip for a high linear power

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 density, it doesn't make sense to the partial trip
2 and not the full trip. So we just made the decision
3 conservatively to not credit RCSL.

4 MEMBER STETKAR: Jeremy, before you get
5 further on down into this, the first bullet says
6 software common cause failures postulated to disable
7 the PS. Does that mean that the only potential
8 common cause failures you thought about where
9 failures that prevented the Protection System from
10 doing what it was supposed to do? In other words,
11 did you also think about common cause failures that
12 makes the protection system do things that it's not
13 supposed to do because of -- We've already discussed
14 several of these priorities and things where you
15 have to make decisions about which particular
16 functions ought to be implemented.

17 MR. SHOOK: Right. We did look at that.
18 I can't recall the specifics of some of that
19 analysis. But in most cases, from what I recall,
20 it's sort of a nonissue. For example, if I isolate
21 containment, I can deal with that. It may not be
22 desirable, but you can deal with that.

23 MEMBER STETKAR: That's documented in
24 your D3 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 MR. SHOOK: I believe so. I'll double-
2 check and get back to you on the break.

3 MEMBER STETKAR: Okay.

4 MR. SHOOK: But I believe that's
5 somewhere in the D3 report.

6 MEMBER STETKAR: Thank you.

7 MR. SHOOK: But the primary focus was
8 the Protection System doesn't operate when it needs
9 to. That's sort of the -- I'll find it. There's a
10 four by four matrix. It's like it operates when
11 it's supposed to. It doesn't operate when it's
12 supposed to.

13 MEMBER STETKAR: I'm asking about the
14 upper right-hand corner of that matrix.

15 MR. SHOOK: Yes. I'll get you that
16 information.

17 In terms of the process automation
18 system and safety automation system, we assume that
19 those systems are operable as long as they're not
20 relying on a Protection System output. For example,
21 the emergency feedwater level control function is
22 started by a signal from the Protection System. So
23 we said, "We're going to assume that that signal
24 doesn't come out of the Protection System.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Therefore, the level control function won't get
2 initiated and therefore it won't start." And so we
3 don't credit that function.

4 But in the case of the flow control
5 function, the flow control for EFW operates
6 independent. It's not triggered off a signal from
7 the Protection System. It's just looking at flow
8 rate in the system and it just starts controlling
9 once flow rate is above the minimum value. So that
10 loop we assume to be operable as an example.

11 As long as those functions weren't
12 relying on the Protection System output, we
13 considered the functions of those systems to be
14 operational and could be credited in the analysis.

15 Then after we established our baseline
16 of what systems within the whole DCS design wouldn't
17 be operable and would be operable, then we started
18 looking at the different Chapter 15 events and then
19 determining what back-up reactor trips in ESF
20 actuations we would need in order to meet our Part
21 100 requirements as defined by the guidance in B-
22 719.

23 And so we went through that process and
24 added a number of additional reactor trip functions,

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 ESF actuation functions, and those are all allocated
2 to the DAS.

3 And then also I'll just make a point
4 that that analysis bounds the requirements of the
5 ATWS rule, 10 CFR 50.62 in terms of initiating
6 emergency feedwater and turbine trip.

7 MEMBER STETKAR: Jeremy, I'm trying to
8 get hands around that third bullet and what the
9 implications might mean. I haven't really thought
10 about it very much. So I don't have a decent
11 question.

12 Do you have a sense? I mean you made
13 that decision to essentially compartmentalize the
14 common cause failures that you were going to say are
15 the subject of your D3 analysis apparently for some
16 reason. What did that buy you?

17 I mean you mentioned the example of you
18 determined you could take credit for the automated
19 feedwater, emergency feedwater level control
20 function, because that was not within the scope of
21 your postulated software common cause failure
22 because it's not a Protection System function.

23 MR. SHOOK: Right.

24 MEMBER STETKAR: What's sort of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 physical basis for it? I mean, is it literally
2 separate, independent, diverse software that runs
3 that function or is it only because you're required
4 to do the D3 for protection signals?

5 MR. SHOOK: When you look at the report
6 and some of the baseline assumptions that we use,
7 there's an IEC standard that defines a common cause
8 failure as -- You sort of need two things to have a
9 common cause failure. One is a latent defect and
10 then the other is an external trigger or a
11 triggering event that exposes that latent defect.

12 When we looked at we had segued already
13 the Protection System in SAS. And we said, "Okay.
14 If I have a design basis event (a) that's my
15 triggering event and then (b) my latent defect is
16 some logic in the system that's not going to operate
17 the way it's supposed to. So that's your common
18 cause failure."

19 What we did with, for example, with the
20 SAS, the analysis is basically most of the SAS
21 inputs are support systems, HVAC, cooling water, so
22 forth. And so the basic premise was those process
23 parameters aren't going to be changing necessarily
24 the initiation of the design basis event 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 way your primary parameters are like pressurized
2 level and pressure.

3 So you have a different input profile.
4 You're not going to get the same latent defect
5 that's going to be triggered in the SAS that you
6 would have in the Protection System by those inputs.

7 So that was the basis for the argument of why we
8 could basically say that the safety automation
9 system is running fundamentally different. It's
10 controlling basically for the most part different
11 systems, mostly support systems.

12 And, secondly, the control functions are
13 looking at signal inputs that are basically
14 different than what are inputs in the Protection
15 System. Because you've got a different triggering
16 event and different potentials for latent defects we
17 felt in our judgment that it was sufficient to be
18 able to credit the SAS.

19 From a practical perspective which I
20 think is maybe what you're interested in is what
21 does this buy you. Right. Now if I have to assume
22 this whole SAS is subject to a common cause failure
23 at the same time as the Protection System, I have to
24 look at backing up all these control functions,

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 cooling water, HVAC and so on and so forth. From a
2 practical perspective, it's not that hard to put a
3 back-up SI actuation in the DAS because it just
4 actuates and then you're done.

5 MEMBER STETKAR: I understand that.

6 MR. SHOOK: But if you have to start
7 looking at "Now I have to have a back-up EFW flow
8 control function," okay, then it gets a lot more
9 challenging to have two control loops. You know
10 you're going to have competing control loops on the
11 same actuator.

12 And then you have to start looking at
13 complicated schemes of "Now do I have both running
14 and have to deal with the potential oscillatory
15 behaviors of both loops running?" Or do I try to
16 have one be the master and then the other one detect
17 when the other one has failed? It's a lot more
18 complicated from a practical perspective. So that's
19 we tried to isolate the failures to the Protection
20 System.

21 And we believe it wasn't just we tried
22 to wave our hands away and say, "It's all good." I
23 mean, we do have some good technical justification
24 in the D3 report as I was talking about with the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 triggers and the latent defects. But there is some
2 I think --

3 MEMBER STETKAR: I guess we'll have to
4 look at that. From a risk perspective, a lot of the
5 risk analyses that have been done show those sort of
6 unimportant support systems can be very, very
7 important to overall plant risk especially if you
8 start dispersally to isolate cooling water systems
9 and things like that. Sort of this notion that
10 those are sort of normally operating support systems
11 and we don't need to worry about that because when
12 we put our design basis event blinders on.

13 It's just something a bit disconcerting.
14 But I'm willing to go read what you did in the D3
15 analysis.

16 MR. SHOOK: Okay. Yes. I think the
17 basic idea is that we're not saying you could have a
18 common cause failure of those functions. What we're
19 saying is it's not likely you're going to have a
20 common cause failure of a component of cooling water
21 control loop function concurrent with the DBE
22 because your input trajectories that are going to be
23 resulting from the DBE aren't necessarily correlated
24 with the component of cooling water temperature

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 control loop for example.

2 MEMBER STETKAR: Temperature control I'm
3 not so worried about.

4 MR. SHOOK: Right.

5 MEMBER STETKAR: I'm worried about
6 reconfiguring systems because of the signals that
7 might be coming in. Things like some things that I
8 mentioned that the system thinks that there is low
9 pressure and for some reason I have a failure of
10 thermal barrier cooler. So I'm going to shut off
11 all component cooling water under conditions where I
12 might want to keep that function.

13 MR. SHOOK: Right.

14 MEMBER STETKAR: That's the type of
15 thought process that -- Let's just leave it.

16 MR. SHOOK: Okay.

17 MEMBER STETKAR: And we'll see.

18 MR. SHOOK: One last point I'd just like
19 to make though just to clarify. Even for the
20 support systems like component cooling water ESW if
21 they're actuated on SI those systems are -- those
22 functions are driven directly from the Protection
23 System. And they're not involved.

24 MEMBER STETKAR: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: So when I start all four
2 trains at CCW --

3 MEMBER STETKAR: They'll get that.

4 MR. SHOOK: -- they'll still get that.
5 It's the follow-on controls.

6 MEMBER STETKAR: Some of the discussion
7 you have -- I was sitting here -- recognizes it's a
8 beyond design basis event that we're talking about,
9 the common cause failure first of all. When you're
10 starting to get concerned about full parallel
11 replication for example of automatic emergency
12 feedwater level control within DAS and how might
13 that interact with SAS.

14 MR. SHOOK: Right.

15 MEMBER STETKAR: Or the complexity of
16 designing that function, perhaps you don't need
17 that. Perhaps an on/off, high level/low level for
18 emergency feedwater, for example, is okay within a
19 DAS function to mitigate a beyond design basis
20 event.

21 MR. SHOOK: Or manual control.

22 MEMBER STETKAR: Or manual control.

23 MR. SHOOK: Right.

24 MEMBER STETKAR: And would obviate this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 need to sort of compartmentalize where the common
2 cause failure might occur or might not occur.

3 MR. SHOOK: Right. That particular
4 example, that's pretty easy.

5 MEMBER STETKAR: Yes.

6 MR. SHOOK: But you are starting to get
7 into some of the support systems.

8 MEMBER STETKAR: Anyway, if it's
9 discussed in the D3 report.

10 MR. SHOOK: Yes. I'll get you that
11 specific section where it talks about that.

12 Okay. In terms of the functions for the
13 diverse reactor trips that were identified out of
14 this analysis, they're listed here. And they're all
15 basically the same I think with the exception of the
16 high neutron flux. It's just an absolute value, not
17 a rate, which is in the Protection System. But the
18 other trip functions are essentially the same type
19 of trip functions that are in the Protection System.

20 One note I'd say about the manual
21 reactor trip for the DAS. Actually, on the SICS, I
22 have actually two trip buttons. I have one set of
23 trip buttons for the Protection System that goes
24 through the Protection System like we showed 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 And that actuates the UV coils and the trip
2 breakers and the trip contactors.

3 For the DAS I have separate for the
4 switches for manual reactor trip that goes through
5 the DAS cabinets, gets combined with the automatic
6 DAS logic. And then out of the DAS you have the
7 coils on the breakers and the control logic
8 thyristors for the CRDCS.

9 MEMBER STETKAR: So in the UPs, what do
10 you instruct the operators to do? Go hit reactor
11 trip. There's typically a confirmatory trip. You
12 instruct the operators to hit it on SICS and go over
13 to DAS and hit it over there to make sure you get
14 the redundant things.

15 MR. SHOOK: We haven't written the UPs,
16 so I can't comment on that. But it's a good
17 question.

18 Going to the next slide we've got
19 Diversity of Set Functions. In here, you can see in
20 terms of how we've implemented those functions,
21 whether it's automated, manual system level or also
22 manual component level.

23 And I'll just summate the point. I
24 won't go through which ones, but BTP 7-19 requires

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that you provide system level actuation for all your
2 critical safety functions. So some of these are not
3 necessarily required per the analysis that was done,
4 but required because of the BTP 7-19. And then you
5 can see also 73 of the component level controls
6 that's credited in the analysis for the operator to
7 perform certain functions.

8 MEMBER STETKAR: Just since we discussed
9 it a couple of minutes ago, the manual component
10 level control of BFW system I'm assuming that would
11 be the level control valves.

12 MR. SHOOK: Level and flow control, yes.

13 MEMBER STETKAR: And those signals
14 override any signals that are coming out of SAS.

15 MR. SHOOK: No, they don't. So if I
16 needed to -- I would have to go and take that loop
17 to manual.

18 MEMBER STETKAR: Over in SAS.

19 MR. SHOOK: Over in SAS before I could
20 manually perform those functions.

21 Seventy-four is showing how we allocate
22 the functions within the DCS. So if it's an
23 automatic reactor trip or ESFAS it's allocated to
24 the SCDS, then DAS for the processing and then PACS

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 for the output. PACS is only for ESF, not for
2 reactor trip.

3 And then grouped controls are allocated
4 to SICS and then implemented through DAS and then
5 into PACS. Again PACS is only for ESF.

6 And then component level controls go
7 directly from SICS to PACS.

8 I'll just make the comment that although
9 not all -- We have provided the design of all
10 component level controls for safety related
11 actuators on SICS. Whether it's credited
12 specifically or not in the D3, that is an aspect of
13 the design. And that path bypass just goes from
14 SICS directly down to the PACS bypassing all the
15 digital control actuation systems. Next slide.

16 MEMBER BROWN: Is -- Okay. I'll wait
17 until you get to the next slide.

18 MR. SHOOK: Okay. So here is a little
19 more detail in terms of the DAS and the design for
20 the diverse reactor trips. You can see I've got the
21 same basic signal path as I used for the Protection
22 System. It's all coming through the SCDS.

23 And then I bring that signal into each
24 of division of the DAS. The DAS we have committed

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 in the FSAR or specified that it will be implemented
2 in non microprocessor based technology. So that
3 could either be electrical or electronic, in relays
4 or --

5 MEMBER BROWN: You dictated that in the
6 DCD.

7 MR. SHOOK: We have, yes.

8 MEMBER BROWN: Because the note down
9 here in Font 006. So technology may be nonmicro --
10 Yes, don't try it this way. May be. It doesn't say
11 it will be.

12 MR. SHOOK: Yes. It's the wording. And
13 I apologize that that's so confusing. What we tried
14 to show with the color scheme is that the blue
15 indicates electrical or electronic technology. And
16 the little note is also a disclaimer to say it could
17 also be non microprocessor programmable or
18 electronic. We didn't know how to make it shaded
19 blue and green.

20 MEMBER BROWN: And green is what again?
21 It's in one of your other slides.

22 MR. SHOOK: Non microprocessor based,
23 programmable electronic. So PLD or FPGA.

24 MEMBER BROWN: Yes. And what's this?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 This is that, isn't it?

2 MR. SHOOK: No, this is electrical or
3 discrete electronics.

4 MEMBER BROWN: Oh, discrete electronics.
5 Analog.

6 MR. SHOOK: Right.

7 MEMBER BROWN: Analog, analog, I should
8 say.

9 MR. SHOOK: Yes.

10 MEMBER BROWN: And you've dictated that.

11 MR. SHOOK: Just forget about what the
12 screen shows because I've made it too complicated.
13 The commitment we've made is that the technology
14 will be non microprocessor based technology. So it
15 could be FPGA. It could be PLD. Or it could
16 discrete electronics or relays. But it can't be a
17 microprocessor with system software or application
18 software.

19 MEMBER BROWN: Okay. Did you talk about
20 the communications from -- I mean, you've got some
21 type of passing stuff from point to point for voting
22 obviously.

23 MR. SHOOK: These are all hardwired
24 signals between the different divisions.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: That means?

2 MR. SHOOK: There's no data
3 communications. It's all zero to 24 volt contact or
4 if you need to -- No, in this case --

5 MEMBER BROWN: You would expect it to go
6 -- I would expect the stuff to be logic gates and/or
7 PLDs configured to be logic gates as a voting
8 regime, environment.

9 MR. SHOOK: That's correct. Yes.
10 Right. For example, if you used PLDs, you'd have one
11 PLD module doing your set point comparison. You'd
12 have another PLD module doing your two out of four
13 voting. You'd have to set that up with the design.

14 But we did specify the specific
15 technology because obviously we wanted to leave
16 ourselves some flexibility from a procurement
17 perspective later on. But we did specify the
18 minimum requirement in order to make the analysis
19 work.

20 MEMBER BROWN: It would be really nice
21 if you used relay logic.

22 MR. SHOOK: All I can say is there's a -
23 -

24 MEMBER BROWN: Good stuff.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: There's a number of
2 considerations that are taken into account with the
3 final technology. Move onto the next slide.

4 Again we're just showing again -- I've
5 already talked about the diversity in reactor trip
6 devices. You can see here that the DAS comes in and
7 at the top comes into the control rod drive, control
8 system cabinets and actually gates off the rod
9 control units. So I've got another diverse means of
10 tripping all the rods. And then also you can see
11 the DAS come in at the bottom and hit the shunt trip
12 coils. And you can also see the Protection System
13 inputs as hitting the trip contactor modules and the
14 UV coil and the trip breakers.

15 MEMBER BROWN: It still does the
16 contactors also, doesn't it?

17 MR. SHOOK: The Protection System does
18 the contactors. The DAS itself only -- I shouldn't
19 say only. The DAS itself trips the rod control unit
20 logic to disable the control logic and the --

21 MEMBER BROWN: I got that far.

22 MR. SHOOK: And then it hits the shunt
23 trip coil on the trip breaker.

24 MEMBER BROWN: I got that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: And that's it. That's all
2 the DAS does.

3 MEMBER BROWN: But in terms of -- I mean
4 you've got this trip breaker configuration that if
5 you trip one and two you don't scram. I mean you
6 don't change the --

7 MR. SHOOK: Yes, I know. It's the same.

8 MEMBER BROWN: It's the same. Right?

9 MR. SHOOK: That's right. That's
10 correct.

11 MEMBER BROWN: So you're really
12 depending upon turning off the gates.

13 MR. SHOOK: In both designs we use
14 single failure criteria.

15 MEMBER BROWN: I've heard you.

16 MEMBER STETKAR: Two-thirds of the time
17 and a random selection logic, they'll get both trip
18 breakers open.

19 MEMBER BROWN: The right two.

20 MEMBER STETKAR: One in each line.

21 MEMBER BROWN: Hopefully.

22 MEMBER STETKAR: One of the SICS
23 combinations will get the right one. Will get you a
24 trip.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. SHOOK: Okay. Moving to Slide 77,
2 we show the diversity in ESF actuation and control.

3 So again your automatic ESF functions, the signals
4 are routed through the SCDS and then are sent to the
5 DAS, each division. And then again you've got
6 hardwired signals going back and forth for voting
7 between the different divisions.

8 You have system level actuation of those
9 functions listed in the tables previous from the
10 SICS going directly to the DAS. And then you can
11 also see manual component control going directly
12 from SICS to the PACS. Okay.

13 And then Slide 78, I would say these are
14 the key elements of diversity for the systems that
15 are relied upon the credit mitigation for common
16 cause failure in Protection System. The SCDS, when
17 you look at the inputs to the DAS show the
18 Protection System, those input signals are
19 conditioned and distributed using electronic I&C
20 technology. So there's no software common case
21 failure.

22 I will point out that there are some --
23 Some of the temperature conditioning modules in the
24 SCDS for inputs going to Protection System do

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 utilize some programmable electronic technology.
2 But those inputs we don't use temperature inputs in
3 the DAS. So the message is that for the inputs that
4 we're relying on to be diverse it's all processed
5 through electronics and therefore we don't have to
6 postulate a software common cause failure.

7 The DAS, as I said we've committed, made
8 the commitment, that it's going to be non-
9 microprocessor based technology.

10 And then when you look at the SICS as we
11 talked about before we have dedicated indicators
12 with hardwired input directly from the SCDS and PACS
13 bypassed in the computers. The Protection System.

14 And then lastly the PACS, the priority
15 module utilizes a PLD. We committed to in the FSAR
16 to be 100 percent tested so to assure that there's
17 no latent defect from a programming.

18 MEMBER BROWN: This is the same priority
19 module that's in the other thing. Right?

20 MR. SHOOK: That's correct.

21 MEMBER BROWN: So you don't change --
22 You don't have a different thing there.

23 MR. SHOOK: No.

24 MEMBER BROWN: It just feeds the same

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 thing that the other system does.

2 MR. SHOOK: That's correct. Yes.

3 MEMBER BROWN: What did you say about
4 the SCDS?

5 MR. SHOOK: The SCDS for the input that
6 are shared between the PS and DAS, the inputs are
7 processed using electronic boards, cards. So I
8 don't need to -- Because they're not programmable, I
9 don't need to consider.

10 MEMBER BROWN: Same ones?

11 MR. SHOOK: It's the same one. Yes.

12 MEMBER BROWN: Okay.

13 MR. SHOOK: But my point is because
14 those cards are just discrete electronics, I don't
15 have to consider those --

16 MEMBER BROWN: That's fine.

17 MR. SHOOK: Okay.

18 MEMBER BROWN: I just didn't understand
19 everything you said the last time.

20 MR. SHOOK: Okay. And that's it for the
21 presentation.

22 MR. GARDNER: That concludes our
23 portion.

24 CHAIR POWER: I almost hate to ask. Are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 there any more questions at this time?

2 (No verbal response.)

3 If I had a silver star to give out for
4 this, I would give you a silver star for an
5 outstanding performance.

6 MR. SHOOK: Thank you. I appreciate
7 that.

8 CHAIR POWER: But I don't. So you're
9 not going to get one from me.

10 (Laughter.)

11 I think at this point we'll turn to the
12 staff.

13 MR. TESFAYE: Okay. Would you like to
14 take a break before we do the staff's presentation
15 or continue?

16 CHAIR POWER: I think we should go right
17 ahead.

18 MR. TESFAYE: Okay. Dr. Powers, before
19 I turn over the presentation to Mike Canova, he's
20 also the lead PM for US EPR design certification. I
21 would like to give an opportunity to Terry Jackson
22 who is the Branch Chief for I&C Branch give us an
23 update on Chapter 7.

24 MR. JACKSON: Thanks, Gatachew. My name

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 is Terry Jackson. I'm the Chief of the
2 Instrumentation Controls and Electrical Engineering
3 Branch No. 1 in the Office of New Reactors. My
4 staff was responsible for reviewing the EPR and I&C
5 design.

6 And since my staff is going to give a
7 little background about themselves, I'll give a
8 little bit about myself as well. I have a bachelors
9 in Computer Engineering and a masters in Electrical
10 Engineering. And I hold a Professional Engineering
11 license in Electrical Engineering in the State of
12 California.

13 I've been with the NRC for 17 years.
14 And I first started out as a digital I&C engineer in
15 the Office of Research. And I worked seven years as
16 a resident and senior resident inspector at Diablo
17 Canyon. And then since 2007 I was the Branch Chief
18 for this branch.

19 Soon after coming here in 2007, we began
20 reviewing the EPR design certification application.

21 One of the things I noted earlier was that I'm also
22 the chair of the MDEP EPR I&C Technical Expert
23 subgroup which is as I mentioned actually six
24 countries when I thought about it a little bit 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 which includes Canada, China, France, Finland,
2 United Kingdom and United States where regulators
3 get together and we discuss common issues and topics
4 with regards to EPR design. Of course, MDEP also
5 covers over design such as AP1000 and some issue
6 specific items such include digital I&C as well.

7 But that group's been meeting for the
8 past three years and it's changing informational EPR
9 I&C design. And as I mentioned we've gained
10 information from the foreign regulators as well as
11 we provide them with some valuable information as
12 well.

13 One of the things I want to note was
14 just the staff effort has been about three and a
15 half years' amount of effort into the EPR I&C design
16 overall. And it's about -- We've invested about
17 20,000 hours into the review.

18 And one of the things that you'll see in
19 our presentation is that the staff has been working
20 hard at addressing key technical issues and so
21 forth. And actually I think we've done a good job
22 addressing a lot of these. There are still a number
23 of open items that we're still working on as well.
24 But I hope that the Committee will see the effort

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 also appreciate what the level of effort the
2 staff has put into the review.

3 CHAIR POWER: Thank you.

4 MR. CANOVA: Good afternoon. My name is
5 Michael Canova. I'm, as Getachew identified, the
6 Chapter 7 PM for the US EPR design certification.

7 By way of background, I'm old. I have a
8 BS from Johns Hopkins. I spent 36 years at
9 Constellation Energy, 20 of that in the I&C area,
10 either in design or procurement engineering. And a
11 good piece of that right at the beginning of my
12 career was working through TMI era and the TMI
13 lessons learned. My phone number is still a bane to
14 the people that call me up. It's 0737.

15 (Laughter.)

16 Today's presentation covers SAS Phase 2
17 safety evaluation report for Chapter 7. The first
18 slide gives the objectives. This is more to keep us
19 on focus than you. We're here to provide you some
20 of the details in our review and provide a common
21 understanding of the background, the efforts and the
22 current status of that review.

23 The review team, the first three members
24 are sitting up here including Jack Zhao, Tung Truong

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 Deanna Zhang. And soon to join us is Ken Mott,
2 Deirdre Spaulding Yeoman. Wendell Morton will be
3 rotating through the chair to go through their
4 various sections.

5 Just by way of introduction, this is
6 just the layout. We'll do an intro, some
7 background, and then go through the key topics of
8 interest in terms of redundancy, independence,
9 determinism, diversity, simplicity of design. And
10 then the other technical topics of interest are self
11 testing and self automation systems. And then a
12 discussion.

13 I'm going to present shortly also a list
14 of the open items. First, I want to just give a
15 little background on how everything was laid out in
16 the SE itself. AREVA submitted the design cert in
17 December of 2007.

18 The Safety Evaluation and related
19 reports represent as Terry said three and a half
20 years of effort by the staff and Applicant.

21 On June 25, 2010, AREVA proposed to make
22 several refinements to their previously submitted
23 design in order to support continued review. The
24 meeting summary is actually indicated here. And it

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 included the staff's evaluation of where we
2 were at that point in time.

3 The SE for Chapter 7 is based on
4 Revision 2. So Member Stetkar was correct.
5 Revision 2 was where we were when we were writing.
6 But there was frequent reference made to Interim
7 Revision 3 mark-ups. These came in with a series of
8 RAIs.

9 These identify AREVA's commitments to
10 changes. They've been submitted with these RAIs.

11 These design changes are reflected in
12 mark-ups submitted for actually unrelated RAIs.
13 There's actually a last RAI in each section which
14 came in with a full set of mark-ups for that entire
15 section. So that we'd have everything in front of
16 us. So we pretty much have that Rev. 3 docketed as
17 interim mark-ups and that's what we used to close
18 the gap.

19 One other thing about that is after we
20 finished the SE Revision 3 was actually docketed and
21 is now in-house. So there's actually a couple of
22 places in there that you'll see us actually talk to
23 Revision 3 because we tried to close some of the gap
24 on the SE as we polished it up and finished it up.

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 is an overview of the DC in terms
2 of RAI questions that were written. Two hundred
3 ninety-three questions total. Thirty-six open items
4 are now standing. I've got a list of them behind
5 us. But the staff is going to integrate those major
6 open item questions into their discussion of each
7 area as we walk through it.

8 As spoke of before, this actually
9 presents a list of primary documents including
10 technical reports, topical reports and the Interim
11 Rev. 3 information that we've been looking at to
12 complete the SE.

13 And I'm just going to page through these
14 quickly if you want to take a look at them. I
15 believe they're in your slide set also. If you see
16 any that is of interest to you, please bring them
17 up at the appropriate time as we go through the
18 sections. We're going to go through section by
19 section.

20 Jack, do you want to take it from here?

21 MR. ZHAO: Yes. Good afternoon. I'm
22 Jack Zhao, a Senior in the Technical Review in the
23 I&C Branch at the NRO office.

24 A little bit of background about me. I

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 went to college and graduate school in China. After
2 working five years there as an I&C engineer, I did a
3 few more years graduate study at Penn State on a
4 scholarship. After graduating from Penn State, I
5 went to work for Bechtel Power Corporation. After
6 working for 12 years for Bechtel, I joined the NRC
7 about three and a half years ago. Basically that's
8 it about me.

9 Today, first, I'll present the major
10 technical issues with the original U.S. EPR and
11 safety issues the staff raised. And also I'll talk
12 about the major technical changes made by the
13 Applicant to address the staff's concerns.

14 For the original and EPR I&C, the first
15 major concern the staff raised is complexity of the
16 EPR I&C architecture. The second major technical
17 issue is communication independence for the safety
18 systems. Because individual communication was
19 extensively used in those safety I&C systems.

20 The third main concern the staff raised
21 is also about the communication independence issue
22 between the safety system and the non-safety systems
23 because in the original I&C design for those systems
24 used a bi-directional data communication.

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 fourth concern the staff had is
2 about continuous connection between the safety
3 systems and non-safety service unit.

4 The final concern the staff raised is
5 related to qualification of the safety display
6 system for the SICS.

7 In the public meeting just mentioned in
8 the presentation, the Applicant made a significant
9 changes to the original I&C designs. They will all
10 be present and talk about some major technical
11 changes for those to address the staff concerns.
12 Next slide please.

13 MEMBER BROWN: So they made all those --
14 They made a number --

15 MR. ZHAO: Significant changes, yes.

16 MEMBER BROWN: -- relative to that
17 meeting, that public meeting, you had where you went
18 through all the concerns and the issues that you all
19 had with the level of complexity. So what we saw
20 today was a fallout of the revised design.

21 MR. ZHAO: Exactly.

22 MEMBER BROWN: Okay. All right. Thank
23 you.

24 MR. ZHAO: To address the staff's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 concerns and the complexity of the original I&C
2 design, the Applicant made substantial changes to
3 reduce the complexity of the original I&C design.

4 First, the Applicant revised the I&C
5 design to minimize the use of the inter-divisional
6 communication for the safety systems.

7 Second, the Applicant modifies the I&C
8 architecture to reduce the safety I&C system's
9 dependence on the plant data network.

10 Third, the Applicant fundamentally
11 changed the safety indication on the control system
12 or SICS design for a micro process based system to a
13 hardware based system.

14 Finally, the Applicant deleted the
15 severe accident I&C system and they incorporated the
16 functions of the other I&C systems.

17 So all those changes simplified the
18 original EPR I&C design. And the current I&C
19 architecture is less complex. Next slide please.

20 The staff as I just mentioned questioned
21 the communication independence issue among the
22 redundant divisions for the original SICS, SAS, and
23 PS Safety Systems. For the SICS to address the
24 communication independence issue, the Applicant

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 fundamentally changes the design to hardwired
2 basically in the I&C system and it does not use any
3 inter-divisional communication.

4 For the SAS, the Applicant originally
5 used the 2nd min/2nd max function. This function
6 requires individual communication. The staff
7 questioned the safety justifications for this
8 function in the SAS system. To address the staff's
9 concern the Applicant modified the design and they
10 reduced the inter-divisional communication in the
11 SAS system.

12 For the PS, the EPR design uses 72 SPNDs
13 as to calculate two reactor-trip functions. In the
14 original PS design, 18 SPNDs of the 72 are hardwired
15 to each division. The design used the inter-
16 divisional communication to get the rest of the
17 SPNDs to calculate the reactor-trip functions. So
18 inter-divisional communication was the extensive use
19 of the original EP and the PS design.

20 The staff raised the concern under
21 communications independence issues for this design.

22 To address the staff's concern, the Applicant
23 revised the SPND design to hardwire all 72 SPNDs to
24 each division basically. As I just mentioned, each

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 division needs all 72 SPNDs.

2 MEMBER BROWN: The white paper or the
3 little paper that I got I don't know somewhere
4 implied that that was the original design and that
5 was to allow the maximum -- I may have read this
6 wrong, but I mean it was as part of the SICS 6031991
7 or 6031998. And in the back of that was the
8 benefits of 72 in each PS division which made it
9 sound like there was no way you could wire this
10 thing up with 18 to each division. MS. ZHANG:
11 In the original design, they had 72 SPNDs coming out
12 of the core.

13 MEMBER BROWN: Right.

14 MS. ZHANG: They still split it into
15 four divisions of 18.

16 MEMBER BROWN: Right.

17 MS. ZHANG: But each division of the
18 production system needs all 72 to make their reactor
19 trip function.

20 MEMBER BROWN: Yes.

21 MS. ZHANG: But instead of hardwiring
22 the outputs from the SPND outputs to each Protection
23 System division, 18 was acquired by each division
24 and then sort of a ringed network.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: I understand that.

2 MS. ZHANG: Yes.

3 MEMBER BROWN: I understand that point.

4 But based on his explanation and yours, yes. I
5 guess maybe the argument was made in here that you
6 couldn't process just 18 and generate a trip in each
7 division from 18 and still achieve the same benefits
8 of the whole core mapping of the flux.

9 MS. ZHANG: Yes.

10 MEMBER BROWN: Power as it's throughout
11 the core. Okay. Maybe that was -- Maybe that's
12 where I'm mixing it up here, apples and oranges.

13 MS. ZHANG: So the 18 that was acquired
14 they're not producing the reactor function.

15 MEMBER BROWN: They're saying that if
16 you just use 18 you don't get as an efficient setup.

17 That's what they were talking about. Okay. I got
18 the picture now. Thank you.

19 MR. ZHAO: Now the 72 SPNDs are not
20 redundant to each other. In other words, the SPND
21 design in the EPR system does not meet the NRC
22 requirements and the independence and the
23 redundancy.

24 But in the duties it's a design and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 there are some safety benefits of the SPND system.
2 So the Applicant supplemented alternative requests
3 to address these deviations. So we will present
4 more in the evaluation on an alternative request.
5 Next slide please.

6 The staff also raised the communication
7 independence issue related to the bi-directional
8 communication using a different safety system and
9 the non-safety system in the original I&C design.
10 To address the staff's concerns, the Applicant
11 changed the design by using the physical limited,
12 one way communication only from safety to non-safety
13 systems.

14 The staff questioned safety
15 justification for the permanent and continuous
16 connection between the safety system and the non-
17 safety service units in the original design. The
18 Applicant, after they revised their designs,
19 disconnected the permanent connection except for the
20 maintenance and surveillance testing. Next slide.

21 During the review process, the staff
22 found there are some issues of independence and the
23 software quality for the original AV482 based on the
24 PACS design. In order to address the independence

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 issue, the Applicant revised the PACS design by
2 separating the non-safety related communication
3 board from the safety related priority logic board.

4 Originally, the two modules are on the
5 same -- too much on the same board. So there is an
6 independence issue there. To address the quality
7 issues, the Applicant provided a commitment to use
8 the 100 percent combination test for the revised
9 PACS system.

10 In the US EPR DCD the Applicant took
11 credit for the TXS self-testing and the monitoring
12 function to meet the part of the TXS surveillance
13 testing requirements. But the EPR DCD does not
14 include enough information on how safety self-
15 testing and then monitoring functions are credited.

16 So in order to address the staff's concern, the
17 Applicant submitted a new technical report for the
18 US EPR DC application.

19 One of my colleagues will present more
20 evaluations in this area. Next slide please.

21 The staff also raised some concerns D3
22 assessment for the original EPR I&C design.
23 Originally, DAS is a diverse actuation system and it
24 was part of the non-safety PAS system by using 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 plant data network. In order to simplify the I&C
2 design, the modified I&C architecture separated the
3 DAS from the PAS and the plant data network.

4 So the revised I&C design morphed as a
5 DAS manual control and an indication from the non-
6 safety PICS to the safety rated SICS system. The
7 DAS design was changed from a microprocess based
8 system to a non-microprocess based system to be
9 diverse from the microprocess based safety systems.

10 During the review, the staff found that
11 the original US EPR DCD under D3 technical report
12 didn't include any best estimate analyses as
13 required by the BTP 7-19. So to address the staff's
14 finding, the Applicant is submitting a best estimate
15 analysis in the revised D3 report to support the
16 design of the D3 functions.

17 That's all from my presentation. Next
18 my colleague Tung Truong will present the staff's
19 technical evaluation and the redundancy requirements
20 for the EPR I&C design. Thank you very much.

21 MR. TRUONG: Good afternoon. My name is
22 Tung and I went to U of I for my bachelors in
23 electrical engineering and I went to work at
24 Motorola as a software developer. And after that I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 went back to graduate school. I got my degree in
2 computer engineering. And after that went to the
3 Navy Center in San Diego for five years and then
4 came here for the past three and a half years.

5 This afternoon I'll be going over slides
6 on redundancy. Overall the US EPR I&C Safety
7 Systems can sustain a single failure and complete a
8 safety function. And it meets the NRC requirements,
9 the GDC and the IEEE standard. And each system has
10 a single-failure ITAAC to verify the design
11 commitment. And the staff's evaluation is in Section
12 7.1.4.5 of the SE. Next slide please.

13 Early this morning or this afternoon,
14 AREVA already presented --

15 MEMBER BROWN: Question on the single
16 failure ITAAC, is that an analysis or is that an
17 actual physical test?

18 MR. TRUONG: They will provide a report.

19 MEMBER BROWN: A report, okay.

20 MR. TRUONG: That confirms.

21 MEMBER BROWN: All right. So they're
22 going to drag themselves through the potential
23 single failures and show that it works okay.

24 MR. TRUONG: Yes, sir. They have -- The

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 next slide. There is an FMEA in the detail of --

2 MEMBER BROWN: Is there any hardware
3 testing where you take something out of service when
4 you're trying to shut something down or trip it?

5 MR. TRUONG: I should let the reviewer
6 answer that question.

7 MEMBER BROWN: As part of the
8 qualification program?

9 MR. STACK: Could you repeat the
10 question?

11 MEMBER BROWN: Yes. You've got
12 redundancy. Do you ever run a test that shows that
13 the redundancy actually performs like it's supposed
14 to? In other words, you introduce a trip into some
15 channel failed or some systems failed or various
16 pieces failed throughout the thing to see that it
17 still does what it's supposed to do.

18 MR. SHOOK: In terms of the -- Let me
19 just answer the -- Are you talking about during
20 design or during operation?

21 MEMBER BROWN: Qualification, not during
22 operation. During qualifications.

23 MEMBER STETKAR: Make sure you're up
24 close to the microphone because that will pick you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 up.

2 MR. SHOOK: So the question is during
3 qualification and testing of the design.

4 MEMBER BROWN: Qualification of the
5 design. Some place where you check to see that if
6 it's wired up the way it's supposed to.

7 MR. SHOOK: I can say that we do failure
8 modes and effects analysis which at the system level
9 FMEA has been supplied as part of the FSAR.

10 MEMBER BROWN: I heard that part.

11 MR. SHOOK: Okay.

12 MEMBER BROWN: I was asking about actual

13 --

14 MR. SHOOK: But during the qualification
15 testing.

16 MEMBER BROWN: Yes. Something failed
17 high or low and one of the other channels at the
18 same time you get trips. Does it still process it
19 as a trip in other words?

20 MR. SHOOK: Yes. As part of the FATT
21 testing they'll run through those various checks.

22 MEMBER BROWN: Hardware testing.

23 MR. SHOOK: Well, we call it -- It's
24 FATT or system integration testing. So you start

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 off and do the software testing. Just the software.
2 Then we'll integrate it with the hardware that's
3 built. And then you'll do a system integrated test
4 or a FATT test. And that's when you're checking --
5 You're essentially treating the protection system as
6 a black box at that point. So you're looking at
7 your inputs and then looking at the outputs. And
8 you'll be failing measurements high and low and
9 making sure the system responds the way you design
10 the two.

