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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

+ + + + +

US EPR SUBCOMMITTEE

+ + + + +

TUESDAY

NOVEMEBER 15, 2011

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

SUBCOMMITTEE MEMBERS PRESENT:

DANA A. POWERS, Chairman

SANJOY BANERJEE

CHARLES H. BROWN, JR.

GORDON R. SKILLMAN

JOHN W. STETKAR

NRC STAFF PRESENT:

DEREK WIDMAYER, Designated Federal

Official

GETACHEW TESFAYE

TERRY JACKSON

MICHAEL CANOVA

JACK ZHAO

TUNG TRUONG

DEANNA ZHANG

KENNETH MOTT

DIERDRE SPAULDING-YEOMAN

WENDELL MORTON

SURINDER ARORA

ALSO PRESENT:

DARRELL GARDNER

JEREMY SHOOK

CHRIS DOYEL

DUC PHAN

SANDRA SLOAN

TIM STACK

VIC FREGONESE

MARK ROYAL

MARK FINLEY

CYRIL RODEN

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

(8:30 a.m.)

CHAIR POWERS: Let's come back in order. This is the second day of the meeting of the Advisory Committee on Reactor Safeguards US EPR Subcommittee. I'm Dana Powers, Chairman of the Subcommittee.

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

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

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

Do members have any opening comments they would like to make? You don't?

MEMBER BROWN: Do you really want me to make an opening --

CHAIR POWERS: No.

MEMBER BROWN: Okay.

CHAIR POWERS: Okay.

MEMBER BROWN: Why did you ask?

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

MEMBER BROWN: You're being polite?

CHAIR POWERS: Yes.

MEMBER BROWN: Let me get that on the record.

(Laughter.)

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

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

CHAIR POWERS: Nothing more to add?

MR. TESFAYE: Nothing more to add.

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

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

MR. TESFAYE: No.

MR. WIDMAYER: Oh, okay.

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

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

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

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

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

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

(Laughter.)

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

MR. GARDNER: Yes, that's it.

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

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

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

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

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

Just a quick background on my professional experience. I started off after a bachelor's degree at Villanova University, I went into the Navy for six years as a submarine officer. I served onboard the USS Tucson for two and a half

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

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

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

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

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

(Laughter.)

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

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

(Laughter.)

MR. SHOOK: I enjoyed it up there.

CHAIR POWERS: Who says he grew up?

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

CHAIR POWERS: Yes, more accurate.

MEMBER STETKAR: I'm sorry. Go ahead.

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

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

CHAIR POWERS: Good.

MR. SHOOK: So with that, I will go

ahead and get started on the presentation.

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

One note. There is section 7.9 which you will see later as part of the staff's review. We didn't put any information specifically in there. We included the data communications descriptions as part of 7.1 with a description of all the other systems. So you will see that.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

And so basically we are going to do here in this section is just basically lay out the systems that are involved in those different pieces. Starting with the instrumentation, you now basically most of the instrumentation in the plant is part of, from a formal system boundary perspective, part of the various process systems. For example, Reactor Coolant System, Main Steam, Feedwater, all contain instruments that are a part of those systems.

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

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

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

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

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

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

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

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

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

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

MEMBER STETKAR: Okay.

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

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

MR. SHOOK: Okay.

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

MR. SHOOK: Okay.

MEMBER STETKAR: Thanks.

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

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

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

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

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

And then we have also a small inventory

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

MEMBER STETKAR: PICS is non-safety related.

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

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

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

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

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

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

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

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

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

MR. SHOOK: Yes.

MEMBER STETKAR: Okay.

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

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

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

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

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

MEMBER STETKAR: Okay. Thank you.

MEMBER BROWN: The lines going to the RSS, are those -- You don't show the server networks going over towards to the RSS in the SICS arrangement, relative to Protection System controls limited. So are those dedicated lines or are they still coming off the servers or the ability to process?

From what I read, I didn't think any of your protection system remote stuff went through the PICS server network system. They go direct but I couldn't figure that out based on -- I was hoping that would be the case but it wasn't very explicit.

MR. SHOOK: That's correct. We'll get into more in the further sections. But the PICS cannot send signals to the protection system in SAS. We physically limit the communication to be unidirectional from the safety systems out to PICS. So in order to perform any controls associated with the protection system, we have to hard-wire directly from the SICS panels, whether it is in the MCR or Remote Shutdown Station directly to the protection system.

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

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

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

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

MR. SHOOK: We can scram the plant.

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

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

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

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

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

Are there other stations that have PICS signals?

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

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

MR. SHOOK: Yes.

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

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct, yes.

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

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

MEMBER BROWN: Could you do it from any place?

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

MEMBER BROWN: May?

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

I don't know if we know.

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

MEMBER BROWN: No.

MR. GARDNER: -- beyond the fire in some

area?

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

MR. GARDNER: Okay.

MEMBER BROWN: I just see two servers --

MR. GARDNER: Well I think what --

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

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

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

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

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

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

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

MR. SHOOK: That is correct. But they are network signals. So the server outputs are, you

know, you have both servers sending signals to all the different clients up on that top level bus.

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

MEMBER BROWN: They melt with fire.

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

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

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

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

MEMBER STETKAR: That is for the

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

MR. SHOOK: That's correct, yes.

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

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

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

MR. SHOOK: Yes, they would be. From an effect on, when you look at the design, from an effect on just the servers themselves, you know, like I have a fire in Safeguards Building 3 and the

Remote Shutdown Station -- MEMBER STETKAR: I understand that fire isn't going to burn the Safeguards Building server.

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

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

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

The question is, I heard a very positive

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

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

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

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

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

MEMBER STETKAR: Okay.

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

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

MR. SHOOK: Yes.

MEMBER STETKAR: Thanks. That helps.

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

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

(Laughter.)

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

MEMBER SKILLMAN: I do have a question, please.

MR. SHOOK: Okay.

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

MR. SHOOK: That's correct.

MEMBER SKILLMAN: Thank you. Got it.

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

MEMBER SKILLMAN: Thank you, Jeremy.

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

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

The PAS, I forgot to mention, is implemented in an industrial type of control system.

We intend to use for our first project the Siemens T3000 system. I will say that is not specified in the FSAR but in terms of our design, that is what we currently intend to use. The RCSL is, while a non-safety system, utilizes the TELEPERM XS platform, which is qualified for safety in the U.S.

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

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

MR. SHOOK: Yes.

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

MR. SHOOK: That is correct.

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

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

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

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

The third category is --

MEMBER BROWN: Does that come down through PACS?

MR. SHOOK: It does.

MEMBER BROWN: For the initiation?

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

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

MR. SHOOK: Okay.

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

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

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

MEMBER BROWN: Okay.

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

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

some band.

If for some --

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

MR. SHOOK: Yes, that's correct.

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

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

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

MR. SHOOK: That's correct.

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

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

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

MEMBER BROWN: Well, it's already running.

MR. SHOOK: Right.

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

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

But you are right. To your point, if the control valve just fails shut, if I actuate it, it is not going to make any difference, you know, if it is mechanically stuck. So depending on the

failure mode that may or not make a difference.

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

MEMBER BROWN: Please go ahead.

MR. SHOOK: Okay.

MEMBER BROWN: Thank you.

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

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

Again --

MEMBER SKILLMAN: Jeremy, just in my

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

MR. SHOOK: With regards to?

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

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

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

MR. SHOOK: Okay. Going down to the bottom level, we have two systems that are used to interface with those sensors and actuators within the plant. We have what is called the Signal Conditioning and Distribution System or the SCDS. And that is used to acquire all safety-related sensors, as well as non-safety-related sensors that

have to go to multiple systems within the DCS. So, typically these signals are related to either SBO or severe accident but the majority of non-safety sensors are wired directly to the PAS because they are just provided for control. There is no other auxiliary safety type of input.

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

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

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

And then at the very --

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

MR. SHOOK: That's correct.

MEMBER BROWN: And it will come back later and say okay, it is time to do it now because I have already done all the other things that come out ahead of it. Why in the world wouldn't you allow an operation say I do from the SICS or from wherever you want to do it, to go ahead and take action instead of saying I'm going to figure out -- I mean, because you are sending all this data in there, it has got to wait to figure out whether it is going to actuate or not? The only one that takes priority over everything is the protection system,

from what I have gathered. It goes direct, and no matter what else is going on, it will override and stop everything else.

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

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

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

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

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

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

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

MR. SHOOK: That's correct.

MEMBER BROWN: It is a combinational logic.

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

MEMBER BROWN: It's all estate type stuff.

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

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

MR. SHOOK: That's correct.

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

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

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

MR. SHOOK: At some level, yes.

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

MR. SHOOK: Yes, they --

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

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

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

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

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

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

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

MEMBER STETKAR: Jeremy, I think I understand how that works. And I certainly don't understand every valve in the entire plant but I have seen plant designs in the past where a single valve performs two different safety functions. One safety function might be to close the valve to isolate the line. Another safety function might be to open the valve to bribe closed through the line. As I said, I can't mention specific valves in this design but that is kind of a moot point. MSRTs come to mind.

The example you just mentioned where signal B, let's call it, from the protection system always has priority over the control system so that that valve, the PACS knows that the valve shall always be open because that is the most important position for that valve to be. How does PACS know

which signal is the correct signal if I have two safety signals? How do those priorities set? Who sets those priorities?

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

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

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

MR. SHOOK: Yes.

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

MR. SHOOK: No, the manual control from

either PICS or SICS comes to the PACS. So those signals get prioritized with all the other signals. What the operator has to do -- So let's say for example we have this case of emergency feedwater and I want to take manual control. What the operator would have to do is go and first re-set EFW actuation signal and if you look at the drawing, you can think of it as you have got an active signal coming in for a protection system. You are essentially just removing that signal. But in accordance with IEEE 603 requirements, the system doesn't reset once you just reset the signal. The system continues to stay in the same state. Then once you have cleared that signal, then the operator can then come in and take manual action as they see fit dictated by the EOPs.

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

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

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

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

MR. SHOOK: That's correct.

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

MR. SHOOK: Yes.

MEMBER STETKAR: Okay.

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

MEMBER STETKAR: Yes.

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

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

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

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

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

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

MEMBER BROWN: I don't remember seeing it.

MR. PHAN: No, we don't.

MR. SHOOK: Okay.

MR. PHAN: We don't discuss that.

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

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

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

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

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

MR. SHOOK: Right.

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

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

So I can't give you a specific example where I have very well defined black and white concern because I don't know enough to be able to

ask that level of question.

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

MEMBER STETKAR: Yes. Yes, I mean --

MR. GARDNER: And that is detailed --

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

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

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

MR. GARDNER: That's correct.

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

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

MR. GARDNER: You know, I think --

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

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

MR. GARDNER: Okay.

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

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

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

MEMBER STETKAR: RCP thermal barrier cooling?

MR. GARDNER: RCP thermal barrier cooling?

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

MR. GARDNER: Okay.

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

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

Essentially what I am probing is if the

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

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

MEMBER STETKAR: Okay.

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

MEMBER STETKAR: Okay.

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

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

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

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

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

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

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

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

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

MR. SHOOK: Well --

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

MR. SHOOK: Just for that particular case --

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

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

MEMBER STETKAR: Okay.

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

MEMBER STETKAR: Okay.

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

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

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

MEMBER STETKAR: It is.

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

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

MEMBER BROWN: Putting him on the spot.

MR. TESFAYE: That's my job.

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

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

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

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

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

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

issues with operating experience with regards to the EPR design, EPR I&C design.

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

MR. SHOOK: Okay.

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

I think that is what you are saying.

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

MEMBER SKILLMAN: Thank you.

MR. SHOOK: Okay.

MEMBER BROWN: Can I step up a level? A response to an earlier question -- no. In your earlier presentation, you talked about the PAS is a normal mode of plan automation controls. So steam generator control, main feed control -- I presume you are controlling main feed pumps separately in a normal manner. Is that correct? You have variable speed -- I don't know the design of that part of it. I haven't looked at. Are they variable speed main feed pumps so that you have a control system for the pumps themselves?

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

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

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

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

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

MR. SHOOK: That is correct. The main

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

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

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

MEMBER BROWN: Is there another control system?

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

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

MEMBER BROWN: That is what I was asking.

MR. SHOOK: Yes.

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

MR. SHOOK: That is correct.

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

MR. SHOOK: No.

MEMBER BROWN: That was just a side question.

MR. SHOOK: No, it doesn't.

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

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

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

own controls.

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

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

MR. SHOOK: No.

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

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

MEMBER BROWN: Okay, thank you.

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

MR. SHOOK: Well, you can --

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

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

So there is an overlap in functionality.

MEMBER STETKAR: Okay, thanks.

MR. SHOOK: Okay?

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

MR. STACK: That's correct.

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

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

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

MEMBER BROWN: Have you got that SCDS?

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

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

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

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

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

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

MR. SHOOK: No.

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

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

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

MEMBER BROWN: Keep trying, right?

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

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

If the only, once I allocate all the functionality associated with that sensor, if it is only needed in PAS, I just route it directly to PAS. That minimizes the amount of cabinets that we need for SCDS.

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

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

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

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

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

MR. SHOOK: Okay.

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

MR. SHOOK: Okay.

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

MR. SHOOK: Okay.

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

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

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

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

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

all those equipment.

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

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

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

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

MR. SHOOK: Yes.

MEMBER STETKAR: Oh, okay. Thanks.

MR. SHOOK: Just a survey.

MEMBER STETKAR: Thank you.

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

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

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

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

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

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

MR. SHOOK: That's correct, yes.

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

MR. SHOOK: That's correct, yes.

MEMBER BROWN: Thank you.

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

CHAIR POWERS: We can.

MR. SHOOK: Okay.

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

MR. SHOOK: Short break.

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

(Laughter.)

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

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

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

MR. GARDNER: I just had wanted to -- Dr. Powers wanted to revisit a question that we

earlier had on the operating experience Mr. Skillman had. And just to say on the record that we understood the question. It was the larger question of all the operating experience considered, I would say that AREVA certainly has a program that considers our international operating experience as well as operating experience here as part of our design efforts. And operating experience obviously is an ongoing program within our design organization. So, I think the larger, you know, the details of all the possible operating experiences that have been considered would be certainly something larger, bigger than we could go into in this meeting but I wanted to set the record straight. It has been considered.

MEMBER SKILLMAN: Thank you, Darrell.

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

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

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

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

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

MEMBER BROWN: What getting a compliment?

CHAIR POWERS: Yes.

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

CHAIR POWERS: Please continue.

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

Here is a list of all the reactor trip functions that are listed in part of our design and are represented in 7.2 in the FSAR. I am not going to go through these in detail again and talk about

the logic. I will say that the majority of these I would say fairly typical of what you find in operating plants, at least in my experience in looking at operating plants.

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

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

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

So here we are showing --

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

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

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

MEMBER BROWN: And is it all ranges?

MR. SHOOK: Just power range.

MEMBER BROWN: Just power range.

MR. SHOOK: Yes. Okay?

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

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

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

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

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

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

We also show on SICS the --

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

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

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

MR. SHOOK: Yes, so there is within the

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

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

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

So slide 13, we are going to talk about a little bit more. So we are going to kind of blow up those boxes we just saw in the previous slide and show a little bit more detail as far as what

components are inside those boxes and how we implement these trips.

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

So we start with the instrumentation --

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

MR. SHOOK: Except for --

MEMBER BROWN: Except for the SPNDs.

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

MEMBER BROWN: Yes, I got that.

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

MEMBER BROWN: Okay.

MR. SHOOK: Okay, so we start with the instrumentation. Again we have four redundant process measurements of each process variable that is being monitored. That signal comes into the

SCDS, is conditioned, and then distributed primarily to the Protection System but if the signal is also used in other systems, we will send that signal out to other systems, whether it be safety-related or non-safety-related.

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

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

MEMBER BROWN: So the APU generates a trip?

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

MEMBER BROWN: Particularly relative to

your figure in the DCD and in your technical report.

MR. SHOOK: That's correct.

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

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

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

MR. SHOOK: It comes on and stays on.

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

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

MEMBER BROWN: Okay.

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

each APU.

That vote to trip, then is then distributed to all the other divisions to the ALUs. And that is distributed over a network, a digital communication network and we will talk more about the means mechanisms, how that works, in the appendix and some subsequent slides.

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

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

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

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

Most of the pictures in this presentation are done using the figure legend that is in the back. I think it is right in back of the acronyms. It is actually the last slide, number 81. And what the figure legend shows is the blue color indicates that it is either electrical or electronic equipment, discrete electronics where you actually have dedicated circuits to configure the functionality. You actually have to solder the circuits together.

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

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

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

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

MEMBER BROWN: -- of stuff.

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

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

MR. SHOOK: Electronic technology or --

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

MR. SHOOK: Right.

MEMBER BROWN: -- PGAs.

MR. SHOOK: This level, I mean, you can -- When you start to try classifying this different technology, it is almost a fool's errand. But what

we are trying to show at this level is that I have got either a programmable technology and then there is two different main flavors that it is either microprocessor-based where I have this --

MEMBER BROWN: I understand that.

MR. SHOOK: Okay.

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

MEMBER BROWN: You said the ALUs -- Gee, I'm going to have to go back and look at that, too. I thought they were non-microprocessor-based. They were the -- They should have been green. That's what I understood from reading the other stuff.

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

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

MR. SHOOK: Okay.

MEMBER BROWN: My brain was ready to explode anyway.

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

And you can see that there is three signals coming in. One is the manual trip coming from the SICS. Then you have the signal from Subsystem A. One of the things I didn't show in this picture but you can see in the Chapter 7 figures, in each division, the protection system there is actually two subsystems. And that is implemented for defense in depth and diversity. So, what we do is we look at trips that implement, that are designed to mitigate the same type of event but utilize different diverse process variables.

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

And then you can see also the manual trip from the SICS goes to both the ALUs and also bypasses the ALUs to the hard-wire Or-ed. The

reason for that is there is some, 603 has a requirement that says any, when you have a manual initiation that you have to perform the same functions that are performed with the automation. And so for example we talked about isolating main feedwater reactor trip. When I trip the reactor manually, I still want it, I am required by 603 to have it perform the same functions as the automatic trip. So that is why we have to wire that signal into the ALU. But we also bypass the ALUs from a defense in depth and diversity perspective so we have a hardwired means of bypassing all the computers. That way, we can manually initiate that trip to perform the function.

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

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

MEMBER BROWN: Well they are both TXS.

MR. SHOOK: They are both TXS.

MEMBER BROWN: And they are both microprocessor-based.

MR. SHOOK: That's correct.

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

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

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

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

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

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

all the measurement signals.

MR. SHOOK: That is correct, yes.

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

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

MR. SHOOK: Right.

MEMBER BROWN: That's missing right now.

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

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

MR. SHOOK: Yes.

MEMBER BROWN: Two words and you don't

explain what it means.

MR. SHOOK: Okay. We inherited --

MEMBER BROWN: The topical report --

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

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

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

MR. SHOOK: Okay.