11 MEMBER BROWN: Okay. Go ahead.

12 MR. DOYEL: This is Chris Doyel for
13 AREVA. And I can't specifically recall, but I do
14 believe that in the development of the topical
15 report for the TXS platform that in the
16 qualification process in Germany that those types of
17 tests were done.

18 MEMBER BROWN: That's the platform
19 itself, not the whole multiple division stuff.

20 MR. DOYEL: Okay.

21 MEMBER BROWN: I mean it's a matter of
22 making sure your two-out-of-four actually work when
23 something shorted or whatever on the input to the
24 voting units. Does it really work that way? That's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 a failure. That's a single failure that can happen
2 depending on -- It could be a logic unit. It can be
3 software. It can be whatever. I'm just curious if
4 you did that. And the answer is don't know.

5 MR. ZHAO: It should be done in the
6 integration testing.

7 MEMBER BROWN: I presume. I just ask if
8 they did it.

9 MR. FREGONESE: I'll make a comment.
10 This is Vic Fregonese with AREVA. I personally
11 witnessed testing of this type in Europe both our
12 Acony systems that's installed there and the system
13 we're deploying at the EPR's worldwide have an
14 extensive hardware and software integration test.

15 The functional requirements for the
16 system rolled down into the test plan. And we have
17 an independent verification and validation group
18 that conducts that test independently. And they
19 validate all the functional requirements of the
20 system that include the failure modes that are
21 assumed, hardware failure, software failure, power
22 supply, power up, power down, all of those tests.
23 And in fact the NRC for the Acony system witnesses
24 those and we have independent witnessing by quality

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 assurance personnel.

2 MEMBER BROWN: It's actual tests, not
3 just on paper.

4 MR. FREGONESE: Absolutely.

5 MEMBER BROWN: Okay. All right.

6 MR. FREGONESE: Full integrated test in
7 the test field.

8 MEMBER BROWN: That's all I ask.

9 MR. FREGONESE: Completely wired up.

10 MEMBER BROWN: That's fine.

11 MR. FREGONESE: Thank you.

12 MEMBER BROWN: That's all I needed. The
13 answer was yes. It was hard to get to, but the
14 answer is yes.

15 MR. TRUONG: Okay. For the protection
16 system, that's the integrated reactor trip system
17 and ESF systems. They are four redundant,
18 independent PS divisions with redundant power
19 supplies and early on represented redundancy at the
20 APL/AOU level. And again there's an FMEA for the PS
21 system.

22 And for the PACS there the redundancy
23 mirrors the mechanical train system. For example,
24 the emergency feedwater is four trains and for each

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 there's an associated PACS module. And again this
2 is also describing in the PS FMEA. Next slide.

3 For the other safety systems, like the
4 SICS, in-core, ex-core, the boron concentration and
5 so on, there are sufficient level of redundancy and
6 there's also ITAACs for each as well. And there are
7 some questions that the staff has asked AREVA and
8 that's just pending.

9 And for the SAS system, there are four,
10 redundant, independent divisions and currently there
11 are a couple open items which my colleague will
12 speak to about later to address later on. And
13 that's it for redundancy.

14 CHAIR POWER: At this point, I'm going
15 to interrupt and avoid a rebellion on my Committee
16 and take a break until 3:30 p.m. Off the record.

17 (Whereupon, a brief recess was taken.)

18 CHAIR POWER: On the record. Let's come
19 back into session. I'm sorry to interrupt.

20 MS. ZHANG: No problem.

21 CHAIR POWER: But I was facing rebellion
22 here. Mutiny is so abashing in public.

23 MS. ZHANG: Hope everyone had a good
24 break. I really like the bathrooms on this floor.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 They have these fu-fu soaps that make your hands
2 smell so good.

3 MEMBER STETKAR: Maybe in your bathroom.

4 MS. ZHANG: Before I go into
5 independence, my name is Deanna Zhang. I graduated
6 from the University of Maryland with both my
7 undergraduate degree in electrical engineering as
8 well as my graduate degree in electrical
9 engineering. I study in the area of magneto-optics
10 and also semi-conductor physics. Nothing to do with
11 I&C.

12 I had my heart set out on going to Intel
13 and being a process engineer there. Well, one life
14 event changed that. I got engaged and then married.
15 So I think it's actually two life events.

16 Then to find a job very quickly, I got a
17 job at BoozAllenHamilton as a consultant for the
18 DoD. I worked there for a couple of years mainly on
19 satellite communication systems. Then I got a job
20 here at the U.S. Nuclear Regulatory Commission and
21 I've been working as a technical reviewer in the
22 area of I&C for the past five years.

23 My presentation today focuses on two
24 topics. The first topic is independence. 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 second topic is determinism. On this slide --
2 Before I begin, I want to start by discussing that
3 my presentation is my only focus on communications
4 independence. Physical separation and electrical
5 isolation of safety systems was in the U.S. EPR
6 design. Relatively straightforward. They are
7 designing with IEEE Standard 603 and IEEE Standard
8 384. So I know Charlie may disagree.

9 MEMBER BROWN: I'm just listening.

10 MS. ZHANG: Okay. So for the evaluation
11 against data communications independence or for
12 conformance to data communications independence, I
13 evaluate each of the major safety systems against
14 the 20 criteria within digital I&C ISG 04.

15 For those of you who are not familiar it
16 was the interim staff guidance. It was developed
17 under the digital I&C subcommittee working groups 04
18 and it provides -- it has three sections. The first
19 section provides 20 criteria on communications
20 independence between safety divisions and between
21 safety and non-safety systems. The second section
22 discusses priority functions. And the last section
23 discusses multi-divisional control and display
24 functions.

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 of the other systems that I did not
2 evaluate for data communications independence are
3 SICS and the SCDS systems. They do not use
4 microprocess servers and they do not perform any
5 data communications.

6 For the safety automation system, that
7 finds that SAS conforms with most of the 20 criteria
8 which was in ISG 04. Specifically the staff found
9 that only information that enhances or is used in
10 safety system functions is accepted from outside its
11 safety division. And although the slide says i.e.,
12 voting logic, it should really be e.g., voting logic
13 because of the cross train functions that were
14 introduced earlier for interlocks.

15 CHAIR POWER: That's okay. We're not
16 good at Latin here anyway.

17 MS. ZHANG: In addition, only discrete
18 data is sent between divisions. And that's only for
19 the cross train functions also.

20 The staff also found the use of dual
21 port RAM between processors and the separation
22 between safety processors and the communications
23 processors meets the criteria within ISG 04. And
24 that only predefined data messages with fixed length

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 headers are generated and accepted by each
2 safety functions processor.

3 The staff does have one open item
4 regarding how invalid signals from outside the
5 division is handled? As was discussed this morning
6 for the Protection System, they do voting logic
7 modification for invalid signals that come in.
8 There is one invalid signal and it modifies the
9 voting to two out of three. It's unclear how in the
10 SAS that's handled whether there is any voting logic
11 modification. Next slide.

12 For the Protection System, with the
13 exception of the use of SPNDs, The staff finds that
14 the Protection System complies with all 20 criteria
15 within ISG 04, Section 1 or provides an acceptable
16 deviation from the guidance. And similar to the
17 SAS, the use of only pre-defined data messages with
18 fixed length and headers that are accepted by the
19 function processors as one way of ensuring that only
20 valid data is accepted and the use of error
21 detection to ensure erroneous messages are not
22 processed by the function processors. And invalid
23 signals are accommodated through identifying invalid
24 signals and modifying the voting logic 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 accommodate.

2 MEMBER BROWN: You all agree that
3 corrupted information will 100 percent be detected
4 and rejected and not utilized in any processors.

5 MS. ZHANG: It's portions of it. The
6 staff will later discuss about the washed-out timer
7 functions.

8 MEMBER BROWN: Okay.

9 MS. ZHANG: Next slide.

10 MEMBER BROWN: I couldn't let you get
11 away without saying that.

12 MS. ZHANG: I know. It's the way these
13 slides are organized. We could jump ahead, but I
14 don't think so.

15 (Laughter.)

16 MS. ZHANG: Next slide.

17 MR. TESFAYE: There is a problem. I
18 don't think we put the last email I sent. It's not
19 just you.

20 MR. WIDMAYER: Actually I did use the
21 last one.

22 MR. CANOVA: This is actually what
23 should be presented on that slide.

24 MS. ZHANG: You know what? I don't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 think we really need to go through a diagram. It's
2 very similar to the one that AREVA showed this
3 morning. So I think we can skip this.

4 MEMBER BROWN: Yours is a little
5 clearer.

6 MS. ZHANG: Yes. Mine's a little
7 prettier. I actually hand-drew that.

8 CHAIR POWER: Let's move ahead.

9 MS. ZHANG: The next slide. So the next
10 couple slides I want to talk about the alternative
11 request for The SPNDs. As had been mentioned
12 before, The LDMBR and The HLPD reactor trip
13 functions are based on the 72 SPND measurements.
14 Each division of the Protection Systems received all
15 72 measurements for evaluating core conditions.

16 Each SPND sensor occupies a unique
17 location within the core and that's multiple
18 redundant SPNDs can't be co-located. As such, these
19 72 SPNDs must be shared among all four divisions of
20 the Protection System.

21 Thus, The SPNDs do not meet the
22 traditional redundancy and independence requirements
23 as required by 603-1991, Clause 5.6.1. However, The
24 SPNDs provides a more localized reading of the core

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 conditions over traditional ex-core detectors. Next
2 slide.

3 In the original design, as we had
4 mentioned before, the 72 SPND measurements were
5 divided into four sets of 18 that were sent to each
6 Protection System division. Each division processes
7 the received SPND signal and then shares the
8 process signals among all four divisions through
9 various ring networks and point-to-point networks.
10 The staff found that this design did not
11 demonstrate compliance with independence
12 requirements.

13 In the new design, analog hardware
14 components are used to amplify and multiply The SPND
15 signals and 72 electrically isolated signals are
16 provided to APUs in each Protection System division
17 via The SCDS. And they are electrically isolated I
18 believe through our OPAMPS. During an audit, we had
19 looked at some of the components for that
20 distribution and multiplication components for The
21 SPNDs.

22 MEMBER BROWN: What do you mean by
23 multiplication? I mean, or isolation? You've got
24 72 detectors independently coming in and they go to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 72 different scaling and conversion.

2 MS. ZHANG: When they come out of the
3 core since there's only one set of them and each
4 division needs it.

5 MEMBER BROWN: One set of what?

6 MS. ZHANG: One set of 72 SPNDs. So
7 there's no duplicates.

8 MEMBER BROWN: They split them out.

9 MS. ZHANG: So they have to split it.
10 They have to multiply the signal, each of The SPND
11 signals four times so that each division gets them.

12 MEMBER BROWN: Okay. Terminology issue.

13 MS. ZHANG: Yes.

14 MEMBER BROWN: We didn't multiply in my
15 program. We split the signal.

16 MR. CANOVA: Seventy-two times four
17 channels.

18 MEMBER BROWN: I got that.

19 MS. ZHANG: That's why not an I&C.

20 MEMBER BROWN: Only terminology, Deanna.

21 I didn't understand what you meant by that. Thank
22 you.

23 MS. ZHANG: After acquisition, by The
24 APUs, each division of The Protection 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 independently performs The HLPD and The LDNBR
2 calculations and downstream voting logic.
3 Therefore, the two reactor trip functions exhibit
4 traditional redundancy and independence from The APU
5 acquisition of the SPND measurements through the
6 reactor trip breaker. So treat them like other
7 sensors from that point on.

8 However, the staff finds that a single
9 failure in the upstream of the SPND input channel
10 does impact all four divisions of the Protection
11 System. So the staff requested the Applicant
12 provide more information as far as how an undetected
13 failure in range can be accommodated by the
14 Protection System.

15 The Applicant included in their
16 alternative request a description of the
17 conservative setpoint selection that will
18 accommodate this single, in-range, undetected
19 failure.

20 Based on the information provided, the
21 staff finds that the alternative request is
22 acceptable pending submittal of necessary revisions
23 to Chapter 15 accident analysis. Specifically, the
24 staff finds the use of the 72 SPNDs relative to ex-

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 core detectors provided more direct measurement of
2 core conditions and provides a reduction in the
3 level of uncertainty in the assumptions made.

4 And the staff finds the use of the 72
5 SPNDs shared by the Protection System divisions to
6 divisional approach provides an acceptable design
7 that can enhance plant safety by accommodating
8 multiple SPND failures. Since it's 72 SPNDs, they
9 can accommodate up to six failed SPNDs before
10 initiating a reactor trip.

11 MEMBER SKILLMAN: Question please.

12 MS. ZHANG: Yes.

13 MEMBER SKILLMAN: You talk at ease about
14 72. But as I understand it, it's really 12 fingers
15 of six detectors each.

16 MS. ZHANG: Yes.

17 MEMBER SKILLMAN: And I'm presuming that
18 those 12 fingers are somewhat geometrically
19 representative of the flux in the core.

20 MS. ZHANG: Yes.

21 MEMBER SKILLMAN: My question is for a
22 particular finger or a particular detector in finger
23 how one knows the heat flux based on the neutron
24 flux is accurate for that location.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. ZHANG: I'm not an expert on that,
2 but there is also a separate system that validates
3 The SPNDs through -- There is Aeroball System that
4 get sent in every 15 days that basically it's like
5 an aero track to make sure that The SPNDs are
6 calibrated correctly. But I could defer to AREVA if
7 you want it explained further.

8 MEMBER SKILLMAN: I would if we could
9 just -- I would like just a brief explanation so
10 that I can become comfortable of the degree of
11 attention that's been given to knowing that The
12 SPNDs that are being used for reactor trip are doing
13 so properly.

14 MR. ROYAL: This is Mark Royal for
15 AREVA. I'll try and address your question. We have
16 provided a lot of information in Chapter 4
17 previously about SPNDs and Aeroball system.

18 MEMBER SKILLMAN: Okay.

19 MR. ROYAL: Also there is a technical
20 report about the in-core system and also a topical
21 report about The Powertrax system which also
22 encompasses information provided about SPNDs and
23 Aeroball system. Both of those have been provided
24 to the staff for review.

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 SKILLMAN: Thank you. I think
2 I'd better take the action and look at Chapter 4 and
3 look at that information.

4 MR. ROYAL: Okay. Specific RAIs that I
5 think you would get really good information for are
6 RAI Set 194 and RAI Set 205 from Chapter 5.

7 MEMBER SKILLMAN: Yes, sir. Thank you.

8 MR. ROYAL: Thank you.

9 MS. SLOAN: This is Sandra Sloan from
10 AREVA. One other place that might be a condensed
11 way to look at the information and save you having
12 to look at that is our Chapter 4 presentation to
13 ACRS. I think that had a lot of good pictorial
14 diagrams and puts it in one place. It saves you
15 having to look in like six different places.

16 MEMBER SKILLMAN: Thank you. Deanna,
17 thank you.

18 MS. ZHANG: Okay. Next slide. Next
19 I'll move onto the evaluation for independence
20 between safety and non-safety control and display
21 systems. The staff also used ISG 04 for this
22 evaluation. Particularly the staff evaluated
23 communications links between the Protection System
24 and SAS with the PICS. And other non-safety 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 and links between the Protection System and SAS with
2 the non-safety QDS was in the SICS and the interface
3 between the PACS and non-safety systems.

4 The staff finds the communication link
5 demonstrates compliance to ISG 04 or provided an
6 acceptable alternative. Particularly, the staff
7 found that since no data is received from non-safety
8 control systems to the SAS and Protection System
9 through the uni-directional communication link from
10 the Protection System SAS out to the plant data
11 network. Any failure from the non-safety control
12 network or the non-safety control systems connected
13 to that network will not be able to virtually impact
14 the Protection System or the SAS. That was
15 described in detail earlier by Jeremy.

16 Also the isolation is achieved through a
17 Class 1E device that enforces uni-directional data
18 flow from the Protection System/SAS to the control
19 systems. Those are those EOCs, electrical optical
20 converters.

21 And for the PACS, the staff finds that
22 only the non-safety communication module that PACS
23 receives data from the non-safety system and that
24 non-safety system data is translated to discrete

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 hard-wire signals before it's sent to the actual
2 priority module. Next slide.

3 The staff also evaluated the data
4 communications between the Protection System and SAS
5 with the service unit. The staff finds the
6 interface between the Protection System and SAS with
7 the service unit is acceptable through demonstrating
8 compliance to ISG 04 or providing an acceptable
9 alternative. Specifically, the staff finds that the
10 communications path between the service unit and the
11 divisional MSIs for the Protection System and SAS is
12 normally disconnected through a hardwired
13 disconnect.

14 This is achieved through isolation
15 switches which ensure that only the one division can
16 be connected at a time between the Protection System
17 or SAS with the service unit. The MSI provides
18 authentication and error detection for messages sent
19 between the service unit and the Protection
20 System/SAS while they are connected.

21 The staff does have one open item to ask
22 for clarification on how isolation is achieved
23 between the RPMS and the service unit. Next.

24 MEMBER BROWN: Before you do that, there

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 was a question I forgot to ask and I'm trying to
2 figure out which slide this applies to. I guess it
3 was 32. I forgot to ask this question earlier and
4 this relates to my later observation of the way the
5 PICS data network server bus is configured.

6 There's a gateway shown in the Figure
7 7.1.2 coming off the Protection System from each
8 division. And it said it feeds the PICS. And I
9 presume it's that data bus of some kind through that
10 gateway.

11 MS. ZHANG: Yes.

12 MEMBER BROWN: And the gateway, I tried
13 to find some discussion of how that gateway is
14 configured. Is that a --

15 MS. ZHANG: It's just like a server.

16 MEMBER BROWN: No, the gateway. The
17 gateway, not the server server. But the gateway
18 itself.

19 MS. ZHANG: It's essentially a computer.

20 It's --

21 MEMBER BROWN: Okay. Now wait for a
22 minute. It's supposed to be one-way device. But
23 how is it configured as a one-way device?

24 MS. ZHANG: The gateway itself is not

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 configured --

2 MEMBER BROWN: There is data that goes
3 from the Protection System to the gateway.

4 MS. ZHANG: The device that's enforcing
5 the one-way communication is the electrical optical
6 convertors. That's before the gateway. So it's
7 between the --

8 MEMBER BROWN: That's out of the
9 Protection System.

10 MS. ZHANG: Out of the Protection System
11 and then to the gateway before it gets fed to the
12 data network.

13 MEMBER BROWN: Okay. So that's -- Is
14 that where they talk about the only the send fiber
15 optic is attached.

16 MS. ZHANG: Yes.

17 MEMBER BROWN: And the receipt is not.

18 MS. ZHANG: So my next figure will show
19 that.

20 MEMBER BROWN: Okay. That's fine.

21 MS. ZHANG: Can you go back to -- That's
22 kind of why I wanted to go to the next figure. Can
23 you?

24 MR. CANOVA: Which one?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. ZHANG: Whatever slide I was at
2 before.

3 MEMBER BROWN: Thirty-four.

4 MS. ZHANG: Thirty-four. So you see how
5 there is two electrical optical convertors there
6 between the safety side and non-safety side. Those
7 two sets between the first one and the second one is
8 what enforces the uni-directional communication. So
9 that's fiber optic out.

10 After the second --

11 MEMBER BROWN: Is that like two OLMs on
12 this picture?

13 MS. ZHANG: Similar but they're only one
14 way. So you're not connecting the one back.

15 MEMBER BROWN: I understand that.

16 MS. ZHANG: Yes.

17 MEMBER BROWN: Okay.

18 MS. ZHANG: Then on the other side
19 there's a gateway. And the difference between The
20 EOCS and The OLMs, The OLMs are configured to talk
21 pro feed bus. These are not I don't think.

22 MEMBER BROWN: No. So these are the
23 ones you're talking about that just have the one way
24 fiber. They don't connect the receipt, only the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 transmit.

2 MS. ZHANG: Yes.

3 MEMBER BROWN: Okay.

4 MR. MOTT: This is also on AREVA Slide
5 21 where they were showing this uni-directional
6 signal only coming out of the first CLC coming out
7 of the safety system from the MSI that we're
8 discussing right now.

9 MEMBER BROWN: Okay. Got it. Thank
10 you.

11 MS. ZHANG: It's the same type of
12 connection.

13 MEMBER BROWN: Shows you how long I
14 remember stuff.

15 MS. ZHANG: This is the same type of
16 connection going between the Protection System and
17 SAS with The QDS also since The QDS is non-safety
18 related.

19 MEMBER BROWN: Okay. Thank you.

20 MS. ZHANG: Next slide. So the next few
21 slides we're going to talk about determinism as well
22 as the TXS features that support deterministic
23 operation. The staff finds that The TXS system
24 operates and communicates in a deterministic manner.

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 includes the use of pre-determined fixed cycle
2 times for all TXS with the same sequence of
3 processing steps in each cycle.

4 MEMBER BROWN: Before you go any farther
5 because it's another question I forgot to ask when
6 AREVA was up here when they were showing the picture
7 of the execution cycle which is what you're talking
8 about here. Is that execution cycle and a
9 description of it actually contained in the topical
10 report?

11 MS. ZHANG: It's actually --

12 MEMBER BROWN: The picture.

13 MS. ZHANG: Yes, it's part of The TXS
14 topical.

15 MEMBER BROWN: The TelePerm topical.

16 MS. ZHANG: Yes.

17 MEMBER BROWN: I just wanted to make
18 sure it was in there and wasn't just a paraphrasing
19 of how it's supposed to work. That's all.

20 MS. ZHANG: No. It's same exact.

21 MEMBER BROWN: Okay. Thank you.

22 MS. ZHANG: The staff also finds that
23 through The use of constant message sizes and
24 communication rates will result in constant

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 communication loads under all circumstances and that
2 The communications protocols used in The TXS system
3 do not require acknowledgment of The transmitted
4 message by The receiver as well as no process-driven
5 interrupts. And The use of The hardwired watchdog
6 timer triggered by self-test features in The run-
7 time environment. These are all features that
8 contribute to The deterministic operation of The
9 U.S. EPR safety systems.

10 In addition, The Applicant provided a
11 response time analysis for The Protection System and
12 an ITAAC to verify that response time. Next slide.

13 This is about The watchdog timer,
14 Charlie.

15 MEMBER BROWN: Are you trying to get my
16 attention as I'm writing The answer down from The
17 previous question?

18 MS. ZHANG: I'll give you time.

19 MEMBER BROWN: You can go ahead. I'm
20 listening.

21 CHAIR POWER: Keep going. It's his job
22 to keep up.

23 MS. ZHANG: Actually, I just wanted to
24 make a note before we begin talking about this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 slide. There's a typo here on The second main
2 bullet or second submain bullet. It should read
3 "does not trigger" instead of "does."

4 MEMBER BROWN: Which bullet?

5 MS. ZHANG: So the second sub.

6 CHAIR POWER: The second dash.

7 MS. ZHANG: Yes. Should read "does
8 not."

9 MEMBER BROWN: Okay.

10 MS. ZHANG: It makes more sense that
11 way.

12 MEMBER BROWN: After the fourth word.

13 MS. ZHANG: Yes.

14 MEMBER BROWN: Thank you.

15 MS. ZHANG: So as described by Jeremy
16 earlier, each TXS function processor is equipped
17 with a hardware watchdog timer.

18 If the run-time environment does not
19 trigger the watchdog timer before its expiration, an
20 error is assumed in which case a hardwired signal is
21 used to indicate processor failure. The hardwired
22 signal also switches off the I/O module power supply
23 placing the processor and puts it in a defined
24 failure state. For reactor trip functions,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 switching off the I/O module power will result in a
2 zero-voltage output which initiates a reactor trip
3 signal. It's different for these.

4 MEMBER BROWN: Okay. So there is four
5 ALUs of subsystem A and subsystem B. Does it only
6 take one watchdog timer to not operate in order to
7 trigger that or does it require a watchdog timer in
8 both subsystems. It should be just one because they
9 process different variables.

10 MS. ZHANG: Since it's an Or function,
11 it's just one. So the outputs on subsystem A and
12 subsystem B don't work together. Therefore it only
13 takes one. But if it's just one ALU since both ALUs
14 are and-ed together it would not result in a reactor
15 trip. Only both ALUs were in one subsystem.

16 MEMBER BROWN: Yes. I'm looking at the
17 picture now.

18 MS. ZHANG: Yes. So these actions are
19 actually independent of the inherent self-monitoring
20 software. So this is hardware based. Next slide.

21 A response time analysis was also
22 provided for the microprocessor based portion of the
23 Protection System. And the microprocessor based
24 portion is defined as the time from the sensor

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 conditioning output, SCDS, to the reactor trip
2 breaker terminals for the reactor trip functions or
3 to the input terminals of the PACS for the ESF
4 actuation functions.

5 This analysis is based on the fixed
6 cycle times of The TXS processor and certain timing
7 assumptions are made to calculate the response time.

8 The response times for typical Protection System
9 functions are calculated and based on the
10 assumptions the longest theoretical response time
11 calculated is about 0.25 seconds. The final
12 response time is verified through an ITAAC. Next
13 slide.

14 That finishes my portion. I'll turn it
15 over to Mr. Kenneth Mott.

16 MR. MOTT: Hey. How are you doing
17 today? My name is Ken Mott. Background, I have a
18 bachelors of science in electrical engineering from
19 Howard University. I have a masters of science and
20 system engineering from George Mason University. I
21 also was a former Naval nuclear reactor operator
22 aboard the USS Enterprise CVN-65, the world's first
23 nuclear powered aircraft carrier.

24 And upon leaving and getting my

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 honorable discharge and getting out, I swore I would
2 never do anything on the planet that deals with
3 nuclear power.

4 (Laughter.)

5 Of course, it's the highest paying job
6 coming out of the Navy was at the Byron Nuclear
7 Generating Station in Byron, Illinois. That's a
8 Westinghouse PWR. It's a sister plant of Braidwood.
9 Back then when I worked there it was owned by
10 Commonwealth Edison which was ComEd.

11 Like I said once again, I left nuclear
12 power, went to telecommunications. I was a project
13 manager specialist for the Northern Virginia region.
14 Verizon Telecommunications for the outside plant
15 engineering group which was doing a fiber to the
16 premise project which the public knows as FiOS.
17 Left there once they snatched our pension. And came
18 here to the NRC back to nuclear power. Thank you
19 very much.

20 (Laughter.)

21 Two things we've been talking about
22 electrical isolation all day. Electrical isolation
23 BTP 7-11 provides guidance for this and it talks
24 about Reg Guide 1.75 which also endorses are IEEE

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 384. And what BTP 7-11 is stating is that you have
2 your maximum creditable voltage. You're going to
3 increase it to some percentage above the maximum
4 creditable voltage and for some time period you're
5 going to apply that voltage, whatever percentage
6 above that, to the electrical isolation device for a
7 particular amount of time. If the failure of this
8 voltage -- if the isolation device is able to
9 prevent the voltage at fault from coming over, then
10 it would be considered a qualified isolation device
11 in addition to meeting the other guidance of the reg
12 guide as well as --

13 MEMBER BROWN: Just electrical
14 isolation.

15 MR. MOTT: That's just electrical
16 isolation. But I know we've been talking all around
17 it and AREVA has committed to all three BTP 7-11,
18 Reg Guide 1.75 and IEEE 384 in their -- I think it's
19 Table 7.1 for the design requirements. They've
20 committed to all three of those for their credited,
21 qualified isolation devices.

22 Another thing we were talking about
23 earlier was the Protection System self-system signal
24 diversity. And I want to say the signal diversity

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's credited between the two subsystems,
2 subsystem A and subsystem B, is specific to reactor
3 trip functions, only not just SFAS functions.

4 And what this is saying as Jeremy was
5 explaining we'll take whatever the primary plant
6 parameter is and it can be pressurized to pressure
7 and we will put that in protective system alpha.
8 And then we'll put a secondary reactor trip
9 function. And it can be T hot or something and
10 Protective System Subsystem B such that if a failure
11 of your original Protection System pressure,
12 pressurized pressure, would have failed it would not
13 affect the secondary reactor trip functional
14 protection system subsystem B. So therefore
15 that would be the signal diversity. One signal could
16 not prevent a particular division subsystem from
17 failing. So that's what's described and the rules
18 for doing that are within the digital protection
19 system technical report. And we do have an RAI open
20 item waiting on an ITAAC to verify that this set-up
21 is going to be as such as built.

22 I'm Ken Mott. I will comment on this D3
23 defense-in-depth and diversity. These are the
24 diversity categories after reviewing and evaluating

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 design that the staff has approved. These are
2 diversity attributes right out of The NUREG 6303.

3 For the software one, we have an open
4 item on that on how the software that's with the
5 credited DAS. Is it sufficiently diverse from the
6 software that's in the Protection System?

7 I think they just sent a draft RAI
8 response in last Thursday or Friday. And I have not
9 had a chance to look at it to update this. So that
10 response is in. And we will discuss with them to
11 make sure it's sufficient and adequate. We can go
12 to the next slide.

13 There are other systems that make up the
14 D3 mitigation systems and once again we're talking
15 about D3. We're looking at it as Charlie was
16 alluding to it earlier. I have an APU that sends a
17 corrupted data signal to all three ALUs and it
18 corrupts all four ALUs. It corrupts.

19 Essentially the Protection System does
20 not work. What happens in that case. And as Jeremy
21 was alluding to, we have a DAS system such that that
22 same failure cannot also fail the DAS system. And
23 these are other systems that a postulated software
24 failed. The Protection System cannot fail as well.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So the PACS would not be failed by that
2 same software common cause failure. And we also
3 have one and the same common cause testing to
4 address software common cause failure to PACs as
5 well as The SCDS. Obviously, we don't want these to
6 fail in any way because these are inputs to the
7 systems. But their functions are not performed by
8 microprocessors and there is no software running in
9 SCDS with the exception of the temperature
10 compensation that Jeremy was discussing.

11 The SICS uses the hardwired panel, uses
12 discrete and analog buttons and switches. It is not
13 a computer on the SICS that's doing a particular
14 function or that could be failed by the same
15 software common cause failure that would fail the
16 Protection System. We can go to the next slide.

17 And this is the one I say this is where
18 all the marbles are right here. What I do when I do
19 my evaluations, I build myself a simplified design
20 such that I would know what I'm looking at and what
21 I'm talking about. And then I go back and make sure
22 that this is equivalent to what they're
23 demonstrating.

24 What we have in red, the red-lettered

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 items are the things that will be credited if there
2 is a failure in the Protection System and the
3 related Protection Systems.. So these are things
4 that are going to protect us in D3 space. The red
5 lines are the lines and the signals that will be
6 credited once again if the Protection System were to
7 be failed by a software common cause failure.

8 All of the lines are hardwired with the
9 exception of the PAS. If you notice the PAS is a
10 data network signal coming from the PAS going to the
11 non-safety related communication module in the PACS.

12 So in the Chapter 15 space we're on the
13 left side of the page and we're crediting the
14 Protection System. We receive sensor inputs from
15 The SCDS going to the Protection System. It senses
16 an input and The setpoint is actuated. It will
17 either wind up as an SAS actuation with sent signal
18 to the PAS module. Or if it needs a turbine
19 generator trip, we go to the turbine generator as
20 well as shown by Jeremy. We go to the reactor trip
21 on the voltage coils or the control rod drive
22 control system trip contactors.

23 Now in D4 the diversity requirement is,
24 the main one, is 10 CFR 50.62 ATWS where you need 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 diverse way to actuate emergency feedwater system
2 and turbine trip as well as depending on your plant
3 built and the diverse reactor trip system. At the
4 bottom three boxes on the right side, these are
5 what's going to meet your diversity for 10 CFR 50.62
6 where we have a diverse way to trip the turbine
7 generator I&C.

8 And as well as the reactor trip
9 breakers, we go to the SHUNT trip coils from the DAS
10 as well as the control rod drive control system.
11 And like I say they placed a more detailed design up
12 on the board. The rod control units will go from
13 the DAS.

14 On the right side the DAS is what is the
15 main actuation system up on a failure, software
16 common cause failure protection system. Since we do
17 have -- We were talking -- As Jeremy mentioned, he
18 was talking about IEC goes over to items that are
19 necessary for a triggering event for a software
20 common cause failure, a latent software failure as
21 well as a common triggering event.

22 Since we're receiving the same input
23 from the -- Essentially what he's saying is he's
24 talking about The SCDS system we can say that we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 have a common triggering event. So therefore that's
2 why the software open item was very important. But
3 the selection of a technology that does not use non
4 microprocessor based technology and no running
5 software to make a decision, we can say that the DAS
6 is sufficiently or adequately diverse for the
7 Protection System once the open item question -- We
8 do state as adequate. That was just in last week
9 Thursday or Friday.

10 So therefore even though we have a
11 common triggering event, we can say that the two
12 systems are diverse enough such that both systems
13 won't be taken out by the same failure.

14 Looking at the PACS module with a lot of
15 the talk about the PACS module. As you can see, not
16 only do we have safety related systems signals going
17 into the PACS module. We also have PAS coming in,
18 non-safety related. We also have manual controls
19 coming into the PACS as well as non-safety related
20 controls coming into the PACS.

21 From the staff one of the items that was
22 brought up was does the PACS itself on a pre-event
23 basis and we're considering the logic built into
24 there. Chapter 7 we don't really get into 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 The explanation we have is a priority set-up and Rev
2 2 priority was that the Protection System had the
3 highest priority such that no matter what was coming
4 into the PACS, the manual controls, non-safety
5 related controls from the PAS. If a Protection
6 System signal came into the PACS, that one would be
7 honored and that would end up going to the actuator,
8 the SAS actuator. So that was a priority.

9 The Rev 3, the one that has just come in
10 is that the DAS being a functional substitute for
11 the Protection System, has the same already as the
12 Protection System. Therefore if we had normal
13 operating with the PAS controlling some functions
14 and the Protection System should be failed, then the
15 DAS would take the next priority and it would
16 override other systems in order to effectuate taking
17 the plant to a safe and subcritical shutdown.

18 MEMBER STETKAR: Kenneth.

19 MR. MOTT: Yes, sir.

20 MEMBER STETKAR: Let me interrupt you
21 for just a second. You just mentioned things. I
22 think I heard you say that in Chapter 7 you simply
23 accept the priorities as they're set and make sure
24 that the system implements those priorities. Is

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 right?

2 MR. MOTT: That is not correct.

3 MEMBER STETKAR: Okay.

4 MR. MOTT: Don't accept anything. What
5 I'm saying is Chapter 15 is what deals with on a
6 pre-event basis. For this event, show me and
7 demonstrate what systems you have to protect this
8 event. But next event show me what happens to
9 protect this event.

10 MEMBER STETKAR: Well, let me interrupt
11 you for a second. I understand Chapter 15 analyses.

12 I'm asking if I have a choice between an open
13 signal and a closed signal for a valve, a particular
14 valve, in a safety system having the higher priority
15 signal, who in the staff during the integrated
16 review of this design looks at that portion of the
17 design and determines that there is indeed an
18 adequate technical basis for determining that, for
19 example, the closed signal ought to have higher
20 priority?

21 MR. MOTT: I know in Chapter 15 they're
22 going to list the systems that are going to come to
23 play in actuation such that if they need isolation
24 I'm pretty sure they would say the PACS module would

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 MEMBER STETKAR: But I don't want to
3 rely on pretty sure and I don't want to rely on
4 deterministic single event analyses that performed
5 in Chapter 15. I'm talking about who in the staff
6 steps back and says, "Yes, I understand the full
7 spectrum of events that can occur in this plant.
8 And it makes sense that for this particular valve
9 the priority signal is to close this valve because
10 that's the best thing that can happen for the full
11 spectrum of events that can happen to the plant."

12 Chapter 15 simply looks at single
13 failure criteria, deterministic design basis
14 accident analyses, one by one and says, "Yes, I can
15 mitigate this event if these things happen." Some
16 of those events require this valve to close. Some
17 of those events require this valve to open.

18 The Chapter 15 analyses don't care about
19 the integrated effects. That's the problem with
20 Chapter 15, the chapter deterministic design basis
21 accident analyses.

22 Now the question is who in the staff
23 looks at the technical justification for why the
24 closed signal has higher priority than the opened

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 signal. It's obviously not Chapter 7 people. It's
2 obviously not Chapter 15 people. Who does it?

3 MR. JACKSON: This is Terry Jackson. I
4 would say because the priority logic is described in
5 Chapter 7 of the application we would take the
6 primary role in addressing that in their chapter.
7 Now we will work with the Chapter 15 folks to
8 understand what accidents are being addressed
9 because some accidents may progress slower than
10 others. And so you may want to give priority to one
11 mitigation versus the other.

12 Also we will work with the human factors
13 branch as well. Because if, for example, an open or
14 a close is given priority, the operator would need
15 to be able to address the other situation. And that
16 may be a manual action that they have to deal with.

17 I think that the staff has an open item
18 with regards to priority. So we're still working on
19 the application with regards to that.

20 MEMBER STETKAR: But some of the issues
21 are priority of how it's achieved. It's sort of the
22 electronics of the system. I'm talking more in
23 terms of integrated safety functions.

24 MR. JACKSON: Yes. And that's our

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 intent. It's an integrated review in that case.
2 We'll take the lead on that in Chapter 7.

3 MEMBER STETKAR: Okay. And it is under
4 Chapter 7.

5 MR. JACKSON: Yes.

6 MEMBER STETKAR: So I ought to see those
7 kind of questions coming out of that part of the
8 review.

9 MR. JACKSON: Yes.

10 MEMBER STETKAR: Okay. Thanks.

11 MR. MOTT: Okay. And also within the
12 SICS the non-safety -- NSR stands for non-safety
13 related. The non-safety related controls that are
14 credited for DAS on the SICS, those are the ones
15 that are credited. And that gives the operator in
16 D3 space for the Protection System coming in with
17 the Protection System in a common cause failure
18 state, these, either one, go directly to the
19 component, the PAS module, or go directly to the DAS
20 bypassing the failed Protection System. And that
21 would meet 0.4 of the staff's requirements
22 memorandum for SECY 93-07.4 If there are no
23 questions, we can go to the next slide.

24 MS. SPAULDING-YEOMAN: Good afternoon.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 My name is Dierdre Spaulding-Yeoman. I have a
2 bachelor of science degree in electrical engineering
3 and a doctor of science degree in engineering
4 management.

5 I first began my career at the Potomac
6 Electric Power Company designing the underground
7 electrical distribution system to commercial
8 buildings in downtown D.C. I then came to the NRC
9 and I worked in a diversity of areas, special
10 inspections branch, instrumentation and controls,
11 division of reactor projects, office of enforcement.

12 I then left the NRC and worked for two years in the
13 intelligence community, returning to the NRC and the
14 Office of New Reactors in the Instrumentation and
15 Control branch.

16 I'm going to speak on the staff's
17 position and review concerning simplicity. As
18 mentioned earlier in the staff presentation by my
19 colleague, Jack Zhao, the NRC staff concern of
20 complexity of the Applicant's design are rather the
21 lack of simplicity existed. A lack of simplicity in
22 design will contribute to the design's inability to
23 meet NRC requirements and guidance and it would be
24 unlikely that the staff review of the design would

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 be completed or found acceptable in the time frame
2 desired by the Applicant or the combined
3 license/applicant's referencing this design.

4 In regard to the contents of the
5 technical information in applications, the Code of
6 Federal Regulations stipulates that the system
7 description shall permit understanding of the system
8 designs. Additionally, the staff guidance indicates
9 that a more complex system increases the likelihood
10 of failures and errors and that a complex design
11 should be avoided.

12 The staff guidance discusses the need
13 for 100 percent testing and manual verification of
14 test results such that the demonstration and
15 achievement of this would ensure that a design is
16 not overly complex. In other words, keep it simple.

17 One example in using staff guidance
18 addresses the staff concerns of the service unit
19 being continuously connected. And this led to the
20 service unit being disconnected in instances where
21 the service unit was not being used for maintenance
22 or testing.

23 Based on staff guidance and throughout
24 the course of the staff's review and interaction

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 the Applicant, the NRC staff indicated that the
2 complexity of the design is not necessary to provide
3 the required safety functions and that the lack of
4 simplicity would require substantially more
5 information to be submitted by the Applicant and
6 reviewed by the NRC staff.

7 During the staff's review and its
8 interaction with the Applicant, it was found, for
9 example, that (1) extensive interconnections existed
10 between redundant safety divisions and between
11 safety systems and non-safety equipment and that (2)
12 most of these interconnections did not directly
13 support or enhance the performance of safety
14 functions and created unnecessary complexity that
15 outweighed any benefit from using bi-directional
16 communication. The increased complexity could
17 generate additional faults and failure modes in the
18 design.

19 The NRC staff would have needed detailed
20 design information potentially including associated
21 software to be submitted on the docket in order to
22 determine the acceptability of these
23 interconnections. Such a review would require
24 extensive resources and time to be completed both

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 during initial certification and throughout the life
2 of licenses issued for such a design. Subsequently,
3 the Applicant proposed a less complex and therefore
4 a simpler design. Next slide please.

5 The following design changes were
6 provided.

7 (1) Reduced inter-divisional
8 communication;

9 (2) Elimination of inter-divisional
10 communication SICS'

11 (3) Implementation of physical uni-
12 directional communication;

13 (4) Changes regarding DAS.

14 The staff reviewed the Applicant's
15 changes to reduce the design complexity and thus
16 make the design simpler. The staff's review of
17 these design changes found that to address the
18 concerns of data communication between the safety
19 divisions, the Applicant remove functions for which
20 there was no inherent safety benefit versus keeping
21 them which would have caused the introduction of
22 potential data communication hazards.

23 The Applicant also implemented the SICS
24 using hardwired controls and indications which

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 reduced inter-divisional communication. The changes
2 to minimize inter-divisional communication also
3 simplified the overall I&C design. In addition, the
4 Applicant made the diverse actuation system to be
5 non-microprocessor based technology. Also the
6 Applicant redesigned The QDS from safety related to
7 non-safety related and this simplified the need to
8 demonstrate adequate diversity and qualification of
9 The QDS.

10 As mentioned previously, the Applicant
11 proposed to disconnect the service unit except for
12 maintenance and surveillance testing. Furthermore,
13 the Applicant proposed the use of physically
14 limited, uni-directional data communication from
15 safety related to non-safety related systems.

16 This concludes the staff's discussion on
17 simplicity and how the complexity was reduced by the
18 Applicant and reviewed by the staff. Next my
19 colleague, Wendell Morton, will discuss self-
20 testing.

21 MR. MORTON: All right. Good afternoon,
22 everyone. I'll be batting clean-up for the staff
23 presentation today. My name is Wendell Morton and
24 just a little bit of background about myself.

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 I graduated from the University of
2 Delaware where I have a degree in electrical
3 engineering, specializing in semiconductor devices
4 and materials. I also have an undergraduate degree
5 from Delaware State University in physics.

6 Upon graduation, I started work at
7 Exelon at the Limerick Generating Station in
8 Pottstown, Pennsylvania, where I was the system
9 engineer in charge of RPS radiation monitoring both
10 process area as well as a number of back-up
11 functions for the electrical systems at that plant.

12 After a few years there, I started work at Bechtel
13 where I worked with my colleague, Jack Zhao, for a
14 couple of years before I started here with the
15 Agency. And I am in the IS-1 branch working with
16 Terry Jackson.

17 So today I'll be covering a number of
18 topics that AREVA has previously touched on earlier
19 in its presentation as well as some of my other
20 colleagues. I just want to touch on a few more
21 points just to kind of give you a source or a better
22 feel for some of the significance of some of the
23 issues that we touched briefly earlier. To the
24 staff, they're a little more significant.

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 my first topic, I'll be talking
2 about the automated self-testing features that are
3 documented in ANP 10315. That's the self-testing
4 feature and surveillance testing philosophy
5 technical report. That report has been talked about
6 earlier today in terms of self-testing. But the
7 report is actually the entire maintenance and
8 surveillance philosophy for the entire U.S. EPR
9 design.

10 One-half of that report specifically
11 touches on the self-testing features. The other
12 half is for surveillance testing. Right now, I'll
13 just focus on the self-testing features.

14 For the self-testing features, they are
15 part of the qualified TXS platform. So they are
16 safety related. AREVA is taking credit for these
17 features to meet certain surveillances to obviate
18 the need for them such as the channel checks
19 operators perform in the control room and, for
20 example, the quarterly functional test that a lot of
21 I&C teams to go out and perform on a regular basis.

22 Now I know that's particularly fair and dear to my
23 heart since I worked a lot of I&C teams performing
24 those kinds of surveillances.

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 with this design by taking credit
2 for it AREVA is basically stating that those types
3 of surveillances will no longer be needed. So
4 within this testing report, the 10315, essentially
5 you're only going to see testing intended for the 24
6 month surveillances. You're not going to see
7 anything designated strictly for anything of a
8 shorter time frame than that. You can go to the
9 next slide.

10 This next slide just summarizes some of
11 the features for the automated self-testing features
12 documented in the 10315. Essentially the self-
13 testing features are split up into two halves
14 according to AREVA. You have the inherent self-
15 testing features which are part of the standard TXS
16 features that exist on every TXS function processor
17 from production. And then you have the engineered
18 self-testing features that are designed as part of
19 another COL applicant's design.

20 You can see if you read through the list
21 that we've talked about the watchdog timers. And
22 that particular device is spoken about in detail in
23 10315.

24 Just want to touch on with one

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 particular item. If you look at the last bullets in
2 each of the subheadings, currently the 10315 report
3 is only applicable for self-testing features to the
4 Protection System in SAS. The staff still has a
5 number of open items concerning the applicability of
6 the self-testing features and how they're actually
7 implemented within SAS as well as the other TXS
8 safety related system such as RPMS which Deanna
9 talked about earlier, radiation monitoring.

10 All the other TXS produced systems, the
11 staff doesn't have a clear indication if self-
12 testing features are used in that regard or the
13 credited self-testing features are used there. It
14 seems my nametag keeps moving slightly back a little
15 further here. Mike, if you could go to the next
16 slide. Do you have any questions?

17 So this is -- Yes.

18 MEMBER BROWN: I just went back to look
19 at their chart so I could -- I guess I didn't
20 realize the extent. I don't have any problem with
21 self-test. Okay. They're valuable.

22 But you said all -- The only test I'm
23 aware of right now is the two year response time
24 test, 24 months. Are there other functional tests

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that are part of the self-testing regiment that are
2 also then performed at a two year interval? Or is
3 that just --

4 MR. MORTON: There are two
5 considerations with that. Per our guidance in BTP-
6 17, it's stated that the self-test feature should be
7 verified on a periodic basis. And that's something
8 we're working with AREVA to determine what that
9 basis is if that's going to be performed along with
10 the surveillance testing for individual function
11 processors such as ALUs or CUs, things of that
12 nature. The self-tests themselves have to be
13 periodic or it's stressed to be periodically
14 verified.

15 MEMBER BROWN: Who tests the self-tests?

16 MR. MORTON: It would have to be the
17 plant personnel at that point. But how that's done
18 is still an open item. It would have an RAI on it
19 because it's still an open question.

20 MEMBER BROWN: I guess my question is
21 I'm trying to get this phrased properly. When we
22 address we utilized self-test in the program that I
23 came from. And at first we continued to do our
24 weekly or biweekly manual, turn-the-switches type

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 stuff. And then after a while, we said, "Okay.
2 We're getting good results from that." And this was
3 before we had the automatic self-testing. So we
4 were trying to look at every time you operate a
5 switch you break them.

6 MR. MORTON: Right.

7 MEMBER BROWN: A lot of maintenance
8 associated with broken switches.

9 MR. MORTON: Right.

10 MEMBER BROWN: And if you got reliable
11 systems particularly the integrated circuit, solid
12 state stuff was much more reliable than the old mag-
13 amp or discrete transistorized stuff. So we started
14 looking early at trying to extend that one weekly
15 calibration check to a long term based on
16 experience.

17 Then once we went to the microprocessor
18 based stuff, we said, "Okay. What can we do?" But
19 we didn't go out to two years. And then the other
20 thing we incorporated was a periodic check of the
21 self-test to make sure that a datapoint that you
22 were using to do the self-test.

23 For instance, say, you put in whatever.

24 If you've got RTDs for temperature, you put in some

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 fixed resistor, high precision plate 0000001 type
2 percent resistors to check that. So we did some of
3 those manually. I retired 12 years ago. So I have
4 no idea what they're doing now.

5 But I guess my question is I don't have
6 any problem with self-testing. But is there a point
7 at which you check that your self-test regiment is
8 still performing satisfactorily with external, you
9 know, some type of external, actual stimulus such as
10 an RTD or a pressure simulated pressure signal or
11 level of whatever? I guess I didn't think of that
12 earlier.

13 CHAIR POWER: I think that's what you're
14 talking about.

15 MR. MORTON: Yes.

16 CHAIR POWER: That's where you have an
17 open item right now.

18 MR. MORTON: Yes. The open item
19 basically is the verification of are you making sure
20 that your self-testing features are doing what you
21 say that they're doing on a periodic basis per the
22 information you find.

23 MEMBER BROWN: All right. If there's an
24 open item on it, I'll wait until you get the 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 We don't have to resolve it. I just feel it ought
2 to be addressed. And Jeremy looks like he wants to
3 talk. But you're going to talk, talk into the mike.

4 MR. SHOOK: So just to follow up on
5 Wendell's point, we are working with the staff on
6 clearing that open item. But I would point to the
7 testing strategy that's been laid out. And if you
8 look on slide --

9 MEMBER BROWN: Forty-five?

10 MR. SHOOK: For reactor trip, it would
11 be slide 28.

12 MEMBER BROWN: Twenty-eight. Yes, I've
13 got the --

14 MR. SHOOK: And so you can --

15 MEMBER BROWN: That's what I was looking
16 at. They're both roughly the same.

17 MR. SHOOK: And you can see that the
18 sensor operational test will test functionally
19 through the ALU. And then The ADOT test will test a
20 portion of the ALU on out. So then you have -- Then
21 you're looking at the self-test, the continuous
22 self-test and the extended self-test, to test the
23 portions in the middle that aren't tested by the
24 sensor operational test in The ADOT.

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 point I wanted to make is that a
2 good portion of this system including the
3 microprocessors are going to be tested through a
4 periodic testing program.

5 MEMBER BROWN: With humans?

6 MR. SHOOK: With humans. But there is a
7 portion of the system that's not tested and that's
8 the part that we're working with the staff on.

9 MEMBER BROWN: Okay. I guess I didn't
10 read the -- When I looked at the sensor operational
11 test, I thought that meant you had an automatic
12 signal being produced as opposed to an external
13 check that that was actually out right periodically.
14 This tech spec will refer to something.

15 MR. SHOOK: That's correct. That sensor
16 operational test is basically functional similar to
17 what we would call the trip point calibration.

18 MEMBER BROWN: Yes, but you still need -
19 - At some point, there is still some processing
20 stuff in terms of the calibration of your software
21 that it's taking the data and producing the desired
22 result from whatever the input is from the analog
23 signals you get from the sensors.

24 MR. SHOOK: That's correct.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BROWN: Okay. All right. So
2 that's being addressed. The pieces that haven't
3 been nibbled on are being addressed.

4 MR. SHOOK: That's correct.

5 MEMBER STETKAR: Jeremy, while you're
6 there, let me ask you or I could ask Wendell.

7 MR. SHOOK: All right.

8 MEMBER STETKAR: Response time test
9 which is the only one that I'll use the term end-to-
10 end tests, the only true end-to-end test, through
11 the whole function is performed according to tech
12 specs once every 24 months on a staggered test
13 basis. Does that mean division one is tested once
14 every eight years?

15 MR. SHOOK: I don't know the answer to
16 that.

17 MR. PHAN: The staggered test basis is
18 referring to is because for the response time
19 testing it's not one test that goes from your sensor
20 all the way down to your actuator. It's made up of
21 overlapped tests between.

22 Say, for instance, your sensor
23 operational tests, that also functions as a response
24 time test. And there's also a response time test

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 your APU and AOU and those processing
2 components. But that overlaps with --

3 MEMBER STETKAR: I guess that discussion
4 is somewhat contrary to the little cartoon that we
5 see in slide 28 from AREVA which would indicate to
6 me anyway that the response time test is a fully
7 integrated sensor to output device tests.

8 MR. SHOOK: I think one of the -- a
9 piece that's sort of not clear what this picture is
10 that these are actually referring to The
11 surveillances. And so when we actually do the
12 testing we may piece different parts of the test to
13 satisfy different pieces of surveillances.

14 MEMBER STETKAR: That's like stroking a
15 valve and making sure that the valve strokes and
16 then testing the pump and making sure the pump
17 works. And never making sure that when the pump
18 works, you actually get flow through the valve. Is
19 that right?

20 MR. SHOOK: Yes, you're essentially
21 testing --

22 MEMBER STETKAR: It's a problem that
23 we've had in the nuclear industry for not doing
24 integrated tests of fluid systems. Because people

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 find out that when the pump starts, the DP across
2 the valve is too high and the valve doesn't open.

3 MR. SHOOK: Right.

4 MEMBER STETKAR: That has happened.
5 That's why in mechanical systems there's a strong
6 advocacy for doing full end-to-end tests verifying
7 that the entire function works when you initiate the
8 function that you don't piece together and assert
9 that the system will function because all the little
10 bits and pieces worked individually.

11 My interpretation of what I thought you
12 had here was that the 24 month test was indeed an
13 end-to-end test. You actually tripped the input and
14 verified that the output behaved according to the
15 way it was supposed to behave. And from what I hear
16 you say that's not true. Is that?

17 MR. PHAN: This is Duc Phan again. It's
18 all described within our ANP 10315 document. We
19 describe why it's impractical for us to end-to-end
20 test and take out a whole division.

21 MEMBER STETKAR: Excuse me. Why is it
22 impractical for you to do that? I worked in a
23 nuclear plant that had relays that sparked and we
24 used to do it. Why is it impractical with these

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 wonderful software driven things that you can't do
2 it?

3 MR. PHAN: Some functions such as your
4 low DNBR function, you have all 72 SPNDs that feed
5 into the system each division.

6 MEMBER STETKAR: I'll give you that one.
7 What about all of the other ones? Reactor
8 protection and safeguards?

9 MR. PHAN: If you would like, I can go
10 and I'll point out the section because there's page
11 full of bullets.

12 MEMBER STETKAR: Okay.

13 CHAIR POWER: Let's do just that.

14 MR. PHAN: Okay. And I'll point to
15 them.

16 MEMBER STETKAR: Okay. Thanks. I'd
17 appreciate to see that. Thanks.

18 MR. MORTON: All right. So just to tie
19 up this slide as far as that open item, it's just
20 that we're working with AREVA still to determine how
21 the automatic self-testing features in TXS are going
22 to periodically verified.

23 Secondly, there is the question of
24 operability for the self-test features. The

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 operability comes in two different steps for the
2 staff's review. How is The operability addressed
3 for a TXS component that's actually been found by
4 self-testing features to be faulted, failed, locked
5 up or any one of those terms to describe a device
6 that is no longer functioning as designed? That's
7 one aspect of it.

8 The second aspect of operability that
9 the staff is looking for is how is operability of a
10 TXS function processor or affected when the self-
11 testing feature fails to a certain degree. And we
12 touched on that earlier with the locked function
13 processor and the hardware watchdog timer. But
14 specifically if you do have a failed self-testing
15 feature when it's not specifically covered in ANP
16 103 what steps the operator would take upon a failed
17 self-test run? So the staff has an open item on
18 that.

19 Specifically, for ANP-10315 we just
20 touched on some of the testing that AREVA has talked
21 about, the actuating device operational test, the
22 sensor operational test. One of the concerns the
23 staff has is that these tests aren't necessarily a
24 one-stop shop for testing or performing

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 surveillances on every TXS safety system.

2 Right in the preface of 10315, the
3 surveillance testing portion of this report really
4 only applies to the Protection System specifically.

5 So the staff has an open item working with AREVA to
6 determine whether the actuating device operational
7 test and other tests mentioned inside there how
8 those tests would be applied to the other TXS safety
9 systems. In staff's determination, they're not
10 quite a one-stop, one-shoe-fits-all type approach.

11 Secondly, and I touched on this earlier,
12 other TXS safety systems that utilize credit self-
13 testing features are still not quite clear to the
14 staff. So we have an open item on that as well. If
15 there are no questions.

16 Now the next topic I'll be touching on
17 and AREVA has touched on it briefly and the staff
18 has as well are the service units and the U.S. EPR
19 design as was -- I believe AREVA had it on a slide
20 previously, the non-safety related computers which
21 serve as the primary means of performing
22 surveillances and trouble-shooting activities
23 specifically for the Protection System, SAS and
24 RPMS.

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 Within The EPR design, AREVA does not
2 specifically state that the service units will only
3 be used for those three systems. This is what the
4 staff has gleaned from our review of the available
5 drawings and documentation. The service unit is
6 spoken about in detail within Section 7.1, also
7 partially within 10315 and also in digital
8 protection system technical report. I believe that
9 number is 10309 where it talks about service unit
10 functionality.

11 I just wanted to impress upon the
12 Committee that the service units are the main ways
13 in which a team of technicians on a future EPR plant
14 would actually perform maintenance on those systems.
15 Next slide.

16 So forgive the graininess of this
17 drawing. This is just another sort of simplified
18 version of what we're dealing with with The service
19 unit. And Deanna touched on this before. If you
20 look at -- You have the service unit to the left.
21 That next blue box is the credited hard disconnect
22 switch per ISG 04 that AREVA is taking credit for to
23 provide the isolation from the divisions.

24 The next block right there is the MSI,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 divisional MSI. The other blocks right there are
2 the CPU state switches. For the service unit
3 function you have two steps in order to perform
4 maintenance on a particular function processor. You
5 have the hard disconnect switch which must be turned
6 to a specific protection system/SAS RPMS division.

7 And then when you've done that you have
8 to turn the CPU state switch for a specific function
9 processor to enable. That enables you to change the
10 state of the CPU of the function processor from a
11 service unit to perform whatever type of maintenance
12 activities you want to perform. If there are no
13 questions, I'll just go to the next slide.

14 Here are some of the major open items
15 the staff has for concerning the service unit. Once
16 again, we'll touch upon the topic of operability
17 when it comes to the service unit. There is still
18 open questions on what is the baseline operability
19 for using an NSR piece of equipment when performing
20 maintenance on a safety related piece of equipment.
21 There is open questions about that.

22 There's questions on when you are
23 performing certain surveillances according to AREVA
24 a function processor may have to be in multiple

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 operating states in order to perform that particular
2 surveillance. Each one of those operating states of
3 a function processor has an operability designation
4 attached to it. So how would a team of individuals
5 performing a surveillance task? How would an
6 operations team determine operability of a function
7 processor when you're dealing with multiple
8 operating states while you're plugged into the
9 service unit?

10 I apologize. That's a little bit of a
11 convoluted explanation. But it's sort of the issues
12 that we're trying to work through with AREVA to
13 determine The operability status while using the
14 service unit.

15 And I touched on earlier the service
16 unit usage for the other TXS safety systems. I'm
17 still trying to pin down how specifically the
18 service unit will be used in the same manner as the
19 Protection System.

20 At this time, we have an okay idea of
21 how it will be used for the Protection System. But
22 still for the other TXS safety systems, SAS, RPMS,
23 even RMS, other safety systems, we're not quite sure
24 where we stand on that yet based upon The AREVA

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 available design documentation. No questions. Go
2 to the next slide.

3 Another open item we have -- I'm sorry.
4 We're going to jump to SAS right now. So we've
5 touched on SAS a number of times already in the
6 presentation earlier, both AREVA and the staff.
7 Just to bring a little more emphasis to some of the
8 points my colleagues had made. Tung Truong had
9 talked about The FMEA for SAS. I believe AREVA has
10 said that's going be coming down the pipeline some
11 time soon.

12 This is significant for the staff's
13 evaluation because it will give us more of an
14 ability to determine whether SAS meets single
15 failure criterion number one. And I know from a
16 number of questions that the Committee has had
17 earlier just The FMEA should provide information on
18 the effects of SAS failures on plant operations
19 which is significant for those systems such as CCW,
20 ESW and all The HVAC systems in which SAS is
21 performing those safety related interlocks for.

22 And that particular document has already
23 been provided for the Protection System. So we're
24 looking for the same level of detail for the SAS

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 FMEA.

2 Generally, just to make a point about
3 SAS, given that it's safety significance and a
4 number of safety related functions and protective
5 actions SAS performs, the staff is looking for
6 information for SAS comparable to what AREVA has
7 already provided for the Protection System since all
8 the regulations essentially apply to the same system
9 as well. For The FMEA, that would be 603, Cause
10 5.1, for that one.

11 As my colleague, Deanna, talked about
12 earlier, we have another RAI specifically requesting
13 more information on SAS voting logic. What SAS
14 functions actually perform voting as we understand
15 it and what SAS functions do not? Or a specific
16 place where they're going to put that. So we have
17 an open item on that. Because obviously some of the
18 conversation we've had earlier today, it's still
19 sort of an open issue as far as SAS voting taking
20 place. There are no questions. Next slide.

21 For SAS system integrity, this is based
22 upon guidance from SRP 71-C. So the staff is
23 looking for some further information on the failsafe
24 configurations for SAS. I know that was a topic

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 came up a little earlier today. We
2 specifically pointed to a loss of power condition,
3 but this is a question that generally covers what
4 AREVA feel are the failsafe configurations for SAS
5 because SAS is utilizing the PAC modules. So that's
6 an important question for the staff to resolve.

7 And as I said that's a significant issue
8 based upon the number of interactions that SAS has
9 with all the various mechanical systems. As one of
10 my colleagues stated earlier, there is a PAC module
11 for every mechanical actuating device whether it's
12 emergency feedwater pumps, valves, something to that
13 extent. If there are no questions, next slide.

14 Now this is a question that come up just
15 for the staff just trying to inquire whether SAS has
16 any response time timing attached to it. Based upon
17 the applicable regulations and guidance the staff is
18 looking for something definitive when the design
19 documentation SAS either does have requirements or
20 does not.

21 There are certain SAS functions that are
22 performed that potentially affect Chapter 15
23 operations. Specifically, the DCB does not
24 particularly go into any detail as far as what kind

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 of requirements it may or may not have. So we have
2 an open item covering that. If there are no
3 questions, we'll go to the next slide.

4 Lastly, for SAS D3, this has been
5 touched on a little bit previously. I also won't
6 belabor this point. But essentially the Applicant
7 has not provided a D3 analysis for SAS. We've
8 touched on a number of the safety related functions
9 that SAS performs, the ESF controls, the continuous
10 loops that it performs for emergency feedwater pump
11 protection. Some of the safety related interlocks
12 it performs for CCW and ESW, some of those systems.

13 Given the fact that SAS has both
14 actuation -- It is actuated from the Protection
15 System and it also has continuous operation
16 capabilities. The staff is looking for some
17 definitive analysis from a diversity standpoint
18 based upon the guidance and rules concerning SAS.
19 If there are no other questions, that's it.

20 MEMBER BROWN: I believe that
21 terminates.

22 CHAIR POWER: Let's see. I have -- You
23 have raised quite a number of open items here. And
24 each of them seems they're worthwhile to pursue.

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 question that I have is do you see a path
2 forward on these or do they represent a major hurdle
3 in the drafting of this SER?

4 MR. MORTON: I will say to that question
5 that we've been working with AREVA pretty closely on
6 all of these topics. We're making progress on many
7 of them. So I guess from that standpoint we do have
8 a path forward on many of these.

9 On some of them, they're going to be a
10 little bit more of a challenge to deal with. But we
11 are making progress in working with the Applicant on
12 many of these issues.

13 MEMBER BROWN: By challenge, you mean
14 you have disagreements on whether anything needs to
15 be done at all. Is that correct?

16 MR. MORTON: By challenge, it means we
17 haven't received a response yet. When we do, we'll
18 get to that.

19 MR. TESFAYE: I guess the question is
20 are there solutions to these questions and the
21 answer is yes. Otherwise, the staff would not leave
22 --

23 CHAIR POWER: That's the question I
24 have.

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. TESFAYE: Absolutely.

2 CHAIR POWER: Right now, I'm looking at
3 all this and saying, "Gee, it looks like we could
4 move Section 7 forward." I mean I don't see things
5 fundamentally, philosophically, hardware-wise
6 barring moving this forward.

7 I asked Mr. Morton because he's raised a
8 number of RAIs that I think are worthwhile and
9 certainly speak to many of the questions that have
10 been raised by the Subcommittee if he has a path
11 forward on these things. And you're saying you
12 think there is.

13 MR. TESFAYE: Yes.

14 CHAIR POWER: Very good. Very good. Do
15 any of the members of the Subcommittee had
16 additional questions for the staff on these
17 particular items?

18 MEMBER STETKAR: No, sir.

19 MEMBER BROWN: Other than I would like
20 to hear on the open-ended stuff.

21 CHAIR POWER: Right. We've identified
22 many things.

23 MEMBER BROWN: End-to-end testing and
24 then the items he raised. The basis and I didn't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 realize the staggered thing when John mentioned
2 that. That was interesting.

3 CHAIR POWER: Yes. I think there are
4 several items that need to be worked out yet. But
5 our criterion is we don't see anything that's
6 fundamentally blocking here. We see a path
7 resolution.

8 MEMBER BROWN: I'm going to look at the
9 watchdog timer stuff in the text in spite of people
10 giving good answers and I understand them. But I
11 just --

12 CHAIR POWER: There can be lots of
13 questions and indeed what send forward into the next
14 phase is an SER with open items. What we don't want
15 to do is send forward an open item that says the
16 plant can't be built.

17 (Laughter.)

18 But I don't see anything there. And you
19 give me assurance that you don't see that either.

20 MR. MORTON: For the time being.

21 MR. CANOVA: At this time.

22 MR. MORTON: At this time.

23 CHAIR POWER: Okay. Thank you.

24 You're done.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. TESFAYE: I'm done.

2 CHAIR POWER: Okay. I think at this
3 point we move back to COLA. And I think we have
4 Mark Finley.

5 Michael, did you want to say anything to
6 begin this section or do we just start with Finley
7 and then get back to you?

8 MR. CANOVA: No, I'll come in afterwards
9 with Dierdre actually to do the staff presentation.

10 CHAIR POWER: Okay. I guess the floor
11 is yours. Did you have an opening comment to make,
12 Surinder?

13 MR. ARORA: Yes, sir.

14 CHAIR POWER: Please make your opening
15 comment.

16 MR. ARORA: Good afternoon. My name is
17 Surinder Arora. I'm the lead PM for Calvert Cliffs,
18 Unit 3 COL Application review by the NRC. And today
19 we are here to present Chapter 7, Instrumentation
20 and Control as it applies to the COL application.

21 I had given the project overview
22 yesterday and I don't believe there's anything I
23 need to add. So in the interest of time we'll get
24 started with The Unistar presentation and with 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 I turn it over to Mr. Finley to introduce his team
2 and let's start the presentation.

3 MR. FINLEY: Thank you, Surinder. So
4 again, my name is Mark Finley. I think most of the
5 members of the Subcommittee here know me.

6 CHAIR POWER: We're spending way too
7 much time together. There's no question about it.

8 (Laughter.)

9 MR. FINLEY: For Dr. Brown here, my
10 career has been with Constellation 27 years. I'm
11 with Unistar five years. I'm a mechanical engineer
12 by training. Recently taken over both engineering
13 and regulatory affairs at Unistar and I'm taking the
14 place of Greg Gibson who was our Senior Vice
15 President of Regulatory Affairs. Also nuclear
16 power, Navy.

17 Thank you first of all for staying late
18 and considering The Calvert Cliffs FSAR.

19 CHAIR POWER: We're right on schedule as
20 a matter of fact. In fact, we're ten minutes ahead
21 of the schedule.

22 MEMBER BROWN: Given the schedule was an
23 extended schedule based on the normal schedule, I
24 just wanted to make sure the Chairman understood

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that.

2 CHAIR POWER: The Chairman understands
3 that the schedules in the past have been lax and
4 loose.

5 MEMBER BROWN: If we don't have this
6 interchange it's not interesting.

7 (Laughter.)

8 MEMBER STETKAR: For those of us who
9 weren't here yesterday.

10 MEMBER BROWN: In the short session,
11 right?

12 MR. WIDMAYER: I'll have you know that
13 the Chairman had nothing to do with the
14 establishment of the schedule.

15 CHAIR POWER: The Chairman is
16 responsible for all that occurs in the Subcommittee.
17 And he'll take responsibility for the schedule and
18 point out that it's still lax and loose.

19 MR. FINLEY: Okay. So slide 2 should be
20 a short and sweet presentation on our part. We
21 essentially have incorporated the U.S. EPR FSAR by
22 reference in terms of Chapter 7. We will discuss
23 two COL information items and one supplemental
24 information item. Other than that, we're very

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 consistent with what AREVA presented today.

2 Slide 3, supporting me today is Cyril
3 Roden. You met him yesterday. He's our manager of
4 instrumentation controls and electrical engineering.

5 And we have other members of The AREVA team that
6 have stayed behind to support us as well. Steve Paul
7 from Bechtel in case we need some support from any
8 experts. And again we'll focus on site specific
9 information that supplements that information in the
10 U.S. EPR FSAR.

11 So with that I'll introduce Cyril Roden
12 for slide 4.

13 MR. RODEN: Thank you, Mark. Good
14 afternoon. So my name is Cyril Roden. I'm still
15 French from yesterday.

16 (Laughter.)

17 MEMBER BROWN: I would have never
18 guessed.

19 CHAIR POWER: We're going to start
20 taking away your French.

21 MR. RODEN: I joined UniStar in August
22 2010 from EDF where I worked for 11 years in I&C and
23 electrical topic both for operating fleet and new-
24 build. And I've got French engineering degree on

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 electrical design, signal processing and automation.

2 And as Mark said we will get through as
3 we did yesterday for Chapter 18 through the
4 different COL items we have on Chapter 7. Next
5 slide.

6 In Slide 5, the first one concerning the
7 accident monitoring communication, we have the list
8 of PAM variables in U.S. EPR Table 7.5-1 which will
9 be confirmed upon completion of the emergency
10 operating and abnormal operating procedures. And
11 this would be done prior to fuel load. Next slide.

12 This COL item is a new one that appears
13 in the Rev 3 of The DCD. It refers to the reactor
14 power limitation with respect to thermal power. Our
15 commitment is following selection of the actual
16 plant operating instrumentation and calculation of
17 the instrumentation uncertainties of the operating
18 plant parameters and prior to fuel load. The
19 primary power calorimetric uncertainty will
20 calculated and the calculation will be completed
21 using an NRC-acceptable method and shall confirm
22 that the safety analysis primary power calorimetric
23 uncertainty bounds the calculated values. Next
24 slide.

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 the next slide we have our
2 supplemental information which in fact we
3 supplemented the inventory of the PAM variables
4 table we have in the DC with the tower basin level
5 indication of The ESWS and also with The
6 meteorological parameters, wind speed, wind
7 directions and the temperature information.

8 CHAIR POWER: That's to get your chi/q
9 values.

10 MR. RODEN: I'm sorry.

11 CHAIR POWER: Get your chi/q values for
12 the site.

13 MR. RODEN: That's correct.

14 MR. FINLEY: Yes.

15 MR. RODEN: That's all we have in
16 Chapter 7. I don't know if you have any questions
17 with that.

18 CHAIR POWER: I don't. I know what
19 you're doing. Not much you can do to get farther
20 along.

21 MR. RODEN: Thank you for your time.

22 MEMBER BROWN: Are you all finished?

23 MR. FINLEY: Yes.

24 MEMBER BROWN: Figured that when I saw

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the conclusion slide. I do have -- and everybody is
2 going to hose me -- But I did have -- Where's my
3 crib sheet? The concern that I voiced relative to
4 the communication of data to The TSC and out to the
5 business.

6 I made mention of that. I realize that
7 I'm not supposed to talk about that. But I'm going
8 to anyway. And if that configuration is not a very
9 -- It's a very vulnerable configuration depending on
10 how that's done. I can't tell you what to do or how
11 to do it.

12 AREVA was very mushy relative to it can
13 be anything that the licensee would like to do as
14 long as the NRC agrees. But the way it's set up
15 right now you can trash everything in the PICS if it
16 gets compromised.

17 MR. FINLEY: I'm sorry. I wasn't here
18 all day today. Maybe --

19 MEMBER BROWN: If you look at the
20 diagram, right off the PICS server lines there's a
21 firewall that feeds the business network. That's
22 their conception of the setup. And what that does
23 is somebody hacks in. They can take out everything.

24 MR. FINLEY: So the concern if I can

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 paraphrase is the communication between the business
2 information system --

3 MEMBER BROWN: And all the rest.

4 MR. FINLEY: And?

5 MEMBER BROWN: And the fixed system.
6 And the main control and TSC and all those.

7 MR. FINLEY: And TSC.

8 MEMBER BROWN: Yes. I said if there's a
9 firewall noted right there and they send all the
10 PICS data gets out to the business system for
11 whatever use people want. I'm not objecting to data
12 going out. That's not the point. It's where and
13 how it's executed.

14 And they were saying that the firewall
15 could be a software configured firewall in terms of
16 a firewall. In other words, where it's easily
17 hackable as opposed to a hardware, one-way, hard
18 core analog data diode per se how it's done. It
19 might be a little slower, but you're much less
20 vulnerable.

21 I can't tell you. I'm just saying
22 that's -- Brought it up. I was told to pound sand
23 in the last meeting.

24 MR. FINLEY: Certainly understand the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 concern.

2 MEMBER BROWN: I will suggest that you
3 all look at that closely. That's all. It comes
4 under The cyber plan and all that other kind of
5 stuff which is not covered under the auspices of
6 this design certification I guess.

7 MR. FINLEY: Chapter 7.

8 MEMBER BROWN: So other than as a plan.

9 MR. FINLEY: So I can say we certainly
10 understand the concern. We share the concern. We
11 haven't done any detailed design of the firewall at
12 this point.

13 MEMBER BROWN: I understand that. I
14 just thought I'd bring it up.

15 MR. FINLEY: We have that as an action
16 certainly.

17 MEMBER BROWN: Thank you. That's all I
18 had, Dana. Thank you.

19 CHAIR POWER: At this point, I think we
20 can move to the staff presentation.

21 MR. ARORA: Mike knows what happens to
22 the Chapter -- for Calvert Cliffs also. He has
23 already been introduced.

24 CHAIR POWER: Yes. They told us he was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 doing double duty here. But he has a tremendous
2 team supporting him. So I'm not feeling so sorry
3 for him. I started out saying, "Boy, this guy is
4 having to work hard."

5 MR. CANOVA: I have actually the easily
6 job in the whole world.

7 CHAIR POWER: And then I saw his team
8 and I said that I don't feel so sorry for him.

9 MR. CANOVA: We'll go through this
10 really quick. This is our presentation on Chapter 7
11 for Calvert Cliffs, Units 3 and 4.

12 We've met. The Applicant has already
13 been here.

14 MR. ARORA: We skipped these slides.

15 MR. CANOVA: We did these slides
16 yesterday. So I don't think we need to them.

17 MR. ARORA: They're the same as
18 yesterday's.

19 MR. CANOVA: Dierdre Spaulding-Yeoman
20 sits to my right. I talked to Terry and Terry's not
21 going to make any remarks on this presentation.
22 It's just a quick overview. There were only
23 questions asked in 7.1, 7.5, 7.7 and 7.9. A total
24 of six questions. There are three questions

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 outstanding, two of them in one RAI set. So that's
2 two RAIs they're discussing.

3 This looks familiar. Dierdre, if you'd
4 like to address it.

5 MS. SPAULDING-YEOMAN: As you've heard,
6 the Safety Evaluation Report for the Chapter 7 U.S.
7 EPR does have several existing open items. The
8 staff will update its safety evaluation for Calvert
9 Cliffs Unit 3 to reflect the final disposition of
10 those open items in the safety evaluation in regard
11 to how they impact The Calvert Cliffs Unit 3 staff
12 evaluation.

13 With the exception of the open items to
14 Calvert Cliffs which are discussed in the following
15 three slides, all other Chapter 7 information has
16 been incorporated by reference. In regard to site
17 specific post-accident monitoring variables, the
18 Applicant identified the site specific PAM
19 variables: essential service water system cooling
20 tower basin level, meteorological monitoring system
21 wind speed at 10 meters and 60 meters,
22 meteorological monitoring system wind direction at
23 10 meters and 60 meters and meteorological
24 monitoring system vertical temperature difference

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 between 10 and 60 meters. These site specific
2 variables provide indication in order to provide
3 data for radiological release assessment. Next
4 slide please.

5 The staff found that The Calvert Cliffs
6 ITAAC as provided in its FSAR contain
7 instrumentation and control design information for
8 which there was no information or details within the
9 Chapter 7. For example, the staff found that The
10 ITAAC mentioned site specific systems such as the
11 ultimate heat sink, makeup water system and the
12 ultimate heat sink makeup water intake structure
13 ventilation system. Again, the staff did not find
14 any information that identified the safety related
15 I&C systems controlling these site specific systems.

16 These systems may be controlled by the
17 safety automation system which is described in the
18 U.S. EPR FSAR. Or they may be controlled by
19 standalone I&C systems. If they are controlled by
20 standalone I&C systems, The FSAR should address how
21 these standalone I&C systems meet applicable I&C
22 requirements.

23 Additionally, the staff was not able to
24 identify any automatic and/or manual functions

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 associated with these site specific systems.
2 Therefore, in request for additional information,
3 325 Question 07.75-01 the staff requested that the
4 Applicant address the identified I&C issues. This
5 is being tracked as an open item. Next slide
6 please.