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

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

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

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

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

MEMBER BROWN: Oh, okay. Well that is

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

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

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

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

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

MR. SHOOK: Yes, we can get that to you. Okay, so let's go to the next slide then, looking at the SPND-based reactor trips. So the main difference with the SPND versus all the other process parameters is that in this case the process variable being neutron flux within the core is not a

homogenous process variable, meaning that it is spatially dependent upon which location you are at. So what we do here is we have 72 SPNDs located axially and radially throughout the core, measuring flux at those various locations.

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

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

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

sending those signals.

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

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

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

MEMBER SKILLMAN: So there are 72 during the which?

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

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

MEMBER SKILLMAN: Okay.

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

MEMBER SKILLMAN: Is it quadrant-symmetrical.

MR. DOYEL: Symmetrical.

MEMBER SKILLMAN: I would think the answer is yes.

MR. DOYEL: No.

MEMBER SKILLMAN: It's not?

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

MEMBER SKILLMAN: It's not accurate.

MR. DOYEL: It is not accurate.

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

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

MR. SHOOK: They are.

MEMBER SKILLMAN: Oh, they are?

MR. SHOOK: Yes.

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

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

MEMBER SKILLMAN: Twelve or 18?

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

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

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

MR. PHAN: -- in our documentation.

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

MR. SHOOK: That's right.

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

MR. SHOOK: Right.

MEMBER BROWN: One string.

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

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

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

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

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

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

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

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

implemented in one out of two, taken twice logic.

Down below, we have the trip contactors. Those again those are located within the CRDCS system and those are implemented in a two out four, straight two out of four logic.

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

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

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

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

MR. SHOOK: That is correct.

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

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

channels for the breakers the contactors will.

MR. SHOOK: That's correct.

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

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

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

MR. SHOOK: They are both safety grade.

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

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

MR. SHOOK: Okay, yes.

MEMBER BROWN: So you can go on.

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

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

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

I would be fairly limited in terms of the operability from a tech spec perspective. So having the two ALUs allowed me to take one out of service. The other one is still operating in much more greater operational flexibility from that perspective. And all your voting is two out of four.

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

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

In this case, we were monitoring a spatially-dependent variable neutron flux inside the core. You know, the benefits of doing this design are that anytime you can measure more closely the parameter of interest that you are interested in is better, both from a safety and an operational perspective. And one of the things that

specifically Clause 6.4 of IEEE 603 says that you should do that because again, that is just good design practice. And also from a margin standpoint and a safety standpoint allows you to move a lot of the uncertainties and assumptions that are baked into a traditional safety analysis when you only can look at Excore instrumentation.

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

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

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

MR. SHOOK: No.

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

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

MR. SHOOK: Yes, that's correct.

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

MR. SHOOK: That's correct.

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

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

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

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

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

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

MEMBER BROWN: How did you demonstrate that?

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

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

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

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

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

MEMBER BROWN: All right. Fire away.

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

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

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

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

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

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

MEMBER BROWN: Oh, out of the SCDS.

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

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

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

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

MEMBER BROWN: Okay.

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

MEMBER BROWN: And then you are going to

division to division.

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

MEMBER BROWN: Go ahead.

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

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

So in this case, sending the signal to the PAS is, we do that via hardwired interface because again at this point everything is hardwired four to 20 outputs. And to provide for independence, we implement physical separation. So the PAS cabinets are physically separated from the

Protection System cabinets. The non-safety cable is separated from the safety-related cable. And for electrical isolation, the distribution module itself has up to four isolated qualified outputs. So a failure of the non-safety system from an electrical perspective can't come back into the SCDS and impact its operation.

MEMBER BROWN: Those are analogue outputs?

MR. SHOOK: That's correct.

MEMBER BROWN: This is all analogue at this point.

MR. SHOOK: This is all analogue.

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

MR. SHOOK: That's correct.

MEMBER BROWN: -- and wherever they go.

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

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

MR. SHOOK: We committed in the FSAR to

meet the requirements at EEE 384, which defines the separation and independence requirements for specific, the details of the electrical, you now, how much separation you need in voltage qualification and so forth.

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

MR. SHOOK: Right.

MEMBER BROWN: Those are easy to isolate.

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

MEMBER BROWN: From a physical separation?

MR. SHOOK: Yes.

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

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

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

CHAIR POWERS: Chris has some comments.

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

MR. SHOOK: Which is 384.

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

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

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

MEMBER BROWN: That's what I thought.

MR. SHOOK: Yes.

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

MEMBER BROWN: I have no idea what those are.

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

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

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

I mean, you ought to have some idea of what these -- if they have got these, you ought to

know what it is and if you are not going to specify them. If you specify them, then you know what you are getting. If you don't, then you don't.

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

MEMBER BROWN: Go on.

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

When we do connect it, whether for

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

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

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

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

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

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

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

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

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

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

MR. SHOOK: Okay. Okay, next slide.

So this is our PICS interface. So, you

know again this is where the operator would be spending most of their time. And here it is again the same basic purpose as the QDS. We want to send information from the Protection System to the PICS for the operators awareness of what is going on in the Protection System. It is a data interface and it is the same basic means of providing independence as we just showed for the QDS. So in this case the only difference is we have gateways in the middle. But the gateways are not credited for independence. It is actually the electrical optical converters with the fiber optic cable and the transmit only path from going out from the MSI to the gateways that is connected and provide for independence.

Okay. Slide 22 is the independence between redundant divisions, specifically at the APU to ALU interface. So this is the only point in the design that we share information between divisions. The purpose is to send reactor trip votes from each division's APU to all four divisions' ALUs to allow for voting.

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

we showed in the Section 7.1 figure. They are physically separated into four different buildings. The electrical isolation, the connections on these networks are done via fiber optic cable. So you know, any electrical fault won't transmit to the other division.

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

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

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

So the main points for which we use to credit communications independence, first of all we

separate the processing of the safety function versus the communications processing via the network, so you can see that the SL21 is performing all the communications functions; whereas, the SVE1 is performing all the actual logic, whether it is the setpoint comparison two out of four voting.

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

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

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

And then lastly there is the token

passing principle. So these networks are implemented using a PROFIbus network or protocol.

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

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

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

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

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

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

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

MEMBER BROWN: On or off?

MR. SHOOK: Yes.

MEMBER BROWN: It's like a dry contact.

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

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

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

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

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

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

So I dropped that thought process based

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

MR. SHOOK: Let me address that.

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

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

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

MR. SHOOK: Right.

MEMBER BROWN: It's not data isolation.

MR. SHOOK: Right.

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

MR. SHOOK: Right.

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

MR. SHOOK: No, we are not saying that. What we are saying is that the mechanisms that are inherent in the platform allow for compensation, compensatory measures that will handle that type of --

MEMBER BROWN: That's what I just said.

MR. SHOOK: Right.

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

MR. SHOOK: Well I mean --

MEMBER BROWN: Your data transmission.

MR. SHOOK: Yes.

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

MR. SHOOK: That's correct.

MEMBER BROWN: And that's a hard spot.

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

MEMBER BROWN: I understand that.

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

is then --

MEMBER BROWN: I understand that. Okay? I understand that but you can't guarantee that it will not be corrupted and not be detected. You can't guarantee that it can be detected.

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

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

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

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

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

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

corrupt data packages.

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

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

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

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

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

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

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

MEMBER BROWN: Sure it is.

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

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

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

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

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

MEMBER BROWN: That's the input.

MR. SHOOK: Right.

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

MR. SHOOK: No, no.

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

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

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

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

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

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

MR. SHOOK: Right.

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

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

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

MR. SHOOK: It's discussed in the PS

Technical Report.

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

MR. SHOOK: Okay.

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

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

MR. SHOOK: Right.

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

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

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

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

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

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

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

MR. SHOOK: Okay, fair enough.

MS. SLOAN: Let's follow-up.

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

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

MR. SHOOK: Okay.

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

MR. SHOOK: Okay.

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

a different issue.

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

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

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

MR. SHOOK: Okay.

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

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

MEMBER BROWN: It is a fundamental point.

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

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

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

MR. SHOOK: And that's true.

MEMBER BROWN: I think you said that in there.

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

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

MR. SHOOK: In terms of --

MEMBER BROWN: Two parts of that.

MR. SHOOK: Okay.

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

MR. SHOOK: Okay.

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

MR. SHOOK: Right. Yes --

MEMBER BROWN: Without waiting.

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

MEMBER BROWN: Okay. You can go on now. Thank you.

MR. SHOOK: Yes, we can address that.

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

MR. SHOOK: Okay. So, okay good.

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

So as you can see here, we have the purpose again is to send 18 SPND signals from one division of SCDS to all four divisions of the PS. It is a hardwired interface. The input coming in and going out are both four to 20 milliamp signals. So there is no data communications here at this level.

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

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

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

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

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

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

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

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

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

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

Based on the TELEPERM XS platform design, there are two key aspects that allow us to demonstrate a deterministic response time behavior. The first is that the application software operates on fixed cycle intervals. Like I said, once you establish that frame rate, whether it is 25 milliseconds or 15 milliseconds, the processor will always operate at that cycle speed. It is not like your Windows computer which is an event-based system which it will start executing something based on a trigger, an external trigger.

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

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

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

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

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

MR. SHOOK: Yes.

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

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

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

MR. SHOOK: That's correct.

MEMBER BROWN: -- within some predetermined time period.

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

MEMBER BROWN: Okay, I was looking at --

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

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

MR. SHOOK: This is actually showing

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

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

MR. SHOOK: That's correct, yes.

MEMBER BROWN: Okay, that's --

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

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

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

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

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

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

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

Then step three is essentially then activating your activation software. Okay? So now that I have got my input data for that frame, then I go through and execute the application logic with that input. So all that input data is put in the memory and I execute the various functions, you know, the comparing inputs, the step points, the so forth on step three and four.

And the output of step five is that all the outputs of my function diagram so then are put back into memory and then are available for sending the output through a hardwired I/O card or a communication module.

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

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

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

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

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

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

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

don't really --

MR. SHOOK: I'm not sure.

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

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

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

MR. BRIXEY: Yes.

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

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

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

MR. WIDMAYER: Eleven.

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

MR. SHOOK: Yes.

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

MR. SHOOK: Not necessarily.

MEMBER BROWN: Okay.

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

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

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

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

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

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

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

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

MR. WIDMAYER: You locked up.

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

MR. BRIXEY: These don't all exist on

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

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

We've got multiple APUs.

MR. SHOOK: That's correct.

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

MR. SHOOK: That's correct.

MEMBER BROWN: Each APU.

MR. SHOOK: Yes.

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

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

MEMBER BROWN: No.

MR. SHOOK: I'm sorry.

MEMBER BROWN: You're going to confuse me.

MR. SHOOK: Okay.

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

MR. SHOOK: Okay. Go ahead.

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

MR. SHOOK: Yes.

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

MR. SHOOK: That's correct.

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

stuff.

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

MEMBER BROWN: Every time.

MR. SHOOK: Yes, that's correct.

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

MR. SHOOK: No.

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

MR. SHOOK: No, no.

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

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

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

MR. SHOOK: And just to make a point,

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

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

MEMBER BROWN: Why is there three and two subsystem?

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

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

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

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

MR. SHOOK: No. Essentially what you will have is when you take this whole list of functions here, you will first allocate these to A and B, depending on the functional diversity aspect. Again like so for example high core power level is a diverse trip to load DMBR. So I am going to put one on one subsystem and one on the other.

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

MR. SHOOK: Exactly.

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

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

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

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

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

MR. SHOOK: Yes.

MEMBER BROWN: Okay, thank you.

CHAIR POWERS: Mr. Stetkar can't help but know that this system is only partly American.

MEMBER BROWN: Only partly what?

CHAIR POWERS: It's kind of like a behaviour. It reflects its European origins.

MEMBER BROWN: Oh, yes.

MR. SHOOK: This is actually a test to see if you noticed.

CHAIR POWERS: We also noticed that CRC is not in your list of acronyms.

MR. SHOOK: Oh.

CHAIR POWERS: Got you!

MEMBER BROWN: Dana, everybody knows what that is.

CHAIR POWERS: Two out of four logic shows that not everyone knows it.

MR. SHOOK: Okay, so moving to slide 26. Here we are talking about the fail-safe behavior. And we have already kind of talked about a piece of this but we will just kind of walk through the whole system.

You know, basically we started with a sensor, signal conditioning and distribution failures. If we have an out of range failure, that is detected by -- that will be detected by the APU. And the reasons for that is for generally most of the inputs are four to 20 milliamp signal input so we use the live zero failure detection mechanism. So if I have a short circuit of zero current. I'm sorry -- A short circuit will be greater than 20 milliamps. An open circle will be a zero. That gets configured within the APU. When I bring that signal in, in terms of defining an out-of-scale high or low range. And if the system detects and out of scale high or low, the system flags that message and when that message is then used in all the subsequent downstream logic, particularly when it gets to the voting, it modifies the voting logic. So if I detect the single sensor failure, I actually modify the voting logic to two out of three, which this is

improvement over analogue systems because I am still satisfying my single priority criteria but in an analogue system, I would be one further sensor failure away from reactor trip. Whereas here, I am at two out of three. So I have reduced the probability of a spurious actuation.

If I have two sensor failures, we modify to a one out of two logic and then three or more sensor failures, we fail to the safe state. In this case, the reactor trip.

In range failures are not detected but obviously those are covered by your single failure analysis.

MEMBER BROWN: So if a pressurizer pressure sensor fails low, it would go to zero and you all would ignore it.

MR. SHOOK: Well, we would modify the voting logic in accordance with these rules. So we wouldn't ignore it. I mean, we would ignore it but modifying the voting logic.

MEMBER BROWN: If one sensor goes, you are requiring -- You still are then two out of three buys two out of four logic.

MR. SHOOK: That's correct.

MEMBER BROWN: So you are effectively ignoring it then, as opposed to generating a trip with it.

MR. SHOOK: That's true. That's correct.

MEMBER BROWN: Okay.

MR. SHOOK: Okay. When look at going down to ALU failures, the ALU outputs are designed to fail low. And a low, a zero signal out of the APU results in a reactor trip signal to be actuated. And then the same with output logic circuit failures. So failures anywhere downstream of the ALU or APU result in a fail low reactor trip actuating signal.

Slide 27. So a little bit more kind of meat on the fail-safe behavior with regards to the APUs and ALUs. There are four main features that allow us for fail-safe fault detection. Then you can configure the system to fail to a safe state. In this case, reactor trip is actuated.

First of all we have the self-monitoring of the function processors. As we talked about before, once I finish all the function diagram processing and I release that primary thread, I will

do self-monitoring to do different memory checks and so forth.

We also have a CRC check sub-monitoring of the software. This is actually more -- This is done during the extended self-test when we reboot the processor. It checks to make sure it is the same software version.

Here we also have the hardware-based watchdog timer, which we have already discussed and we will get you some information on the details of how that operates.

And then lastly, we talked about already the data messages going between the APUs and the ALUs utilize a checksum as well as a sequence number. So the receiving processor will look at the checksum of the sequence to make sure it is a valid message before processing. If it detects it, it is an invalid message and will then modify the building logic.

MEMBER BROWN: A question I didn't ask on your processing of the --

(Simultaneous speakers.)

MEMBER BROWN: -- cycle. Do you have a monitor, independent monitor that looks for short

cycle, like in other words if a sample period doesn't go for its full 50 milliseconds or if it goes in overtime?

MR. SHOOK: I don't know that.

MEMBER BROWN: Probably the short cycle is of more interest. I was just curious as to whether you do that or not. In other words, if it goes short cycle, you may not do some stuff that you may have -- In other words, you have skipped something.

For some reason, you know, your software has skipped through. Don't ask me how. It was a concern of ours years ago and we typically look at that.

MR. SHOOK: Okay.

MR. BRIXEY: So the watchdog is what we use for watching the long cycle. The short cycle I can't think of anything off the top of my head that we are using to monitor for short cycles or how it would happen. So I will look for an answer for that.

MEMBER BROWN: I mean, the watchdog has to get triggered by the end of function cycle. I mean, this trip is it supposed to trigger it and say

don't pay any attention. I'm going back to start over again.

MR. BRIXEY: Yes.

MEMBER BROWN: Okay.

MR. SHOOK: Depending on the particular failure mode, there could be some mechanism that will detect that. For example, if you didn't complete all the function diagram processing and that message didn't get updated with the next sequence counter, the receiving processor will then detect that and then modify its logic.

MEMBER BROWN: That update is not based on a change of the output but it just didn't get updated.

MR. SHOOK: Right.

MEMBER BROWN: That's what you are talking about.

MR. SHOOK: Right. So again, that is one potential failure mode where it would get detected. But without kind of going through all the details, it is hard to say exactly how that would operate.

MEMBER BROWN: Okay, thank you.

MR. SHOOK: Okay, then the last slide

for reactor trip, next slide is 28.

And this is just showing the various surveillances on how we test the various pieces of the entire string of the reactor trip function. We start with the calibration. We calibrate the detector. We essentially do a calibration check of the detector and then make sure that the scaling factor in the APU matches the calibration. We have sensor operational tests that will basically check the input circuitry starting with the SCDS into the APU. We have the continuous self-test. It is shown to go up to the sensor. The continuous self-test is only being performed on the TXS processing units, the ALUs and APUs. The reason why we show it all going over these sensors that the self-testing will detect failures, upstream failures coming into the system, based on whether it is out of range high or low.

Once we get within the APU and ALU, we rely on the continuous self-test, as well as the extended self-test. The extended self-test basically is once every 24 months you have to reboot the processors and it will check certain things about the processor operation that can't be tested

in a continuous self-test.

Then we have the ADOT which checks the outputs from the ALU all the way through the trip device. And then we also have setpoint verification on the APUs, as well as the calibration. It is not quite shown very clearly but really that other calibration on the other side is to check the manual trip, the operation of the manual trip switches from the Main Control Room and RSS into the ALUs to the hardwired Or gates.

And then lastly, we have a response time check to check the response time of the whole loop.

Okay. So moving on to ESFS. For the topics, we are going to discuss the same topics. In the cases where the topics are the same as the protection system, I will just note that or as for the reactor trip, I will just note that and then we will move on and not spend too much time rehashing the same information.

Starting with Slide 31, we have a listing of all your ESFS functions. And where is the -- Mr. Stetkar, one thing I wanted to point out here is we do have an automated steam generator isolation function for the tube rupture event. I

will just give you --

MEMBER STETKAR: Yes, okay.

MR. SHOOK: -- a quick background. The reason is in Europe they analyze multiple tube ruptures as part of their design basis. So the event progressed quickly enough that they automated the function because they needed action within 30 minutes. And we analyzed it for the U.S. We analyzed the single tube rupture as part of the design basis and the event didn't progress quickly enough. So that is why there is not manual operator action, Chapter 15. However, we did retain the automated function because in reality you may have more than one tube rupture. So the automated is still there. It is just not credited.

MEMBER STETKAR: But it is only the isolation. It is not the cooldown and depressurization that is implemented in Europe.