7 The staff concluded that the Applicant
8 appropriately incorporate by reference U.S. EPR FSAR
9 Tier 2, Section 7.5. However, the staff issued an
10 RAI to the Applicant, U.S. EPR, which retain to the
11 U.S. EPR FSAR Section 7.5 that questions the
12 necessity for a COL item.

13 The staff finds that the post-accident
14 monitoring instrumentation in U.S. EPR FSAR, Tier 2,
15 Section 7.5 needs to be a complete list with the
16 exception of site specific instrumentation.
17 Therefore, there does not appear to a need to update
18 the post-accident monitoring instrumentation list.

19 The staff issued RAI 325 Question 07.05-
20 2 to track coordination of the applicable changes in
21 the U.S. EPR FSAR regarding post-accident monitoring
22 in regard to the site specific Calvert Cliffs Unit
23 3. Next slide please.

24 In regard to Section 7.7 for The Calvert

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Cliffs application, the staff issued RAI 326
2 Question 07.07-1. The staff did not find where the
3 Applicant addressed the COL item related to primary
4 power calorimetric uncertainty.

5 In its review of the U.S. EPR design
6 certification, the staff identified the following
7 information from Section 7.7.2.3.5, Interim Revision
8 3 markups. The information states in part "a COL
9 applicant that references the U.S. EPR design
10 certification will following selection of the actual
11 plant operating instrumentation and calculation of
12 the instrumentation uncertainties of the operating
13 plant parameters prior to fuel load calculate the
14 primary power calorimetric uncertainty."

15 And RAI 326 Question 07.07-1 the staff
16 requested that the Applicant provide design
17 information that addresses this COL information
18 item. If the COL information is address in another
19 part of The SER, information should be provided in
20 Section 7.7 that acknowledges the COL information
21 item and points to the applicable location where the
22 design information is provided. This question is
23 being tracked as an open item.

24 This concludes the staff presentation,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 technical presentation on Calvert Cliffs Unit 3.
2 Thank you.

3 CHAIR POWER: There does not appear to
4 be any barrier to resolving these issues since the
5 Applicant just said he was going to do. So it looks
6 like this is moving right forward.

7 MR. ARORA: And just for the record, we
8 also have the generic open item on this chapter as
9 well. That's the DC reviews.

10 CHAIR POWER: Yes. That's right.

11 Do members have any additional questions
12 on this?

13 MEMBER BROWN: I don't.

14 CHAIR POWER: I would like, Mr. Stetkar,
15 you had two items that you spoke on heavily if you
16 would give me a note on those.

17 MEMBER STETKAR: I'd be happy to, but I
18 don't remember which two.

19 CHAIR POWER: I have them in my notes.

20 MEMBER STETKAR: Thank you. I would
21 appreciate that.

22 CHAIR POWER: I would like to thank
23 everybody that participated in this meeting. I
24 certainly learned a lot. I can tell you it is very

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 evident that a heroic amount of work has been done
2 both by the Applicants and by the NRC staff in this
3 regard. And I come away much more confident than I
4 came into the meeting on the progress being made in
5 this direction.

6 And with that I'm going to adjourn this
7 Subcommittee meeting. Off the record.

8 (Whereupon, at 5:08 p.m., the above-
9 entitled matter was concluded.)

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

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

NEAL R. GROSS

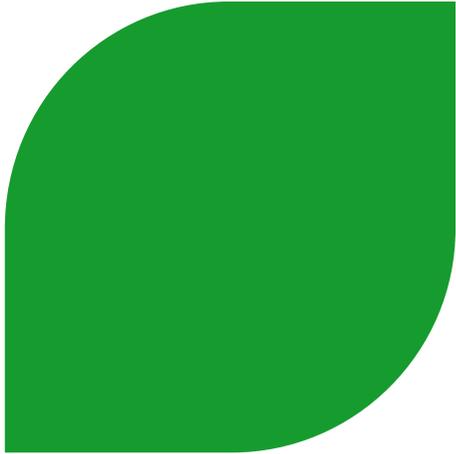
COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

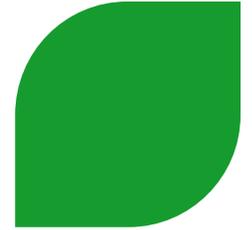


U.S. EPR Chapter 7 Presentation for ACRS

Jeremy Shook, I&C Engineering Discipline Lead



Agenda



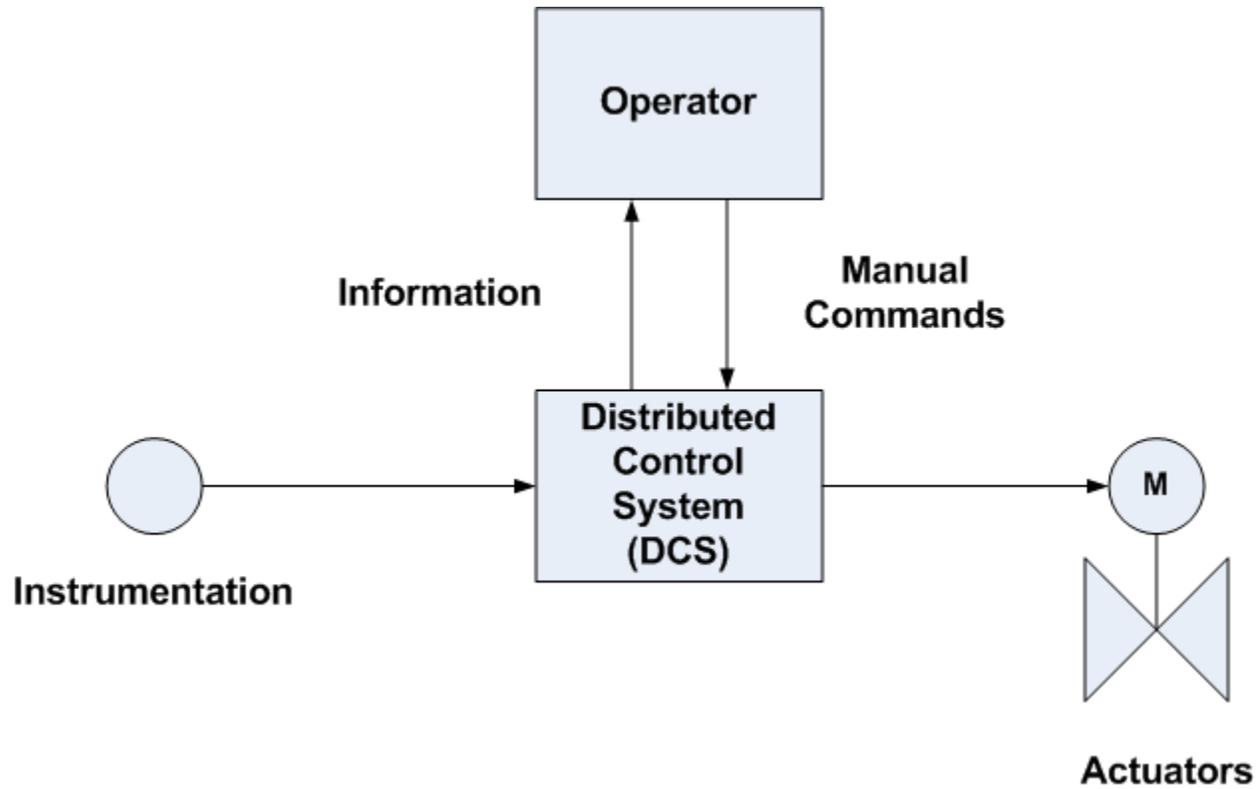
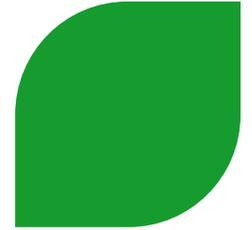
- ▶ **Section 7.1 - Introduction**
- ▶ **Section 7.2 – Reactor Trip System**
- ▶ **Section 7.3 – Engineered Safety Features Systems**
- ▶ **Section 7.4 – Systems Required for Safe Shutdown**
- ▶ **Section 7.5 – Information Systems Important to Safety**
- ▶ **Section 7.6 – Interlock Systems Important to Safety**
- ▶ **Section 7.7 – Control Systems Not Required for Safety**
- ▶ **Section 7.8 – Diverse I&C Systems**



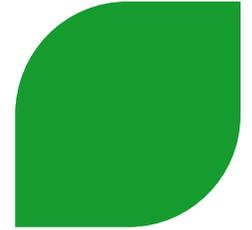
SECTION 7.1: INTRODUCTION



Basic I&C Concept

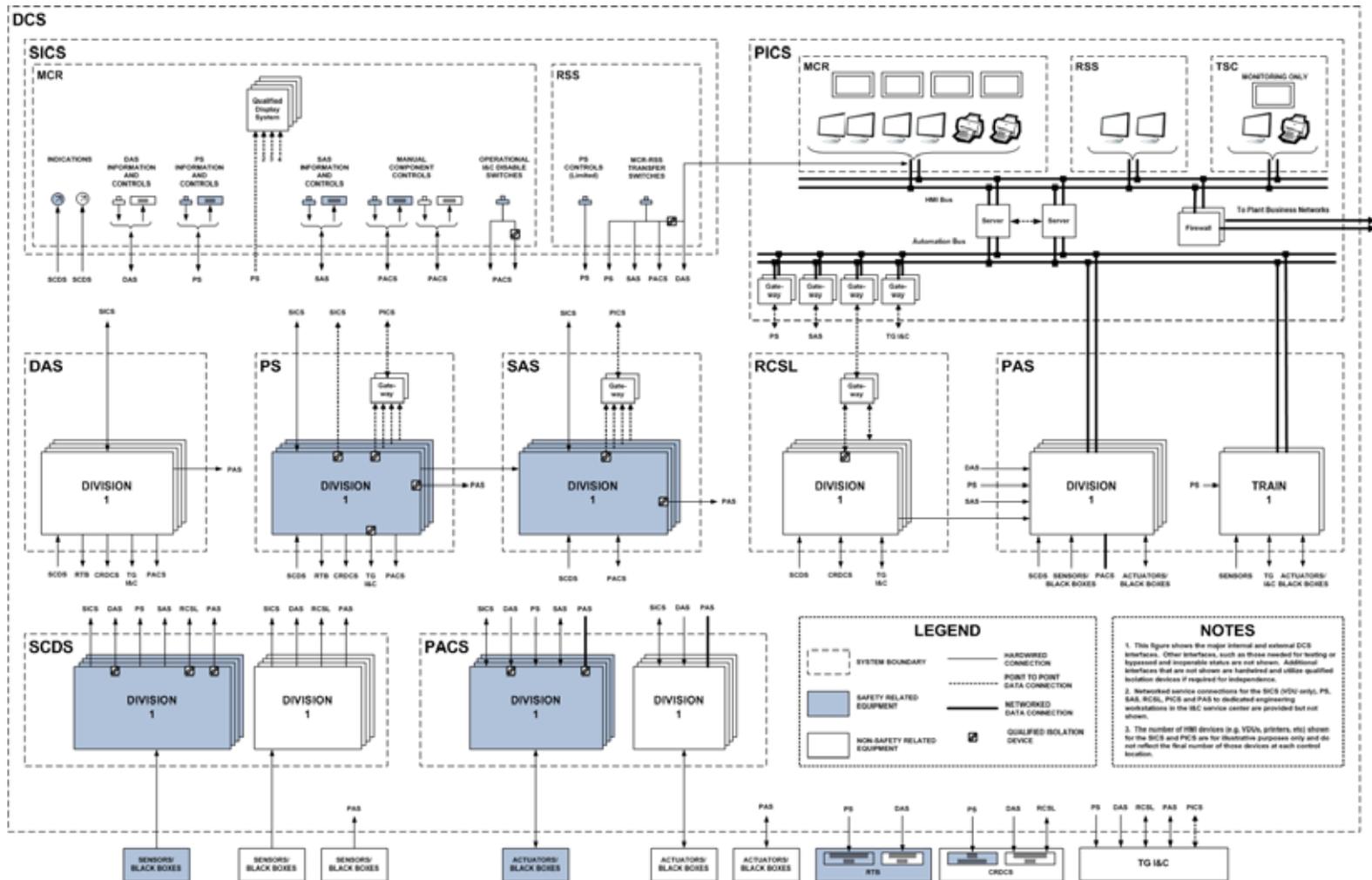


Instrumentation Systems

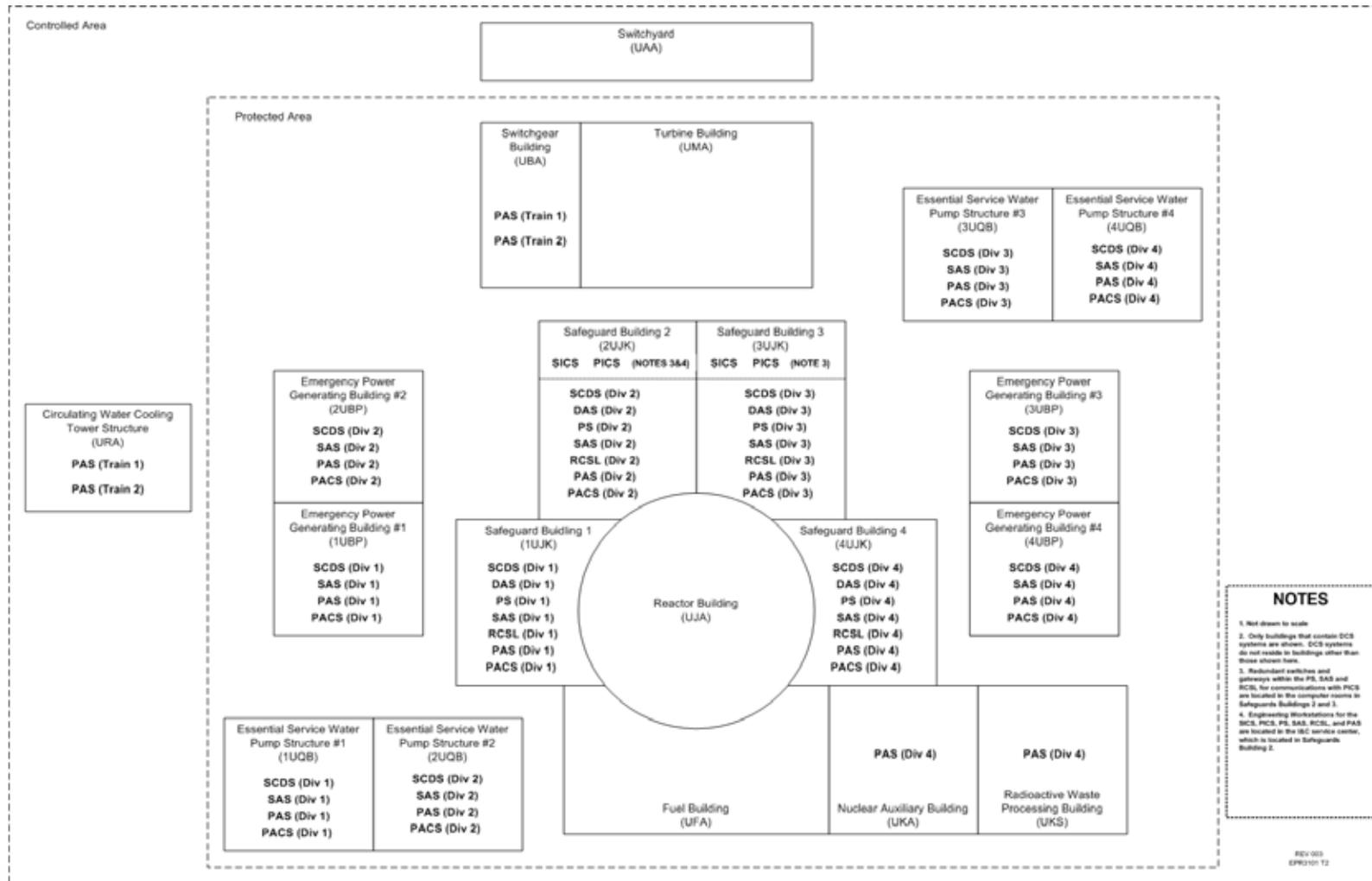


SYSTEM	SYSTEM
Process, HVAC, Electrical Systems	Reactor Pressure Vessel Level Measurement System
Incore Instrumentation System	Seismic Monitoring
Excore Instrumentation System	Loose Parts Monitoring System
Boron Concentration Measurement System	Vibration Monitoring System
Radiation Monitoring System	Fatigue Monitoring System
Hydrogen Monitoring System	Leak Detection System
Rod Position Measurement System	

DCS Functional Architecture



DCS Physical Architecture



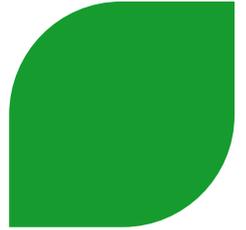
NOTES

- Not shown to scale.
- Only buildings that contain DCS systems are shown. DCS systems do not reside in buildings other than those shown here.
- Redundant switches and gateways within the PS, SAS and RC SL for communications with PICS are located in the computer rooms in Safeguard Buildings 2 and 3.
- Engineering Workstations for the SICS, PICS, PS, SAS, RC SL, and PAS are located in the IEC service center, which is located in Safeguard Building 2.

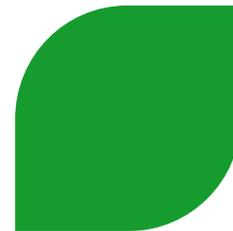
REV 003
EPR10112



Actuator Systems

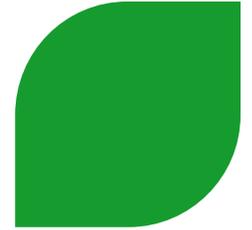


SYSTEM
Process, HVAC, Electrical Systems
Control Rod Drive Control System
Turbine Generator I&C



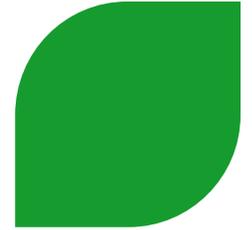
SECTION 7.2: REACTOR TRIP SYSTEM

Topics



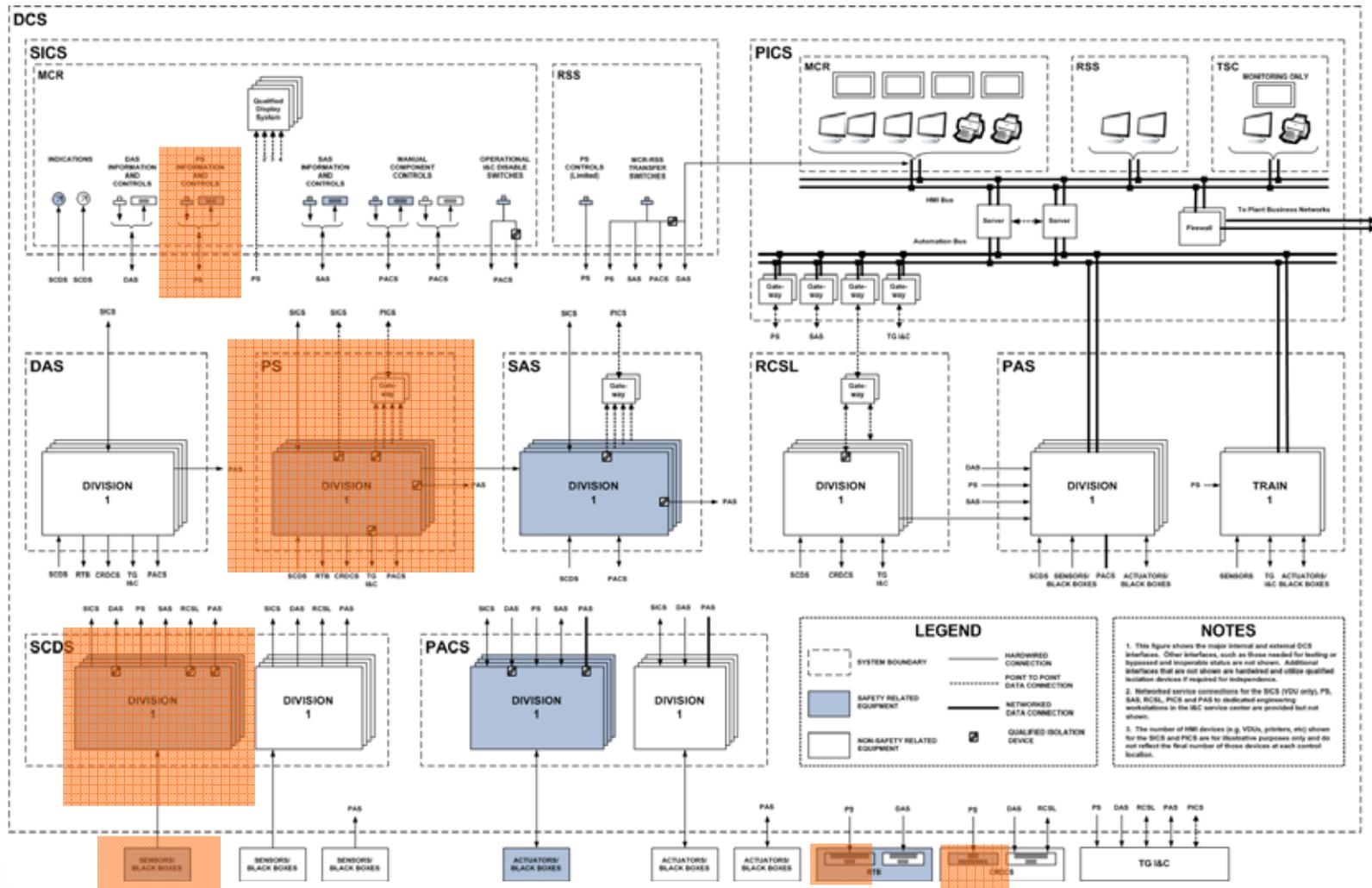
- ▶ **Functions**
- ▶ **Design**
- ▶ **Redundancy**
- ▶ **Independence**
- ▶ **Deterministic Response Time**
- ▶ **Fail-Safe Behavior**
- ▶ **Testing**

Functions

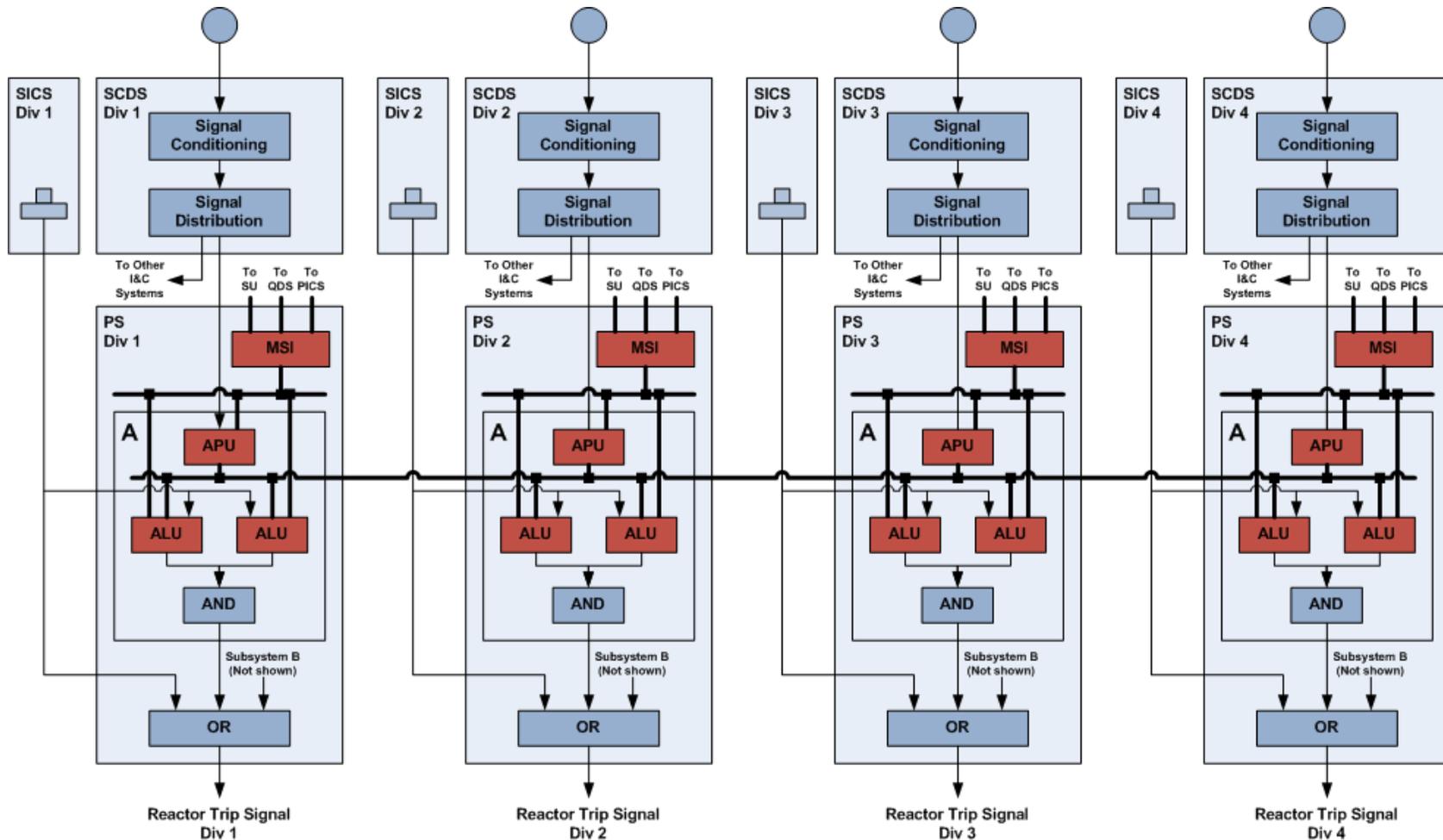
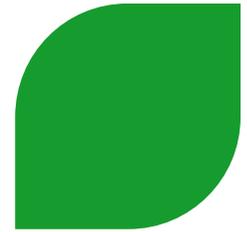


FUNCTION	FUNCTION
Low Departure from Nucleate Boiling Ratio	High Pressurizer Level
High Linear Power Density	Low Hot Leg Pressure
High Neutron Flux Rate of Change	High Steam Generator Pressure Drop
High Core Power Level	Low Steam Generator Pressure
Low Saturation Margin	High Steam Generator Pressure
Low Reactor Coolant System Flow Rate (Two Loops)	Low Steam Generator Level
Low-Low Reactor Coolant System Flow Rate (One Loop)	High Steam Generator Level
Low Reactor Coolant Pump Speed	High Containment Pressure
High Neutron Flux	SIS Actuation
Low Doubling Time	EFWS Actuation
Low Pressurizer Pressure	Manual Actuation
High Pressurizer Pressure	

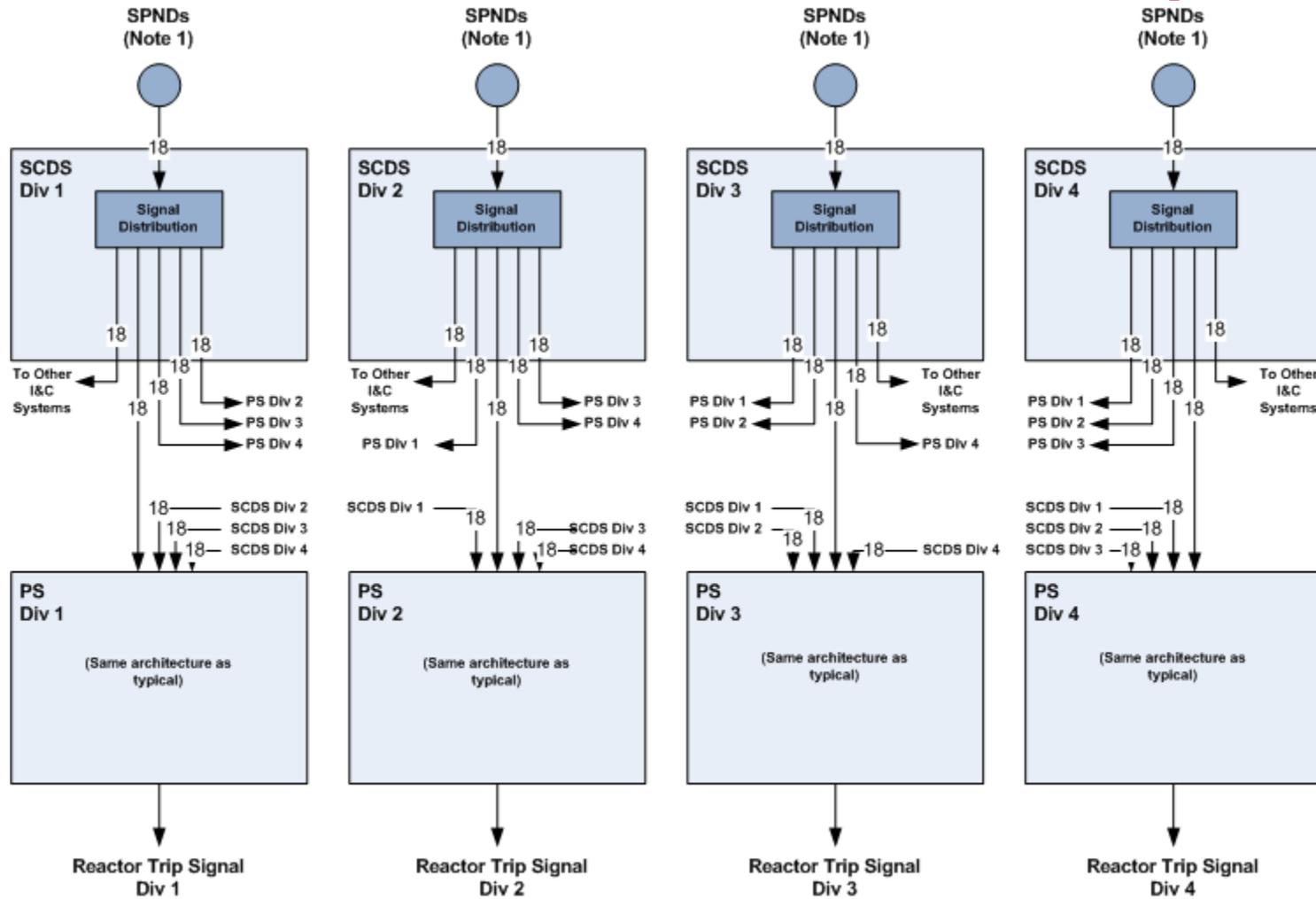
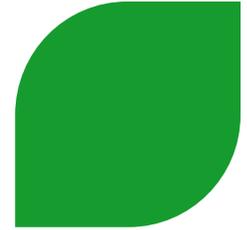
Design: Allocation within DCS



Design: Standard Reactor Trips

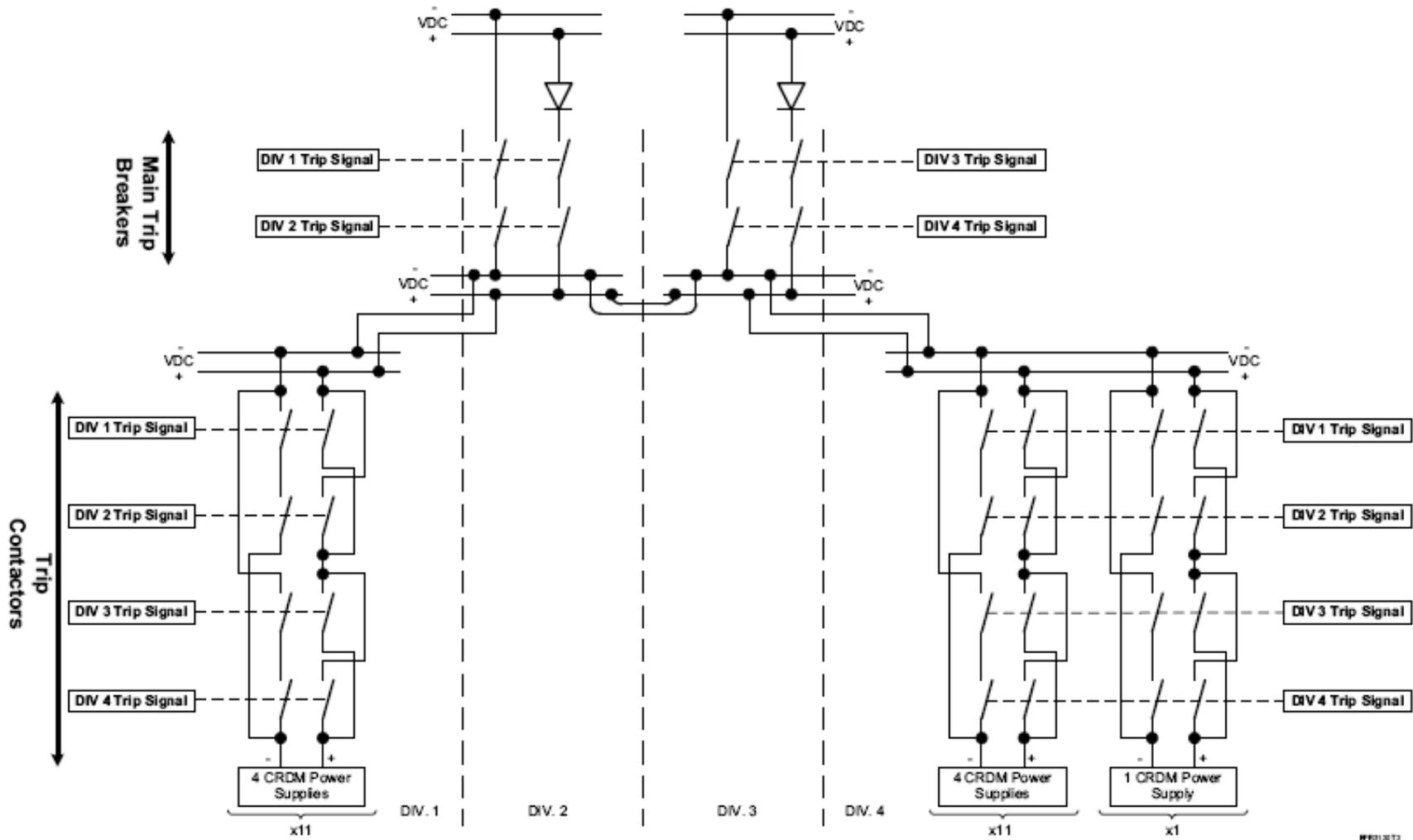
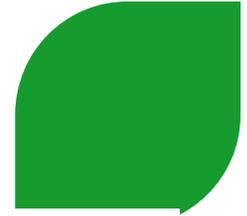


Design: SPND Reactor Trips

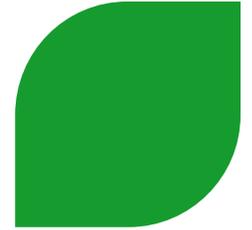


Note 1 – Includes SPNDs and signal conditioning cabinets that are part of the Incore Instrumentation System

Design: Reactor Trip Devices

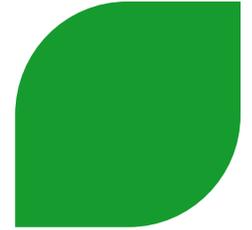


Redundancy: Standard Reactor Trips



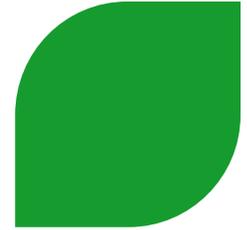
- ▶ **Sensors/signal conditioning/APU (setpoint comparator)**
 - ◆ 4-fold redundant for each process variable
- ▶ **Manual actuation**
 - ◆ 4 reactor trip buttons (1 per I&C division)
- ▶ **ALU (Voting)**
 - ◆ 8-fold redundant
 - 4 divisions => meet single failure
 - 2 ALU per division => improve plant availability
 - ◆ All voting 2/4
- ▶ **Actuation devices**
 - ◆ 4-fold redundant for trip breakers (1/2 taken twice)
 - ◆ 4-fold redundant for trip contactors (2/4)

Redundancy: SPND Based Reactor Trips



- ▶ **Same as standard reactor trips except that all 72 SPND signals needed in all four PS divisions to recreate complete flux distribution**
- ▶ **Benefits of Design**
 - ◆ Provides more direct measurement of neutron flux (Clause 6.4 of IEEE 603)
 - ◆ Removes uncertainties and assumptions with excore based trips
- ▶ **Regulatory Issue**
 - ◆ Does not meet strict interpretation of IEEE 603 Clause 5.6.1 (Independence between redundant divisions)
 - ◆ Alternative request submitted against 10 CFR 50.55 a(h)(3)
- ▶ **Technical Basis for Alternative Request**
 - ◆ Conservative setpoint approach handles single failures in lieu of redundant and independent sensors
 - ◆ Single detectable failure of an SPND result in more conservative setpoint selection by PS
 - ◆ Single non-detectable failure of an SPND to be included within safety analysis
- ▶ **Open Item is tracking re-analysis of Ch 15 events for single non-detectable failure**

Independence: SCDS Output to Other I&C Systems



► Purpose

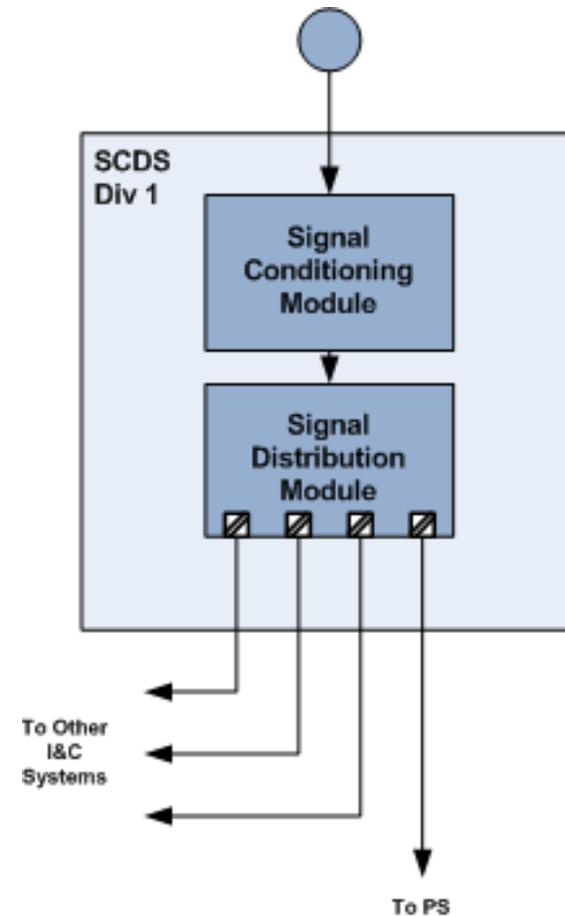
- ◆ Send sensor signals to safety and non-safety systems in the same division for other functions (independence needed for non-safety interface)

► Type

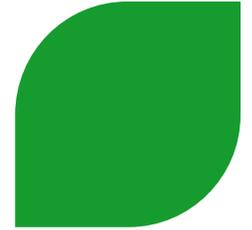
- ◆ Hardwired

► Means of independence

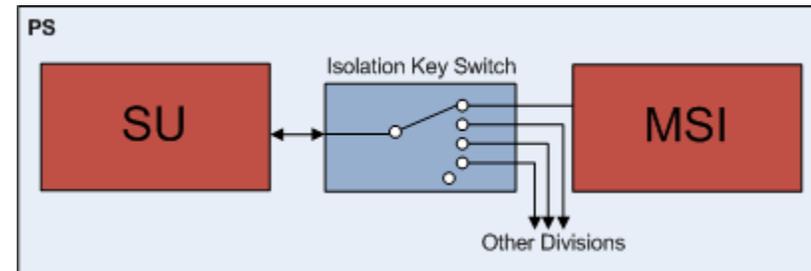
- ◆ Physical separation
 - Non-safety related cabinets are physically separated from SCDS
 - Non-safety cable is separated from safety cable
- ◆ Electrical isolation
 - Signal distribution module has up to four electrically isolated outputs



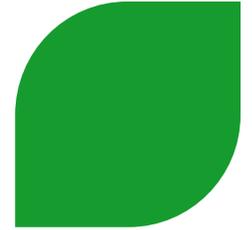
Independence: Service Unit Interface



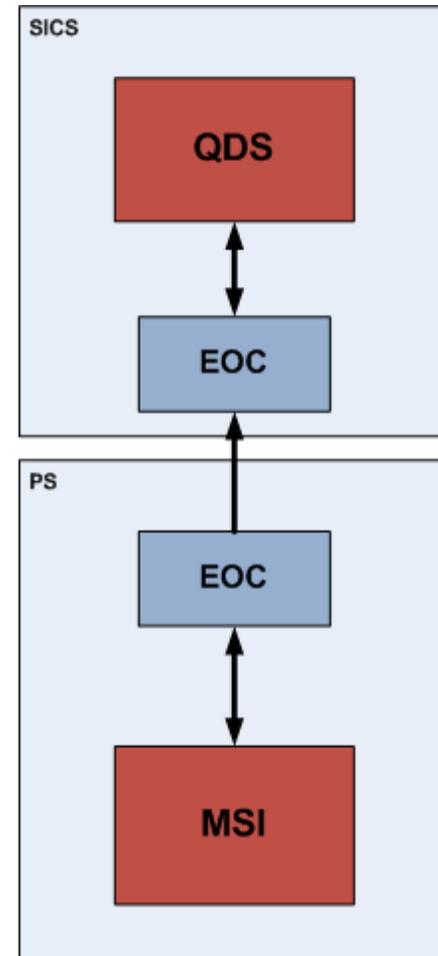
- ▶ **Purpose**
 - ◆ Allow Service Unit to connect to Protection System via MSI for system testing and maintenance
- ▶ **Type**
 - ◆ Data
- ▶ **Means of independence**
 - ◆ Normally disconnected via key locked switch
 - ◆ Not intended to be continuously connected
 - ◆ Switch physically restricts SU to connecting only one division at a time



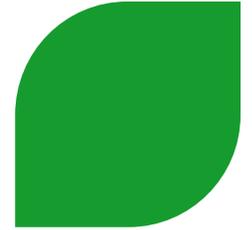
Independence: QDS Interface



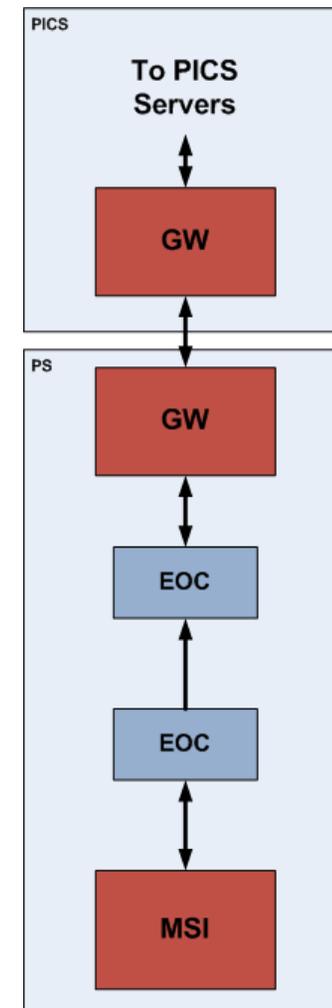
- ▶ **Purpose**
 - ◆ To send information from the PS to the QDS on SICS for the operator
- ▶ **Type**
 - ◆ Data
- ▶ **Means of independence**
 - ◆ **Physical Separation**
 - QDS is physically separated from PS cabinets
 - ◆ **Electrical Isolation**
 - Connection is via fiber optic cable
 - ◆ **Communications independence**
 - Communications path is physically restricted to unidirectional from the PS to the QDS



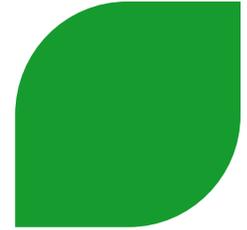
Independence: PICS Interface



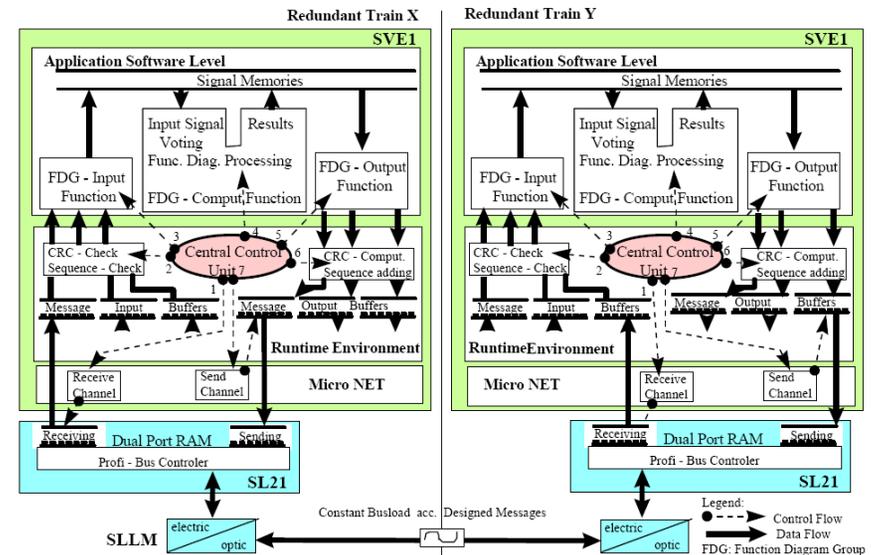
- ▶ **Purpose**
 - ◆ To send information from the PS to the PICS for the operator
- ▶ **Type**
 - ◆ Data
- ▶ **Means of independence**
 - ◆ **Physical Separation**
 - PICS is physically separated from PS cabinets
 - ◆ **Electrical Isolation**
 - Connection is via fiber optic cable
 - ◆ **Communications independence**
 - Communications path is physically restricted to unidirectional from the between the MSI and GW via the EOCs



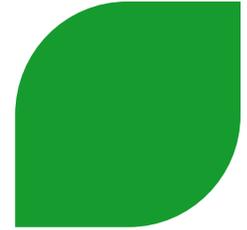
Independence: APU-ALU Interface



- ▶ **Purpose**
 - ◆ To send reactor trip votes from each division APU to all four divisions ALUs for voting
- ▶ **Type**
 - ◆ Data
- ▶ **Means of independence**
 - ◆ **Physical Separation**
 - PS division are physically separated
 - ◆ **Electrical Isolation**
 - Connections are via fiber optic cable
 - ◆ **Communications independence**
 - Separation of safety function and communication processing
 - Separation of send and receive paths
 - Cyclic processing of function processors and communication modules
 - Asynchronous processing of function processors and communication modules
 - Token passing principle



Independence: SPND Outputs from SCDS to PS



▶ Purpose

- ◆ Send 18 SPND signals from one division of SCDS to all four divisions of PS

▶ Type

- ◆ Hardwired

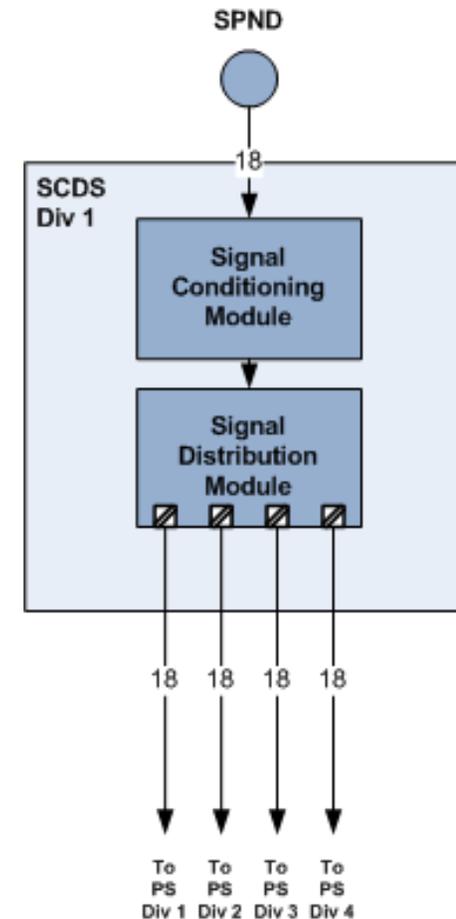
▶ Means of independence

◆ Physical separation

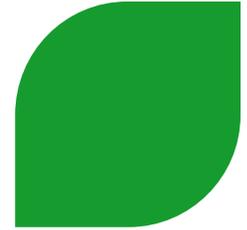
- Divisional SCDS and PS cabinets are physically separated
- Divisional cable is physically separated

◆ Electrical isolation

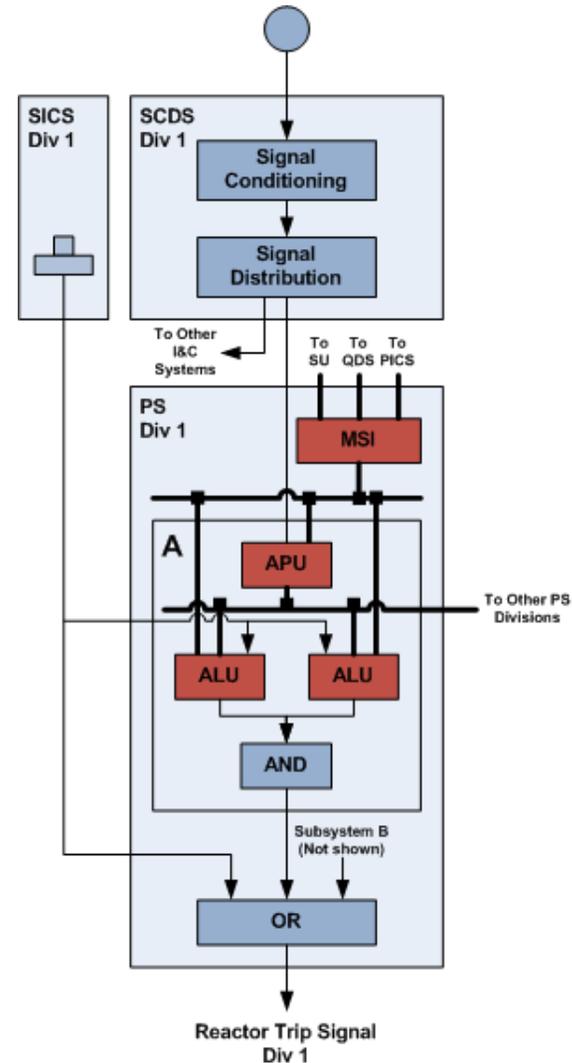
- Signal distribution module has up to four electrically isolated outputs



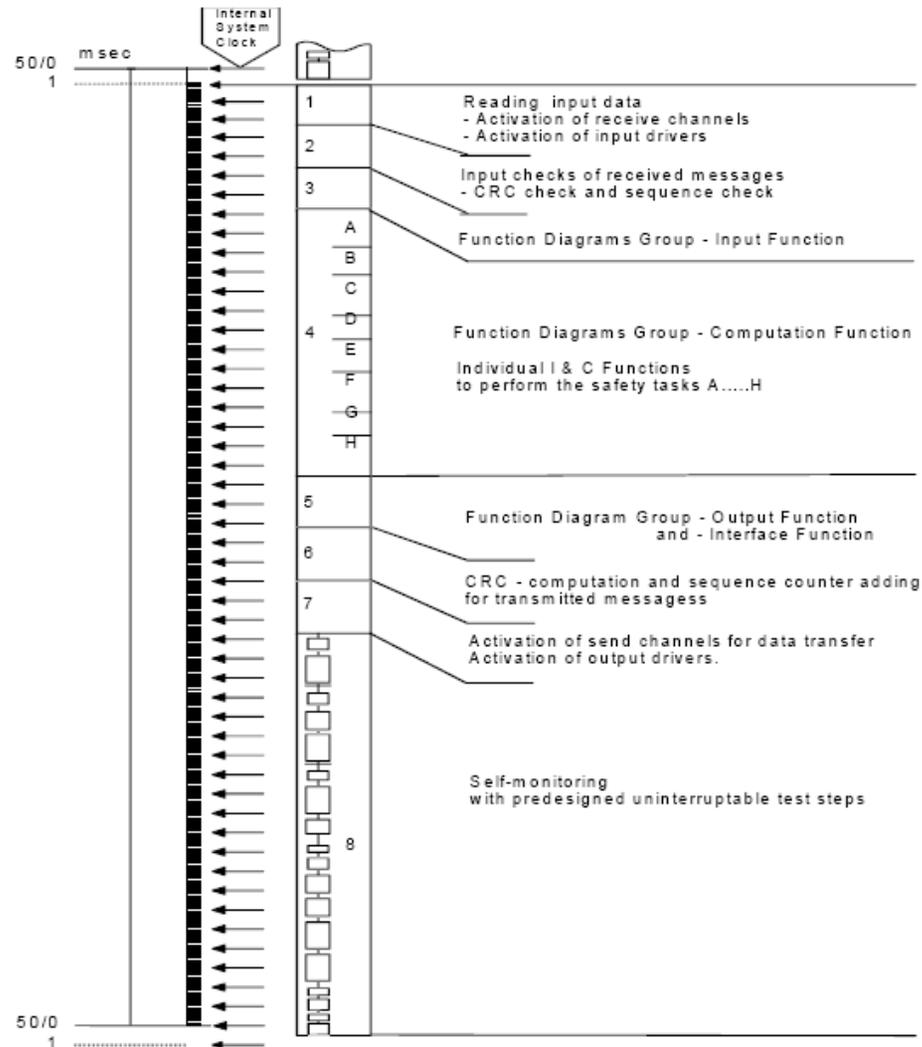
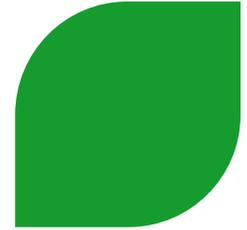
Deterministic Response Time: System Design



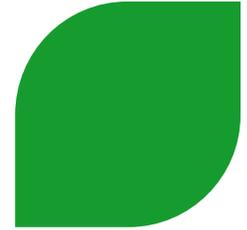
- ▶ **Sensor, signal conditioning and distribution**
 - ◆ Technology provides inherent predictable response time characteristics
- ▶ **APU and ALU**
 - ◆ Application software operates on fixed cycle intervals
 - ◆ System software operation is independent of system inputs
- ▶ **Output Logic Circuits**
 - ◆ Technology provides inherent predictable response time characteristics



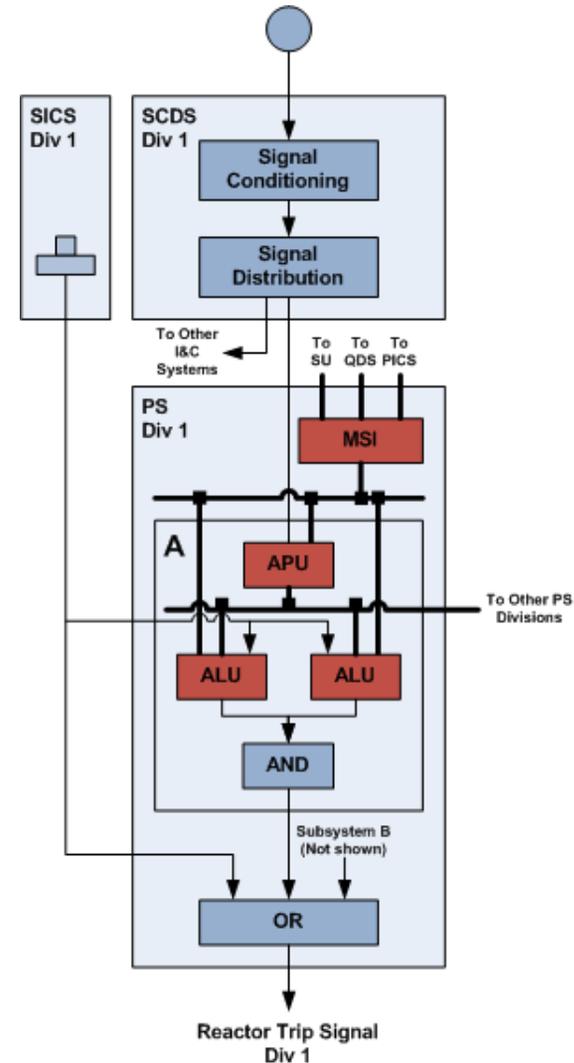
Deterministic Response Time: Cyclic TXS Processor Execution



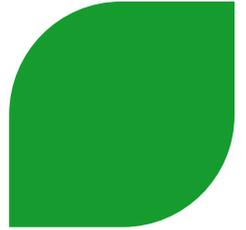
Fail Safe Behaviour: System Design



- ▶ **Sensor, signal conditioning and distribution failures**
 - ◆ **Out of range failure => detected by APU and flag signal, modify voting in ALU**
 - 1 sensor to 2/3 logic
 - 2 sensors to 1/2 logic
 - 3 or more sensors => reactor trip actuated
 - ◆ **In range failure => not detected**
- ▶ **APU failures**
 - ◆ **APU output messages either sent faulted or not sent => modify voting in ALU as above**
- ▶ **ALU failures**
 - ◆ **ALU outputs designed to fail low => reactor trip actuated**
- ▶ **Output logic circuit failures**
 - ◆ **Circuit outputs designed fail low => reactor trip actuated**

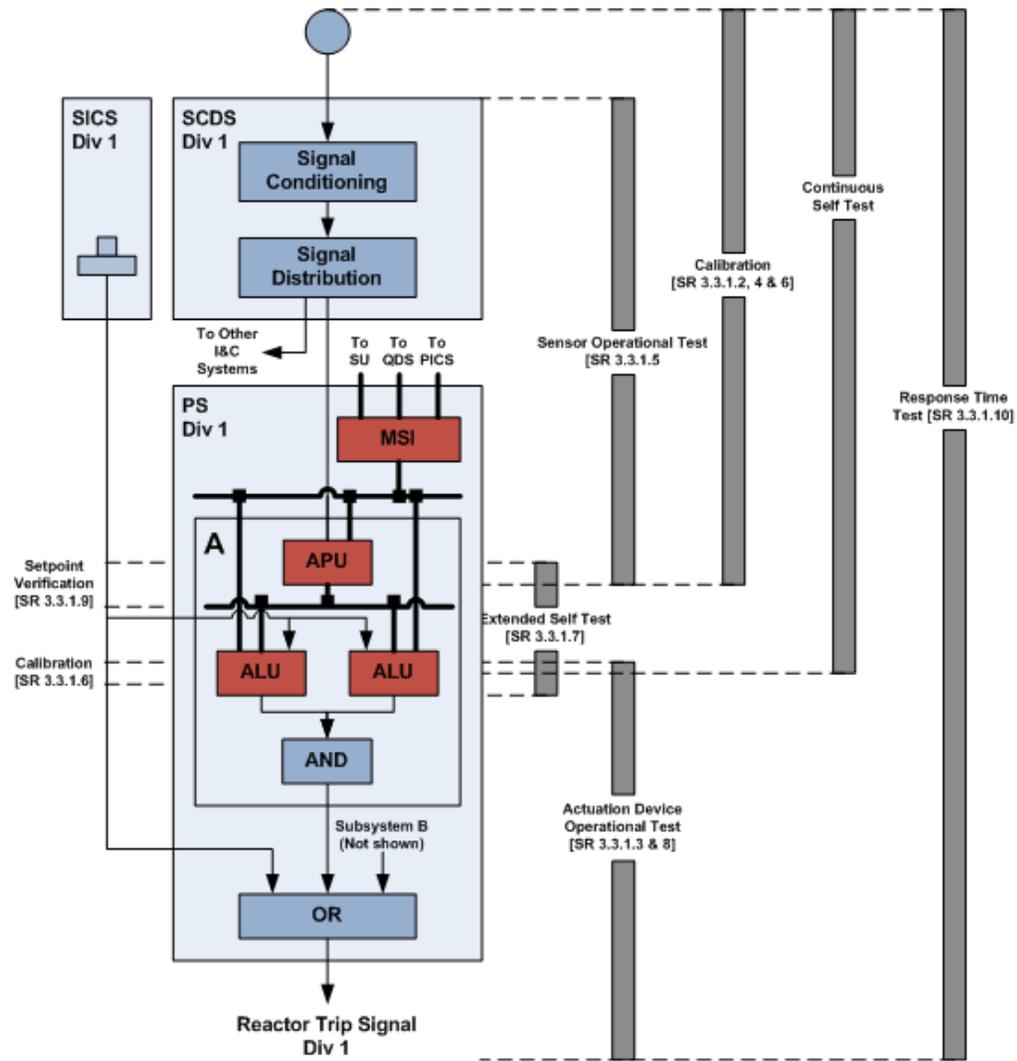


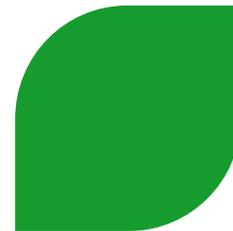
Fail Safe Behaviour: TXS Fault Detection Mechanisms



- ▶ Self-monitoring of the function processors,
- ▶ CRC checksum monitoring of software
- ▶ Hardware based watchdog timer
- ▶ CRC checksum of incoming messages

Testing

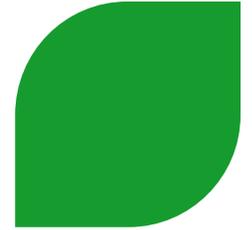




SECTION 7.3: ENGINEERED SAFETY FEATURES SYSTEMS

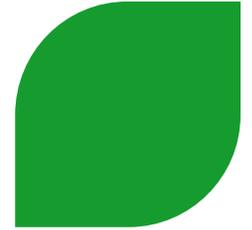


Topics



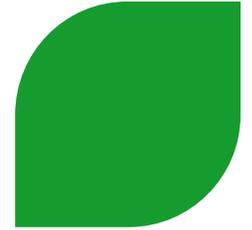
- ▶ **Functions**
- ▶ **Design**
- ▶ **Redundancy**
- ▶ **Independence**
- ▶ **Deterministic Response Time**
- ▶ **Fail-Safe Behavior**
- ▶ **Testing**

Functions: ESF Actuation



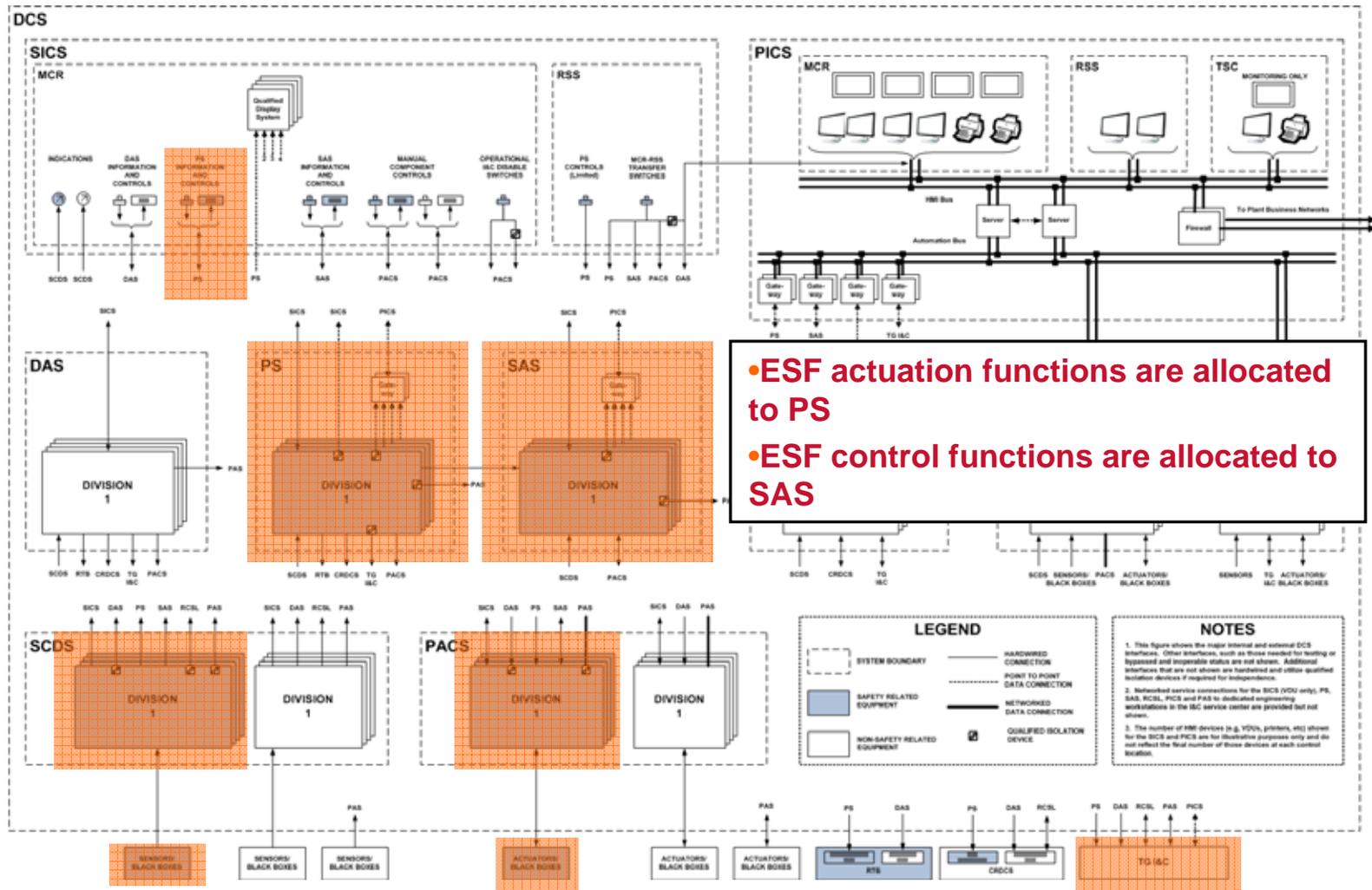
FUNCTION	FUNCTION
Safety Injection System Actuation	Chemical and Volume Control System (CVCS) Charging Isolation
Emergency Feedwater System Actuation	CVCS Isolation for Anti-Dilution
Emergency Feedwater System Isolation	Emergency Diesel Generator (EDG) Actuation
Partial Cooldown Actuation	PSRV Opening (LTOP)
Main Steam Relief Isolation Valve Opening	Steam Generator Isolation
Main Steam Relief Train Isolation	Reactor Coolant Pump Trip
Main Steam Isolation	Main Control Room Air Conditioning System Isolation and Filtering
Main Feedwater Isolation	Turbine Trip
Containment Isolation	Hydrogen Mixing Dampers Opening

Functions: ESF Control

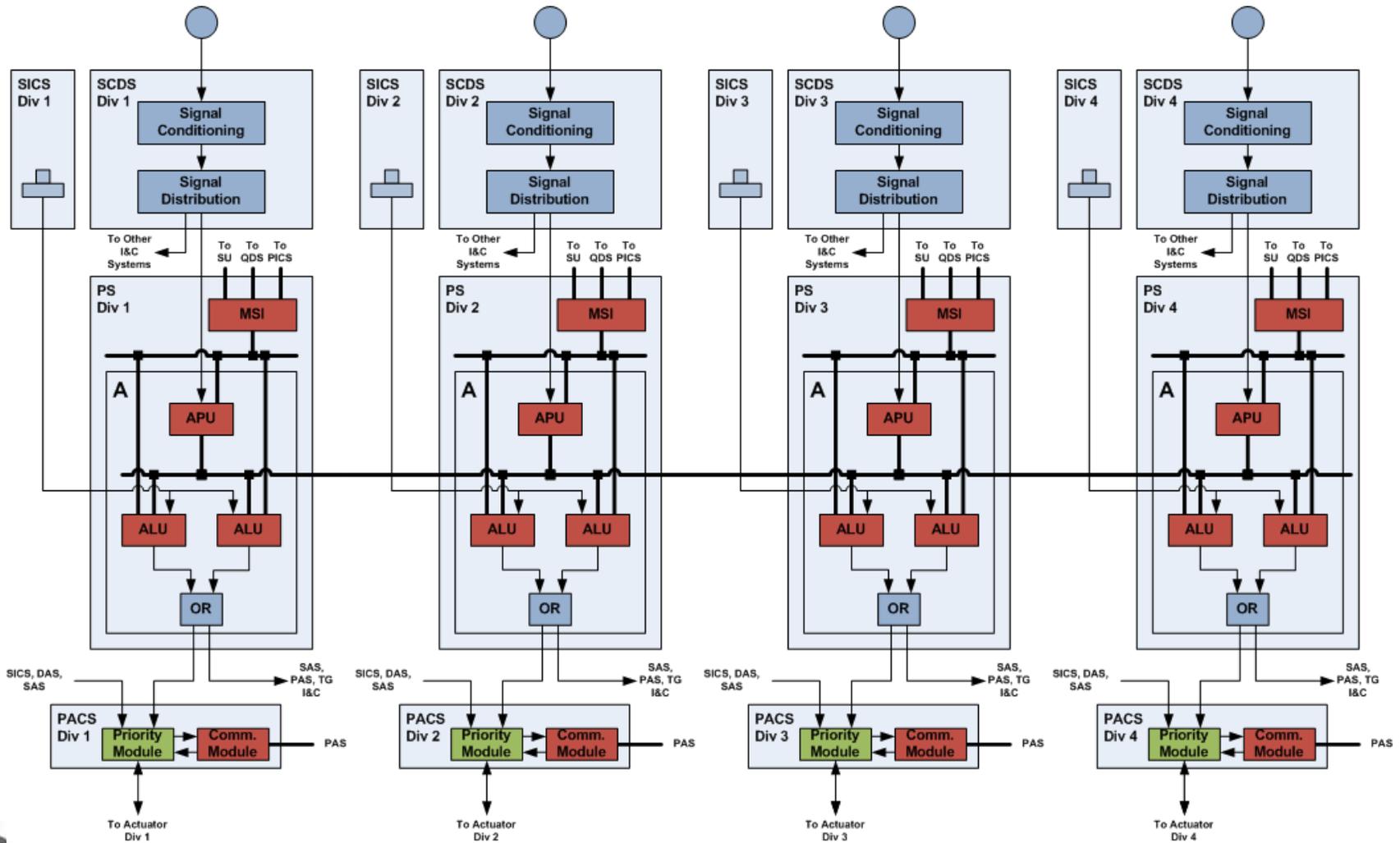
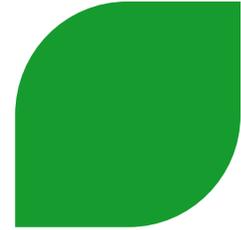


FUNCTION
Emergency Feedwater System: Steam Generator Level Control
Emergency Feedwater System: EFW Pump Flow Protection
Main Steam Relief Control Valve Control

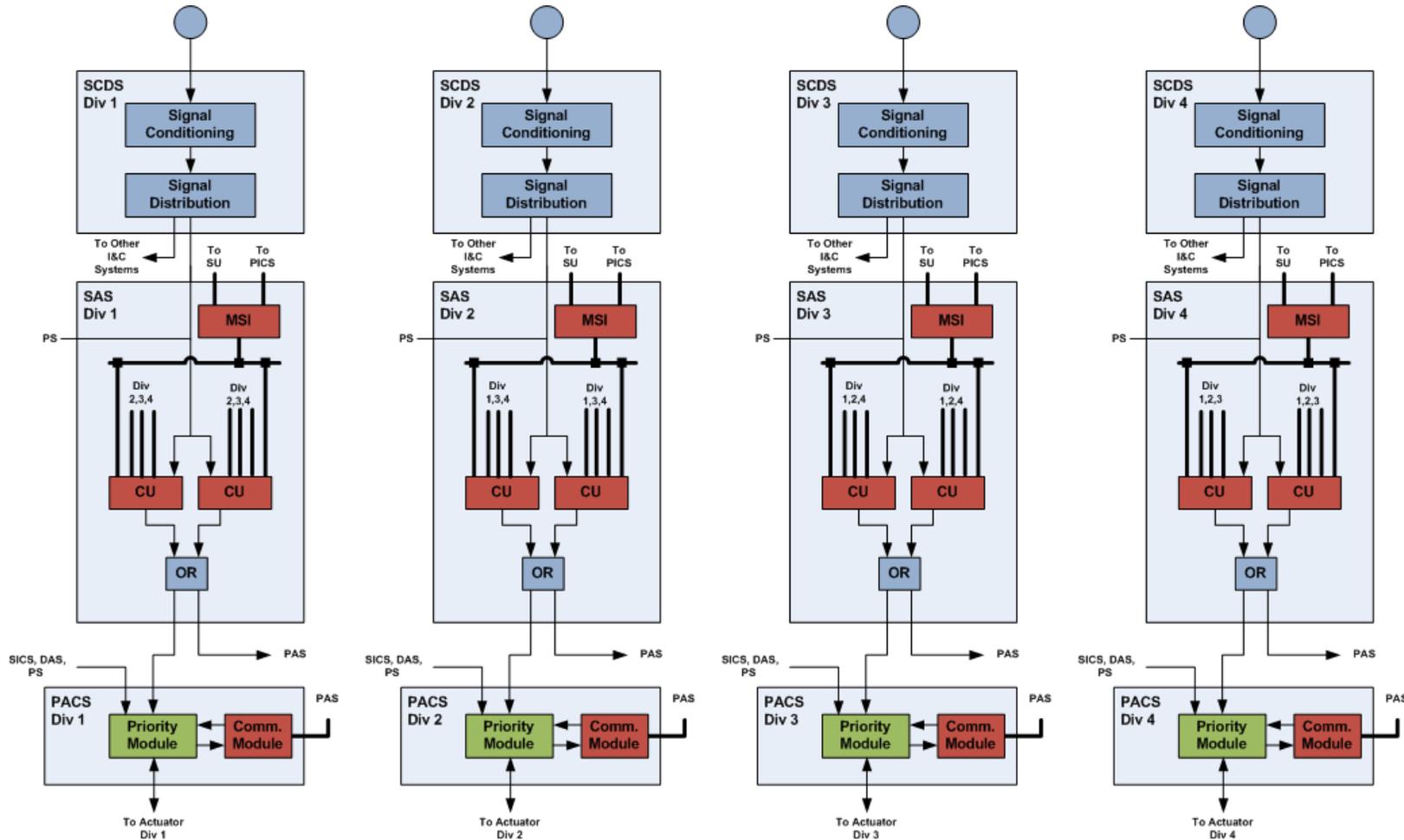
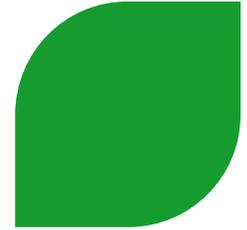
Design: Allocation within the DCS



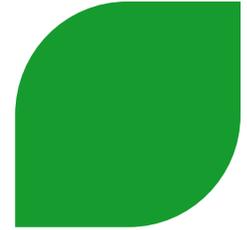
Design: ESF Actuation



Design: ESF Control

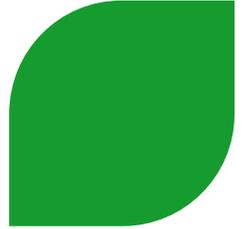


Redundancy: ESF Actuation



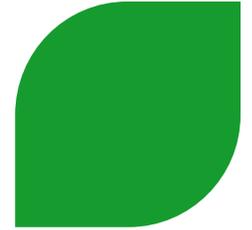
- ▶ **Sensors/signal conditioning/APU (setpoint comparator)**
 - ◆ Most ESF actuations are 4-fold redundant for each process variable
 - ◆ Exceptions:
 - EDG Actuation (3 voltage sensors per division)
 - RCP Trip (2 D/P sensors per division)
- ▶ **Manual actuation**
 - ◆ All Trains
 - 4 switches (2/4 voting) – Safety Injection System Actuation, Partial Cooldown Actuation, Main Steam Isolation, Containment Isolation, Turbine Trip, Hydrogen Mixing Dampers Opening
 - 2 switches (1/2 voting) – Main Control Room Air Conditioning System Isolation and Filtering
 - ◆ Per Train
 - 4 switches (2/4 voting) – Steam Generator Isolation
 - 2 switches (1/2 voting) – Emergency Feedwater System Actuation, Emergency Feedwater System Isolation, Main Steam Relief Isolation Valve Opening, Main Steam Relief Train Isolation, Main Feedwater Isolation, Emergency Diesel Generator Actuation, Reactor Coolant Pump Trip
 - 2 switches (2/2 voting) – PSRV opening
 - 1 switch – CVCS Charging Isolation, CVCS Isolation for Anti-Dilution
- ▶ **ALU (Voting)**
 - ◆ 8-fold redundant
 - 4 divisions => meet single failure
 - 2 ALU per division => improves plant availability
 - ◆ Most voting 2/4
 - ◆ Exceptions
 - EDG actuation (2/3 per division)
 - RCP trip (1/2 per division per pump, 2/4 pumps)
- ▶ **PACS**
 - ◆ 1 set of priority/communication modules per actuator
- ▶ **Actuators**
 - ◆ 4-fold redundant (Majority of ESF functions)
 - ◆ 2-fold redundant (EFW isolation, MSRT actuation, MSRT isolation, MFW isolation, containment isolation, SG isolation, RCP trip, MCR HVAC, CVCS)

Redundancy: ESF Control



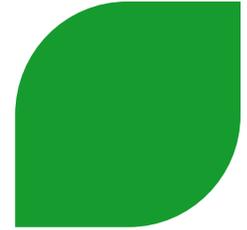
- ▶ **ESF control functions follow redundancy of mechanical trains**
 - ◆ EFW => 4 redundant trains
 - ◆ MSRT => 4 redundant trains
- ▶ **Redundant CU's per SAS division for improved availability**