MR. SHOOK: No, we still have that as well, the partial cooldown.

MEMBER STETKAR: Well you have the partial cooldown for any --

MR. SHOOK: Right. Right. So the steam generator isolation, that function is the same as

what is in Europe.

MEMBER STETKAR: Okay.

MR. SHOOK: And I guess my point is it does use the N16 detectors as an input to help detect that.

MEMBER STETKAR: Oh, okay.

MR. SHOOK: Yes.

MEMBER STETKAR: I must have missed that. So, thanks.

MR. SHOOK: Okay. Other than that, these are the functions. And I'm going to guess that the differences that I have already been talked about in various different chapters. So I'm not going to spend too much time on these. These are the ESFS functions.

Moving to slide 32, these are the ESF control functions. And I will say these are what is currently listed in the FSAR. We have an ongoing open item with the staff that will be modifying this list but this is what is being presented here today as far as the current design.

We have the emergency feedwater level and control and flow control, which we discussed and then also the MSRT control.

Okay, slide 33. We are showing here again the allocation of these functions within the DCS. The signal input path is the same. We have safety related sensors coming in through the SCDS to be distributed out. And those signals are distributed either to the Protection System, if it is an actuation function or to the SAS if it is a control function. Both the PS and SAS send outputs out to the PACS. As a general rule, actuation always has priority over controls so the Protection System outputs without priority over the safety automation system.

And then you see on SICS in the Main Control Room, we also have system level means of actuating the actuation functions as well.

And again I apologize, I missed the shading but we also have controls for the SAS for the control function as well on SICS in the Main Control Room.

MEMBER STETKAR: Jeremy, just before, because I am more linear and worse than Charlie is in terms of being able to hold a thought. Do you remember where in the DCD that N16 signal for steam generator isolation is described?

MR. SHOOK: We talk about it in Section 7.3. We show the logic for that.

MEMBER STETKAR: Okay, 7.3.

MR. SHOOK: Yes.

MEMBER STETKAR: Okay. I just did a quick word scan and I didn't see it. I will look for it. Thanks.

MR. SHOOK: Okay. And then we also show here at the bottom we have safety-related actuators which are sent signals from the PACS as well as also the turbine generator I&C which is a turbine trip signal from the protection system.

Okay, going to slide 24 for the design ESF actuation. Basically the SCDS and Protection System implementation of these functions is the same, as for reactor trip. So there is really no need -- Well actually, so let me, there is one difference.

We only implement functional diversity for reactor trips. We don't implement functional diversity for ESFS. So the ESFS essentially gets assigned to whatever subsystem is most convenient from the sizing or the signal routing perspective. And the other key difference here is the output of

the ALUs are Or-ed instead of And-ed.

And let's see what else we have here. And then the main difference is at the bottom. With the reactor trip there is no PACS associated with reactor trip but here we have signals coming from the Protection System into the PACS, as well as prioritizing with other signals coming from other systems. So you can see there that we have hardwired signals coming into the diversity module -- sorry. Excuse me -- the Priority Module from the SICS. Those would be your manual commands. Component level commands go into the PACS, as well as automated ESFS actuations from DAS and automated control functions from SAS.

Also SAS, if we threw the EOP development and task analysis and so forth, if we find that there is a post-accident manual action that we want to -- we use the term manual boot command. So if there is a manually initiated sequence, that would be performed in SAS and then come through that path as well. An example of that would be going to hot leg recirc and following the LOCA.

So then we come down to the PACS. And

you can see there that the Priority Module is implemented.

MEMBER BROWN: Before you get to the PACS, okay, you come down -- I understand what you are doing as you go through the cycle here. You come down, the Or goes off and hits the Priority Module and does something. But you were just talking about there is another arrow that goes off the SAS, PAS, TG, I&C, and such and such.

MR. SHOOK: Okay.

MEMBER BROWN: Are those -- SAS you have already said. Once you actuate something then the SAS takes over for the control, if it has got an automated control function.

MR. SHOOK: That's correct.

MEMBER BROWN: Under the ESFS function, it does the control work.

You send a signal to PAS. Does that turn off the other system? I mean, what is the -- Is there a reason for that to go over there?

MR. SHOOK: There is --

MEMBER BROWN: I mean I take it this is just an electronic signal like an on/off switch.

MR. SHOOK: Yes. It is just, basically

you are going to send that signal to PAS. There is a couple of -- I would say there are two main categories of why I would send that to PAS. One is specific to the partial cooldown function. So with the partial cooldown, the basic idea is there is no high-head safety injection in the plant. So I need to cool down and depressurize the primary to the point where I can get medium head safety injection pumps to come down below the shutoff head so I can provide water into the primary.

There is two ways that is done. There is the preferred way and then the safety credited way. So the preferred way is to use the turbine bypass valve to actually perform that cooldown function. And so to initiate that, --

MEMBER BROWN: You use bleed steam.

MR. SHOOK: -- we just bleed steam around the turbine to the condenser. And so now it is important to note that is preferred but it is not credited in the safety analysis. Okay?

So the PAS, we send a signal to the PAS to initiate that close of control for the turbine bypass valve. Now for some reason if that fails to operate properly because it is non-safety, your

MSRTs are your safety grade credited means of performing partial cooldown.

MEMBER BROWN: And that is the RT?

MR. SHOOK: The Main Steam Relief Train.

MEMBER BROWN: Oh, train. Okay.

MR. SHOOK: Right. You relief. Essentially it is your relief valve of the steam generators. And then that control is done within the SAS.

So that is sort of a unique function in the EPR.

The other more general category is if there is operational systems that need to know that an ESFS has occurred to put them in a state that is more amenable to sort of post-accident. You know, once you remove your ESFS signal. For example, and we haven't done a lot of the detailed design yet to give every single list of specific examples but for one example would be isolate main feedwater. Okay? And normally I have got the control valve in an automated loop. I am probably going to want to just kick that loop to manual, once I have the feedwater isolation signal sent. Because when I restore main feedwater, I don't want to start coming back in

automated mode. So that is one example of why you would send those type of ESFS signals. But is basically just so that non-safety, any non-safety controls associated with that actuated equipment knows that an ESFS has occurred and you can do -- You can then do whatever logic you need to do to make the plant recover make a little bit more sense for the operator.

Does that answer your question?

MEMBER BROWN: Yes, I think it does.

MR. SHOOK: And then turbine generator --

MEMBER BROWN: I liked the example you gave.

MR. SHOOK: Okay. And then the turbine generator I&C is for turbine trip.

Okay, and then we come down to the PACS. So again we have the signals from the Protection System as well as the other systems. And then we have the Priority Module. The Priority Module is, as we discussed before, it is a Programmable Logic Device, PLD, that is subject to 100 percent combinatorial testing to basically preclude consideration for common cause failure for that

device. And we will talk a little bit more about that in the 7.8 when we talk about D3.

We also have a Communication Module, which allows us to interface the PAS because we want all the nice features and functions for the operator using on the PICS as a modern type of HMI. So we provide that pathway as well.

And then we have the output of the Priority Module interface to the switchgear in the actuators themselves.

And in general, the general priority which is established in the FSAR, the Protection System and DAS are implemented essentially at the same level priority. Okay? And the reason for the DAS being at the same level of priority is because the DAS is essentially a functional substitute for the protection system. So while the DAS is technically not a safety-related system, I can't have the DAS be a lower order of priority than the SAS or the SICS because it just functionally wouldn't work properly. You know, that would mean that your EFW closed-loop control would have a higher priority over the non-safety DAS, EFW actuation, which just doesn't make any sense.

So the PS and DAS have the same level of priority and we provide for independence measures coming from the DAS to make sure a failure doesn't affect the PACS.

And then so the PS and the DAS are basically equivalent and then we have SAS for control, being the next level of priority. Then we have the SICS being the next level of priority. And then lastly the inputs from the PAS are the bottom priority, coming from the communication module.

Okay, any more questions on this before we move to the next slide?

MEMBER BROWN: Yes. I'm still puzzled on the priority circumstance. I mean, if you want two or three to actuate or to be responded at the same time, why can't you do that? I mean, that is -- We did that. I don't remember seeing Priority Modules or priority methodologies in some of the more conventional plants. I mean, we had time-delayed relays that trigger certain things starting on the switchgear so you didn't unload it or overload it but that was about it. I mean, if you were -- I mean, I could trigger the fill system and I could trigger the scram and I could trigger a feed

operation. I could trigger every one of them simultaneously and I didn't worry about they would all operate. They didn't wait for somebody else to tell them it was okay or finish some other operation first.

So is there a plant basis for doing this? I mean, is there some -- or is just because you have only got -- Are all these Priority Modules -- Is there only one Priority Module for the whole first division that deals with every one of the systems that is covered by Division 1?

MR. SHOOK: No. Each actuator gets its own pair of priority and communication modules. So like let's take the EFW pump, for example. It has the pump itself has a Priority Module and Communication Module. And so each actuator gets its own pair.

You know, I would say two main reasons why you have -- Actually, Shaun if you could go back to slide 33. The two main reasons why you have to do priority as opposed to some of the naval plant designs, first of all is I am providing two manual control stations in both of our control locations, Control Room and RSS, so the operator can manually

control the plant either from PICS or SICS. So as a first basis, I have got two manual paths I have to prioritize, I have to deal with. And then the second piece is --

MEMBER BROWN: Why? Somebody operated something from the SICS? Why can't you just operate?

MR. SHOOK: Well you know, again --

MEMBER BROWN: I've got two -- Just a simple example. I've got a switch over here that will start a pump and I've got a switch over here that will start the pump. They are in parallel. Turn one, it start. Turn the other one, it starts. As opposed to well, gee, I haven't figured out whether I want to allow this one to do it or not. Is there a reason for not wanting to allow the SICS not to do it if you can do it from the PICS?

MR. SHOOK: I would say the main -- Well at some point you have to choose because the operator can turn the pump on or off from both locations. Right?

MEMBER BROWN: Yes.

MR. SHOOK: So at some point once you get to the switchgear, there is only two signals

going to the switch gear on or off. Right? So you have to have some -- If you provide on/off capability from two locations, there has got to be some gatekeeping because going to the switchgear I only have two signals.

MEMBER BROWN: I can turn it off and turn it on from both places.

MEMBER STETKAR: Let me interject. One of the things that I mentioned about three hours ago was that some of the things that I came across in terms of human factors engineering and just design of the system that sort of relates to the conversation is statements in the FSAR that say if an operator begins using SICS, it has priority for safety-related components, which means that this Priority Module says that if I push a button in SICS, the Priority Module knows that that is the right thing that is supposed to happen. Is that true?

MR. SHOOK: That's true.

MEMBER STETKAR: Even though that might not be the right thing?

MR. SHOOK: Well, you know, again --

MEMBER STETKAR: It always knows that

SICS is perfect and PICS is not.

MR. SHOOK: I mean within the design, because we have provided the capability to control safety-related equipment from PICS, we want the safety systems to take priority -- SICS priority to take over that.

MEMBER STETKAR: The safety systems are always perfect and non-safety systems are never perfect.

MR. SHOOK: Exactly.

MEMBER STETKAR: Okay.

MR. SHOOK: So I mean for example, we could postulate. You could postulate control system failure. That would be sending an antagonistic signal to the PACS, at which point you want to be able to make sure you can deal with that situation. Okay?

MEMBER STETKAR: If you have a faulty signal from SICS, there is no way that PACS -- that PICS --

MEMBER BROWN: That's right.

MR. SHOOK: That's correct.

MEMBER STETKAR: -- can compensate for that.

MR. SHOOK: That's correct.

MEMBER STETKAR: The thing is going not block.

MR. SHOOK: That's correct but again, in that case, the Protection System is going to win over anybody else. So --

MEMBER BROWN: What do you mean? Which Protection System? If the SICS blocks something but it is not actuating it --

MR. SHOOK: Well again, the SICS is just a hardwired panel. So if the operator goes to SICS and says you know, to give you an example, emergency feedwater, if the operator says okay I want to go close those valves, if I close the valves and then the level starts to drop, the Protection System is going to say well I don't care what you want to do operator. I am going to go and re-actuate and open these valves back up.

Now, ultimately the operator can still reset the signal, in which case you have then defeated the automation. But then that is controlled through EOPs and operator training and so forth.

So at the end of the day, we still give

the operator the capability to do what they need to do but we have built in some measures of checks and balances so that it is not necessarily, you know, you have to -- there is a thought process that has to be involved with those actions.

MEMBER STETKAR: Resets of hardware or software?

MR. SHOOK: The actual --

MEMBER STETKAR: I understand the button is --

MR. SHOOK: The reset is done within the ALUs.

MEMBER STETKAR: Okay. So you could get software faults that would spuriously reset signals on you.

MR. SHOOK: I mean, we don't think that is likely but yes.

MEMBER STETKAR: Don't use the word lightly with me.

MR. SHOOK: I'm sorry.

MEMBER STETKAR: Two words you don't want to use here are likely and probability.

MR. SHOOK: And so that is the first thing we have is manual control from two locations

and then we also have control of if we have actuators that have what I call shared functions. So let's take the main feedwater control valve for steam generator level. That has both an operational and safety function. So the operational function is to maintain level during normal operations, during control some band during normal operation. And then there is a safety function that says to isolate main feedwater. So that valve has to go close.

Because I could have a feedwater control system failure that leads to me needing to isolate main feedwater, that safety function has to have priority over the control function.

So generally any actuators that have shared purposes, and there is not a lot in the plant but there is some and that is an example, then I have to make sure that that safety function always has priority over the control function.

MEMBER STETKAR: Let me ask you a question that came up yesterday and since we are kind of delving into this area of priorities, emergency service water system has a flooding protection logic that isolates emergency service water and trips the pumps on high level in

safeguards building sumps. Does that signal override the safeguard signal to start the pumps and open the valves?

MR. SHOOK: So the answer is the ESF actuation would override that signal.

MEMBER STETKAR: It will.

MR. SHOOK: Yes.

MEMBER STETKAR: Definitely?

MR. SHOOK: Yes.

MEMBER STETKAR: Okay, thank you.

MR. SHOOK: Based on the criteria that we currently have laid out in the FSAR.

MEMBER STETKAR: No, that's -- It was either going to be yes or no or I don't know.

MR. SHOOK: Okay.

MEMBER STETKAR: Thanks. Thank you.

MR. SHOOK: Okay, so --

MEMBER STETKAR: That's the type of question, by the way when we are talking about these priorities that the reason earlier I said that if that information is available, and obviously it is, I think it is very useful information, at least for the staff to have in their hands.

When I asked yesterday, everybody failed

open. They said well I have to ask the I&C folks because the people who know the pumps and pipes and valves don't understand all of this signal stuff.

MR. SHOOK: Right.

MEMBER STETKAR: So I figured well I'll ask the I&C folks today but that's why I am sort of interested in that integrated priority.

MR. SHOOK: Right.

MEMBER STETKAR: It demonstrates sort of a philosophy, if you will, of the design.

MR. SHOOK: Yes, I mean we basically, with an I&C we have established this overall philosophy and I would say all of the functions we have today follow that. But with the detailed design, there is a particular case where there is a --

MEMBER STETKAR: The problem is yesterday people were focused on my god you don't want flooding in the safeguards building because if it is high enough it could potentially affect two redundant divisions and that is really bad so you want to be really, really careful that you get that isolation. Well, okay that is good if you are centricon flooding. On the other hand, if you want

to keep diesel generators cool or if the flooding has occurred from not ESWS, it might not necessarily be a good thing to such down your Emergency Service Water System. So those are the sort of trade-offs that I, in particular, are interested in seeing.

MR. SHOOK: And again, you know, I mean because once you get in the scenarios, it is very specific to what the actual failure --

MEMBER STETKAR: Absolutely. There is never a perfect solution.

MR. SHOOK: But you know, again with the system design, I can go and reset SI, which is what is going to start your ESW. The system will keep operating but I could go and isolate those particular portions if the operator chose to do that.

That's what you are looking for?

MEMBER STETKAR: Yes.

MR. SHOOK: Okay. Yes, the system is designed with that capability.

Okay, so slide 35, we are showing the EFS control. So we have the same top-end input. We have the sensors and SCDS. And then we have the signal input to the SAS. The SAS is designed

differently than the protection system is assigned as a control system. So we have essentially redundant control units within teach division. And then again, the number of control units is determined by the sizing of the system in terms of the amount of I/O and function processing that is required.

The network design we have got, we do have interdivisional communication. Not all functions with the SAS require interdivisional communication. It is on a function-by-function basis. And actually the control function shown here in 7.3 do not require individual communication. They are all straight up and down -- I'm sorry -- except for the partial cooldown MSRT control, we look at four divisions of MSRT position. So there is some interdivisional communication there. But in terms of actual level control and flow control and pressure control loops, those loops themselves are all straight up and down, you know, one sensor to one valve.

Yes?

MEMBER BROWN: When I look at 34 and 35, 34 says I have got a Protection System and there is

an ESF actuation system that gets processed pick a division, Division 3, whatever it is. It goes to Priority Module. It says turn this actuator on/off, open and close the valve, whatever it is. That is what it says. To actuator Division 3. That is on slide 34.

Slide 35 says now I have got the same data coming to the SAS system.

MR. SHOOK: From the SCDS, you mean?

MEMBER BROWN: Yes, well it says SCDS Division 3.

MR. SHOOK: Sure.

MEMBER BROWN: The signal comes into SAS.

MR. SHOOK: Yes.

MEMBER BROWN: And then the SAS goes to these little things called CUs, control units, and they generate an Or, which I presume open or close the same actuator.

MR. SHOOK: That's correct.

MEMBER BROWN: So there is two paths here for automatically operating that actuator. Is that correct?

MR. SHOOK: Well you know, again -- Yes.

But the PS is your actuation path. So the Protection System is going to -- Like let's take EFW. When I actuate EFW -- Let's go back to the previous slide, Shaun.

So emergency feedwater, I am going to look at I have got four steam generator level sensors per steam generator. Those come into the APUs get paired to sub-point. I share my information between the networks, do two out of four voting and then basically train one, a VFW gets actuated out of Division 1 of the Protection System through the PACS. Okay?

Now that is just the actuation. So out of the PS I will essentially get a one, a logical 1 and then that starts the pump and opens the isolation valve and the control valve.

Now at the same time I send a signal from the PS to SAS to initiate the closed-loop level control. So, --

MEMBER BROWN: There is no closed-loop level control. In here it just shows you have on and off operating and actuator or a signal which is kind of a --

MR. SHOOK: Right. The control units

are doing that control and we use -- because most of the actuators are it is like the main feedwater valve in our previous slide. So it is a --

MEMBER BROWN: It is not -- Is this going to be a variable control signal going through the Priority Module?

MR. SHOOK: It's an on/off control. No, it is not a variable control signal.

MEMBER BROWN: Is it just open the valve?

MR. SHOOK: It's open --

MEMBER BROWN: If you do the same thing, I am just trying to figure out the difference between the PS and the SAS. They both look like they are doing the same thing, opening a valve.