Independence: Common Features with Reactor Trip



- ▶ **SCDS Output to Other I&C Systems**
- ▶ **Service Unit Interface**
- ▶ **QDS Interface**
- ▶ **PICS Interface**
- ▶ **APU-ALU Interface**

Independence: PS to PAS Signals



► Purpose

- ◆ Send signals from PS to PAS for coordination of logic for actuators

► Type

- ◆ Hardwired

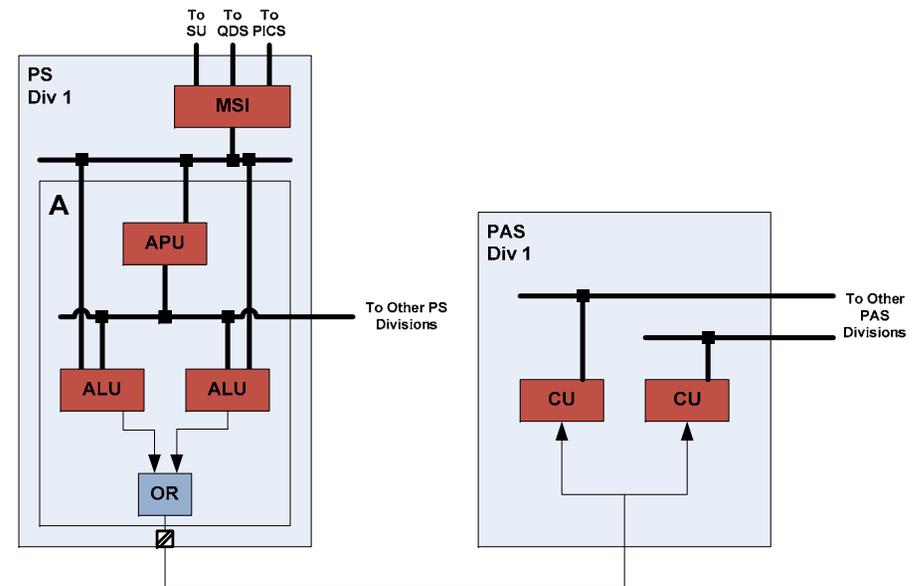
► Means of independence

◆ Physical Separation

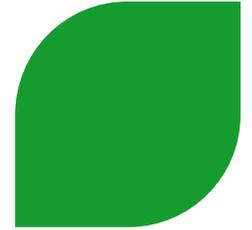
- PS and PAS are physically separated

◆ Electrical Isolation

- Connections are electrically isolated within PS



Independence: CU-CU Interdivisional Communication



▶ Purpose

- ◆ To send signals for voting (MSRT isolation valve position)

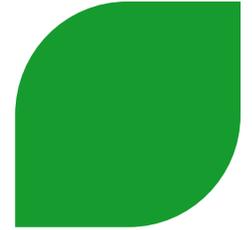
▶ Type

- ◆ Data

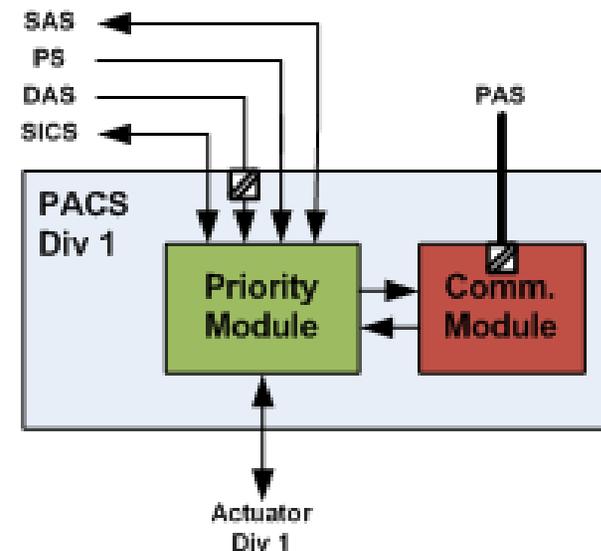
▶ Means of independence

- ◆ Same as APU-ALU

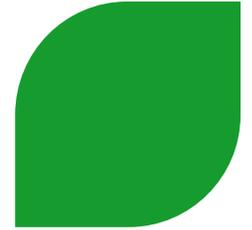
Independence: PACS



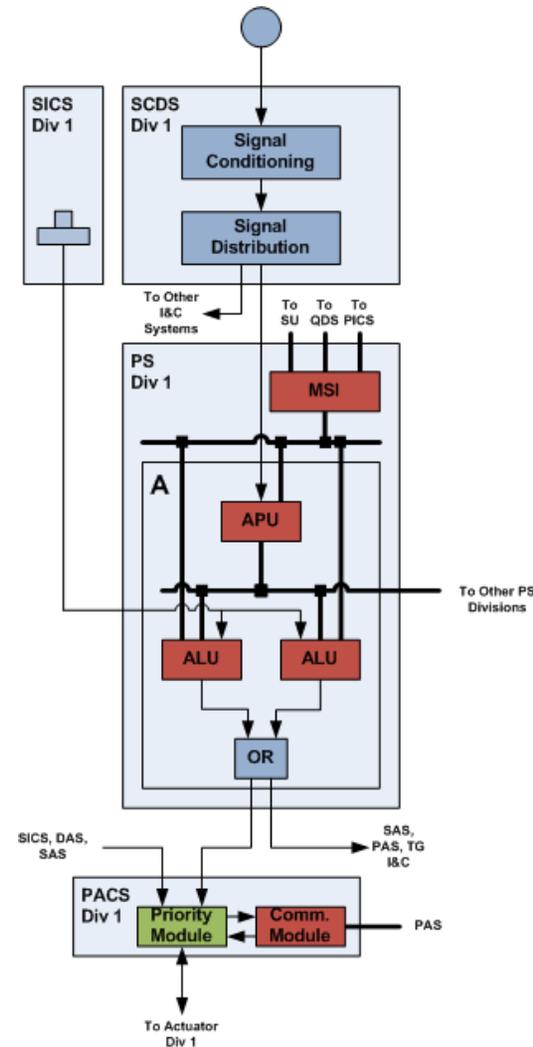
- ▶ **Purpose**
 - ◆ To send non-safety signals to PACS
- ▶ **Type**
 - ◆ Hardwired
 - ◆ Data
- ▶ **Means of independence**
 - ◆ **Physical Separation**
 - Non-safety systems and PACS cabinets are physically separated
 - Physical separation of safety and non-safety cable
 - ◆ **Electrical Isolation**
 - Hardwired connections are electrically isolated
 - Data connections are via fiber optic cable
 - Communication module qualified as an associated circuit
 - ◆ **Communications independence**
 - Separation of communications module and priority module by hardwired signals



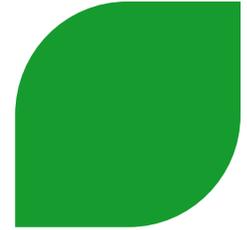
Deterministic Response Time



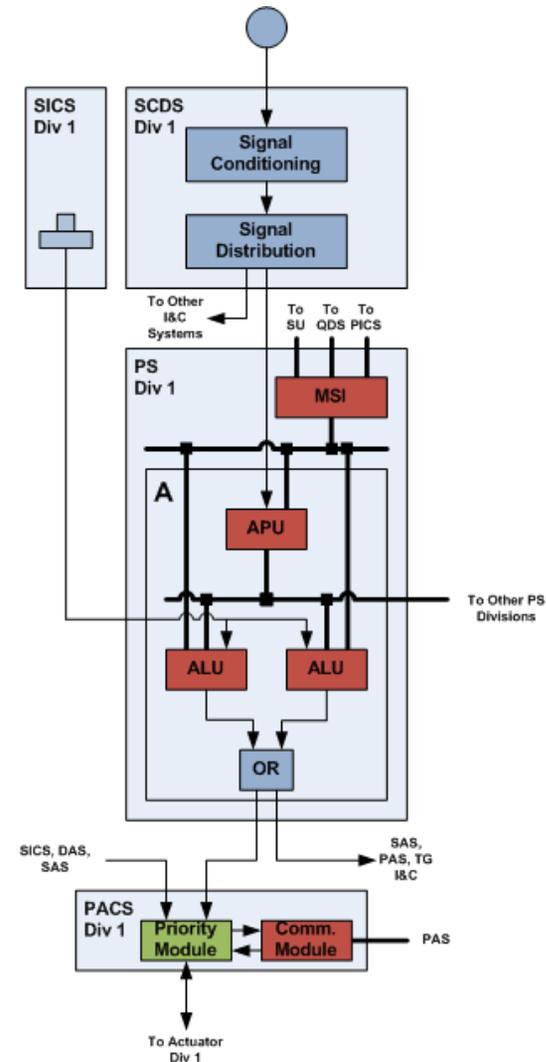
- ▶ **Sensor, signal conditioning and distribution**
 - ◆ Same as reactor trip
- ▶ **APU and ALU**
 - ◆ Same as reactor trip
- ▶ **Output Logic Circuits**
 - ◆ Same as reactor trip
- ▶ **PACS**
 - ◆ Technology provides inherent predictable response time characteristics



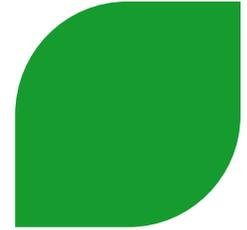
Fail Safe Behaviour: ESF Actuation



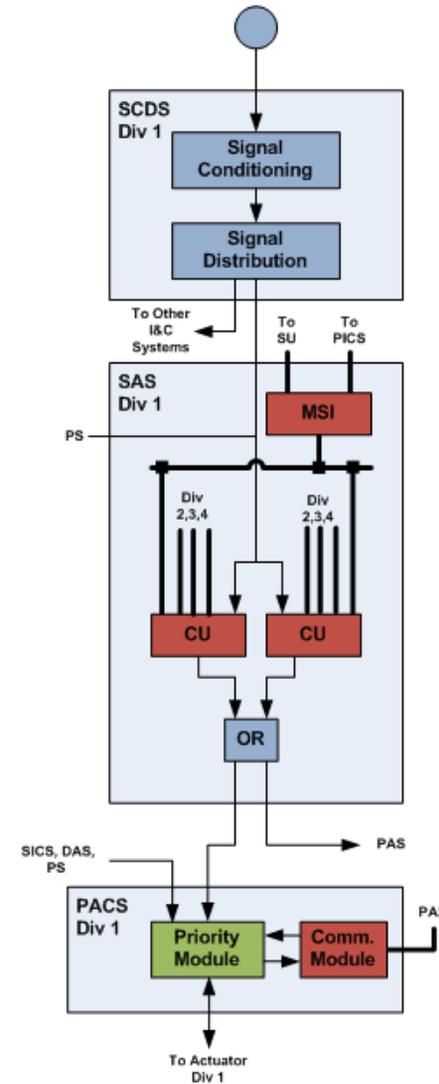
- ▶ **Sensor, signal conditioning and distribution failures**
 - ◆ **Out of range failure => detected by APU and flag signal, modify voting in ALU**
 - Modify towards no actuation (most functions)
 - 1 sensor to 2/3 logic
 - 2 sensors to 2/2 logic
 - 3 or more sensors => ESF not actuated
 - Modify towards actuation (MCR HVAC realignment and H2 mixing damper actuation)
 - 1 sensor to 2/3 logic
 - 2 sensors to 1/2 logic
 - 3 or more sensors => ESF actuated
 - ◆ **In range failure => not detected**
- ▶ **APU failures**
 - ◆ **APU output messages either sent faulted or not sent => modify voting in ALU as above**
- ▶ **ALU failures**
 - ◆ **ALU outputs designed to fail low => no ESF actuation**
- ▶ **Output logic circuit failures**
 - ◆ **Circuit outputs designed to fail low => no ESF actuation**
- ▶ **PACS failures**
 - ◆ **PACS outputs design to fail low => no ESF actuation**



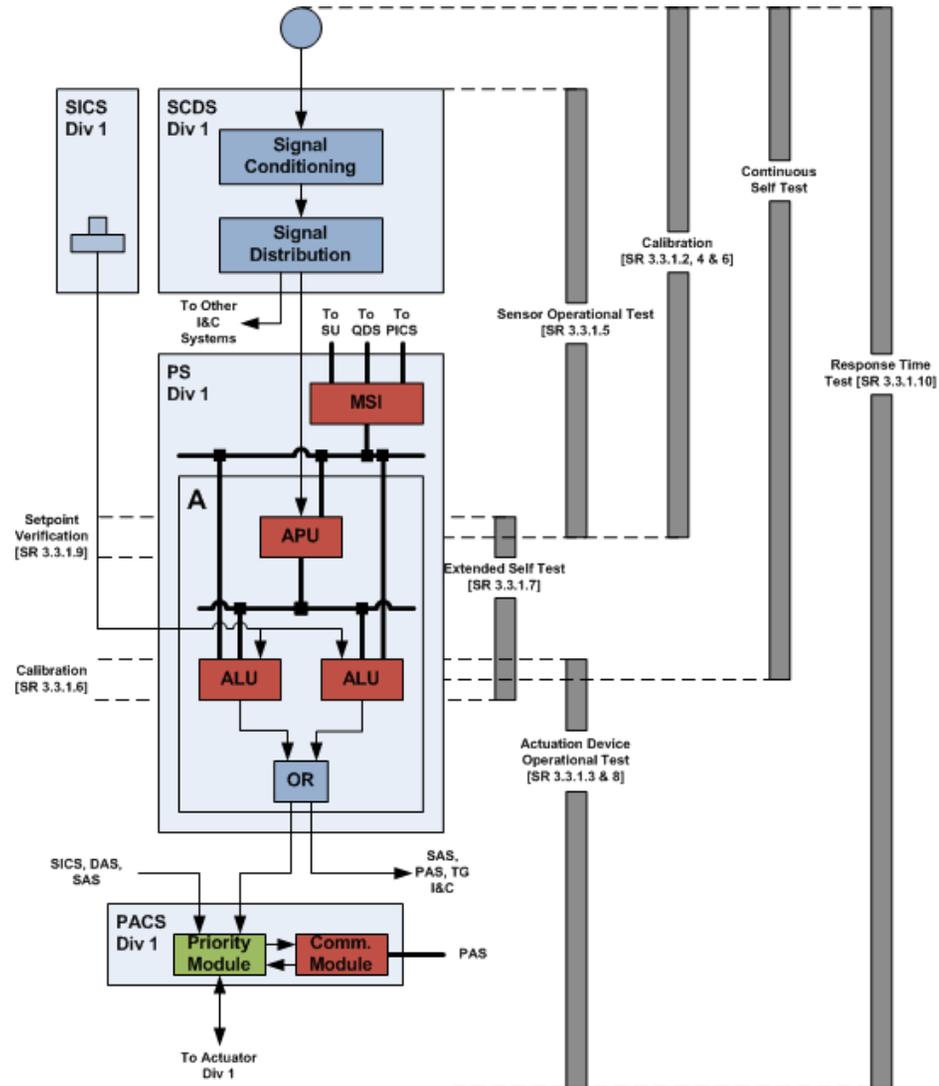
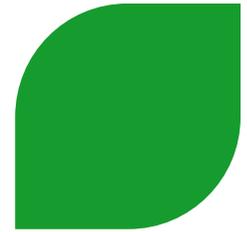
Fail Safe Behaviour: ESF Control



- ▶ **Sensor, signal conditioning and distribution failures**
 - ◆ Out of range failure => detected by CU and flag signal, outputs of PI controller failed low => actuators fail as-is
 - ◆ In range failure => not detected
- ▶ **CU failures**
 - ◆ CU operate in master/hot-standby configuration => failure of master is detected by hot-standby and switched over => no loss in functionality
- ▶ **Output logic circuit failures**
 - ◆ Circuit outputs designed to fail low => actuators fail as-is
- ▶ **PACS failures**
 - ◆ PACS outputs design to fail low => actuators fail as is



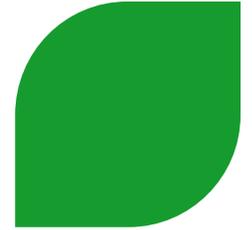
Testing





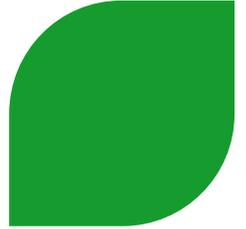
SECTION 7.4 : SYSTEMS REQUIRED FOR SAFE SHUTDOWN

Topics



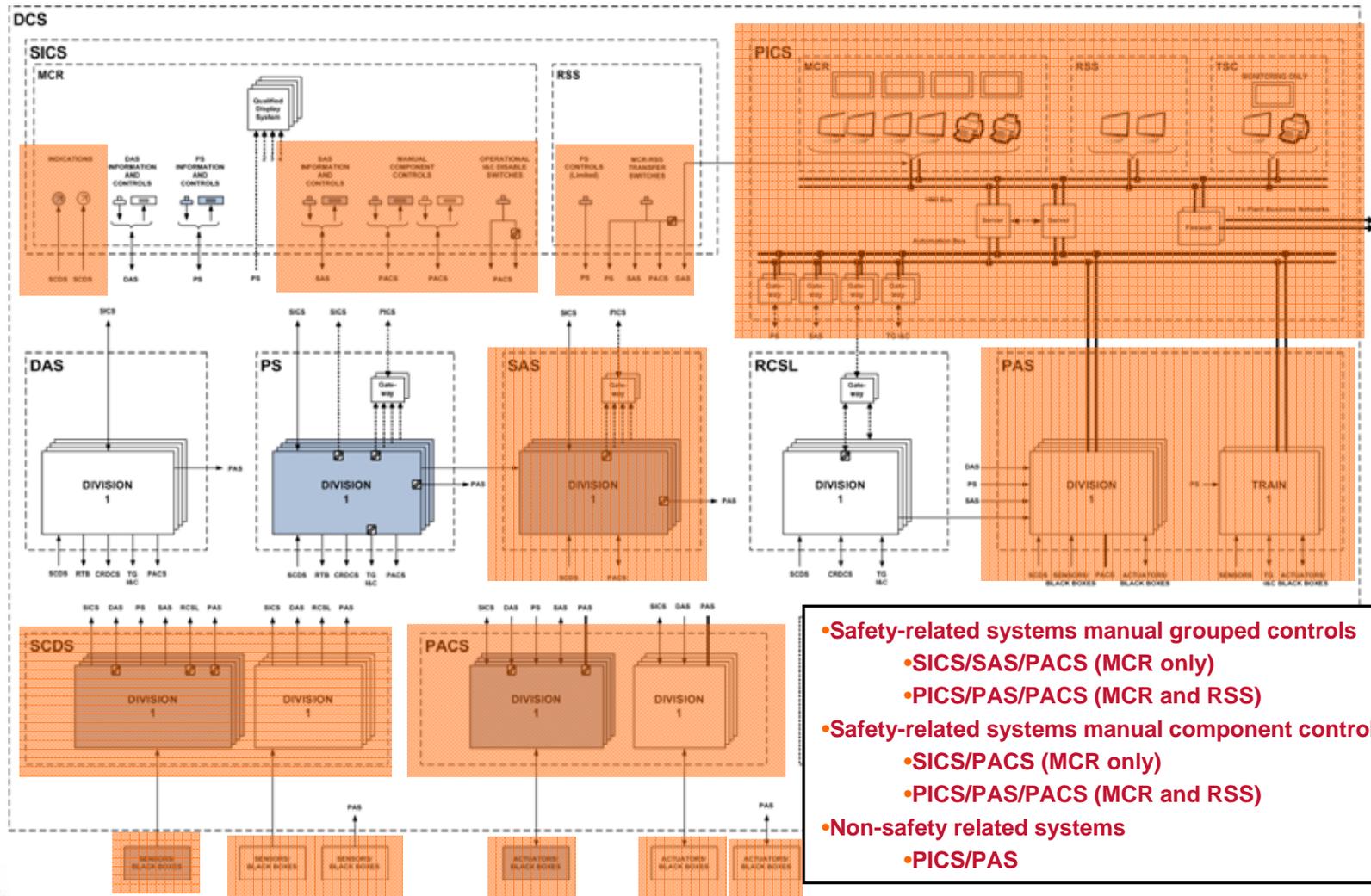
- ▶ **Safe Shutdown Basis**
- ▶ **Design**
- ▶ **MCR to RSS Transfer**

Safe Shutdown Basis



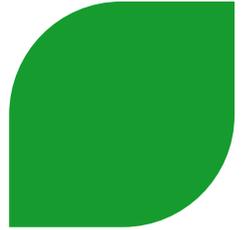
- ▶ **Following events are specifically analyzed for safe shutdown:**
 - ◆ **Accidents (Chapter 15)**
 - ◆ **Fires (include loss of MCR) (Chapter 9)**
 - ◆ **SBO (Chapter 8)**
- ▶ **Both safety related and non-safety related plant systems are credited to reach and maintain safe shutdown, depending on the event**

Design



- Safety-related systems manual grouped controls
 - SICS/SAS/PACS (MCR only)
 - PICS/PAS/PACS (MCR and RSS)
- Safety-related systems manual component controls
 - SICS/PACS (MCR only)
 - PICS/PAS/PACS (MCR and RSS)
- Non-safety related systems
 - PICS/PAS

MCR to RSS Transfer

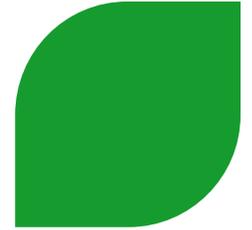


- ▶ **Activate MCR to RSS transfer switches**
 - ◆ Disables MCR inputs to PS, SAS and PACS
 - ◆ Disables DAS outputs
 - ◆ Disables signals from PICS workstations in MCR
- ▶ **Log in to PICS workstations in RSS**
- ▶ **Operator uses PICS for most actions, with some controls only available on SICS**
- ▶ **RSS independence from MCR**
 - ◆ Redundant PICS servers are physically separated (1 in Safeguard Building 2, 1 in Safeguard Building 3)
 - ◆ PICS data connections made with fiber optic cable
 - ◆ SICS cables from RSS are physically separated from MCR cabling



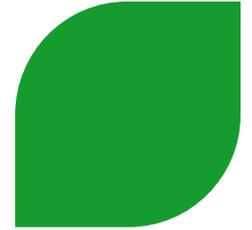
SECTION 7.5: INFORMATION SYSTEMS IMPORTANT TO SAFETY

Topics



- ▶ **Alarms**
- ▶ **Post-Accident Monitoring (PAM)**
- ▶ **Safety Parameter Display System (SPDS)**
- ▶ **Emergency Response Data System (ERDS)**
- ▶ **Technical Support Center (TSC)**
- ▶ **Bypassed and Inoperable Status Indication (BISI)**

Alarms



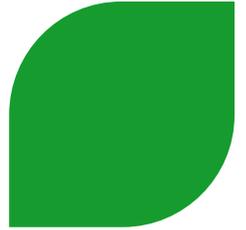
▶ Inventory

- ◆ Determined via task analysis (Chapter 18)

▶ Design

- ◆ Alarms are processed by automation systems (DAS, PS, SAS, RCSL and PAS)
- ◆ Alarms are displayed as follows
 - PICS => all alarms
 - SICS => limited number of hardwired alarms as determined for accident mitigation and safe shutdown

Post Accident Monitoring (PAM)



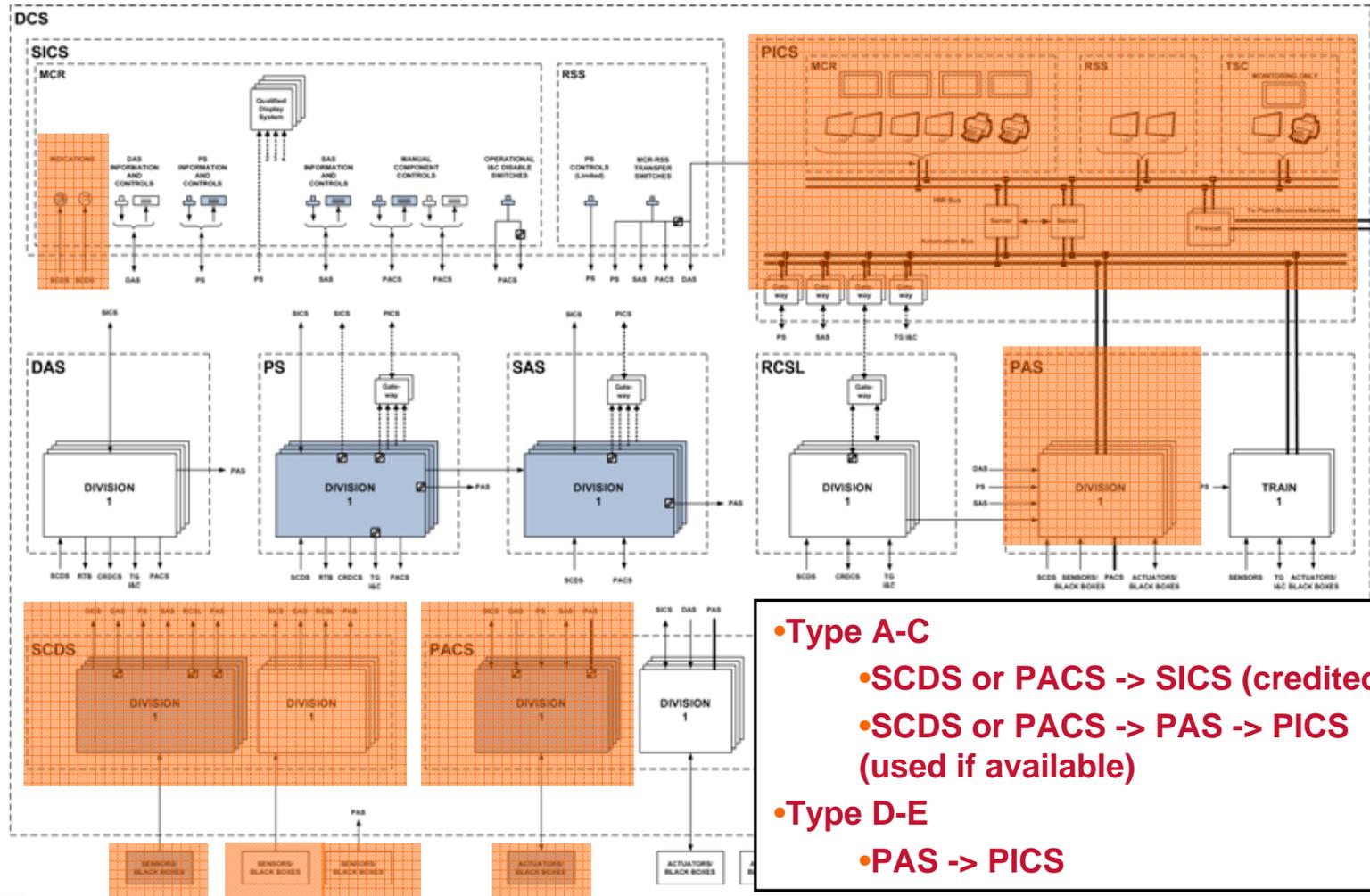
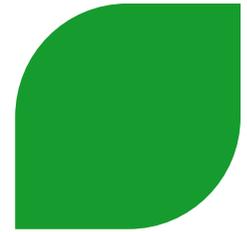
▶ List of Variables

- ◆ Shown in Table 7.5-1

▶ Method of Development

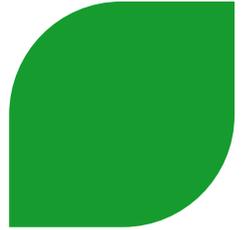
- ◆ Evaluation of B&W owners group emergency operating procedures technical basis document (symptom based approach)
- ◆ Evaluation of differences between B&W design plants and EPR
- ◆ Evaluation of credited operator actions in Chapter 15
- ◆ Evaluation of critical safety functions and fission product barriers (per IEEE 497-2002)

PAM: Allocation within the DCS



- Type A-C
 - SCDS or PACS -> SICS (credited)
 - SCDS or PACS -> PAS -> PICS (used if available)
- Type D-E
 - PAS -> PICS

SPDS/ERDS/TSC/BISI

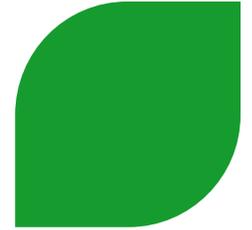


- ▶ **Safety Parameter Display System (SPDS)**
 - ◆ **Functionality incorporated into PICS and SICS (QDS)**
- ▶ **Emergency Response Data System (ERDS)**
 - ◆ **The PICS provides information from the DCS to external plant networks via a unidirectional firewall, which can be transferred to the NRC for emergency response**
- ▶ **Technical Support Center (TSC)**
 - ◆ **The TSC contains view-only PICS workstations and plant overview screens to assist in emergency response**
- ▶ **Bypassed and Inoperable Status Indication (BISI)**
 - ◆ **The safety related I&C systems provide indication of their status to the PICS to meet BISI requirements**



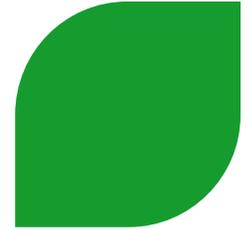
SECTION 7.6: INTERLOCK SYSTEMS IMPORTANT TO SAFETY

Topics



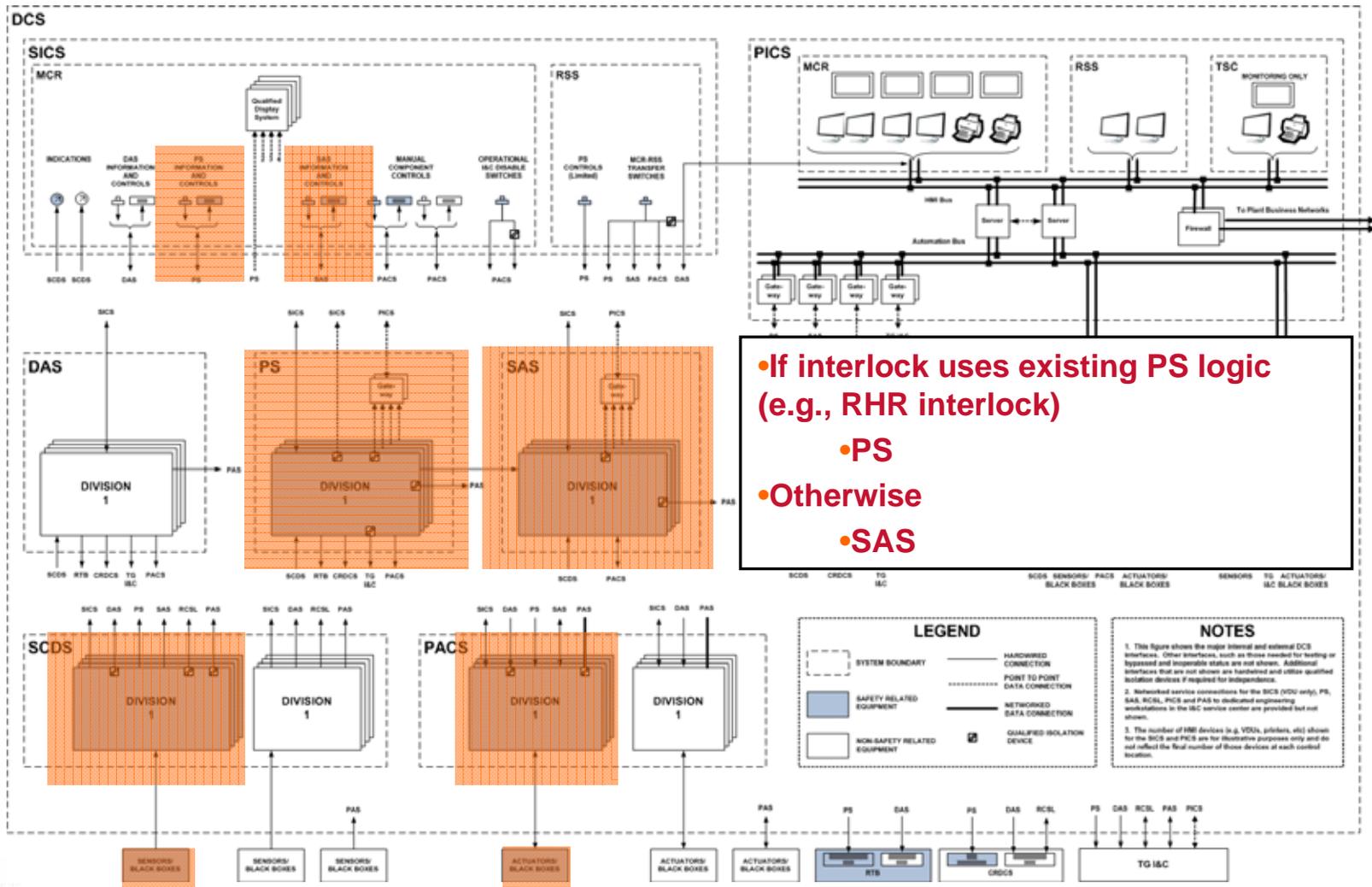
- ▶ **Functions**
- ▶ **Design**

Functions

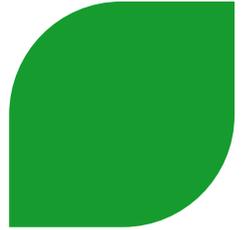


FUNCTION
RHR Suction Valve Interlocks
Safety Injection Accumulator Interlocks
Interlocks Isolating Redundant CCWS Trains
Interlocks to Provide Low Temperature Over-Pressure Protection

Design: Allocation within the DCS



Design: Aspects of Interlock Functions



▶ Interdivisional communications

- ◆ Voting => reduce probability of spurious actuation
- ◆ Cross-train function (e.g., CCWS cross connect interlock) => necessary for performance of the safety functions

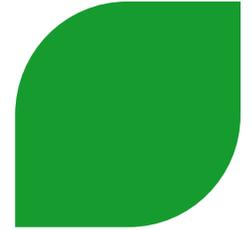
▶ Independence

- ◆ Utilize features already described for reactor trip and ESF



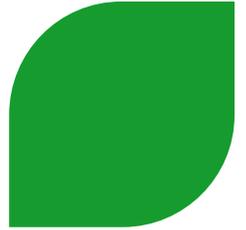
SECTION 7.7: CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

Topics



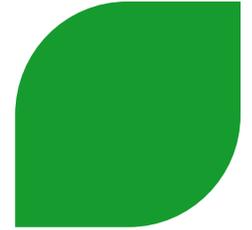
- ▶ **Functions**
- ▶ **Design**
- ▶ **Features to Reduce Probability of Control System Failures**

Functions: Process Control Functions



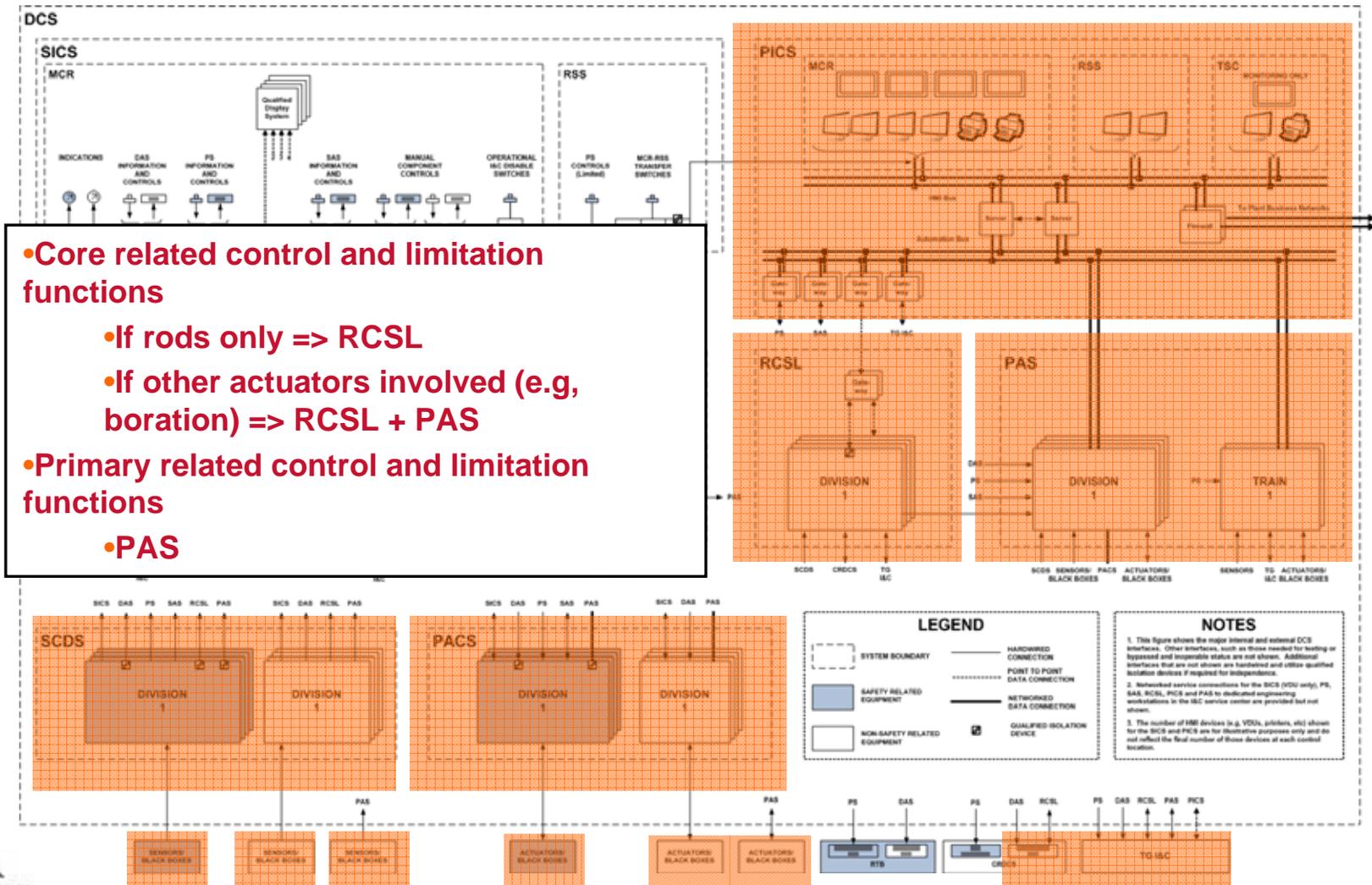
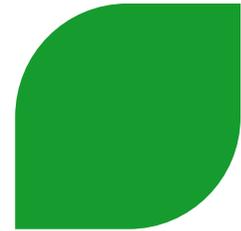
CORE RELATED FUNCTIONS	PRIMARY RELATED FUNCTIONS
RCCA Control	RCS Pressure Control
Average Coolant Temperature Control	Pressurizer level Control
Neutron Flux Control	RCS Loop Level Control
Axial Offset Control	Steam Generator Level Control
	Main Steam Pressure Control

Functions: Process Limitation Functions



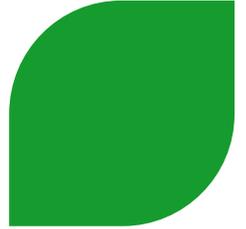
CORE RELATED FUNCTIONS	PRIMARY RELATED FUNCTIONS
Axial Offset Limitation	Reactor Power Limitation with Respect to Feedwater Flow Rate
Rod Drop Limitation	Reactor Power Limitation with respect to Generator Power
Intermediate Range High Neutron Flux Limitation	Reactor Power Limitation with respect to Thermal Power
High Linear Power Density Limitation (Partial Trip)	RCS Dilution (Shutdown Condition) Limitation
Low Departure from Nucleate Boiling Limitation (Partial Trip)	Reactor Coolant System Pressure Limitations
	Pressurizer Level Limitations
	Reactor Coolant System Loop Level Limitation
	Steam Generator Level Limitations
	Loss of One Reactor Coolant Pump Limitation (Partial Trip)

Design: Allocation within the DCS



- **Core related control and limitation functions**
 - If rods only => RCSL
 - If other actuators involved (e.g, boration) => RCSL + PAS
- **Primary related control and limitation functions**
 - PAS

Features to Reduce Probability of Control System Failure

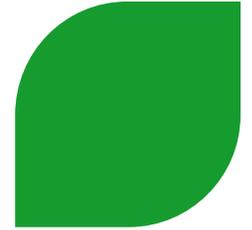


- ▶ **Redundant sensors and signal selection algorithms**
 - ◆ Prevent single sensor failure from causing plant event
- ▶ **Redundant controllers in RCSL and PAS**
 - ◆ Prevent single controller failure from causing a plant event



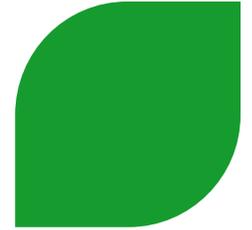
SECTION 7.8: DIVERSE I&C SYSTEMS

Topics



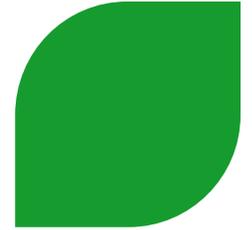
- ▶ **Defense-in-Depth and Diversity (D3) Analysis**
- ▶ **Functions**
- ▶ **Design**
- ▶ **Diversity of Mitigating Systems**

D3 Analysis



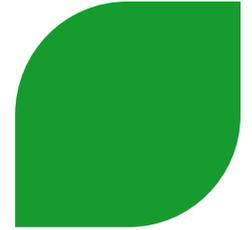
- ▶ **A software common cause failure (SWCCF) is postulated to disable the PS.**
- ▶ **A conservative decision was made to assume a SWCCF of the PS also disables the RCSL (same inputs, similar functions).**
- ▶ **PAS and SAS functions that do not rely on a PS output are assumed to be unaffected by a postulated SWCCF. Their normal operation is used to model the plant response to an event.**
- ▶ **Analysis was performed to determine additional functions (reactor trip, ESF) to mitigate a postulated SWCCF to meet Part 100 limits using best estimate analysis**
- ▶ **Additional functions allocated to SCDS, SICS, DAS and PACS, which are unaffected by postulated PS SWCCF due to diversity**
- ▶ **SWCCF bounds ATWS analysis and required functions to meet 10CFR50.62**

Functions: Diverse Reactor Trip



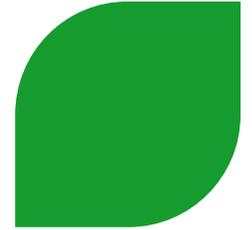
FUNCTION	FUNCTION
Low SG Pressure	High Neutron Flux (Power Range)
Low SG Level	Low Hot Leg Pressure
High SG Level	High Pressurizer Pressure
Low Reactor Coolant System Flow Rate (Two Loops)	Manual Reactor Trip
Low-Low Reactor Coolant System Flow Rate (One Loop)	

Functions: Diverse ESF



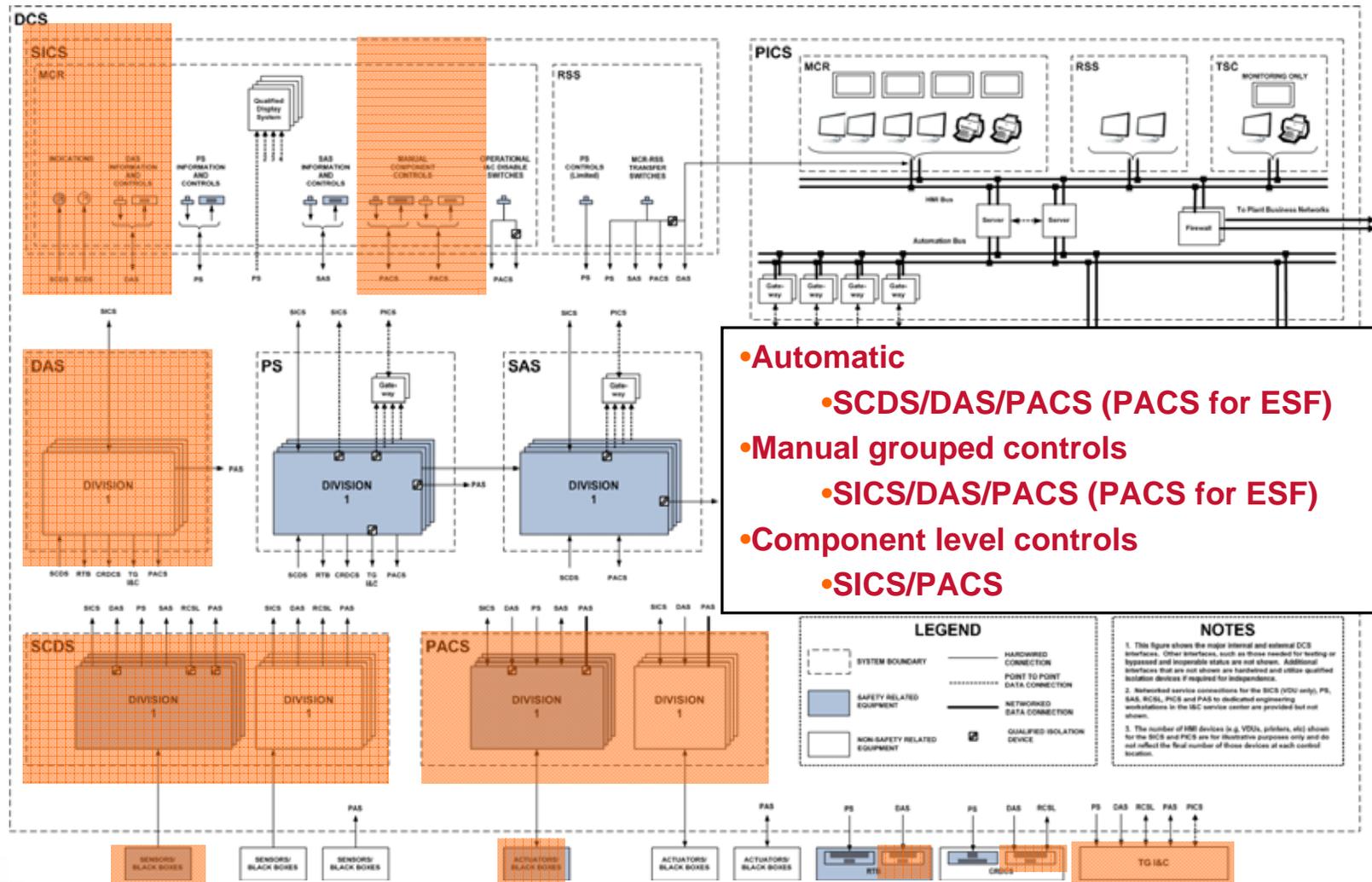
FUNCTION	AUTOMATIC	MANUAL SYSTEM LEVEL	MANUAL COMPONENT LEVEL
Emergency Feedwater System Actuation	x	x	
Control of EFW System after actuation			x
Safety Injection System Actuation	x	x	
Control of SI System after actuation			x
Main Steam Isolation	x		x
Containment Isolation	x	x	
Main Feedwater Isolation	x		x
Containment Hydrogen Mixing Dampers Opening	x	x	
Start SBO Diesels	x		x
Turbine Trip	x		

Functions: Diverse ESF (cont'd)



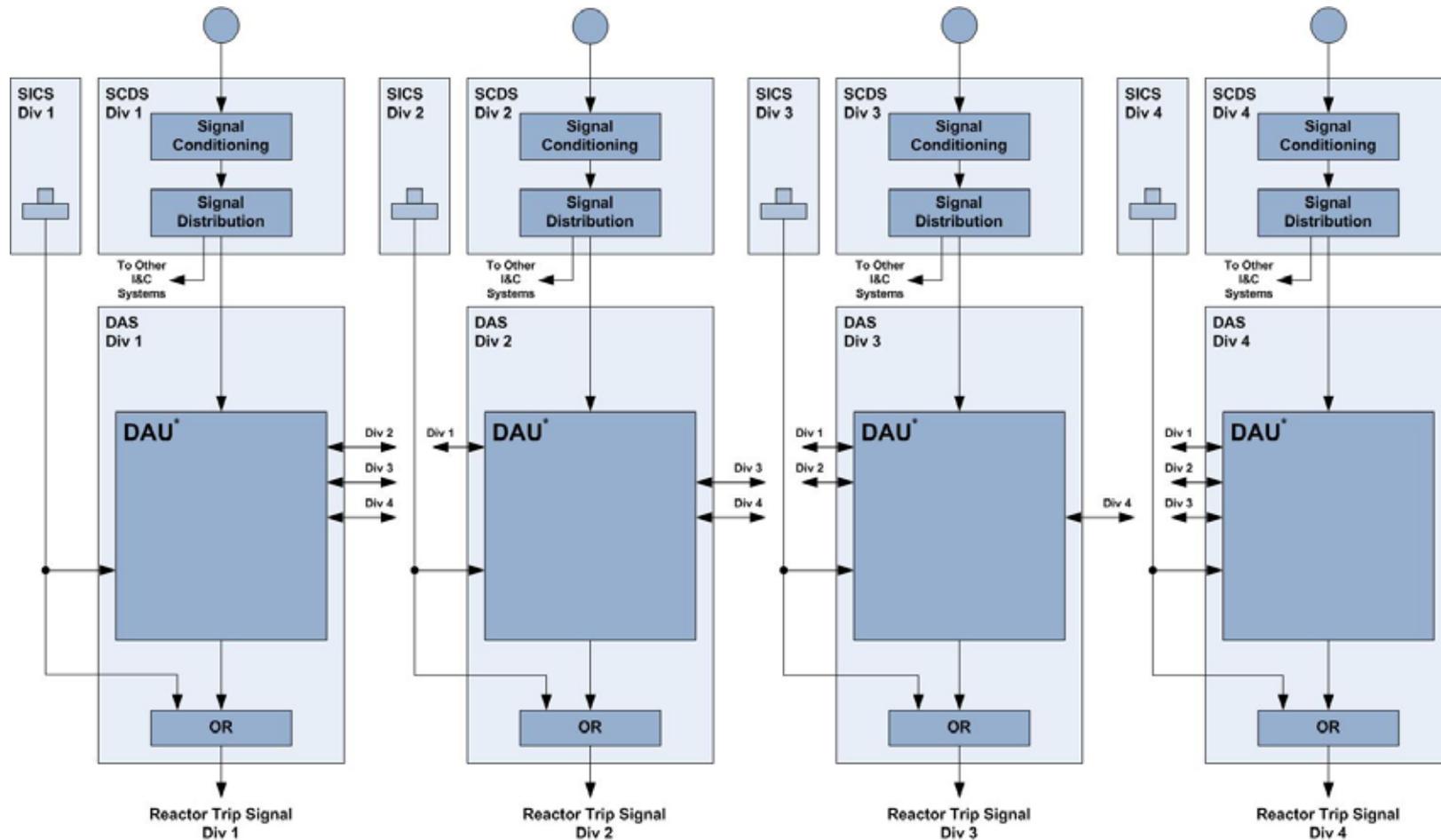
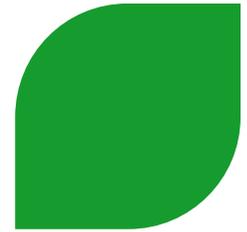
FUNCTION	AUTOMATIC	MANUAL SYSTEM LEVEL	MANUAL COMPONENT LEVEL
Start Emergency Diesel Generators			x
Emergency Diesel Generator Loading			x
Extend Partial Cooldown			x
Safety Injection Switchover to Hot Leg Injection			x
Depressurize Reactor Coolant System with Pressurizer Sprays			x
Extra Borating System Actuation			x
Control Room HVAC Reconfiguration			x
CVCS Isolation			x
Main Steam Relief Train Control			x
Reactor Coolant Pump Trip			x
Emergency Feedwater Isolation			x

Design: Allocation within the DCS



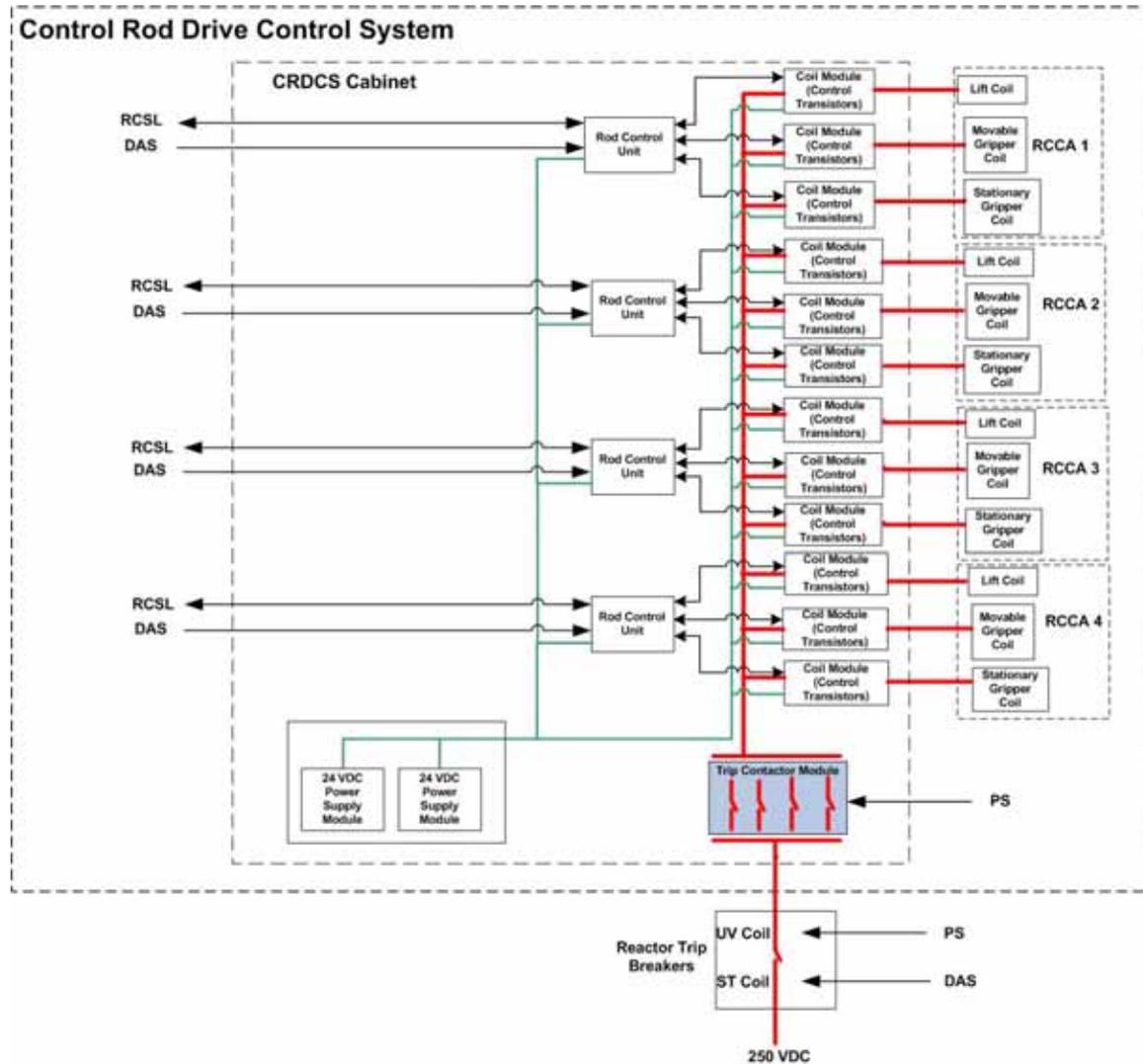
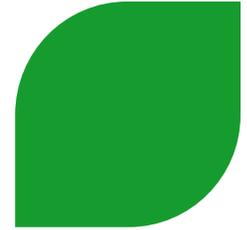
- Automatic
 - SCDS/DAS/PACS (PACS for ESF)
- Manual grouped controls
 - SICS/DAS/PACS (PACS for ESF)
- Component level controls
 - SICS/PACS

Design: Diverse Reactor Trip

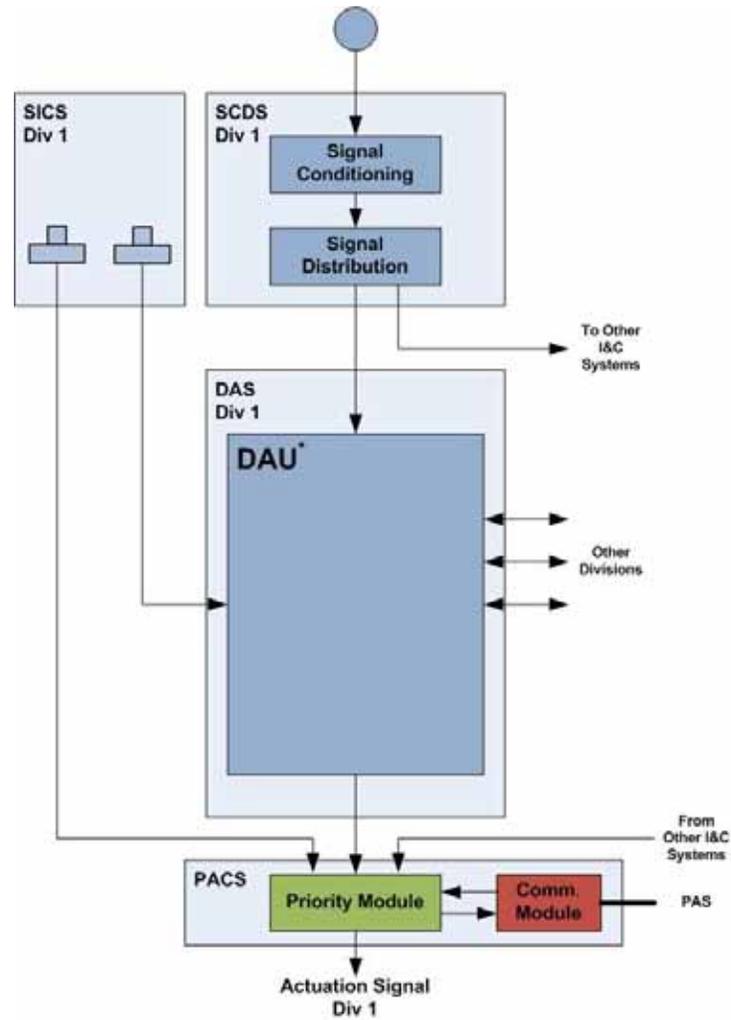
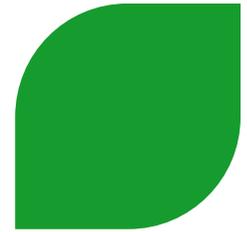


*Technology may be non-microprocessor based programmable electronics also

Design: Diverse Reactor Trip Devices

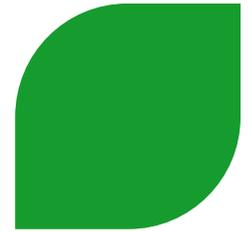


Design: Diverse ESF



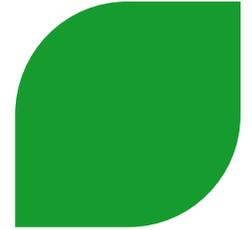
One division shown -
Same for Divisions 2, 3 & 4

Diversity of Mitigating Systems

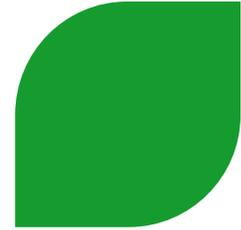


- **SCDS**
 - All inputs to DAS are conditioned and distributed using electronic I&C technology => no SWCCF
- **DAS**
 - Non-microprocessor based technology
- **SICS**
 - Dedicated indicators with hardwired input from SCDS/PACS
- **PACS**
 - Priority module utilizes programmable logic device that is 100% tested

Acronyms



ACRONYM	TERM	ACRONYM	TERM
ALU	Actuation and Logic Unit	EPR	Evolutionary Power Reactor
APU	Acquisition and Processing Unit	ERDS	Emergency Response Data System
BISI	Bypassed and Inoperable Status	HMI	Human Machine Interface
CCWS	Component Cooling Water System	HVAC	Heating, Ventilation and Air Conditioning
CRDCS	Control Rod Drive Control System	I&C	Instrumentation and Control
CU	Control Unit	IRWST	In-Containment Refueling Water Storage Tank
CVCS	Chemical Volume and Control System	LHSI	Low Head Safety Injection
DAS	Diverse Actuation System	MCR	Main Control Room
DAU	Diverse Actuation Unit	MSI	Monitoring and Service Interface
DCS	Distributed Control System	PACS	Priority and Actuator Control System
EDG	Emergency Diesel Generator	PAM	Post Accident Monitoring
EOC	Electrical to Optical Converter		



Acronyms (cont.)

ACRONYM	TERM	ACRONYM	TERM
PAS	Process Automation System	SBO	Station Blackout
PE	Programmable Electronic	SCDS	Signal Conditioning and Distribution System
PLD	Programmable Logic Device	SG	Steam Generator
PICS	Process Information and Control System	SICS	Safety Information and Control System
PS	Protection System	SPDS	Safety Parameter Display System
QDS	Qualified Display System	SPND	Self Powered Neutron Detector
RCP	Reactor Coolant Pump	SU	Service Unit
RCSL	Reactor Control, Surveillance and Limitation	SWCCF	Software Common Cause Error
RHR	Residual Heat Removal	TG I&C	Turbine Generator I&C
RSS	Remote Shutdown Station	TSC	Technical Support Center
RTB	Reactor Trip Breaker	TXS	Teleperm XS
SAS	Safety Automation System		

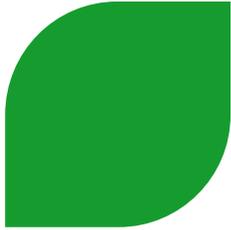
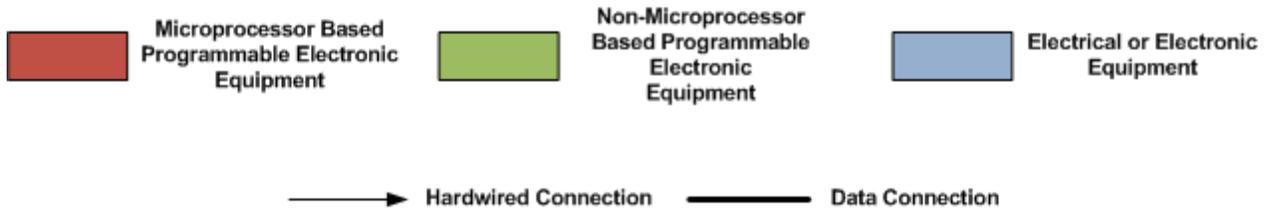


Figure Legend (except for DCS Functional Architecture)







Presentation to the ACRS Subcommittee

U.S. EPR Design Certification Application Review

Safety Evaluation Report with Open Items

Chapter 7: Instrumentation and Controls

November 15, 2011

Objective and Outcome

Objective

- Brief the Subcommittee on the staff's review of the U.S. EPR Instrumentation and Control (I&C) System.

Expected Outcome

- Common understanding of the background, the staff's evaluation efforts, and current status of the U.S. EPR I&C system review.

Staff Review Team

Technical Staff from NRO/DE/ICE1

Jack Zhao

Tung Truong

Deanna Zhang

Ken Mott

Deirdre Spaulding Yeoman

Wendell Morton

Terry Jackson

Project Managers

Getachew Tesfaye

Michael Canova

Outline of Presentation

- Introduction
- Background
- Key Technical Topics of Interest
 - Redundancy
 - Independence
 - Determinism
 - Diversity
 - Simplicity

Outline of Presentation

- Other Technical Topics
 - Self Testing
 - Safety Automation System
- Discussion/Committee Questions

Introduction

- **AREVA submitted the U.S. EPR design certification application on December 11, 2007.**
- **This Safety Evaluation and related reports represent 3 1/2 years of effort for both staff and the applicant.**
- **On June 25 2010 AREVA proposed to make several refinements to their previously submitted design in order to support continued review (Meeting Summary ML102300529).**

Introduction

- **Although the SE for Chapter 7 is based on Revision 2 of the application, frequent reference is made to “Interim Revision 3 mark-ups.”**
- **These identify AREVA’s commitments to changes in the FSAR, as submitted with RAIs against the various sections of the FSAR.**
- **It is these design changes that are reflected in the mark-ups submitted for unrelated RAI questions.**
- **This was done to docket a complete re-write of Chapter 7 to provide the staff with complete sections, for the purposes of the Phase 2 review.**

Overview of DCA

SRP Section/DCA Section		No. of Questions	No. of Open Items
7.1	Introduction	51	19
7.2	Reactor Trip System	33	0
7.3	Engineered Safety Features Systems	38	3
7.4	Systems Required for Safe Shutdown	15	1
7.5	Information Systems Important to Safety	11	2
7.6	Interlock Systems Important to Safety	3	0
7.7	Control Systems Not Required for Safety	21	1
7.8	Diverse Instrumentation and Control Systems	50	8
7.9	Data Communication Systems	71	2
Totals		293	36

Background

Major Documents Reviewed

Doc. Number	Title	Revision
Docket 52-020	U.S. EPR DCD FSAR, Tier 1 Section 2.4 and Tier 2 Chapter 7	Interim Revision 3
ANP-10309P	U.S. EPR Protection System Technical Report	3
ANP-10304	U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report	4
ANP-10310P	Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report	1
ANP-10315P	U.S. EPR Protection System Surveillance Testing and TXS Self-Monitoring Technical Report	1
ANP-10272-A	Software Program Manual for TXS Safety Systems Topical Report	3
NP-10273P	AV42 Priority Actuation and Control Module Topical Report (Withdrawn and Replaced by ANP-10310P)	0

Description of Open Items

- RAI 505, Question 07.01-33: Tracks the applicant commitment to revise Topical Report ANP-10287P, “In-core Trip Setpoint and Transient Methodology For U.S. EPR Topical Report,” adding the method for including the undetected SPND failure. Based on the revised in-core trip set point and transient methodology, the applicant also committed to re-analyze FSAR Tier 2, Chapter 15 events which take the credit for the in-core DNBR and linear power density (LPD) trips
- RAI 505, Question 07.01-34: Requested the applicant to address how the guidance from SRP BTP 7-17 or ISG-04 Staff Position 1, Points 10 and 11, are satisfied with regards to the non-safety Service Unit’s direct connection to safety systems, and whether this type of connection applies to all TXS safety systems.
- RAI 505, Question 07.01-35: Requested the applicant to provide an FMEA, or similar single failure analysis, for the SAS. In addition, the staff requested that the applicant provide ITAAC to verify the SAS single failure analysis, similar to the PS ITAAC to verify its FMEA.
- RAI 505, Question 07.01-36, Requested the applicant to provide more details on the new SAS voting configuration and document this information in FSAR in order to address how SAS voting logic compensates for single failures.

Description of Open Items

- RAI 505, Question 07.01-37: Requested the applicant to add ITAAC that would link the testing done with SAS-related mechanical system PACS testing to ITAAC Item 4.4 in FSAR Tier 1, Section 2.4.5 to ensure that completion of the SAS ITAAC is tied to the various mechanical system PACS ITAAC being satisfactorily completed.
- RAI 505, Question 07.01-38: Requested the applicant to provide information in FSAR Tier 1 and FSAR Tier 2 concerning how their credited fail-safe design is incorporated into SAS. and specifically with respect to a loss of power.
- RAI 505, Question 07.01-39: Requested the applicant to address the issues associated with periodic self-testing, as the applicant does not intend to directly test the self-testing features of the U.S. EPR design.
- RAI 505, Question 07.01-40, Requested the applicant to address why the applicant does not consider failures detected by software-based means as not significant enough to warrant an automatic interruption of operation of the affected function processor.
- RAI 505, Question 07.01-41: Requested the applicant to address how “halted,” “disabled,” and “out of service” device malfunctions are automatically treated by the U.S. EPR design.

Description of Open Items

- RAI 505, Question 07.01-42: Requested the applicant to address surveillance testing on the other safety-related I&C systems, including SAS, which have Technical Specification surveillance requirements.
- RAI 505, Question 07.01-43: Requested the applicant to clarify the self-test features of SICS for both FSAR Tier 1 and FSAR Tier 2 design descriptions and address the need for any ITAAC to verify the self-test features.
- RAI 505, Question 07.01-44: Requested the applicant to identify the credited self-test features for the other safety-related I&C systems, or whether the scope and design of the self-test features for the PS and SAS provide coverage for the other safety-related I&C systems.
- RAI 505, Question 07.01-45: Requested the applicant to address the issue of PACS self-testing, particularly as it relates to the PLD self-test features and the PACS ability to meet GDC 23 to ensure that the PS fails into a safe state, or into a state demonstrated to be acceptable on some other defined basis, upon loss of electrical power or postulated adverse environments.
- RAI 505, Question 07.01-46: Requested the applicant to provide additional information on operation of the I&C disable switch. Specifically that the applicant identify if the switch is safety-related, and if so, how it meets the requirements, such as those for single failure protection.

Description of Open Items

- RAI 505, Question 07.01-47: Requested the applicant to revise the acceptance criteria of ITAAC Item 4.24 to ensure it includes the PACS.
- RAI 505, Question 07.01-48: For automatic controls this question requests the applicant to identify the design elements of the PS which meet the requirements of Clauses 6.1 regarding an approved; setpoint methodology, the operating margins for process variables monitored for reactor trip (RT) and engineered safety features (ESF) systems, the setpoints and corresponding system response times (time delays) for each RT and ESF function, and ITAAC from Tier 1 which verifies the completion of protective action for automatic ESF actuation signals. For manual controls, this question requests the applicant to add information to Tier 1 concerning SAS manual grouped controls. The staff also requests the applicant add ITAAC to verify the manual control design function, as well as the display and controls location in the MCR.
- RAI 505, Question 07.01-49: Requested the applicant to identify the nature of the operating bypasses as they relate to SAS, especially those that are outside the bounds of the system interaction with PS.

Description of Open Items

- RAI 505, Question 07.01-50: Requested the applicant address the intent and use of the impending approved version of Topical Report ANP-10272 and clarify how the U.S. EPR design addresses the application-specific action items within that topical report.
- RAI 505, Question 07.01-51: Requested the applicant to provide a clear and complete description of the implementation of the SU, including effects on equipment function and operability while the SU is in use.
- RAI 414, Question 07.03-30: Requested that the applicant clarify how the as-built configuration of the PS will meet the bounding response times of the Chapter 15 safety analyses.
- RAI 505, Question 07.03-37: Requested that the applicant to clarify why changes have been made to the ESF protective function variable monitoring ranges and associated initiating conditions.
- RAI 505, Question 07.03-38: Requested the applicant to provide justification for design basis requirements that have either been excluded, or are not applicable to SAS and other safety-related systems in order to show compliance with IEEE Std 603-1998, Clause 4.k, single failure criterion.

Description of Open Items

- RAI 505 Question 07.04-15: Requested the applicant to clarify the display and control capabilities SICS provides at the RSS.
- RAI 505, Question 07.05-10: This question tracks the applicant's impending changes to clarify the completeness of the identified PAM variables, based on the applicant's stated intent revise the current description of the PAM variable inventory information,
- RAI 505, Question 07.05-11: Requested the applicant to re-address the need for a combined license information item regarding a need to update or supplement the PAM variable information as presented in the DCA.
- RAI 505, Question 07.07.23: Requested the applicant to remove, or further clarify, the parenthetical qualifier in the 7.1.1.3.2 statement that "equipment selected for use in the PICS will be rated by the manufacturer (or otherwise reasonably expected) to operate under the mild environmental conditions expected to exist at its location.." (in the safeguard buildings).
- RAI 505, Question 07.08-43: Requested the applicant to clarify apparent conflicting statements in Technical Report ANP-10304 regarding the intended design diversity between the PS TXS platform and the DAS platform.

Description of Open Items

- RAI 505, Question 07.08-44: Requested that the applicant to clarify how a credited manual D3 RCP Trip is being provided on the SICS as part of the credited D3 manual actuations available to the operator.
- RAI 505, Question 07.08-45: Requested the applicant to clarify how signal diversity is credited between PS subdivisions, given apparent conflicts between the PS and D3 technical reports.
- RAI 505, Question 07.08-46: Requested the applicant to address their March 15, 2011 commitment to provide ITAAC for signal assignments among PS subdivisions.
- RAI 505, Question 07.08-47: Requested the applicant to clarify their capability to test DAS at power in line with the guidance of GL-85-06, Section XI.
- RAI 505, Question 07.08-48: Requested the applicant to address their quality assurance commitments as they will be applied to the non-safety portion of SCDS and SICS.
- RAI 505, Question 07.08-49: Requested the applicant to define and clarify the DAS structures software issues particularly as they relate to diversity attributes.

Description of Open Items

- RAI 505, Question 07.08-50: As SAS plays a minimal role in the overall D3 analysis as is only credited to limit EFW flow for some events, staff requested the applicant to provide the basis for this function in the D3 analysis and the overall necessity of SAS in the D3 analysis.
- RAI 505, Question 07.09-71: Requested the applicant to clarify how invalid signals are identified by SAS processors and state whether the voting logic in the SAS is modified to accommodate the identified invalid signals.
- RAI 505, Question 07.09-72: Requested the applicant to demonstrate that a failure within one division will prohibit non-predefined messages from propagating to other safety divisions and how this feature is verified in the as-built safety system to meet the requirements of 10 CFR 52.47(b)(1).

Main Technical Issues With Original U.S. EPR I&C Design

- Complex I&C Architecture
- Extensive inter-divisional communications used for PS, SAS, and SICS safety systems
- Bi-directional data communication between safety systems and non-safety systems
- Continuous connection between safety systems and non-safety service unit
- QDS used for safety-related SICS

Major I&C Design Changes

- **Less Complex I&C Design**
 - Minimized inter-divisional communication for safety systems
 - Reduced dependence on plant data network
 - Hardwired SICS
 - Elimination of Severe Accident I&C System

Major I&C Design Changes

- **Independence Among Divisions for SICS, SAS, and PS Safety Systems**
 - SICS uses hardwired control and indication to remove inter-divisional communication in SICS
 - Reduced inter-divisional communication by removing 2nd min/2nd max functions in SAS
 - Modified self-powered neutron detector (SPND) system through use of hardwired design thus reducing inter-divisional communication in PS
 - Alternative request to include an SPND undetected single failure in the safety analysis

Major I&C Design Changes

- **Independence Between Safety and Non-Safety Systems**
 - Physically limited, uni-directional data communication from safety systems to non-safety systems
 - Non-safety service units (SU) are disconnected, except for maintenance and surveillance testing.