MR. SHOOK: Okay. So level drops in the steam generator. I actuate EFW. And EFW level starts to go back up. Right?

MEMBER BROWN: No, before it goes back up. You have got to actuate -- You have got to open the valve and start the pump.

MR. SHOOK: Right.

MEMBER BROWN: Which one of these starts those?

MR. SHOOK: The actuation path through the Protection System.

MEMBER BROWN: What does the one out at the SAS do?

MR. SHOOK: So I am getting to that.

So, I get down to the actuation level setpoint and I actuate EFW. So I start the pump and I open the control valve and the isolation valve. When I open the control valve --

MEMBER BROWN: The EF system?

MR. SHOOK: -- by the PS through the PACS, independent of the SAS.

MEMBER BROWN: Uh-huh.

MR. SHOOK: Okay? So now I am basically, I am putting in 440 GPM into the steam generator and the level is going to start to recover.

MEMBER BROWN: Yes.

MR. SHOOK: Okay? Now, if I didn't do anything else, I am just going to overfill the steam generator. So what I do then is I do two things. When I first actuation, I send that signal not only to the PACS but I send it to SAS to initiate the closed-loop level control. So that level control

starts. So you can think about it on the PACS I have opened the control valve and then from the SAS I also have the signal that says open the control valve.

So even if the SAS said close the control valve, it is not going to do anything. It is going to open. Once level clears its minimum setpoint, the protection system automatically resets EFW and removes the actuation signal off the pump, the isolation valve, and the control valve. So now I have no active signals from the PS. So the pump will keep running and the isolation valve will stay open but now the level control valve, it goes from the closed to control mode and as it reaches its normal control setpoint, it will start modulating back and forth, open/closed to maintain level within its prescribe band.

And the valve itself is a motor-operated control valve, again, similar to the feedwater control valves that we used in submarines. So the output is just an on/off. It uses a PID step controller or a PI step controller, to be clear.

So the output of the PI is an open/close, not a continuous four to 20 position

signal.

MEMBER BROWN: Okay. So you just cycle between two bands, then, an upper band and a lower band. You hit an upper band and it tells it to close. And it is closed and it goes down and tells it open and it comes open.

MR. SHOOK: Again, it works just like the Steam Generator Water Level Control System on the submarines where it is a PI controller but the output, it is a discrete output. It is either open or closed. It is not an analogue output. You know, so as the PI controller, as you start to deviate your error at some point, --

MEMBER BROWN: Our is an analogue output.

MR. SHOOK: Not on the 688 --

MEMBER BROWN: We don't just close them?

MR. SHOOK: The 688s was at least --

MEMBER BROWN: Don't talk about it.

MR. SHOOK: Okay. All right. See, I told you they warned me.

Anyway, the way this -- If I were to trace the output of the -- As it is modulating to maintain level within the band, if I were to look at

the output, it would say open and then there would be no -- and then once it is back within its error band, there would be no open or closed. And then if it went high, then it would say closed.

MEMBER BROWN: Oh, okay. We are just talking different language. That is what I was trying to say.

MR. SHOOK: Okay. Okay, so we are aligned.

MEMBER BROWN: Yes, we are aligned.

MR. SHOOK: Okay, good. So yes, this closed-loop control is going to be operating in SAS to keep the level here. But then the protection system, you have got the actuation and the isolation at the top and bottom to keep it within its --

MEMBER BROWN: But that open and closed still goes through the priority module?

MR. SHOOK: That's correct, yes. So both the PS --

MEMBER BROWN: So if something else takes priority, it will just let the water keep going out or coming in until it is allowed to do something.

MR. SHOOK: Yes, if the Protection

System -- If the SAS is going to have an open/close signal and the PS has an open/close signal for this particular case. Right? So as long as I am controlling normally with SAS, the PS is not going to do anything. There won't be any active signals on the PACS. So I am happy.

But if I have a control system failure that drives level high or low, the protection system will come in and take the appropriate actions whether it is isolate or actuate. You can think of it like this. If my SAS fails, --

MEMBER BROWN: The only priority it has to evaluate is between SAS or PS, --

MR. SHOOK: Well --

MEMBER BROWN: -- in this particular function.

MR. SHOOK: In this particular example, right.

MEMBER BROWN: Well, for emergency feedwater.

MR. SHOOK: Well and DAS because I have -- Below the PS setpoint I have a DAS EFW actuation. I also have a manual control from SICS and a manual control from PICS.

MEMBER BROWN: Okay.

MR. SHOOK: Okay? All right. Okay, 36. Okay, we looked at -- Yes, I apologize about the eye test.

So when we look at redundancy for the ESF actuation, again we are going to look at the different levels. We look at the sensors, signal conditioning APU level, main actuation ALU and then PACS and actuators.

So for the signal sensors and signal conditioning APUs, most ESF actuations are four-fold redundant for each process variable. The same as protection system. Some exceptions for the EDG actuation, we look at three voltage sensors per division. So within each division, I am looking at voltage on that bus and I do a two out of three vote on those values.

And then for the RCP trip, we have two D/P sensors per division. So those are the exceptions at this sensor level.

For manual actuation, this is, we basically you can think of it as -- And this is all driven by the requirements from IEEE 603.

So when you look at the actuation of the

functions, some functions are what I call all four trains and then some functions you do on a per train basis. So when we look at all train functions, we look at safety injection actuation, partial cooldown, main steam isolation, containment isolation, turbine trip, hydrogen mixing dampers opening. And in those cases, I have our switches and I need two out of four of those switches to get the function to actuate. But once I get that two out of four, all the trains of those functions operate.

And then for Main Control Room System Isolation and Filtering, I have two switches and that is done on a one out of two voting. And either of those switches will cause both MCR trains to switch into filter and isolate.

When I look at the functions that are done on a per train basis, I first look at for the steam generator isolation function, we have four switches per steam generator, and that is implemented in two out of four voting.

MEMBER BROWN: Does it isolate all four steam generators?

MR. SHOOK: No, that is just per steam

generator. So I have got four switches for one steam generator; four for another; four for another; four for another.

For the EFW actuation isolation MSR T actuation isolation, main feedwater isolation, EDG actuation, reactor coolant pump trip, I have two switches per train and I just need one of those two to perform the function.

And then for PSRV opening, I essentially have enough there in the PSRV design, I have for LTOP, you know, normally there is now power operation but for LTOP we utilize to solenoid valves in series and you essentially need both of those solenoid valves to open to get the PSRV to open. So in this case I have two switches that are two out of two voting.

And then the final one is CVCS charging isolation anti-dilution I have got one switch per train. And those are very simple functions. There is essentially a couple of valves, you know, two valves in one division and one valve in a different division.

MEMBER STETKAR: Jeremy, just because you mentioned it and I don't know where else to ask

the question, anti-dilution function during normal power operation, I understand how it works. There is two valves in the letdown line. There is one valve from the VCT that goes closed. When you are in cold shutdown, it is five and six.

When you are letting down from the RHR system, does the anti-dilution logic, is the VCT valve the only valve that is preventing you from dilution?

MR. SHOOK: I'm going to ask --

MEMBER STETKAR: In other words, does the anti-dilution logic close the low pressure letdown flow path from the RHR system? It is a question -- I can't get anybody to answer that question. I have been poked from section four to section nine and now you have got it.

(Laughter.)

MR. SHOOK: So just to be clear, this is for anti-dilution specifically?

MEMBER STETKAR: This is specifically anti-dilution.

MR. SHOOK: Okay.

MEMBER STETKAR: Because the low pressure letdown line comes into the letdown flow

path downstream from the two valves that are normally closed, you know, by the signal during power operation.

MR. SHOOK: Okay.

MEMBER STETKAR: There is a lot of discussion in the FSAR about redundancy and things like that for anti-dilution protection and that the isolation is the only safety-related function. And it is not clear to me that you would have -- It is not clear to me whether or not you are vulnerable to a single failure to prevent dilution during shutdown when you are on that low pressure letdown flow path.

So the basic question is, you know, are the low pressure letdown valves closed automatically by the anti-dilution signal?

MR. SHOOK: Okay.

MEMBER STETKAR: I probably won't get an answer at the moment. You might have to take it away just to keep the discussion going.

MR. SHOOK: Okay.

MEMBER STETKAR: I couldn't figure out where else -- since you mentioned it here, I thought I would interject it.

MR. SHOOK: All right. You want to take

this as an action item?

MR. PHAN: Yes, we will take it as an action item.

MEMBER STETKAR: Thanks. It's been bouncing around since March 3, 2010. So, I'm hoping that sometime in the next couple of years I can get an answer.

MR. SHOOK: Okay. So just to make sure I understand it. So this is anti-dilution and how we deal with it when we are in RHR.

MEMBER STETKAR: Exactly. Yes.

MR. SHOOK: Okay.

MEMBER STETKAR: When you are in that low pressure letdown mode.

MR. SHOOK: Okay.

MEMBER STETKAR: Because you know, the tech specs require the function to be operable in all six modes.

MR. SHOOK: Right. Okay.

MEMBER STETKAR: And indeed, there may be situations when you are in shutdown where you are actually vulnerable to dilution.

MR. SHOOK: Okay. Yes, we will take a look at that.

Okay, going on to the ALUs, again we are eight-fold redundant on the ALUs. Again, four divisions to meet single failure and two ALUs per division to improve plant availability. In this case, it is specifically if I have an ALU out of service, I don't have to spec for losing that one division.

Most voting is two out of four. The exceptions, as we discussed, EDG actuation is two out of three, and RCP trip is one out of two per division per pumps and then two out of four voting for all pumps.

The PACS essentially as I mentioned before, I have one pair of priority and communication modules for each actuator. And actually to be more specific per each actuation device. So for example, PSRVs, I actually have two solenoids. So each solenoid gets a pair, a priority and communication module. Sometimes when we say actuator and actuation device we are not always clear on that point. So I just wanted to make sure we are clear.

And then actuators themselves, then we are just in the mechanical design of the plant.

Most ESF functions are four-fold redundant. You know, for example, we have four EFW trains. We have four safety injection trains but there are a number of functions that are two-fold redundant. And this is kind of counterintuitive. EFW isolation, even though we have four trains for actuation, the isolation function, the safety function is on a per steam generator basis. So you are two-fold redundant there. So you have two valves that can isolate the line. You need control valve and the isolation valve.

MSRT actuation and isolation are two-fold redundant systems. Main feedwater isolation, containment isolation, steam generator isolation, and RCP trip, MCR HVAC and CVCS are all essentially two-fold redundant systems.

For ESF control it is a little bit more straight forward. Next slide. Basically the control functions just follow straight up and down the redundancy of the mechanical train. And we provide for redundant control units per SAS division and provide for improved availability. Because like I said, if we take one control unit out of service, we still have a fully redundant one in that division

to perform all the functions needed.

CHAIR POWERS: I wonder if this would not be an appropriate time to break for lunch. Independence is a subject of interest.

MR. SHOOK: Yes, I think we could get through this section because a lot of the features for independence are the same. So there is only a couple of differences we just have to talk through. I mean, I think we need probably about five to ten minutes and we could probably get through the rest of the slides.

And this is about from our dry runs, about halfway through the presentation.

CHAIR POWERS: Halfway through the view graphs.

MEMBER BROWN: I would note the time for the afternoon session is less than the time for the morning session for you to finish the other half.

MR. SHOOK: Okay.

MEMBER BROWN: I just thought I would point that out.

MR. SHOOK: Okay, well we can accelerate.

Slide 38. So the main point here is

that for all these points, it is the same features for independence as we have reactor trip because it is implemented in the same system. So I am not going to go back and speak to those again. So we will just talk about the differences.

The first difference is sending signals from the PS to the PAS. Those are hardwired output via an Or and an isolation device from the ALUs over to the PAS. Again, we already talked about why we do that and the means that we do physical separation, electrical isolation. It is non-dated communication so fairly straight forward to provide for independence.

The next slide.

MEMBER BROWN: Now you have the same issue on independence that you had in the other.

MR. SHOOK: For the isolation, the electrical isolation?

MEMBER BROWN: Communications isolation.

MR. SHOOK: Yes.

MEMBER BROWN: So the same issue applies here in how you want it to fail.

MR. SHOOK: For the control units, you mean?

MEMBER BROWN: For the actuation ESFS. And I'm just looking at --

MR. SHOOK: Yes. Yes.

MEMBER STETKAR: But here it is different. If the system hangs, you don't get the ESFS signal.

MEMBER BROWN: Well that is a question of how they want the lockup to perform.

MR. SHOOK: Yes. We have a slide to speak to that.

MEMBER STETKAR: Okay.

MR. SHOOK: So we will go through that.

For the control units, this is slide 40, we have networks between the control units that require interdivisional communication. We send signals for voting for the ESF control functions, this is the only reason right now per Rev. 3 that we send those signals. It is a data-based means of communication and we provide the same mechanisms for independence are used as what we already talked about between the APUs and the ALUs.

MEMBER BROWN: But that is in the SAS.

MR. SHOOK: This is in the SAS, yes.

MEMBER BROWN: And that is not what it

actuates.

MR. SHOOK: That's right. This is for control.

Okay, for PACS, basically we have non-safety inputs into the PACS and those are dealt with differently. For the DAS, the hardwired connections are implemented via isolation device within the PACS cabinets. Again, we have physical separation in terms of the cabinet locations and cables. And then our interface to the PAS, a couple of key points. One, we use fiber optic cable to connect between the communication module and the PAS. The communication module itself is qualified as an associated circuit. So even though it is not performing a IE function, it is qualified to that level of specification. And so we can credit the electrical independence point to be the fiber optic connection.

And then lastly, communications independence. So the Communication Module implements a microcontroller but the interfaces to the PLD are hardwired, you know, just zero to 24-volt signals. So in this case, there is no data communication going to the priority module. Just on/off signals.

Okay, next slide is deterministic response time. Basically, up until the PACS, everything is the same as we have already discussed for the reactor trip. And then the PACS itself, the Priority Module, that technology of the PLD provides for inherent and predictable response time characteristics. Again, there is no operating system, no fixed cycle time. It is just performing combinatorial logic on a signal basis.

MEMBER BROWN: Is the PAS the same for all logic processing operations? In other words, is there a discrete -- because I just don't know what it looks like. Is there a discrete max processing time regardless of how you sew in the logic devices internally?

MR. SHOOK: Yes, we specify a maximum response time based on -- So again the safety functions specify with an overall loop response time and then we sort of divide that up to, you know, SCDS gets this much, PS gets this much, PACS gets this much. So it will get allocated a certain percentage of that, let's say ten milliseconds or 15 milliseconds. And then we will do testing to verify that. But I guess the point is is that based on the

type of technology in terms of demonstrating that the response time will be deterministic that we don't have to worry about time-dependent behavior like you would have to look at a microprocessor system.

MEMBER BROWN: So it is fixed once you program it. Once you decide what the logic array is, you want the PLD to reflect.

MR. SHOOK: That's correct.

MEMBER BROWN: It becomes fixed and -- Okay. There has got to be multiple paths depending on -- Because this is not a simple module.

MR. SHOOK: I see your point, yes. But --

MEMBER BROWN: Some of them go straight through faster, it would seem to me.

MR. SHOOK: Right.

MEMBER BROWN: And some of them will be longer and you have got to be able to determine which one, which request sequence could result in the longest response time. I assume it is variable.

MR. SHOOK: The one that we are --

MEMBER BROWN: Not variable. That is the wrong way.

MR. SHOOK: No, I understand.

MEMBER BROWN: There is three steps. There is a longer term and shorter term.

MR. SHOOK: The path that we are interested from a response time perspective is a path that the protection system signals take through the PACS module. Because that is --

MEMBER BROWN: That is the credited one?

MR. SHOOK: Well, the ESFS functions, your actuation functions are ones that come with very strict response time requirements. And so when we demonstrate that the loop meets the overall response time for the actuation function, we are going to test specifically the path that the protection system signals go through that circuit card.

So for example, we don't care necessarily what the response time of the signal path from the PAS through the PACS because that is not -- I mean, we care to some extent but it is not something that is really discretely very specified very clearly and concisely as we do have for the ESFS functions.

So from a safety perspective, from an

actuation function perspective, the protection system path is the one that we are interested one and that is the one that we will test to make sure that we meet that response time behavior.

MEMBER BROWN: Will the controllability thing, since you use the SAS for the automatic control? Isn't there some interest in the time response of the -- because that is where you are telling the valves to open and close or whatever --

MR. SHOOK: Right.

MEMBER BROWN: -- based on your bandwidth.

MR. SHOOK: Yes, there would be, I mean obviously it is, I mean that is something we are interested in but it is not generally, with this type of technology, it is not something that we need to -- I mean, we could specify that but it is typically not something you have to worry about because the technology itself is generally fast enough. You know, it is going to be generally faster than the control units, much faster than the control units. For the control functions, we are not quite as concerned about it.

MEMBER BROWN: All right.

MR. SHOOK: And also the control functions, because it is a closed-loop control, you know, those type of things will generally work themselves out, as long as you know, you are not putting 20 things in series.

Okay, 43, fail safe behaviour. So this is addressing Mr. Stetkar's question. Again, for the out of range failures, we have the same detection mechanism with the APU and then flag the signal and modify the voting. Here we do things a little bit differently in reactor trip. For most functions, we modify the logic towards no actuation. So for a signal sensor failure, we go to two out of three. For two sensors, we go to two out of two and then three or more sensors, we go to ESF not actuated.

There are two functions that we modify towards actuation for sensor failures, MCR HVAC realignment and hydrogen mixing damper actuation. Those go through the same sensor reconfigurations reactor trips. So we do two out of three, one out of two, and then actuation.

And then essentially where it talked about the APU failures, essentially dealt with the

same as the signal conditioning. And then everything downstream of that, if we design to fail low and that results in no ESF actuation for all functions.

MEMBER BROWN: So if the function processors all lock up in this, that is what the ALUs are.

MR. SHOOK: Yes, right.

MEMBER BROWN: If they all lock up, it will -- Is that a fail low? Does that by definition go in that direction if they lock up?

MR. SHOOK: Yes, that is how it is designed. We design it to fail low.

MEMBER BROWN: Forget sensors or stuff like that. I'm talking about ALU outputs. You say they are designed to fail low. But you have to consider the failure modes in order to do that.

MR. SHOOK: That's correct, yes.

MEMBER BROWN: And my concern is that assumes it is processing. And if it is not processing, what tells it to fail low?

MR. SHOOK: Well in this case, the hardwired-based watchdog timer will --

MEMBER BROWN: Fail it low.

MR. SHOOK: -- drive the output cards to fail low.

MEMBER BROWN: That is going to be acknowledged or explained at some point --

MR. SHOOK: Yes.

MEMBER BROWN: -- later?

MR. SHOOK: We will get to that information.

MEMBER BROWN: And how that is done?

MR. SHOOK: Yes. Yes, we can give you that detail.

MEMBER BROWN: All right, thank you.

MR. SHOOK: Okay, slide 44. The control function, typically the safe state for a control function is fail as-is. And so when we look at the sensor signal conditioning and distribution failures, the out of rage of failures are flagged and the outputs of the PI step controllers are failed low. So there is no control signal set. There is no open or closed signal sent out of the SAS. And again, in range failures aren't detected.

Control unit failures, since they operate in a master/hot-standby configuration so if one control unit fails, it will swap over to the

other control unit. And so the end result is you have no loss in functionality.

And then output logic circuit failures and PACS failures --

MEMBER BROWN: How fast do they have to transfer?

MR. SHOOK: What's that?

MEMBER BROWN: How fast do they have to transfer? Have you all done this before?

MR. SHOOK: They are using this -- Yes, this has been done before in control systems that use TXS, as well as I believe this is being done in Europe for the Protection System design because it is a little bit different but I will have to double check on that.

MEMBER BROWN: Continue.

MR. SHOOK: Okay, next slide. And then testing, you know, it essentially follows the same protocol as we had for the reactor trips. The one difference being for the actuation device operational test. That is sort of done in two parts. We do what is called a no-go test, where we send outputs from the ALUs to the priority module and we disable the priority module outputs so that

we can test the connection between the PS and the PACS but not actually actuate the final end device.

And then separately, we will do a go test where we will check the actual actuator configuration. And in that case, we will do that test from PICS and it will just be at a component level through the PICS to the PAS through the Priority Module. So between those two tests, we will be overlapping a section of the circuitry within the PACS to make sure we have complete coverage of the whole test path or the whole actuation path.

MEMBER BROWN: Have you got time-response testing down here? Is there a periodicity on doing that?

MR. SHOOK: Yes.

MEMBER BROWN: Is this just a qualification test and you never do it again?

MEMBER STETKAR: It is 24 months.

MEMBER BROWN: Oh, okay. I was just curious. Twenty-four months you said?

MEMBER STETKAR: Yes, 3.3.1.10 is 24 months.

MEMBER BROWN: Yes, I saw that there, I

just didn't -- I hadn't looked at that. That's all. All right.

MR. GARDNER: I think, Dr. Powers, we are now at the appointed break point.

CHAIR POWERS: Okay. We will recess for lunch until 20 minutes after the hour.

(Whereupon, at 12:20 p.m., a lunch recess was taken.)

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.

MR. STACK: It is screened in now.

MEMBER STETKAR: Thanks, Tim.

MS. SLOAN: By the expert panel?

MEMBER STETKAR: Yes. It's not necessarily surprising that it wouldn't meet the numerical goals given the plant design from the fire PRA. But I was surprised. So the expert panel did screen it. Thank you. That's good.

MR. GARDNER: Okay. We have one other. We will wait until Mr. Brown returns because it was one of his questions. And we'll proceed along with Section 7.4.

CHAIR POWER: All right.

MR. SHOOK: Okay. So starting on slide 48, actually I'm sorry. We skipped that one. We have three topics with regard to Section 7.4. We're going to talk about the basis for safe shutdown. We'll talk about the design and how we implement safe shutdown functions within the DCS and then talk specifically about transfer from the main control room to the RSS.

Slide 48. So when we talk about safe shutdown, there's a number of different scenarios you've look at for safe shutdown. For normal, what

I call, design-based events, accidents are described in Chapter 15. For fires including loss of MCR it's discussed in Chapter 9. SBOs talked about in Chapter 8.

We're not going to get into the specifics of exactly what systems are used to mitigate those particular events. But the key points you have to know for the INC are that depending on the scenario we can use credit either safety related or non-safety related systems to reach and maintain safe shutdown, depending on that particular event.

Having said that, going to Slide 49, then talk about how we control those systems from the different locations. Within the DCS, we look at a couple different things. First of all, we have what we call manual group controls. And so we have manual controls overall. And then I'm --

MEMBER STETKAR: Before you get into the details here, I'm trying to get spun up after lunch. You said you're not going to go into details for each of the different types of scenarios. Station Blackout, the rated battery life is two hours. Is that correct?

MR. SHOOK: For the EUPS, that's correct.

MEMBER STETKAR: For the -- I'm sorry.

MR. SHOOK: For the EUPS. For the power supply for the safety related --

MEMBER STETKAR: Safety related.

MR. SHOOK: That's correct.

MEMBER STETKAR: So after two hours I'm dark.

MR. SHOOK: That's correct.

MEMBER STETKAR: Okay. I just wanted to make sure. I sort of remembered that from somewhere.

MR. SHOOK: For the non-safety systems --

MR. STACK: Excuse me, Jeremy. Let me interject. Tim Stack from AREVA again. But the battery chargers are powered off the SBO diesels.

MEMBER STETKAR: I understand. I tend to think of Station Blackout as no AC power. Thanks.

MR. SHOOK: And I would also make the comment that the non-safety systems at least on the nuclear island received power from the 12-hour UPS.

The SBO power supplies.

MEMBER BROWN: Which systems? From the?

MR. SHOOK: The non-safety. The PICS, PAS, RCSL and DAS and specifically PS in the nuclear island receive power of the 12-hour UPS.

MEMBER BROWN: Twelve-hour?

MR. SHOOK: Yes. But I want to be clear. The 12-hour USP, the UPS isn't sized to keep all the systems powered for 12 hours. It's only sized to keep -- It's sized basically to keep all the systems powered for two hours and then from two to 12 only those systems that are needed for basically severe accident monitoring and so forth.

MEMBER STETKAR: So with load-shedding you can assimilate that to hold on.

MR. SHOOK: That's right.

MEMBER STETKAR: Thank you.

MR. SHOOK: So if you didn't load shed, there would be somewhere between two and 12.

MEMBER STETKAR: Okay. Thank you.

MR. SHOOK: Okay. So if we look at the safety shutdown, we have manual controls needed to transition the plant down to safe shutdown. We divide those into two categories. We have what we

call manual grouped controls and this is defined as a manual action that results in the positioning of two or more actuators. For example, if I'm going to -- Like an example that would be manual actuation of a trade of EFW. So I hit actuate train one. The pump starts and both valves open all at the same time.

Contrast that with component level control, I start the pump with one manual action and I open the control valve with another action. I open the isolation valve with a third manual action. That's the difference between grouped in and control level controls. And the reason I highlight that difference is that it affects how we sort of allocate those different functions within the design.

We first looked at manual grouped controls related to safety related systems. I allocate that to two paths within the design. Within the MCR we allocate that to two paths. One is from the SICS through the SAC and to the PACS. And then I allocate that to the PICS and PACS and PS.

And you're probably asking why I am

putting the same function in two places. Again, the reason is because I want to the operate to stay on PICS as long as it's available. So I'm going to provide them all the capability and functionality that I can provide from PICS given the constraints of the design that we currently have.

Since we don't allow communication directly from the PICS to the SAS, but we do allow communication from the PS to the PACS, I allocate to this alternate path. And that path is also available in the remote shutdown stations. And since I can credit PICS in the remote shutdown station, I don't need to duplicate that on the SICS in the remote shutdown station.

For component level controls, from the main control room I have two paths. I have controls that are credited on SICS and those are directly to the PACS modules. They don't go through a automation system of either the PS or the SAS. And I also have the same path from PICS and PS to PACS through the control safety related equipment. And again that's done so that the operator can stay on PICS as long as it's available. And if it's not available, then they can transition to SICS. So

they can perform a safe shutdown in the main control room from either control locations.

And again in the RSS because I have that capability on the PICS that I can credit PICS for that scenario, I don't need to duplicate those controls on the SICS.

For the control non-related safety systems, it's a little bit simpler. We provide controls on PICS through PS directly. So since there are not any safety related systems, I don't need to go through the PACS. And there's not really any overlap between the non-safety systems that we have on SCDS and PACS as those that were during safe shutdown here.

I guess the main takeaway is if I'm in the control room I can do safe shutdown either completely from PICS or completely from SICS. And from the MCR -- I'm sorry. From the RSS, I can do -- I need the combination of both PICS and SICS to reach and maintain a safe shutdown. I can't do it from either location by itself. Let's go to the next slide.

So we're going to talk about here specifically MCR and RSS transfer. The operators,

if required to leave the main control room due to an event that required that loss of main control room, for example, like a fire or toxic gas, will leave the main control room, ideally trip the reactor before they leave.

But once they get down to the remote shutdown station they'll perform these actions. They will activate the main control room to RSS transfer switches which does the following functions. First of all, it will disable the inputs from the main control room to the Protection System, the SAS and the PACS. All those hard-wired inputs from the MCR will no longer be operable.

It also just disables the DAS outputs completely. So this is a little bit different from the first three systems. The reason why we do this is because the DAS there are certain permissives that you would have to implement in order to transition to say shutdown. We decided that it was simpler to do this than it would be to add those permissives in a remote shutdown station and increase cabling and potential for complications with fires and so forth.

Since we already had these signals

running down into the safeguards buildings, we just decided to go ahead and disable DAS. It's not needed for this scenario and it was a simpler design approach.

Then the next thing the operators will do is log into the PICS workstations in the remote shutdown station which we already discussed. And again as we said they'll use the PICS for most actions again with only a limited amount of controls available on SICS.

That list is listed in Section 7.4. You can go look at it. Essentially that list consists of a manual reactor trip and then permissives needed to transition the plant down to cold shutdown. For example, P14 to allow going on to RHR.

And then we also provided a limited number of ESF resets. And the thinking behind that was what if the operator does something that causes an actuation of safety injection. How am I going to deal with that if I don't have those controls? We decided to put a limited number of ESF resets, basically those that directly affect your ability to control inventory and remove the decay heat from the plant, so SI, EFW, MSRT in the remote shutdown

station. And that way in case those systems weren't to automatically actuate, the operator can reset those and then take control back from PICS to go and shut down the plant.

And then lastly to demonstrate independence of the RSS from MCR, we already talked about we've got redundant PICS servers physically separated and we've got fiber optic cables. And the six cables from the RSS are physically separated from the main control room cables. That's it for safe shutdown.

One of the things we're going to do is address the issue of the hardwired watchdog timer. We went back and looked at our submittals. We do discuss that in two different Technical Reports. One is the self-test report which is ANP 10315.

MEMBER BROWN: Let me get the right sheet up.

MR. SHOOK: Sure.

MEMBER BROWN: Okay. Tell me that again. ANP?

MR. SHOOK: It's ANP 10315 and the specific section is 2.2.6.2.

MEMBER BROWN: 2.2.6.2?

MR. SHOOK: That's correct. And the other place where we discuss it is the TXS Topical Report.

MEMBER BROWN: Okay. The TELEPERM?

MR. SHOOK: That's correct. Yes. And that's EMF 2110.

MEMBER BROWN: Yes.

MR. SHOOK: And the specific section is 2.4.3.4.2.

MEMBER BROWN: Okay.

MR. SHOOK: Okay. And just a -- I'll just give a 30 second description of how it works and then I'll let you go in detail.

MEMBER BROWN: Okay.

MR. SHOOK: So it's actually the watchdog timer which is going to look at -- which essentially gets reset every time the processor finishes its fixed cycle operation along with some time delay or it gets reset. If it doesn't reset within the fixed cycle operation plus the time delay, it will essentially put the processor into a safe state and then set the output drivers to a defined fail-safe state. So, in the case of reactor trip, it will trip the reactor. In the case of ESF,

it will be the safe states we've already described.

MEMBER BROWN: Okay. Does it say what the defined state is for each of those circumstances in either place?

MR. SHOOK: In the specific sections, it just says it's going to fail to a predefined safe state. And then in another section's report it talks about what the safe states are for those different functions.

MEMBER BROWN: Does it refer to those? Does it reference those in that section?

MR. SHOOK: Not specifically. So I'll say it's not completely laid out as I'm describing it here. But you can piece together the information from the different sections.

MEMBER BROWN: Which one is 10315?

MR. SHOOK: That's the self test and -- What's it called?

MR. PHAN: Protection System --

MEMBER BROWN: Is it referenced in the DCD?

MR. SHOOK: Yes.

MEMBER BROWN: It's referenced in the DCD as being a source for defining how it's supposed

to operate.

MR. SHOOK: Yes. The Technical Report is used as essentially an extension of the DCD to further incorporate specific technical information.

MEMBER BROWN: In other words, my point being is that the designers, whoever gets the contract, would have to comply with that.

MR. SHOOK: That's correct.

MEMBER BROWN: About regulation or because it's been certified in that.

MR. TESFAYE: It is incorporated by reference.

MEMBER BROWN: Okay.

MR. SHOOK: Okay.

MR. PHAN: One more reference section that you wanted was you were asking where we established our design rules for signal diversity in the Protection System and how we allocated it.

MEMBER BROWN: Functional diversity thing you were talking about?

MR. PHAN: Yes, functional diversity/signal diversity.

MR. SHOOK: Right.

MR. PHAN: That's in Section 10.2 of the

Protected System Technical --

MEMBER BROWN: Before you go any further, you made that comment relative to the SCDS I think. The one about which -- I want to make sure we're talking about the same thing.

MR. SHOOK: This was the rules that tell you whether it goes to subsystem A or B.

MEMBER BROWN: Okay.

MR. SHOOK: For the signal -- Or what I was calling function diversity, but what in the report is called signal diversity.

MR. BRIXEY: I think that we might have come around to answer on that question because we talked about how we allocate functions back and forth.

MR. SHOOK: But he still wanted to see the criteria for that.

MR. BRIXEY: Okay.

MEMBER BROWN: Okay. You said that was where?

MR. PHAN: Section 10.2 of ANP 10309.

MEMBER BROWN: That is the Protection System --

MR. PHAN: Technical Report.

MEMBER BROWN: -- Technical Report.

MR. PHAN: Yes.

MEMBER BROWN: No wonder I didn't get to that. It was in section -- It was just so exciting I couldn't hold my eyes open.

The one other area I think I asked for criteria you went through a discussion was on what defines what goes through SCDS and what doesn't. And you said there was a bunch of them.

MR. SHOOK: That's right. I'll get that. I'll look that up. Can you write that down?

I'll get that on the next break.

MEMBER BROWN: Okay. Thank you.

MR. SHOOK: That's sort of all the look-ups that we had to far. Let's go to slide 52.

Now we're discussing Section 7.5 which is Information Systems Important To Safety. The main -- This is sort of a catchall section, but here are the main topics that we'll be discussing: alarms, post-accident monitoring, PAM, safety parameter display system or SPDS, emergency response data systems or ERDS, tech support center, TSC, and then bypassed and inoperable status indication, BISI.

With alarms, the inventory of alarms is basically -- I'm going to punt to my Chapter 18 counterparts and essentially the alarms will be determined via task analysis and alarm criteria developed within the scope of the HFE programs. So I'm not going to go into that detail today.

In terms of implementing the alarms within the design, the various alarms are processed within the different automation systems whether they be DAS, PS, SAS, RCSL or PAS. And then they're displayed both PICS and SICS. So PICS is going to show all the alarms that are defined for the plant. And then SICS will have a limited number of hardwired alarms as determined for accident mitigation, safe shutdown and any other potential events like severe accidents or SBO.

MEMBER STETKAR: Jeremy, I am trying to tie together a few things from different chapters that we've seen. And this is in Chapter 18 of the FSAR. There are statements of the sort that says, "Alarm signals include logic so that only operationally relevant conditions are alarmed. The overall plant state is considered for the generation of alarms or at least to inhibit alarms that are not

relevant for the actual plant state. Pre-alarms are provided before automatic actuation only when an operator has sufficient time to identify and perform mitigative actions."

That tells me this isn't a simple alarm system. It's some sort of smart alarm system that contains again this term priorities and logic so that the system knows what I, the operator, must know and provides me only that information that it knows I need. Is that a fair characterization? And, if so, how does it know what I need to know?

I hate to be told by a machine that "Don't worry your pretty little head. This isn't something you need to worry about."

CHAIR POWER: I can assure you. Not even a machine would say, "Don't worry your pretty head."

(Laughter.)

They don't make that programming. That is a non computable function.

MEMBER STETKAR: You've given them enough time to think now.

(Laughter.)

MR. SHOOK: I'll say that -- I guess

I'll answer that question in terms of the general process and capability of the system. When you look at the alarms, the two main ways that we can use to essentially filter alarms to the operator, one is to define the alarm in terms of a plant state. So whether that's mode one through six or some other criterion that we can use to set the alarm and say, "Hey, don't -- " Or even as simple as "Don't give me a low flow alarm if I turn the pump off." Right. You know something as simple as that. And that could range from broad criteria about studying modes one through six and more detailed criteria about the particular pumping sample.

The second main way we have to filter alarms is actually by assigning a priority to the alarm. And then the operator can use that to filter based on the priority. So, for example, if I get a reactor trip, I can say "Okay, I just want to look at priority one alarms and I don't care about all the other stuff." And then it lets me look at and say, "Okay. I have low pressurizer pressure. I've got this. I've got that." And then I can very quickly diagnose the event as opposed to having to look at a whole board of red lights lighting up

which is not an easy task.

So the system I'd say the general process is there. And the system is capable of it. But all that would be defined basically at an alarm-by-alarm basis.

But to your point I mean that's all specified with the alarm definition when the alarm is shown in honest. It's just that we don't leave it up to the vendor to make that decision. That's part of the alarm specification.

And I want to be clear about that. Those two features are really only available on PICS. You know, SICS, you're not going to have that capability. SICS is just you get what you get.

MEMBER STETKAR: You get what you get on SICS.

MR. SHOOK: Yes. But again there would be a limited number of alarms on SICS. You're not going to have a complete annunciator like you expect to see --

MEMBER STETKAR: Now are all alarms available to the operator to pull up on PICS or?

MR. SHOOK: Yes.

MEMBER STETKAR: You mentioned there is

some sort of prioritization or hierarchy. I have to think about that. When are those priorities set? Is that part of the human factors engineering? Is it part of --

MR. SHOOK: Yes.

MEMBER STETKAR: I mean how does one determine, for example, that the system knows that I have a LOCA rather than overcooling event which can give me a lot of the same types of indications.

MR. SHOOK: Right.

MEMBER STETKAR: And Alarm X has priority one and because the system knows I have a LOCA rather than Alarm Y that might have told I had an overcooling event, that type.

MR. SHOOK: Right.

MEMBER STETKAR: Is there a scenario type analysis that's done? Is there -- How is that done and when is that done?

MR. SHOOK: It is done through when we develop the logics as part -- You know, the logics are essentially part of the human factors process. And when we define the alarms for the system that all gets worked out at that point in time. And we will have -- I can't say we will have criteria that

defines all that.

MEMBER STETKAR: You don't have a map.

MR. SHOOK: We don't have -- To my knowledge, we don't have them. And I think all we have in the HFE program is just implementation plans that state that we will develop that criteria at some point.

MEMBER STETKAR: Okay.

MR. SHOOK: But I would say it depends. If the alarm is filtered based on what I was saying. Like if I turn the alarm off because I'm turning the pump off and I disable the low flow water --

MEMBER STETKAR: That one I have no problem with.