Major I&C Design Changes

- **Independence and Software Quality for the PACS**
 - Separate communication and priority logic boards in the new PACS
 - 100 percent combination testing for the new PACS
- **Self-testing and Monitoring for Teleperm XS (TXS) Systems**
 - Submitted Technical Report ANP-10315 to provide necessary design information

Major I&C Design Changes

- **Defense-in-Depth and Diversity (D3)**
 - DAS is separated from the PAS and plant data network
 - Manual control and indication on SICS
 - Implemented using non-microprocessor-based technology
 - Best estimate analysis supports the proposed D3 functions

Redundancy

- **U.S. EPR I&C Safety Systems**
 - Sustain a single failure and complete safety function
 - Meets GDC 21 and Clause 5.1 of IEEE Std. 603-1998
 - Have single-failure ITAAC
- **Staff's evaluation is in Section 7.1.4.5 of the SE**

Redundancy

- **Protection System**
 - Four redundant, independent PS divisions
 - Redundant power supplies for PS cabinets
 - System level failure modes and effects analysis (FMEA)

- **PACS**
 - Redundancy mirrors mechanical systems trains
 - FMEA (described in PS FMEA)

Redundancy

- **SICS, ICIS, EIS, BCMS, RMS, HMS, SCDS, and RPMS**
 - Sufficient level of redundancy: ITAACs
- **Safety Automation System (SAS)**
 - Four redundant, independent SAS divisions
 - Open Item: How does SAS voting logic compensate for single failures within a division? (RAI 505, Question 07.01-36)
 - Open Item: Applicant to provide a FMEA (RAI 505, Question 07.01-35)

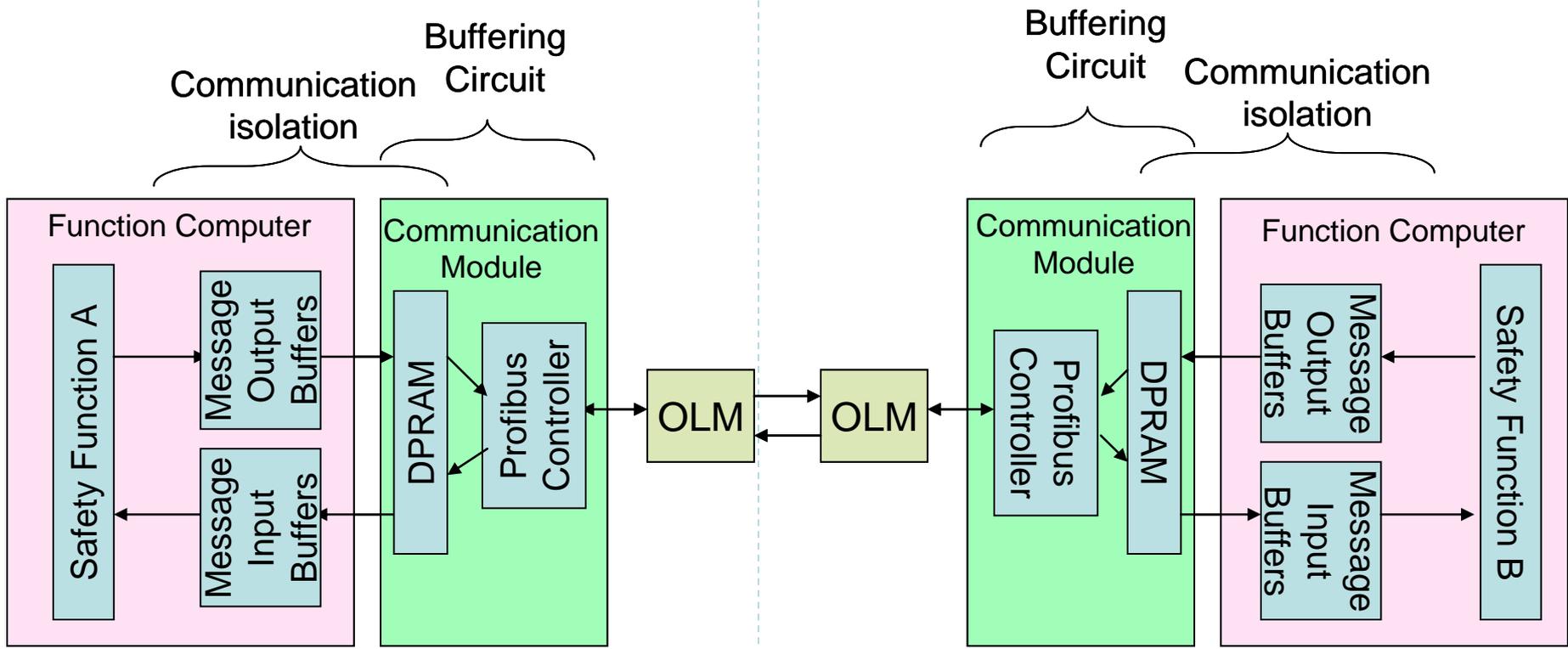
- **Independence Between SAS Divisions**

- Only information that enhances or is used in safety functions is accepted from outside its safety division (i.e. voting logic)
- Only discrete data is sent between divisions
- Use of DPRAM between processors
- Only pre-defined data messages with fixed length and headers are generated and accepted
- Open Item: How are invalid signals from outside its division handled? (RAI 505, Question 07.09-71)

Independence

- **Independence Between PS Divisions**
 - Only pre-defined data messages with fixed length and headers are accepted and generated
 - Error detection ensures erroneous messages are not processed by the function processor
 - Invalid signals are accommodated through identification and modification of voting logic

Independence



Divisional Separation

Independence

- **Alternative Request for SPNDs**
 - Alternative request to use conservative setpoint selection to satisfy the single failure criteria for PS
 - Unique aspects of SPNDs
 - Each SPND occupies a unique location within the core
 - Flux is not uniform throughout the core
 - SPNDs do not operate redundant to one another
 - Redundancy and independence between divisions cannot be used to satisfy the single failure criterion

Independence

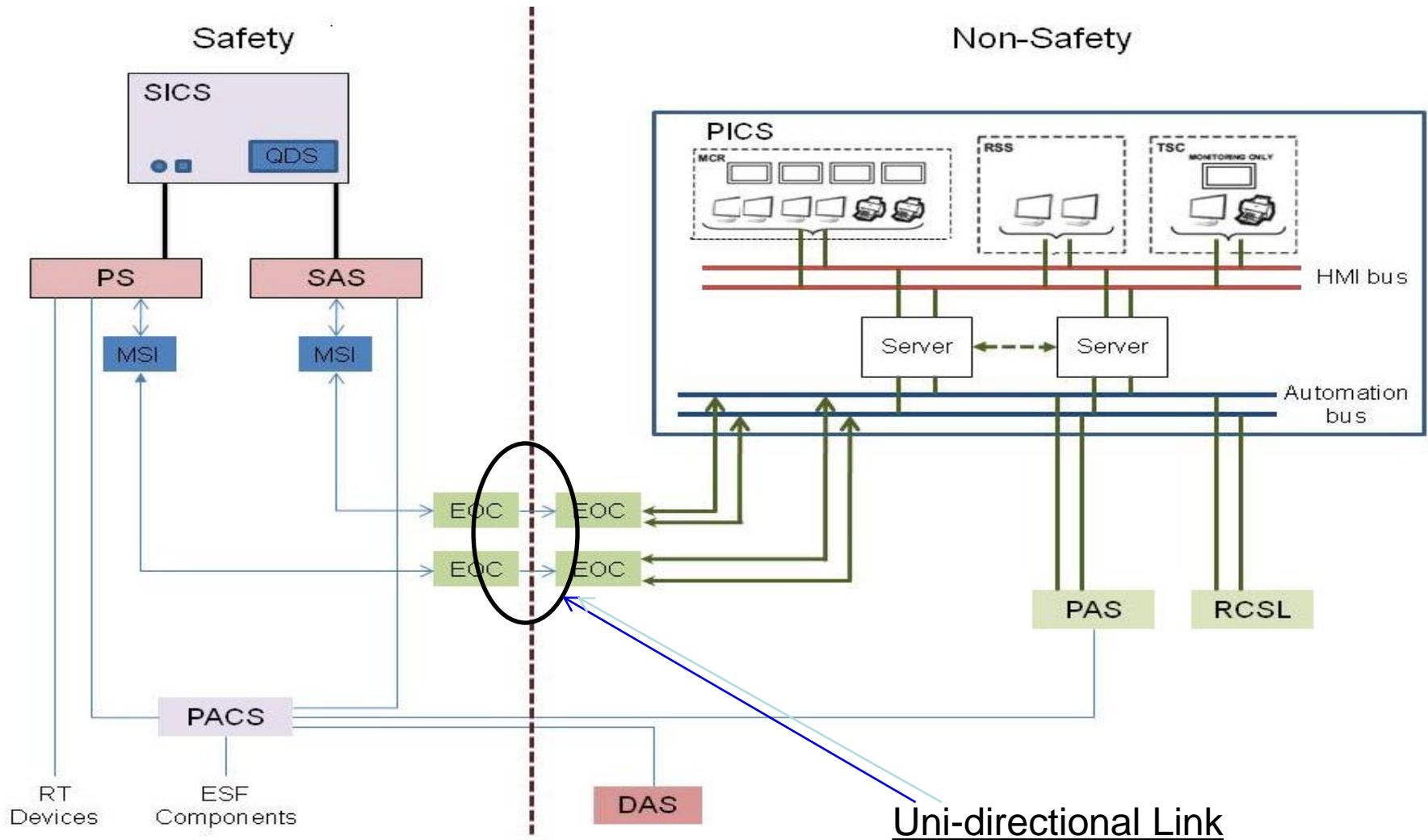
- **Accommodation of SPND Single Failures:**
 - Detection of failures and use of setpoint modification for detected failures
 - Conservative setpoint selection within each PS division to accommodate a single, undetected failure upstream of the PS
 - Open Item: Applicant to submit necessary revisions to Chapter 15 accident analysis and documentation for events crediting use of SPNDs. (RAI 505 Question 07.01-33)

Independence

- **Independence Between Safety and Non-Safety Control and Display Systems**
 - No data is received from non-safety control systems to SAS and PS by data communications
 - Isolation is achieved through a Class 1E device that enforces uni-directional data flow from PS/SAS to control systems
 - Only the PACS non-safety communication module receives data from non-safety systems
 - Non-safety system data is translated to discrete hardwired signals before transmission to the priority module

- **Data Communication Between Safety Systems and the Service Unit**
 - Communication path between the SU and the divisional MSIs for the PS and SAS is normally disconnected through hardwired disconnects
 - Isolation switches are employed to ensure connection to only one division at a time
 - The MSI provides authentication and error detection for messages sent between the SU and the PS/SAS
 - Open Item: Clarification on how isolation is achieved between the RPMS and the SU

Independence



Determinism

- **Software Failures or System Malfunctions are Accommodated by the TXS Internal Diagnostic Functions and the Built-In Watchdog Timers**
 - Pre-determined fixed cycle times for all TXS processor modules, with the same sequence of processing steps each cycle
 - Message sizes and communication rates are constant, resulting in constant communication loads under all circumstances
 - Communication protocols used in the TXS system do not require acknowledgement of the transmitted message by the receiver
 - No process-driven interrupts
 - Hardwired watchdog timer that are triggered by self-test features in the run-time environment (RTE)
 - Response time analysis and ITAAC verification

Determinism

- **Watchdog Timer**

- Each TXS function processor is equipped with a hardware-based watchdog timer
- If the RTE does trigger the watchdog timer before its expiration, an error is assumed in which case:
 - A hardwired signal is used to indicate processor failure
 - The hardwired signal switches off the I/O module power supply placing the processor in a defined failure state
 - For reactor trip functions, switching off the I/O module power supply results in a zero-voltage output, which initiates a reactor trip signal
 - These actions are independent of the inherent self-monitoring software.

- **PS Response Time Analysis**

- Response time is estimated for the computerized portion of the PS
- A theoretical bounding response time is established for typical types of functions
- Total response time spans from a process variable exceeding the pre-defined limit to completion of the protective function
- Final response time is verified through ITAAC

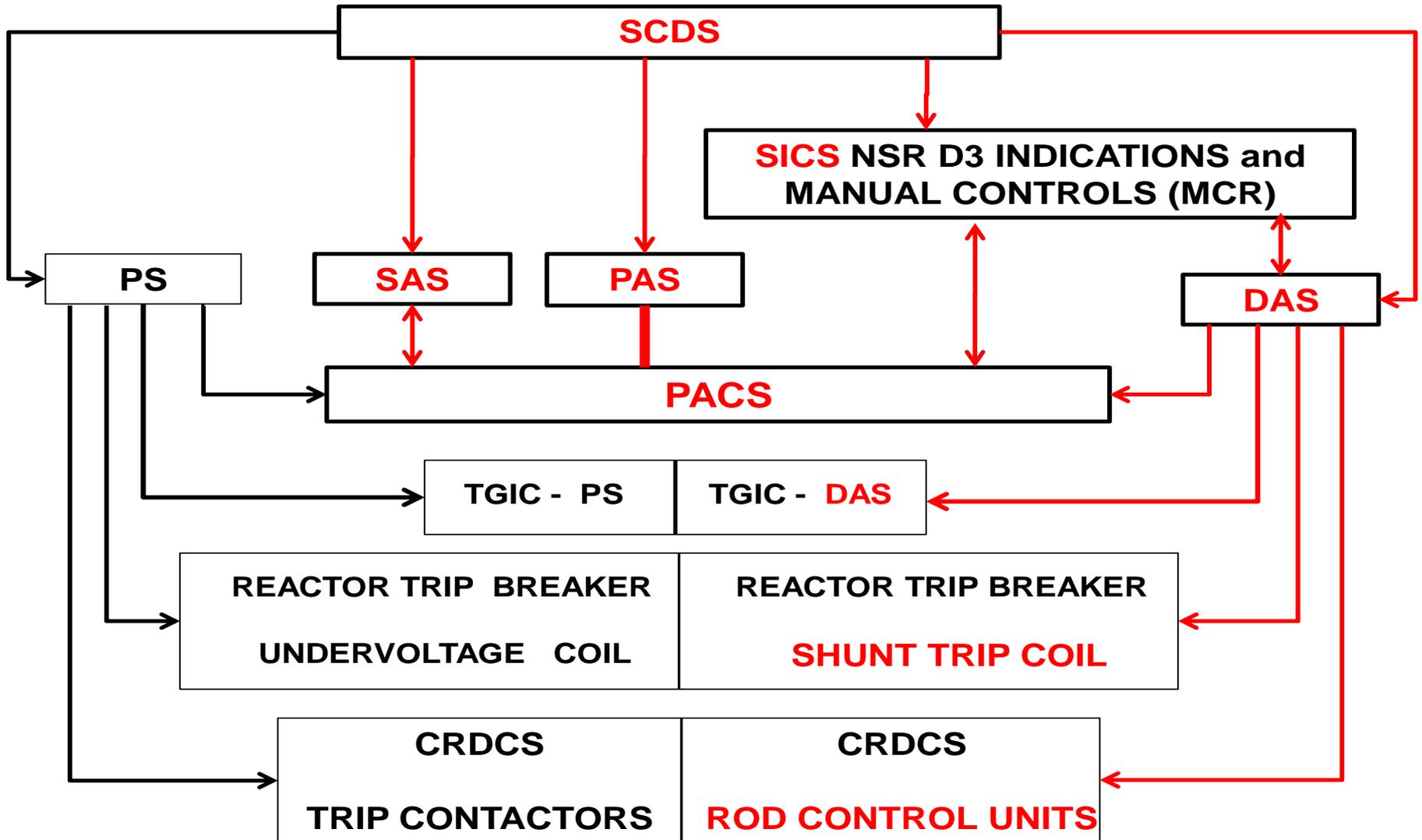
Defense-in-Depth and Diversity

- DAS provides diversity to the PS

Diversity Attributes	DAS-PS Staff Approved Design Diversity
Design	
different approaches within the a technology	YES
different architecture	YES
Equipment	
same manufacturer of fundamentally different designs	YES
different logic processing equipment architecture	YES
Function	
different purpose, function, control logic, or actuation means	YES
different response time scale	YES
Human	
different designers, engineers, and/or programmers	YES
Software	
	Open Item (RAI 505, Question 07.08-49)

- **Other systems that make up the D3 mitigation systems**
 - PACS: 100% combinatorial testing to address a software common cause failure
 - SCDS: Functions are not performed by microprocessors and there is no software running in the SCDS
 - SICS: Utilizes discrete and analog controls and indications

Defense-in-Depth and Diversity



Simplicity

- **Staff Approach to the Review:**
 - Staff guidance provides a simple means to address hazards for specific design aspects like data communications
 - More complex design alternatives require a more comprehensive and detailed review by the staff
- **The applicant proposed several design changes to reduce design complexity**

Simplicity

- **Changes Resulting in a More Simple Design**
 - Reduced the amount of inter-divisional communication within the PS and SAS
 - Eliminated inter-divisional communications in the SICS
 - Implemented physical uni-directional data communication from safety to non-safety systems
 - Selected non-microprocessor-based technology for DAS
 - DAS is less dependent on other I&C systems

Surveillance and Self-Testing

- **Automated TXS Self-Testing**
 - The applicant takes credit for automated self-testing to meet applicable regulatory requirements
 - Automated self-testing to substitute for traditional surveillance activities such as channel checks and channel functional tests

Surveillance and Self-Testing

- **Automated Self-Testing Features**
 - Inherent TXS Self-Testing (Standard TXS features)
 - Error code monitoring of TXS components
 - Communication monitoring
 - Verification of cyclic self-test run completion (once every hour)
 - Hardware Watchdog Timers
 - Applicable to PS and SAS only
 - Engineered TXS Self-Testing features (Project-based) –
 - Monitoring of input signal status
 - Monitoring of RTE message flags used to for alarm processing
 - Cross-divisional analog input comparison for fidelity
 - Range monitoring for analog inputs
 - Faulty signals are excluded from further processing and initiate MCR alarms as appropriate.
 - Applicable to PS and SAS only

Self-Testing Open Items

- **TXS Self-Testing and Surveillance Testing**
 - Verification of Self-tests: How is automated self-testing periodically verified? (RAI 505, Question 07.01-39)
 - How is operability addressed for detect failures and failures of the self-test functions itself? (RAI 505, Question 07.01-40)

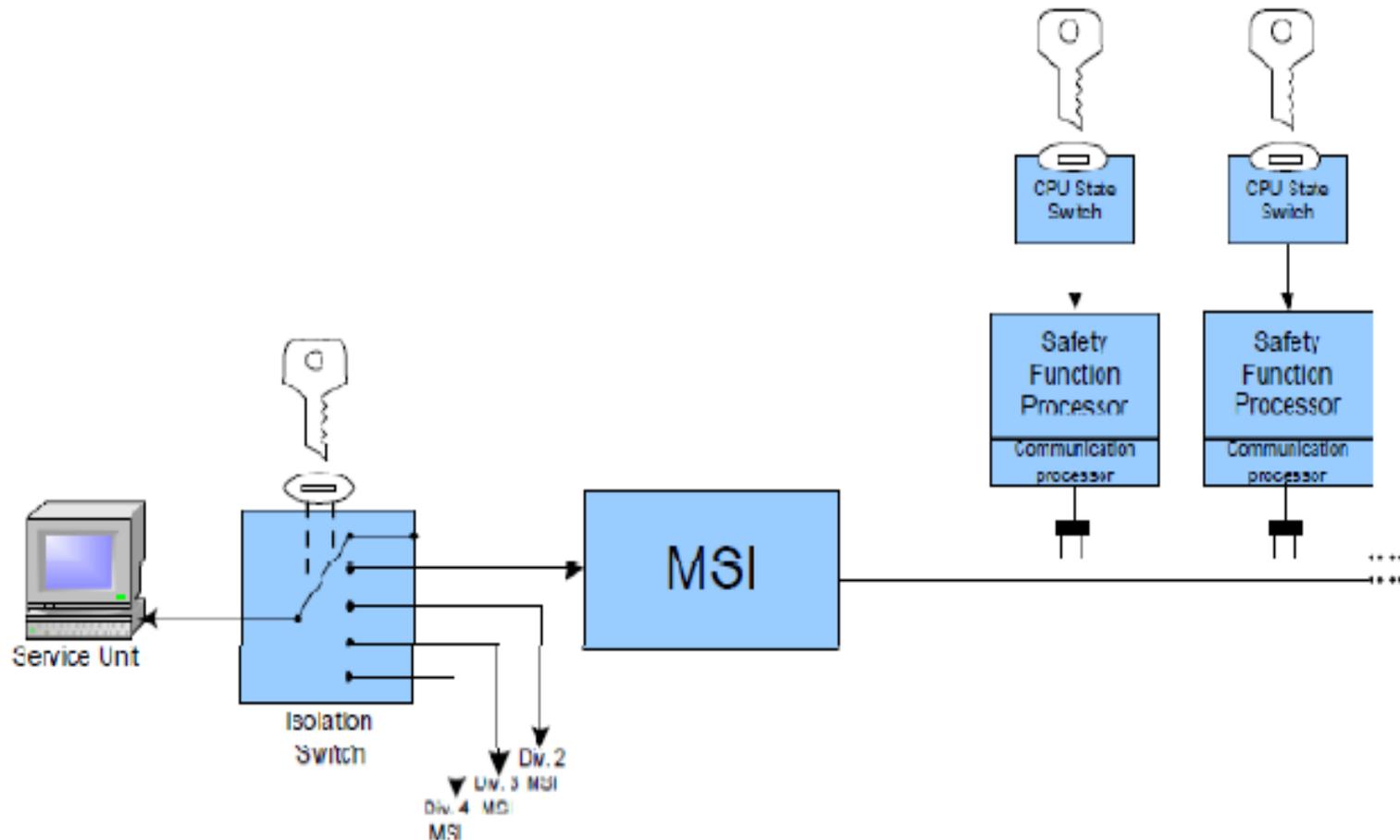
Self-Testing Open Items

- **TXS Self-Testing and Surveillance Testing**
 - Besides the PS, ANP-10315 does not adequately demonstrate how surveillances will be performed for all other TXS safety systems besides the PS. (RAI 505, Question 07.01-42)
 - It is unknown whether other TXS safety systems utilize credited self-testing features as described in ANP-10315. (RAI 505, Question 07.01-42)

Surveillance and Self-Testing

- **Service Units**
 - Non-safety related computers which serve as the primary means of performing surveillance and troubleshooting activities for PS, SAS and RPMS.

SU Connection - Simplified



Service Unit - Open Items

- **Service Unit (SU) - RAI 505, Question 07.01-51:**
 - Operability of a TXS function processor while plugged into the SU:
 - What is the baseline operability of a function processor in each of it's four operating states and subsequent effects on system operations?
 - What is the baseline operability of a Function processor during surveillance tests requiring the Function processor to be in multiple operating states?
 - How is the SU utilized for the other TXS safety systems besides the PS?
 - Is the SU used in a similar manner for other TXS safety systems as it is for PS?

SAS Open Items

- **RAI 505, Question 07.01-35**
 - The applicant has not provided the staff a failure modes and effects analysis(FMEA), as a means of demonstrating:
 - Compliance to Single Failure Criterion
 - The effects of a SAS single failure(s) on plant operations.
 - How is SAS voting logic modified in the presence of single failure(s)? (RAI 505, Question 07.01-36)

SAS Open Items

- **SAS System Integrity**
 - How does SAS recover from a loss-of-power condition and what are the 'fail-safe' configurations for SAS?
 - This is significant due to the interaction of SAS with numerous safety-related mechanical systems (RAI 505, Question 07.01-38)

SAS Open Items

- **SAS Response Timing Requirements**
 - The staff has created an open item RAI to the applicant to gain clarity on whether SAS has any associated timing requirements
 - Currently, the US EPR DC does not contain any information regarding setpoint analysis or response time requirements for SAS
 - SAS performs both safety-related functions and protective actions (EFW Pump Flow protection and SG EFWS Level control) (RAI 505, Question 07.01-48)

SAS Open Items

- **SAS D3**
 - Applicant has not provided an analysis of SAS common-cause-failure plant response.
 - Staff issued RAI 07-08-50 as an Open Item.
 - SAS is credited for D3 mitigation to limit emergency feedwater flow to a depressurized steam generator
 - If SAS fails, how will the protective flow limitation function be actuated? What is the credited diverse means for initiation?

Discussion / Committee Questions

List of Acronyms

- BCMS Boron Concentration Monitoring System
- CRDCS Control Rod Drive Control System
- D3 Diversity and Defense-in-Depth
- DAS Diverse Actuation System
- DPRAM Dual-Port Random Access Memory
- EIS Excore Instrumentation System
- EOC Electrical-to-Optical Converter
- ESF Engineered Safety Feature
- FMEA Failure Modes and Effects Analysis
- FSAR Final Safety Analysis Report
- GDC General Design Criteria
- HMI Human-Machine Interface
- HMS Hydrogen Monitoring System
- I&C Instrumentation and Control
- ICIS In-Core Instrumentation System
- IEEE Institute of Electrical and Electronics Engineers
- ITAAC Inspections, Tests, Analyses, and Acceptance Criteria

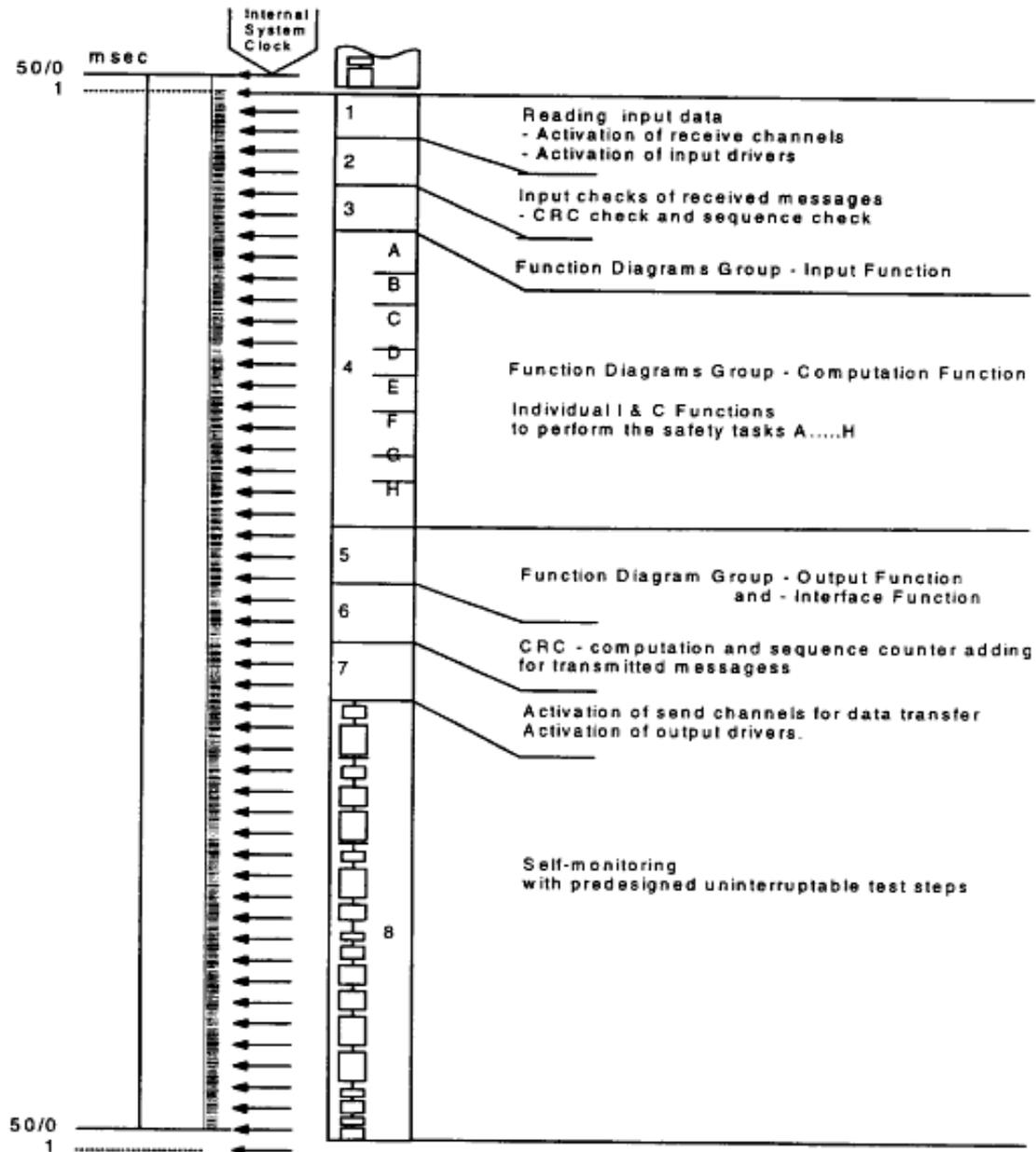
List of Acronyms

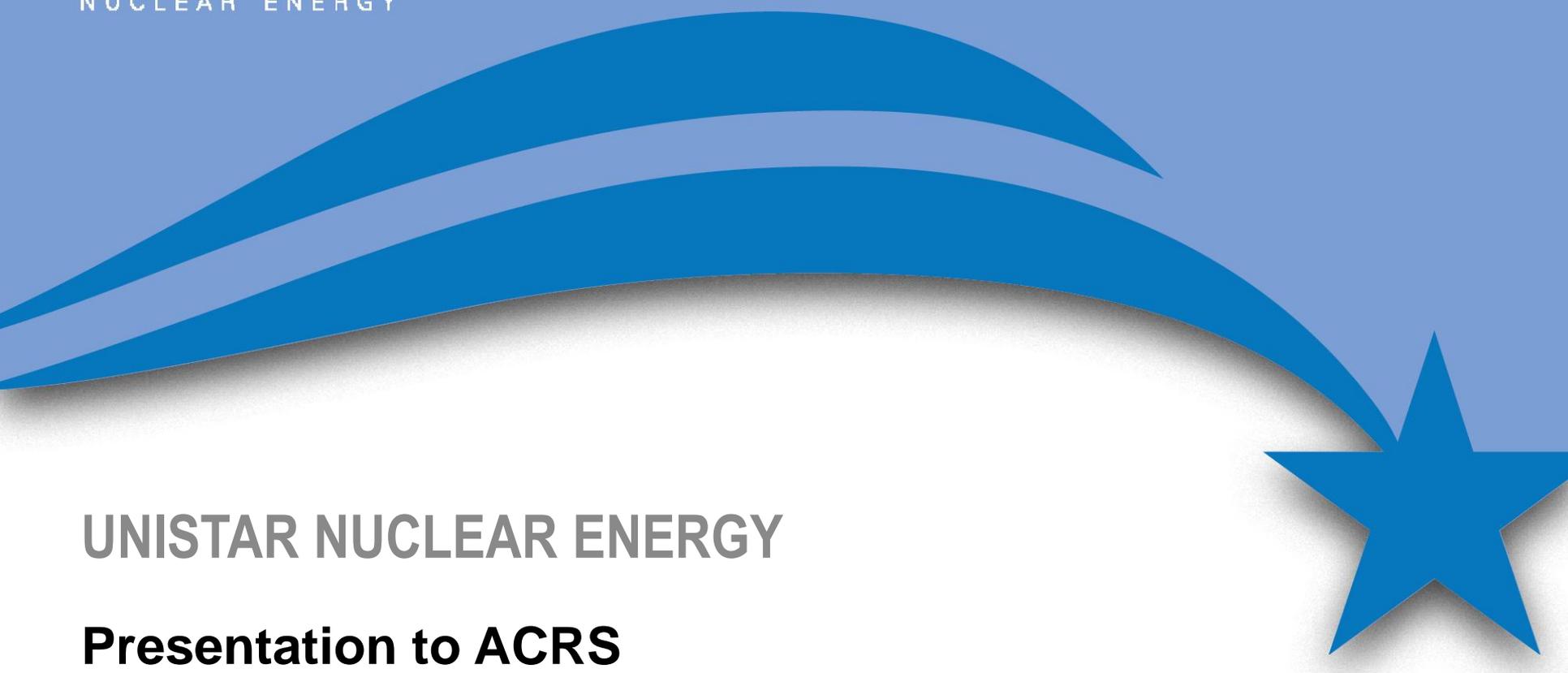
- MCR Main Control Room
- MSI Monitoring and Service Interface
- NSR Non-Safety Related
- OLM Optical Link Module
- PACS Priority and Actuator Control System
- PAS Process Automation System
- PICS Process Information and Control System
- PS Protection System
- QDS Qualified Display System
- RMS Radiation Monitoring System
- RSS Remote Shutdown Station
- RTE Run-Time Environment
- SAS Safety Automation System
- SCDS Signal Conditioning and Distribution System
- SE Safety Evaluation

List of Acronyms

- SICS Safety Information and Control System
- SPND Self Powered Neutron Detector
- SU Service Unit
- RAI Request for Additional Information
- RCSL Reactor Control Surveillance and Limitation
- RPMS Rod Position Monitoring System
- RT Reactor Trip
- TGIC Turbine-Generator Instrumentation and Control
- TSC Technical Support Center
- TXS Teleperm XS

Reference Slide TXS Processing Cycle



A large, decorative graphic element consisting of two overlapping blue swooshes that curve from the left side of the slide towards the right. A large, solid blue five-pointed star is positioned on the right side, partially overlapping the swooshes. The background is a light blue gradient.

UNISTAR NUCLEAR ENERGY

**Presentation to ACRS
U.S. EPR™ Subcommittee
Calvert Cliffs Nuclear Power Plant Unit 3
FSAR Chapter 7, Instrumentation and Controls
November 15, 2011**

Introduction



- RCOLA authored using 'Incorporate by Reference' (IBR) methodology
- To simplify document presentation and review, only supplemental information, or site-specific information, or departures/exemptions from the U.S. EPR FSAR are contained in the Calvert Cliffs Unit 3 COLA
- AREVA U.S. EPR FSAR ACRS Meeting for Chapter 7, Instrumentation and Controls occurred on November 15, 2011.

Introduction



- Today Cyril Roden, UniStar - Instrumentation & Controls Supervisor, will present the Calvert Cliffs Unit 3 FSAR Chapter 7.
- Today's Presentation was prepared by UniStar and is supported by Bechtel and AREVA (U.S. EPR Supplier).
 - Tom Roberts, UniStar - Director Operations, Maintenance & Services
 - Shaun Brixey, AREVA - I&C Engineer
 - Jeremy Shook, AREVA - I&C Engineering Discipline Lead
 - Chris Doyel, AREVA - Department Manager I&C Engineering
 - Shelby Small, AREVA - I&C Engineer
 - Steve Paul, Bechtel - I&C Supervisor
- The focus of today's presentation will be on site-specific information that supplements the U.S. EPR FSAR.

Chapter 7, Instrumentation and Controls Agenda



- Chapter 7, Instrumentation and Controls
 - COL/Supplemental Information Items
- Conclusions

Chapter 7, Instrumentation and Controls

COL Information Items



- Conformance with RG 1.97, Accident Monitoring Instrumentation
 - The inventory list of Post Accident Monitoring (PAM) variables in U.S. EPR Table 7.5-1 will be confirmed upon completion of the emergency operating and abnormal operating procedures, prior to fuel load.

Chapter 7, Instrumentation and Controls

COL Information Items

New COL Item In Response to RAI 326-SER Open Item



- Reactor Power Limitation with Respect to Thermal Power
 - Following selection of the actual plant operating instrumentation and calculation of the instrumentation uncertainties of the operating plant parameters, and prior to fuel load.
 - The primary power calorimetric uncertainty will be calculated.
 - The calculations will be completed using an NRC acceptable method and shall confirm that the safety analysis primary power calorimetric uncertainty bounds the calculated values.

Chapter 7, Instrumentation and Controls

Supplemental Information

Table 7.5-1, Inventory of PAM Variables



- Site-Specific Post Accident Monitoring (PAM) Variables
 - Ultimate Heat Sink Cooling Tower Basin Level Indication
 - Meteorological Parameters
 - Wind Speed at 10 and 60 Meters
 - Wind Direction at 10 and 60 Meters
 - Vertical Temperature Difference between 10 and 60 Meters

Chapter 7, Instrumentation and Controls Agenda



- Chapter 7, Instrumentation and Controls
 - COL Information Items
 - Supplemental Information
- **Conclusions**

Conclusions



- Two COL Information Items, as specified by U. S. EPR FSAR, are addressed in Calvert Cliffs Unit 3 FSAR Chapter 7, Instrumentation and Controls.
- No Departures/Exemptions from the U.S. EPR FSAR for Chapter 7 of the Calvert Cliffs Unit 3 FSAR.
- There are three NRC SER Open Items and No Confirmatory Items.
- No ASLB Contentions.
- Responses to two RAI Questions will be submitted.
(RAI 325 Questions 07.05-1 & -2).

Acronyms

- ACRS – Advisory Committee on Reactor Safeguards
- AOO – Anticipated Operational Occurrences
- ASLB – Atomic Safety & Licensing Board
- COL – Combined License
- COLA – Combined License Application
- EQ – Environmental Qualification
- FSAR – Final Safety Analysis Report
- IBR – Incorporate by Reference
- NRC – Nuclear Regulatory Commission
- NS – Non Safety-Related
- NSC – Non Seismic Classification
- PAM – Post Accident Monitoring
- RCOLA – Reference COL Application
- S – Safety-Related
- SER – Safety Evaluation Report



Presentation to the ACRS Subcommittee

**UniStar Calvert Cliffs Nuclear Power Plant (CCNPP) Unit 3
COL Application Review**

Safety Evaluation Reports

CHAPTER 7: Instrumentation and Controls

November 14-15, 2011

Order of Presentation

- **Surinder Arora – Calvert Cliffs COLA Lead PM**
- **UniStar – RCOL Applicant**
- **Michael Canova – Chapter 7 PM**
- **Technical Staff**

Major Milestones Chronology

07/13/2007	Part 1 of the COL Application (Partial) submitted
12/14/2007	Part 1, Rev. 1, submitted
03/14/2008	Part 1, Rev. 2, & Part 2 of the Application submitted
06/03/2008	Part 2 of the Application accepted for review (Docketed)
08/01/2008	Revision 3 submitted
03/09/2009	Revision 4 submitted
06/30/2009	Revision 5 submitted
07/14/2009	Initial Review schedule milestones published
09/30/2009	Revision 6 submitted
04/12/2010	Phase 1 review completion milestone
12/20/2010	Revision 7 submitted
August 2011	ACRS Sub Committee review complete on Chapters 2 part 1, 4, 5, 6, 8,10, 11,12, 15, 16, 17 & 19

ACRS Phase 3 Review Plan



United States Nuclear Regulatory Commission

Protecting People and the Environment

FSAR CHAPTERS BY COMPLETION DATES

Chapter(s)	Completion Date	Subcommittee Meeting
8	1/6/2010	2/18/2010
4	3/24/2010	4/20/2010
5	3/22/2010	4/20/2010
12	3/19/2010	4/20/2010
17	3/12/2010	4/20/2010
19	4/19/2010	5/21/2010
10	6/11/2010	11/30/2010
11	10/30/2010	
16	10/11/2010	
2 (Part 1)	10/29/2010	1/12/2011
6	4/1/2011	4/5/2011
15	7/22/2011	8/18/2011
7 & 18	10/17/11, 10/31/11	11/14-15/2011
1, 2 (Part 2), 3, 9, 13, 14	Various	Meeting dates to be finalized

Technical Staff Review Team



- **Technical Staff - Instrumentation and Controls Branch 1**
 - **Deirdre Spaulding Yeoman**
 - **Terry Jackson**

- **Project Management Staff**
 - **Surinder Arora**
 - **Michael Canova**

Overview of COLA Review

SRP Section/Application Section		No. of Questions	Number of OI
7.1	Introduction	2	0
7.5	Information Systems Important to Safety	2	2
7.7	Control Systems	1	1
7.9	Data Communication Systems	1	0
Totals*		6	3

*Note: Open Item count does not include the Generic Open Item RAI 222, Question 01-5 which was created to track changes to the U.S. EPR Design Certification

Calvert Cliffs Unit 3

Site Specific Items

- The following are site-specific post accident monitoring (PAM) variables:
 - ◆ ESWS Cooling Tower Basin Level
 - ◆ Meteorological Monitoring System Wind Speed - 10 meters
 - ◆ Meteorological Monitoring System Wind Speed - 60 meters
 - ◆ Meteorological Monitoring System Wind Direction - 10 meters
 - ◆ Meteorological Monitoring System Wind Direction - 60 meters
 - ◆ Meteorological Monitoring System Vertical Temperature Difference - between 10 and 60 meters

Section 7.5

Information Systems Important to Safety

- RAI 325 - Open Item No. 07.05-1:
 - ◆ Site-specific systems
 - Ultimate heat sink (UHS)
 - Makeup water system
 - UHS makeup water intake structure ventilation system
 - ◆ Requested applicant to identify the safety-related I&C systems controlling these site-specific systems.
 - ◆ Requested applicant to identify the associated automatic and manual functions

Section 7.5

Information Systems Important to Safety



RAI 325 - Open Item 07.05-2

Tracks coordination of changes in the U.S. EPR FSAR regarding PAM.

U.S. EPR FSAR Tier 2, Section 7.5, needs to be a complete list with the exception of site-specific instrumentation.

Questions need for COL to update the PAMs list.

Section 7.7

Control Systems

RAI 326 - Open Item 07.07-1

- ◆ Requested design information that addresses the new COL Information Item found in U.S. EPR FSAR Tier 2, Section 7.7.2.3.5, Interim Revision 3 mark-ups.
- UniStar had not yet addressed the new COL item related to primary power calorimetric uncertainty for Calvert Cliffs Unit 3.

Acronyms

- COL – combined license
- COLA – combined license application
- ESWS – Essential Service Water System
- FSAR – Final Safety Analysis Report
- GDC – General Design Criteria
- IBR – incorporated by reference
- I&C – Instrumentation and Controls
- PAM – Post Accident Monitoring
- SER – Safety Evaluation Report
- RAI – request for additional information
- RCOL – reference combined license
- UHS – Ultimate heat sink