MR. SHOOK: Yes.

MEMBER STETKAR: It's having been an operator in the old style plant there were a lot of number of high priority alarms that we got used to ignoring because some designer decided that they shall be high priority. And to us they were really more confusing. There were a lot of other lower priority alarms that we paid a lot more attention to because they gave us a lot more indications of what

was going on in the plant.

MR. SHOOK: Right.

MEMBER STETKAR: Simply because the designer doing design basis licensing type deterministic analyses hadn't quite thought about how the whole plant works.

MR. SHOOK: Right.

MEMBER STETKAR: And that's my fundamental concern because it finally comes down to the operator having the information at his hand.

MR. SHOOK: Right. Right. And I will say --

MEMBER STETKAR: To understand what's evolving in the plant without too much extraneous filtering.

MR. SHOOK: And I will say as sort of a general comment I do share your concerns as a former operator and trainer of operators.

MEMBER STETKAR: Okay.

MR. SHOOK: It's hard as a designer to foresee is this going to be important in this situation or that situation. I will say the modern systems, it's a tool. They offer a lot of capability to improve the operators' performance and

be able to diagnose situations and respond to that. But you have to be -- When we actually develop that criteria, we'll have to be careful about not trying to over design the scenario.

MEMBER STETKAR: And the flip side is the operators after several years and generations become complacent. They know that the system knows more than they do.

MR. SHOOK: Right.

MEMBER STETKAR: And they've never been challenged unless people running simulator scenarios get pretty doggone clever. They've never been challenged to kind of question whether or not the information they're receiving indeed is the information that they need.

MR. SHOOK: Right.

MEMBER STETKAR: It's sort of "Well, the system is telling me this and that's the way I should react."

MR. SHOOK: Right. I will say I'm not an expert on the NUREG-0711 process or anything like that. But I will say that the part of the process I understand in looking at trying to get operator feedback early on in the process and also the

verification I think will help out significantly to drive out a lot of those things where before the designers just did what they thought was right. And then the operators get in there and say, "Well, why do I need this?"

MEMBER STETKAR: In principle, it works.

MR. SHOOK: Yes.

MEMBER STETKAR: It's just in many cases it's the selection of the scenarios that you use to sort of test the process that's kind of critical.

MR. SHOOK: Right.

MEMBER STETKAR: Okay. Thanks. Let's get back to the wires and electrons.

MR. SHOOK: Again, at some point we could have a beer and I could talk to you more about philosophical things.

MEMBER STETKAR: It would take several beers, but that's okay.

MR. SHOOK: Okay. Moving to Slide 54. So we're going to talk about post accident monitoring. I didn't bother to show the list here in the presentation, but it's in Section 7.5, Table 7.5-1. And just a couple of bullets here and how that was developed. We thought it was important for

background information.

Essentially we looked at -- We evaluated the B&W owners group EOP technical basis document. AREVA's predecessor company was B&W. So we got access to this information and used that as a starting point essentially. The one important piece to note especially for Member Brown coming from the Navy it's a symptom based approach, not event based which is like different.

And again you can have people on either side argue the merits of one or the other. I'm not going to get into that approach. But it is a symptom based approach.

And then we looked at the differences obviously in the B&W plant design versus the EPR. Then we also looked at credited operator actions in Chapter 15 specifically for the tube rupture event and a couple other things. And then per IEEE-497, we went and looked at the critical safety functions and fission product barriers functions as discussed in the 497. So it was a process based on information we had access to and then essentially tweaked it from there.

MEMBER SKILLMAN: Credited operator

action, Chapter 15, is that all of Chapter 15?

MR. SHOOK: Yes.

MEMBER SKILLMAN: Thank you.

MR. SHOOK: Okay.

MEMBER STETKAR: A couple questions on procedures. You have redundant procedure -- You have computerized procedures in the design. Correct? Both?

MR. SHOOK: Well, let me -- I'll say this because there's some discussion. I can't remember if it's in the Design Certification or COL. The PICS has the capability to implement a computerized base procedure system. And so in that design if you recall we have redundant servers. So the procedures will be loaded on both servers.

MEMBER STETKAR: So you do have redundancy.

MR. SHOOK: Right. But the SICS would be paper based procedures. There's no computer based procedure system for SICS. It's just open up the boo and --

MEMBER STETKAR: Are the computer based procedures point and click to implement actions or are they simply X-files that --

MR. SHOOK: I don't think we have that level of detail defined yet.

MEMBER STETKAR: Because you can control the whole plant from PICS, what sort of functions are not in the computerized procedures?

MR. SHOOK: Go back to the --

MEMBER STETKAR: That's okay. It's too much detail.

MR. SHOOK: No, no. That's fine.

MEMBER STETKAR: We need to kinda keep on track with the time here a little bit.

MR. SHOOK: Okay. I'll just say if you look at the design. I don't communicate at all directly with DAS.

MEMBER STETKAR: Okay.

MR. SHOOK: And I can't send signals from PICS to the Protection System or SAS. So I'll have information from those systems flowing up to the PICS so I can see what's going on. But if you get to a point where it says go trip the reactor, I can't do that from PICS. So I have to go to SICS to do that. So there might be some points in there.

MEMBER STETKAR: Thanks.

MR. SHOOK: Okay, 55. So here you can

see the allocation of the PAM variables within the DCS. And it's the same kind of story that we have for Type A through C. It's the same kind of story we have for the safe shutdown control functions.

So for Type A through C we have two paths. For a credited path, we go from the SCDS directly to SICS. So this is a key point. All indications needed on SICS are directly hardwired from the SCDS to the SICS. They don't go through any microprocessors or any processing. It's just directly hardwire connection.

When you see the QDS on SICS, the QDS' purpose is basically only providing those variables that are deemed to be important to show from a graphical display or a trending capability. But that will be in duplicate to the hardwired indicator. And the hardwired indicator is the credited indication as far as meeting all the 1E requirements.

MEMBER BROWN: The QDS is the PAM?

MR. SHOOK: It is essentially like an SPDS. It's an easy way to think of it.

MEMBER BROWN: Yes. But it's what you call the QDS. PAM's not on your big diagram.

MR. SHOOK: Right. Right.

MEMBER BROWN: So is it the QDS displays that you -- Are those where the PAM executed or implemented?

MR. SHOOK: Again, all the PAM variables are provided via dedicated indicators. And only those variables as well as all the other variables I've provided on SICS are all provided through dedicated indicators that are hardwired, four to 20 loops directly from SCDS to the SICS panel.

MEMBER BROWN: I got that.

MR. SHOOK: Separate from that, the QDS will provide -- You might say pressurized level I'd like to see a trend of that parameter. I'll provide that parameter on QDS. But it's a duplicate indication of the hardwired and still has the hardwired indicator for the pressurized level indication which is my primary credit.

MEMBER BROWN: That's a little more sophisticated post accident monitoring panel.

MR. SHOOK: Yes.

MEMBER BROWN: That was my whole point.

MR. SHOOK: Okay. Yes, it's essentially what it is.

MEMBER BROWN: I understand you had the hardwired stuff which is separate from everything.

MR. SHOOK: Right.

MEMBER BROWN: Based on your earlier statement. That was it. Thank you.

MR. SHOOK: Okay. And then we have a duplicate path where we go from SCDS through the PAS to the PICS and again that's to support the operator being able to continue operation from PICS as long as it's available.

And again the PICS is a non-safety system. But we have specified some additional quality requirements for the PICS. And due to the improvement in human factors and a lot of the features with the PICS we want the operator to use that system again as long as it's available. So that's we provide the dual paths for both systems.

MEMBER BROWN: Are all the SICS, those indications, switches, controls, whatever you show in here, are all those on a separate panel? Or are they scattered throughout the panels where the operator sits?

MR. SHOOK: I'd say that basic concept is that you have the PICS are the primary

workstations and they're be essentially a couple of those where operators will sit at. And then the SICS is a separate panel located in a somewhat different location within the control room.

MEMBER BROWN: I just questioned that they're segregated separate so that you know what you're operating with.

MR. SHOOK: Right. Now we have had some discussions. I will say that with the design change we've made to eliminate communication from the PICS to the Protection System and SAS we have had some preliminary discussions with our HFE folks about either maybe co-locating some of those controls with the PICS or perhaps duplicating some of controls. Those details have yet to be worked out and that will be done as far as the detailed design of the plant.

But the basic concept we inherited that we're trying to keep as much as we can is the operator uses PICS as our primary means of control in the plant. And if that fails then they transition to the SICS as a backup HMI.

And then Type D through E we just processed through PAS to PICS. We won't display

Type D and E on SICS.

Okay. And the rest of these are fairly straightforward. SPDS, the functionality we don't have a dedicated thing we call the SPDS. But we incorporate that functionality into PICS primarily and also with the QDS on SICS.

Emergency Response Data System, we have the PICS. And if you look at the previous picture we show the ability to communicate out from the DCS to external plant networks within the plant. So we can get all the data from the DCS out to business networks. And then ultimately that data can be transferred to the NRC for emergency response.

MEMBER BROWN: So your PICS sends data to the TSC as you would expect. Correct?

MR. SHOOK: Yes. Well, the TSC, you have to be careful. The system matters. We have PICS equipment actually in the TSC if you look at the previous drawing.

MEMBER BROWN: But you just said something about getting from someplace out to the business network.

MR. SHOOK: Right. So if you go back and look at slide 55. You can see here that we have

dedicated, fixed equipment located in the TSC. And then you can also see --

MEMBER BROWN: It doesn't say fixed on it. It just says TSC monitoring only.

MR. SHOOK: Right. But it's all --

MEMBER BROWN: It's in the box.

MR. SHOOK: Right. It's all within the fixed --

MEMBER BROWN: Yes.

MR. SHOOK: But then you can see off the HMI bus we have a pair of redundant firewalls that we send data out from the PICS to external business networks within the plant.

MEMBER BROWN: Are those unidirectional firewall?

MR. SHOOK: Those are unidirectional firewalls.

MEMBER BROWN: And how unidirectional? Are they software determined, unidirectional firewalls?

MR. SHOOK: We haven't got to that point in the design yet of actually specifying exactly how that's going to work. Because as you probably know, there's different ways of doing that. We could use

a data diode approach like we use with the Protection System to the PICS. Or there is the software based approach. We haven't gotten to that point of specifying that detail yet.

MEMBER BROWN: Why would you want a software based system where somebody could come in and hack it and they'll gum up your software and servers?

MR. SHOOK: I'm not saying we would want that. I'm just saying that we haven't specified that.

MEMBER BROWN: I'm saying why haven't you -- My question is why haven't you specified it to make sure it's secure?

MR. GARDNER: I think maybe you're asking questions that would be more in the cybersecurity area.

MEMBER BROWN: You picked up on that.

MR. GARDNER: And so the cybersecurity I believe is being addressed by the COL Applicant.

MEMBER BROWN: About?

MR. GARDNER: Outside of design certification.

MEMBER BROWN: In other words, we don't

know.

MR. GARDNER: It's just not part of the scope of design certification.

MEMBER BROWN: And I've heard that every time which causes me great angst considering the Department of Defense team -- their computer systems. I'm trying to figure out why you all think you can. I haven't gotten a satisfactory answer and I'm sure your licensees don't either.

All right. We can address it later.

MEMBER SKILLMAN: Question please. What drove you to make the Tech Support Center information important to safety?

MR. SHOOK: Tech Support Center. Well, this chapter is entitled Information, Systems, Support and Safety. That's just what the SRP -- That's just the title of the chapter. That's all I'm going to say.

In terms of the TSC specifically it's non-safety related. It's not relied upon directly to mitigate a design basis event. So it does meet the safety related criteria, 10 CFR --

MEMBER SKILLMAN: That's what they all say until you spend a couple weeks in one. Then you

realize it's one of the most important places in the plant. So I commend you for this, but you've answered my question. It's the SRP.

Is there any special quality given to the equipment that's in the TSC so that the people in the TSC know that they've got good stuff?

MR. SHOOK: We have specified a number of quality requirements, environmental and some other things that are listed in Section 7.1 of the FSAR to provide some assurance that it will operate during the time when it's needed. So I could get the specific criteria that we've laid out for that to help.

MEMBER SKILLMAN: No. You've answered my question.

MR. SHOOK: Okay.

MEMBER SKILLMAN: Thanks.

MR. SHOOK: Well, quite frankly, Dick, if somebody hacks their servers the way it's hooked up the guys in the incident main control room are going to get the same crummy data that the TSC does. If it's corrupted, they won't know what's in the plant in the first place because that's just the way the plant is configured.

So if they come in and corrupt the servers, it's going to go both places. So they'll both have the same information that will both be bad. So that's an interesting way of looking at it. I didn't think about that one when I was looking at it. It's just a side thought that you might keep in mind.

MR. SHOOK: Okay. Thank you.

And then lastly the Bypassed Inoperable Status. Basically the safety related I&C system are required by IEEE-603 and various reg. guides to provide status indication when the systems are bypassed or inoperable. And that's all provided to the PICS from those systems. Okay.

Keep moving onto Section 7.6, Interlock Systems. The topics we have the functions and then we'll just talk briefly about the design.

Slide 59, it lists the four functions. And again this is what's currently in Rev 3 of the FSAR. And this is being updated to address some open items from the staff. But this is what it currently reflected in design. We have the RHR Suction Valve Interlocks, the Accumulator Interlocks, and then Interlocks Isolating Redundant

CCWS Trains and then LTOPP Interlock.

Moving to Slide 60, in terms of allocating the interlocks with the new DCS, essentially the sensors come through the same path. They come through the SCDS. And then interlock function itself is either allocated to the Protection System or SAS.

Essentially, in terms of the criteria, why you put one in one system versus the other, if the interlock already uses a signal that's in the Protection System, for example, P14 is using some pressure signals and that's already in the Protection System. We'll allocate the interlock there. So we don't end up running additional cable to the SAS for no real benefit.

Essentially if we already have the system in the PS, we'll just allocate it to the PS. If we don't have the signal already in the PS, we'll allocate it to the SAS. Both the Protection System and the SAS perform interlock functions.

And again the signal out will go back through the PACS. And then if I need to -- If there's a need to manually interact with the interlock function, I'll provide those controls on

the SICS only. For example, if I want to validate P14 I go do that from SICS. I can see the indication on PICS of the status of it. But I can't actually change the permissive until I go to SICS.

Okay. The design, just some inert aspects of interlock functions. We do have inter-divisional communications for interlock functions. There are two main reasons why we do that. One is to provide for voting. And the reason for that is we want to reduce the probability of spurious actuation of that function.

The other reason is what we call a cross-train function. An example of this would be your CCWS cross connect interlock.

What happens there is if essentially I can't do something with Train 2, for example, open some suctions valves, until those same valves on Train 1 are closed, then Train 2 needs to know the status of components in Train 1. In order to actually accomplish the safety function I have to send information from Division 1 to Division 2 within the SAS.

So this isn't a -- In this case, it's not a nice to have. But it's actually required to

implement safety function with those communications.

And then the futures for independence we've already described in terms of the ESF actuation and control functions in the futures and Protection System in SAS.

MEMBER STETKAR: Jeremy, CCWS, you have the unfortunate pleasure of coming the day after we talked an awful lot about pumps and pipes and valves yesterday. And you know about signals. That's not fair.

There are a number of CCWS cross connect functions on -- One is the main loops from like you mentioned Train 1 to Train 2 on the common headers. There's also either common header can supply all of the reactor coolant pump thermal barriers.

And reading the material at least in Chapter 9 of the FSAR, Rev. 2 of the FSAR anyway, I got really confused about what types of interlocks and functions there are for those thermal barrier supply valves. I read things that say "In the event of an RCP thermal barrier fault such as tube rupture a single RCP thermal barrier is isolated via inlet and outlet isolation valves in the RCS."

I couldn't find any valves. But I don't

have good diagrams of that system to see if there are any valves on the inlet and outlet sides on the primary coolant side of the thermal barrier coolers. I'm not sure where they are if they're there. So I'm not sure whether that statement is correct or not.

It also says "Isolation valves at the inlet and outlet of the thermal barrier are used to automatically isolate faulted thermal barrier from the CCWS."

And then the one that really got me thinking. It says, "Possibly of diluting the RCS via faulty RCP thermal barrier exists only when the RCS is in a low pressure state. After a predetermined time delay which allows for RCP coast down and when the RCS pressure is low, the CCWS will be automatically isolated from the RCP thermal barrier via CCWS inlet and outlet isolation valves. Now you can't isolate CCW from an individual thermal barrier. You can only allow isolate it from all four."

How does all of that work? Do you know how any of that works? I didn't ask the folks yesterday because everybody I asked yesterday about

anything to do with signals said, "Our I&C people aren't here. You need to ask them."

CHAIR POWER: These guys also claim to be your friends.

(Laughter.)

MEMBER STETKAR: This one was rather complicated. So I didn't even want to bother them yesterday with that.

MR. SHOOK: I would first like to make the point that both my degrees are mechanical. So not only knowing signals, I also can dabble in the pumps and pipes and valves piece as well.

MEMBER STETKAR: You're doing real good on the signals by the way.

MR. SHOOK: Thank you. Thank you. I don't know if I'd be interested in sealing any mechanical drawings at this point.

MEMBER STETKAR: You know what I'm talking about. I'm talking about where you can cross tie Common Loop 1 and Common Loop 2 or feed the thermal barriers.

MR. SHOOK: What I'll say is we went through an exercise I'd say earlier this year where we went back with the system engineers and we kinda

scrubbed the list of all these interlocks and so forth. So the details in that are not currently in the FSAR, but they will be coming with Rev. 4. So you'll have detailed logic diagrams.

MEMBER STETKAR: Rev. 4?

MR. SHOOK: Yes.

MEMBER STETKAR: You're talking to somebody who has seen Rev. 2.

MR. SHOOK: Okay.

MEMBER STETKAR: Anyway, I'm happy to wait to see the details if it hasn't been worked out.

MR. SHOOK: Okay. I mean I can try to go through it now.

MEMBER STETKAR: No, that's fine.

MR. SHOOK: But it would be a lot easier for you to just look at the logics.

MEMBER STETKAR: It will. Thanks. That's all I needed to know for now. Thank you.

MR. SHOOK: The material that's going to be in my Rev. 4 should address all the questions you just asked.

MEMBER STETKAR: Okay. Thanks. And it is, Sandra, Rev. 4, not Rev. 3.

MS. SLOAN: The Rev. 3 is the latest. This is Sandra from AREVA. Rev. 3 is the latest docketed revision. But we are working on Rev. 4 which incorporates mark-ups in responses to still open RAIs.

MEMBER STETKAR: Okay. I'm sure we'll keep that.

MR. WIDMAYER: I'll get that and explain it to you later.

MEMBER STETKAR: Okay. Fine.

CHAIR POWER: The important thing to remember is the SER has been written on Rev. 2.

MR. WIDMAYER: Until such time as it isn't.

CHAIR POWER: Don't confuse me, Derek.

MEMBER STETKAR: Thanks. I'm good.

CHAIR POWER: Okay.

MEMBER STETKAR: Thanks a lot.

MR. SHOOK: Moving onto Section 7.7, this is Control Systems Not Required For Safety. So we're going to talk about again the functions, the basic design and then we'll touch on features in the control systems to reduce probability of failures that would cause an event to occur.

The functions, we divide things into two categories. We have what we call Process Control Functions. And then those are subdivided in core related and primary related functions. And you can see the list here. And again there's nothing here that's really different from what you see in an operating plant today. The next slide.

Here we have process limitation functions. The idea of the limitation function is that if I have a basic control band between two values and my LSSS is up here, the limitation functions is going to be somewhere in between the two to take some initial preventive action or mitigation action to help keep you within your safety battery as well as keep the plant online.

In some cases, it either prevents you from getting out of band like, for example, with the reactor power limitation with respect to feedwater flow or generator power would actually in some cases block power increases. And then in other cases it's more of an initial mitigation action. For example, we look at high linear power density and low DNBR. We actually initiate partial trips which drop a certain number of rods into the core.

MEMBER STETKAR: I was going to ask you just for my own edification. I haven't looked at this part of the design and I'm not really sure how much it's in there. But is this design fairly similar to the -- I've forgotten what they called it -- but in the Convoy plants the sort of different parameters you look at. You drop selected groups of rods, runback turbines. Take a look at what's happening and run it back a little further.

MR. SHOOK: Yes. That's correct.

MEMBER STETKAR: Okay.

MR. SHOOK: So the idea is it's basically these are all measures to improve plant availability. Right. So I don't just trip the plant which is not necessarily the best either from an operational or a safety perspective. So I can do a little bit and keep the plant operating and keeping it within the safety limit, that's what we like to do.

You can see I've noted in there which functions are partial trips. You've got the DMBR, high linear power density as well as the loss of one reactor coolant pump. Go to the next slide.

In terms of allocation, there are

control and limitation functions within the design. If it's a core related control and limitation function if it's only acting on control rods, for example average temperature control, then it's allocated wholly to RCSL with operator interface of PICS.

If we implement -- if the control function uses actuators other than just control rods, for example for borating, then we have to involve some components from the CBCS system. We'll utilize RCSL as doing most of the control logic and then send signals for the actuators, you know, specific actuator signals to the PAS.

The idea behind that was between the PAS and the PICS there's a lot of integration in terms of tracking actuator position with respect to its demand and signaling and so forth. And so we wanted to keep that integration between the PAS and the PICS because they're the same platform. RCSL is TXS. So we have to manually configure all those interfaces. It's a lot easier to just send the signal over to PAS and that's why we do that.

And then if it's just primary related, we just implement those control functions all in

PAS. And then you can see here obviously if we use safety related sensors or actuators, it will go through SCDS and PAS. If not, it goes directly to those sensors and actuators. Next slide.

Some features that are implemented within design to reduce the probability of control system failure. First of all, we have redundant sensors and signal selection algorithms, for example, second min-max. And that helps us prevent a single sensor failure from causing a plant event. For example, an inadvertent rod-withdrawal casualty.

And then within the RCSL and PAS you have redundant controllers. If I have a single controller failure, I have a master hot standby. I swap over to the standby. So I continue plant operation and I don't cause an event to occur in the first place. Both of those taken together I've got a decent amount of redundancy at different levels within the control system design to reduce probability of failures in the control systems.

MEMBER BROWN: You don't use the signal selection algorithms in the Protection System as PAS.

MR. SHOOK: So we just do loading of the Protection System.

MEMBER BROWN: And it's the straight signals coming in and whatever are allocated to that division are the ones that are used to make that decision by division.

MR. SHOOK: That's correct.

MEMBER BROWN: And these are used where? Are they used in the PAS?

MR. SHOOK: The signal section, yes. The signal section algorithms are used in PAS or RCSL.

MEMBER BROWN: And you say that's for the control purposes?

MR. SHOOK: That's correct.

MEMBER STETKAR: And typically where you see things like T water control and pressurized level control, that sort of stuff. Right?

MR. SHOOK: Right. Like, for example, you look at average coolant temperature control. I have four divisions of T-hot or T-cold. I'm bringing all four of them. And then I'll do a second min to select to get a final one that I use that for my calculation and control logic. Again,

we can discuss this over a beer sometime if you'd like.

(Laughter.)

MEMBER STETKAR: Bourbon and branch water would be better.

CHAIR POWER: The number of discussions you're going to have over beer leads to cirrhosis of the liver.

(Laughter.)

MEMBER BROWN: It's interesting. You make a decision for the operator based on what he's going to control with as opposed to letting the operator figure out what he will control with.

MR. SHOOK: That's correct. The first, when you look at it, thing you have to do is say "Okay. Am I going to automate the function or I'm going to do it manually. For example, the plant I was on we manually controlled T-ave. So the operator had to go and pick which sensor he's going to look at. Right.

When you automate it and you tell the system to run a PID loop to control T-ave and send some band, the control system then has to decide which one they're going to look at. And that's when

you utilize these signal selection algorithms like a second min-max.

Or you can even do -- I mean, there's not within this design, but there's even more sophisticated means of determining what the actual process variable is. Because that's what you're really trying to accomplish. You've got these sensors looking at different specific points. But ultimately you're trying to determine what the process variable actually is and then control that. So the second max algorithm is one way to do that. But there are other ways to do that.

MEMBER STETKAR: US EPR, though from what you said, is carte blanche, a second min-max type control.

MR. SHOOK: No, not necessarily. I mean it depends on the process framework.

MEMBER STETKAR: Do you do any -- I've seen clever algorithms that try to figure out what a mean value might be among a number of unfailed parameters. Do you do any of that sort of stuff?

MR. SHOOK: No, we don't. We try to keep it simple.

MEMBER STETKAR: Thanks.

MR. SHOOK: Like I was saying before, with some of my experience with GE, where you can do model based prediction of -- You know, we were predicting a firing temperature of a gas turbine based on measure parameters because you can't measure the firing plane. So there's all sorts of little tricks you can do. But a second min-max --

MEMBER STETKAR: You do a basic selection.

MR. SHOOK: Yes. It's good enough for our purposes. We don't need to make it more complicated.

MEMBER STETKAR: Pretty fault-tolerant.

MR. SHOOK: Yes. So we're moving onto Section 7.8. We'll go to Slide 69. I'll kind of touch on the D3 analysis that was performed and the assumptions and basis for the analysis. Then we'll go into the functions that were developed as a result of that analysis, the design and then we'll look at the main diversity attributes of the mitigating systems. Slide 70. Basically what we did was we essentially postulate a software common cause failure of the Protection System that disables the Protection System, like what Member

Brown was talking about before. We designed the system such all detectable failures and faults are detected. And we failed to a safe state.

In the case that we've missed something and I think when you look at B2B719 it sort of addresses the point and it says in a digital system it may be harder to detect all -- identify all your faults in all our systems. So we go ahead and do this analysis. When we looked at the Protection System, we had to look at what we were going to assume from an analysis perspective as far as the operations of some of the systems in the design.

We made a conservative decision to assume -- With a software common cause failure Protection System, basically RCSL we don't credit. We assume that it just doesn't work as well. The reason for that is it's using the same inputs as the Protection System. So your common trigger could be coming from the same sensors.

And they are similar functions where I'm doing like -- For example, in the Protection System, I've got the high linear power density full reactor trip. Well, if I'm using the same algorithm in the RCSL to do a partial trip for a high linear power

density, it doesn't make sense to the partial trip and not the full trip. So we just made the decision conservatively to not credit RCSL.

MEMBER STETKAR: Jeremy, before you get further on down into this, the first bullet says software common cause failures postulated to disable the PS. Does that mean that the only potential common cause failures you thought about where failures that prevented the Protection System from doing what it was supposed to do? In other words, did you also think about common cause failures that makes the protection system do things that it's not supposed to do because of -- We've already discussed several of these priorities and things where you have to make decisions about which particular functions ought to be implemented.

MR. SHOOK: Right. We did look at that. I can't recall the specifics of some of that analysis. But in most cases, from what I recall, it's sort of a nonissue. For example, if I isolate containment, I can deal with that. It may not be desirable, but you can deal with that.

MEMBER STETKAR: That's documented in your D3 analysis.

MR. SHOOK: I believe so. I'll double-check and get back to you on the break.

MEMBER STETKAR: Okay.

MR. SHOOK: But I believe that's somewhere in the D3 report.

MEMBER STETKAR: Thank you.

MR. SHOOK: But the primary focus was the Protection System doesn't operate when it needs to. That's sort of the -- I'll find it. There's a four by four matrix. It's like it operates when it's supposed to. It doesn't operate when it's supposed to.

MEMBER STETKAR: I'm asking about the upper right-hand corner of that matrix.

MR. SHOOK: Yes. I'll get you that information.

In terms of the process automation system and safety automation system, we assume that those systems are operable as long as they're not relying on a Protection System output. For example, the emergency feedwater level control function is started by a signal from the Protection System. So we said, "We're going to assume that that signal doesn't come out of the Protection System.

Therefore, the level control function won't get initiated and therefore it won't start." And so we don't credit that function.

But in the case of the flow control function, the flow control for EFW operates independent. It's not triggered off a signal from the Protection System. It's just looking at flow rate in the system and it just starts controlling once flow rate is above the minimum value. So that loop we assume to be operable as an example.

As long as those functions weren't relying on the Protection System output, we considered the functions of those systems to be operational and could be credited in the analysis.

Then after we established our baseline of what systems within the whole DCS design wouldn't be operable and would be operable, then we started looking at the different Chapter 15 events and then determining what back-up reactor trips in ESF actuations we would need in order to meet our Part 100 requirements as defined by the guidance in B-719.

And so we went through that process and added a number of additional reactor trip functions,

ESF actuation functions, and those are all allocated to the DAS.

And then also I'll just make a point that that analysis bounds the requirements of the ATWS rule, 10 CFR 50.62 in terms of initiating emergency feedwater and turbine trip.

MEMBER STETKAR: Jeremy, I'm trying to get hands around that third bullet and what the implications might mean. I haven't really thought about it very much. So I don't have a decent question.

Do you have a sense? I mean you made that decision to essentially compartmentalize the common cause failures that you were going to say are the subject of your D3 analysis apparently for some reason. What did that buy you?

I mean you mentioned the example of you determined you could take credit for the automated feedwater, emergency feedwater level control function, because that was not within the scope of your postulated software common cause failure because it's not a Protection System function.

MR. SHOOK: Right.

MEMBER STETKAR: What's sort of the

physical basis for it? I mean, is it literally separate, independent, diverse software that runs that function or is it only because you're required to do the D3 for protection signals?

MR. SHOOK: When you look at the report and some of the baseline assumptions that we use, there's an IEC standard that defines a common cause failure as -- You sort of need two things to have a common cause failure. One is a latent defect and then the other is an external trigger or a triggering event that exposes that latent defect.

When we looked at we had segued already the Protection System in SAS. And we said, "Okay. If I have a design basis event (a) that's my triggering event and then (b) my latent defect is some logic in the system that's not going to operate the way it's supposed to. So that's your common cause failure."

What we did with, for example, with the SAS, the analysis is basically most of the SAS inputs are support systems, HVAC, cooling water, so forth. And so the basic premise was those process parameters aren't going to be changing necessarily the initiation of the design basis event the same

way your primary parameters are like pressurized level and pressure.

So you have a different input profile. You're not going to get the same latent defect that's going to be triggered in the SAS that you would have in the Protection System by those inputs. So that was the basis for the argument of why we could basically say that the safety automation system is running fundamentally different. It's controlling basically for the most part different systems, mostly support systems.

And, secondly, the control functions are looking at signal inputs that are basically different than what are inputs in the Protection System. Because you've got a different triggering event and different potentials for latent defects we felt in our judgment that it was sufficient to be able to credit the SAS.

From a practical perspective which I think is maybe what you're interested in is what does this buy you. Right. Now if I have to assume this whole SAS is subject to a common cause failure at the same time as the Protection System, I have to look at backing up all these control functions,

cooling water, HVAC and so on and so forth. From a practical perspective, it's not that hard to put a back-up SI actuation in the DAS because it just actuates and then you're done.

MEMBER STETKAR: I understand that.

MR. SHOOK: But if you have to start looking at "Now I have to have a back-up EFW flow control function," okay, then it gets a lot more challenging to have two control loops. You know you're going to have competing control loops on the same actuator.

And then you have to start looking at complicated schemes of "Now do I have both running and have to deal with the potential oscillatory behaviors of both loops running?" Or do I try to have one be the master and then the other one detect when the other one has failed? It's a lot more complicated from a practical perspective. So that's we tried to isolate the failures to the Protection System.

And we believe it wasn't just we tried to wave our hands away and say, "It's all good." I mean, we do have some good technical justification in the D3 report as I was talking about with the

triggers and the latent defects. But there is some I think --

MEMBER STETKAR: I guess we'll have to look at that. From a risk perspective, a lot of the risk analyses that have been done show those sort of unimportant support systems can be very, very important to overall plant risk especially if you start dispersally to isolate cooling water systems and things like that. Sort of this notion that those are sort of normally operating support systems and we don't need to worry about that because when we put our design basis event blinders on.

It's just something a bit disconcerting. But I'm willing to go read what you did in the D3 analysis.

MR. SHOOK: Okay. Yes. I think the basic idea is that we're not saying you could have a common cause failure of those functions. What we're saying is it's not likely you're going to have a common cause failure of a component of cooling water control loop function concurrent with the DBE because your input trajectories that are going to be resulting from the DBE aren't necessarily correlated with the component of cooling water temperature

control loop for example.

MEMBER STETKAR: Temperature control I'm not so worried about.

MR. SHOOK: Right.

MEMBER STETKAR: I'm worried about reconfiguring systems because of the signals that might be coming in. Things like some things that I mentioned that the system thinks that there is low pressure and for some reason I have a failure of thermal barrier cooler. So I'm going to shut off all component cooling water under conditions where I might want to keep that function.

MR. SHOOK: Right.

MEMBER STETKAR: That's the type of thought process that -- Let's just leave it.

MR. SHOOK: Okay.

MEMBER STETKAR: And we'll see.

MR. SHOOK: One last point I'd just like to make though just to clarify. Even for the support systems like component cooling water ESW if they're actuated on SI those systems are -- those functions are driven directly from the Protection System. And they're not involved.

MEMBER STETKAR: Yes.

MR. SHOOK: So when I start all four trains at CCW --

MEMBER STETKAR: They'll get that.

MR. SHOOK: -- they'll still get that. It's the follow-on controls.

MEMBER STETKAR: Some of the discussion you have -- I was sitting here -- recognizes it's a beyond design basis event that we're talking about, the common cause failure first of all. When you're starting to get concerned about full parallel replication for example of automatic emergency feedwater level control within DAS and how might that interact with SAS.

MR. SHOOK: Right.

MEMBER STETKAR: Or the complexity of designing that function, perhaps you don't need that. Perhaps an on/off, high level/low level for emergency feedwater, for example, is okay within a DAS function to mitigate a beyond design basis event.

MR. SHOOK: Or manual control.

MEMBER STETKAR: Or manual control.

MR. SHOOK: Right.

MEMBER STETKAR: And would obviate this

need to sort of compartmentalize where the common cause failure might occur or might not occur.

MR. SHOOK: Right. That particular example, that's pretty easy.

MEMBER STETKAR: Yes.

MR. SHOOK: But you are starting to get into some of the support systems.

MEMBER STETKAR: Anyway, if it's discussed in the D3 report.

MR. SHOOK: Yes. I'll get you that specific section where it talks about that.

Okay. In terms of the functions for the diverse reactor trips that were identified out of this analysis, they're listed here. And they're all basically the same I think with the exception of the high neutron flux. It's just an absolute value, not a rate, which is in the Protection System. But the other trip functions are essentially the same type of trip functions that are in the Protection System.

One note I'd say about the manual reactor trip for the DAS. Actually, on the SICS, I have actually two trip buttons. I have one set of trip buttons for the Protection System that goes through the Protection System like we showed before.

And that actuates the UV coils and the trip breakers and the trip contactors.

For the DAS I have separate for the switches for manual reactor trip that goes through the DAS cabinets, gets combined with the automatic DAS logic. And then out of the DAS you have the coils on the breakers and the control logic thyristors for the CRDCS.

MEMBER STETKAR: So in the UPs, what do you instruct the operators to do? Go hit reactor trip. There's typically a confirmatory trip. You instruct the operators to hit it on SICS and go over to DAS and hit it over there to make sure you get the redundant things.

MR. SHOOK: We haven't written the UPs, so I can't comment on that. But it's a good question.

Going to the next slide we've got Diversity of Set Functions. In here, you can see in terms of how we've implemented those functions, whether it's automated, manual system level or also manual component level.

And I'll just summate the point. I won't go through which ones, but BTP 7-19 requires

that you provide system level actuation for all your critical safety functions. So some of these are not necessarily required per the analysis that was done, but required because of the BTP 7-19. And then you can see also 73 of the component level controls that's credited in the analysis for the operator to perform certain functions.

MEMBER STETKAR: Just since we discussed it a couple of minutes ago, the manual component level control of BFW system I'm assuming that would be the level control valves.

MR. SHOOK: Level and flow control, yes.

MEMBER STETKAR: And those signals override any signals that are coming out of SAS.

MR. SHOOK: No, they don't. So if I needed to -- I would have to go and take that loop to manual.

MEMBER STETKAR: Over in SAS.

MR. SHOOK: Over in SAS before I could manually perform those functions.

Seventy-four is showing how we allocate the functions within the DCS. So if it's an automatic reactor trip or ESFAS it's allocated to the SCDS, then DAS for the processing and then PACS

for the output. PACS is only for ESF, not for reactor trip.

And then grouped controls are allocated to SICS and then implemented through DAS and then into PACS. Again PACS is only for ESF.

And then component level controls go directly from SICS to PACS.

I'll just make the comment that although not all -- We have provided the design of all component level controls for safety related actuators on SICS. Whether it's credited specifically or not in the D3, that is an aspect of the design. And that path bypass just goes from SICS directly down to the PACS bypassing all the digital control actuation systems. Next slide.

MEMBER BROWN: Is -- Okay. I'll wait until you get to the next slide.

MR. SHOOK: Okay. So here is a little more detail in terms of the DAS and the design for the diverse reactor trips. You can see I've got the same basic signal path as I used for the Protection System. It's all coming through the SCDS.

And then I bring that signal into each of division of the DAS. The DAS we have committed

in the FSAR or specified that it will be implemented in non microprocessor based technology. So that could either be electrical or electronic, in relays or --

MEMBER BROWN: You dictated that in the DCD.

MR. SHOOK: We have, yes.

MEMBER BROWN: Because the note down here in Font 006. So technology may be nonmicro -- Yes, don't try it this way. May be. It doesn't say it will be.

MR. SHOOK: Yes. It's the wording. And I apologize that that's so confusing. What we tried to show with the color scheme is that the blue indicates electrical or electronic technology. And the little note is also a disclaimer to say it could also be non microprocessor programmable or electronic. We didn't know how to make it shaded blue and green.

MEMBER BROWN: And green is what again? It's in one of your other slides.

MR. SHOOK: Non microprocessor based, programmable electronic. So PLD or FPGA.

MEMBER BROWN: Yes. And what's this?

This is that, isn't it?

MR. SHOOK: No, this is electrical or discrete electronics.

MEMBER BROWN: Oh, discrete electronics. Analog.

MR. SHOOK: Right.

MEMBER BROWN: Analog, analog, I should say.

MR. SHOOK: Yes.

MEMBER BROWN: And you've dictated that.

MR. SHOOK: Just forget about what the screen shows because I've made it too complicated. The commitment we've made is that the technology will be non microprocessor based technology. So it could be FPGA. It could be PLD. Or it could discrete electronics or relays. But it can't be a microprocessor with system software or application software.

MEMBER BROWN: Okay. Did you talk about the communications from -- I mean, you've got some type of passing stuff from point to point for voting obviously.

MR. SHOOK: These are all hardwired signals between the different divisions.

MEMBER BROWN: That means?

MR. SHOOK: There's no data communications. It's all zero to 24 volt contact or if you need to -- No, in this case --

MEMBER BROWN: You would expect it to go -- I would expect the stuff to be logic gates and/or PLDs configured to be logic gates as a voting regime, environment.

MR. SHOOK: That's correct. Yes. Right. For example, if you used PLDs, you'd have one PLD module doing your set point comparison. You'd have another PLD module doing your two out of four voting. You'd have to set that up with the design.

But we did specify the specific technology because obviously we wanted to leave ourselves some flexibility from a procurement perspective later on. But we did specify the minimum requirement in order to make the analysis work.

MEMBER BROWN: It would be really nice if you used relay logic.

MR. SHOOK: All I can say is there's a --

MEMBER BROWN: Good stuff.

MR. SHOOK: There's a number of considerations that are taken into account with the final technology. Move onto the next slide.

Again we're just showing again -- I've already talked about the diversity in reactor trip devices. You can see here that the DAS comes in and at the top comes into the control rod drive, control system cabinets and actually gates off the rod control units. So I've got another diverse means of tripping all the rods. And then also you can see the DAS come in at the bottom and hit the shunt trip coils. And you can also see the Protection System inputs as hitting the trip contactor modules and the UV coil and the trip breakers.

MEMBER BROWN: It still does the contactors also, doesn't it?

MR. SHOOK: The Protection System does the contactors. The DAS itself only -- I shouldn't say only. The DAS itself trips the rod control unit logic to disable the control logic and the --

MEMBER BROWN: I got that far.

MR. SHOOK: And then it hits the shunt trip coil on the trip breaker.

MEMBER BROWN: I got that.

MR. SHOOK: And that's it. That's all the DAS does.

MEMBER BROWN: But in terms of -- I mean you've got this trip breaker configuration that if you trip one and two you don't scram. I mean you don't change the --

MR. SHOOK: Yes, I know. It's the same.

MEMBER BROWN: It's the same. Right?

MR. SHOOK: That's right. That's correct.

MEMBER BROWN: So you're really depending upon turning off the gates.

MR. SHOOK: In both designs we use single failure criteria.

MEMBER BROWN: I've heard you.

MEMBER STETKAR: Two-thirds of the time and a random selection logic, they'll get both trip breakers open.

MEMBER BROWN: The right two.

MEMBER STETKAR: One in each line.

MEMBER BROWN: Hopefully.

MEMBER STETKAR: One of the SICS combinations will get the right one. Will get you a trip.

MR. SHOOK: Okay. Moving to Slide 77, we show the diversity in ESF actuation and control. So again your automatic ESF functions, the signals are routed through the SCDS and then are sent to the DAS, each division. And then again you've got hardwired signals going back and forth for voting between the different divisions.

You have system level actuation of those functions listed in the tables previous from the SICS going directly to the DAS. And then you can also see manual component control going directly from SICS to the PACS. Okay.

And then Slide 78, I would say these are the key elements of diversity for the systems that are relied upon the credit mitigation for common cause failure in Protection System. The SCDS, when you look at the inputs to the DAS show the Protection System, those input signals are conditioned and distributed using electronic I&C technology. So there's no software common case failure.

I will point out that there are some -- Some of the temperature conditioning modules in the SCDS for inputs going to Protection System do

utilize some programmable electronic technology. But those inputs we don't use temperature inputs in the DAS. So the message is that for the inputs that we're relying on to be diverse it's all processed through electronics and therefore we don't have to postulate a software common cause failure.

The DAS, as I said we've committed, made the commitment, that it's going to be non-microprocessor based technology.

And then when you look at the SICS as we talked about before we have dedicated indicators with hardwired input directly from the SCDS and PACS bypassed in the computers. The Protection System.

And then lastly the PACS, the priority module utilizes a PLD. We committed to in the FSAR to be 100 percent tested so to assure that there's no latent defect from a programming.

MEMBER BROWN: This is the same priority module that's in the other thing. Right?

MR. SHOOK: That's correct.

MEMBER BROWN: So you don't change -- You don't have a different thing there.

MR. SHOOK: No.

MEMBER BROWN: It just feeds the same

thing that the other system does.

MR. SHOOK: That's correct. Yes.

MEMBER BROWN: What did you say about the SCDS?

MR. SHOOK: The SCDS for the input that are shared between the PS and DAS, the inputs are processed using electronic boards, cards. So I don't need to -- Because they're not programmable, I don't need to consider.

MEMBER BROWN: Same ones?

MR. SHOOK: It's the same one. Yes.

MEMBER BROWN: Okay.

MR. SHOOK: But my point is because those cards are just discrete electronics, I don't have to consider those --

MEMBER BROWN: That's fine.

MR. SHOOK: Okay.

MEMBER BROWN: I just didn't understand everything you said the last time.

MR. SHOOK: Okay. And that's it for the presentation.

MR. GARDNER: That concludes our portion.

CHAIR POWER: I almost hate to ask. Are

there any more questions at this time?

(No verbal response.)

If I had a silver star to give out for this, I would give you a silver star for an outstanding performance.

MR. SHOOK: Thank you. I appreciate that.

CHAIR POWER: But I don't. So you're not going to get one from me.

(Laughter.)

I think at this point we'll turn to the staff.

MR. TESFAYE: Okay. Would you like to take a break before we do the staff's presentation or continue?

CHAIR POWER: I think we should go right ahead.

MR. TESFAYE: Okay. Dr. Powers, before I turn over the presentation to Mike Canova, he's also the lead PM for US EPR design certification. I would like to give an opportunity to Terry Jackson who is the Branch Chief for I&C Branch give us an update on Chapter 7.

MR. JACKSON: Thanks, Gatachew. My name

is Terry Jackson. I'm the Chief of the Instrumentation Controls and Electrical Engineering Branch No. 1 in the Office of New Reactors. My staff was responsible for reviewing the EPR and I&C design.

And since my staff is going to give a little background about themselves, I'll give a little bit about myself as well. I have a bachelors in Computer Engineering and a masters in Electrical Engineering. And I hold a Professional Engineering license in Electrical Engineering in the State of California.

I've been with the NRC for 17 years. And I first started out as a digital I&C engineer in the Office of Research. And I worked seven years as a resident and senior resident inspector at Diablo Canyon. And then since 2007 I was the Branch Chief for this branch.

Soon after coming here in 2007, we began reviewing the EPR design certification application. One of the things I noted earlier was that I'm also the chair of the MDEP EPR I&C Technical Expert subgroup which is as I mentioned actually six countries when I thought about it a little bit more

which includes Canada, China, France, Finland, United Kingdom and United States where regulators get together and we discuss common issues and topics with regards to EPR design. Of course, MDEP also covers over design such as AP1000 and some issue specific items such include digital I&C as well.

But that group's been meeting for the past three years and it's changing informational EPR I&C design. And as I mentioned we've gained information from the foreign regulators as well as we provide then with some valuable information as well.

One of the things I want to note was just the staff effort has been about three and a half years' amount of effort into the EPR I&C design overall. And it's about -- We've invested about 20,000 hours into the review.

And one of the things that you'll see in our presentation is that the staff has been working hard at addressing key technical issues and so forth. And actually I think we've done a good job addressing a lot of these. There are still a number of open items that we're still working on as well. But I hope that the Committee will see the effort

and also appreciate what the level of effort the staff has put into the review.

CHAIR POWER: Thank you.

MR. CANOVA: Good afternoon. My name is Michael Canova. I'm, as Getachew identified, the Chapter 7 PM for the US EPR design certification.

By way of background, I'm old. I have a BS from Johns Hopkins. I spent 36 years at Constellation Energy, 20 of that in the I&C area, either in design or procurement engineering. And a good piece of that right at the beginning of my career was working through TMI era and the TMI lessons learned. My phone number is still a bane to the people that call me up. It's 0737.

(Laughter.)

Today's presentation covers SAS Phase 2 safety evaluation report for Chapter 7. The first slide gives the objectives. This is more to keep us on focus than you. We're here to provide you some of the details in our review and provide a common understanding of the background, the efforts and the current status of that review.

The review team, the first three members are sitting up here including Jack Zhao, Tung Truong

and Deanna Zhang. And soon to join us is Ken Mott, Deirdre Spaulding Yeoman. Wendell Morton will be rotating through the chair to go through their various sections.

Just by way of introduction, this is just the layout. We'll do an intro, some background, and then go through the key topics of interest in terms of redundancy, independence, determinism, diversity, simplicity of design. And then the other technical topics of interest are self testing and self automation systems. And then a discussion.

I'm going to present shortly also a list of the open items. First, I want to just give a little background on how everything was laid out in the SE itself. AREVA submitted the design cert in December of 2007.

The Safety Evaluation and related reports represent as Terry said three and a half years of effort by the staff and Applicant.

On June 25, 2010, AREVA proposed to make several refinements to their previously submitted design in order to support continued review. The meeting summary is actually indicated here. And it

also included the staff's evaluation of where we were at that point in time.

The SE for Chapter 7 is based on Revision 2. So Member Stetkar was correct. Revision 2 was where we were when we were writing. But there was frequent reference made to Interim Revision 3 mark-ups. These came in with a series of RAIs.

These identify AREVA's commitments to changes. They've been submitted with these RAIs.

These design changes are reflected in mark-ups submitted for actually unrelated RAIs. There's actually a last RAI in each section which came in with a full set of mark-ups for that entire section. So that we'd have everything in front of us. So we pretty much have that Rev. 3 docketed as interim mark-ups and that's what we used to close the gap.

One other thing about that is after we finished the SE Revision 3 was actually docketed and is now in-house. So there's actually a couple of places in there that you'll see us actually talk to Revision 3 because we tried to close some of the gap on the SE as we polished it up and finished it up.

This is an overview of the DC in terms of RAI questions that were written. Two hundred ninety-three questions total. Thirty-six open items are now standing. I've got a list of them behind us. But the staff is going to integrate those major open item questions into their discussion of each area as we walk through it.

As spoke of before, this actually presents a list of primary documents including technical reports, topical reports and the Interim Rev. 3 information that we've been looking at to complete the SE.

And I'm just going to page through these quickly if you want to take a look at them. I believe they're in your slide set also. If you see any that is of interest to you, please bring them up at the appropriate time as we go through the sections. We're going to go through section by section.

Jack, do you want to take it from here?

MR. ZHAO: Yes. Good afternoon. I'm Jack Zhao, a Senior in the Technical Review in the I&C Branch at the NRO office.

A little bit of background about me. I

went to college and graduate school in China. After working five years there as an I&C engineer, I did a few more years graduate study at Penn State on a scholarship. After graduating from Penn State, I went to work for Bechtel Power Corporation. After working for 12 years for Bechtel, I joined the NRC about three and a half years ago. Basically that's it about me.

Today, first, I'll present the major technical issues with the original U.S. EPR and safety issues the staff raised. And also I'll talk about the major technical changes made by the Applicant to address the staff's concerns.

For the original and EPR I&C, the first major concern the staff raised is complexity of the EPR I&C architecture. The second major technical issue is communication independence for the safety systems. Because individual communication was extensively used in those safety I&C systems.

The third main concern the staff raised is also about the communication independence issue between the safety system and the non-safety systems because in the original I&C design for those systems used a bi-directional data communication.

The fourth concern the staff had is about continuous connection between the safety systems and non-safety service unit.

The final concern the staff raised is related to qualification of the safety display system for the SICS.

In the public meeting just mentioned in the presentation, the Applicant made a significant changes to the original I&C designs. They will all be present and talk about some major technical changes for those to address the staff concerns. Next slide please.

MEMBER BROWN: So they made all those -- They made a number --

MR. ZHAO: Significant changes, yes.

MEMBER BROWN: -- relative to that meeting, that public meeting, you had where you went through all the concerns and the issues that you all had with the level of complexity. So what we saw today was a fallout of the revised design.

MR. ZHAO: Exactly.

MEMBER BROWN: Okay. All right. Thank you.

MR. ZHAO: To address the staff's

concerns and the complexity of the original I&C design, the Applicant made substantial changes to reduce the complexity of the original I&C design.

First, the Applicant revised the I&C design to minimize the use of the inter-divisional communication for the safety systems.

Second, the Applicant modifies the I&C architecture to reduce the safety I&C system's dependence on the plant data network.

Third, the Applicant fundamentally changed the safety indication on the control system or SICS design for a micro process based system to a hardware based system.

Finally, the Applicant deleted the severe accident I&C system and they incorporated the functions of the other I&C systems.

So all those changes simplified the original EPR I&C design. And the current I&C architecture is less complex. Next slide please.

The staff as I just mentioned questioned the communication independence issue among the redundant divisions for the original SICS, SAS, and PS Safety Systems. For the SICS to address the communication independence issue, the Applicant

fundamentally changes the design to hardwired basically in the I&C system and it does not use any inter-divisional communication.

For the SAS, the Applicant originally used the 2nd min/2nd max function. This function requires individual communication. The staff questioned the safety justifications for this function in the SAS system. To address the staff's concern the Applicant modified the design and they reduced the inter-divisional communication in the SAS system.

For the PS, the EPR design uses 72 SPNDs as to calculate two reactor-trip functions. In the original PS design, 18 SPNDs of the 72 are hardwired to each division. The design used the inter-divisional communication to get the rest of the SPNDs to calculate the reactor-trip functions. So inter-divisional communication was the extensive use of the original EP and the PS design.

The staff raised the concern under communications independence issues for this design. To address the staff's concern, the Applicant revised the SPND design to hardwire all 72 SPNDs to each division basically. As I just mentioned, each

division needs all 72 SPNDs.

MEMBER BROWN: The white paper or the little paper that I got I don't know somewhere implied that that was the original design and that was to allow the maximum -- I may have read this wrong, but I mean it was as part of the SICS 6031991 or 6031998. And in the back of that was the benefits of 72 in each PS division which made it sound like there was no way you could wire this thing up with 18 to each division. MS. ZHANG: In the original design, they had 72 SPNDs coming out of the core.

MEMBER BROWN: Right.

MS. ZHANG: They still split it into four divisions of 18.

MEMBER BROWN: Right.

MS. ZHANG: But each division of the production system needs all 72 to make their reactor trip function.

MEMBER BROWN: Yes.

MS. ZHANG: But instead of hardwiring the outputs from the SPND outputs to each Protection System division, 18 was acquired by each division and then sort of a ringed network.

MEMBER BROWN: I understand that.

MS. ZHANG: Yes.

MEMBER BROWN: I understand that point. But based on his explanation and yours, yes. I guess maybe the argument was made in here that you couldn't process just 18 and generate a trip in each division from 18 and still achieve the same benefits of the whole core mapping of the flux.

MS. ZHANG: Yes.

MEMBER BROWN: Power as it's throughout the core. Okay. Maybe that was -- Maybe that's where I'm mixing it up here, apples and oranges.

MS. ZHANG: So the 18 that was acquired they're not producing the reactor function.

MEMBER BROWN: They're saying that if you just use 18 you don't get as an efficient setup. That's what they were talking about. Okay. I got the picture now. Thank you.

MR. ZHAO: Now the 72 SPNDs are not redundant to each other. In other words, the SPND design in the EPR system does not meet the NRC requirements and the independence and the redundancy.

But in the duties it's a design and

there are some safety benefits of the SPND system. So the Applicant supplemented alternative requests to address these deviations. So we will present more in the evaluation on an alternative request. Next slide please.

The staff also raised the communication independence issue related to the bi-directional communication using a different safety system and the non-safety system in the original I&C design. To address the staff's concerns, the Applicant changed the design by using the physical limited, one way communication only from safety to non-safety systems.

The staff questioned safety justification for the permanent and continuous connection between the safety system and the non-safety service units in the original design. The Applicant, after they revised their designs, disconnected the permanent connection except for the maintenance and surveillance testing. Next slide.

During the review process, the staff found there are some issues of independence and the software quality for the original AV482 based on the PACS design. In order to address the independence

issue, the Applicant revised the PACS design by separating the non-safety related communication board from the safety related priority logic board.

Originally, the two modules are on the same -- too much on the same board. So there is an independence issue there. To address the quality issues, the Applicant provided a commitment to use the 100 percent combination test for the revised PACS system.

In the US EPR DCD the Applicant took credit for the TXS self-testing and the monitoring function to meet the part of the TXS surveillance testing requirements. But the EPR DCD does not include enough information on how safety self-testing and then monitoring functions are credited. So in order to address the staff's concern, the Applicant submitted a new technical report for the US EPR DC application.

One of my colleagues will present more evaluations in this area. Next slide please.

The staff also raised some concerns D3 assessment for the original EPR I&C design. Originally, DAS is a diverse actuation system and it was part of the non-safety PAS system by using the

plant data network. In order to simplify the I&C design, the modified I&C architecture separated the DAS from the PAS and the plant data network.

So the revised I&C design morphed as a DAS manual control and an indication from the non-safety PICS to the safety rated SICS system. The DAS design was changed from a microprocess based system to a non-microprocess based system to be diverse from the microprocess based safety systems.

During the review, the staff found that the original US EPR DCD under D3 technical report didn't include any best estimate analyses as required by the BTP 7-19. So to address the staff's finding, the Applicant is submitting a best estimate analysis in the revised D3 report to support the design of the D3 functions.

That's all from my presentation. Next my colleague Tung Truong will present the staff's technical evaluation and the redundancy requirements for the EPR I&C design. Thank you very much.

MR. TRUONG: Good afternoon. My name is Tung and I went to U of I for my bachelors in electrical engineering and I went to work at Motorola as a software developer. And after that I

went back to graduate school. I got my degree in computer engineering. And after that went to the Navy Center in San Diego for five years and then came here for the past three and a half years.

This afternoon I'll be going over slides on redundancy. Overall the US EPR I&C Safety Systems can sustain a single failure and complete a safety function. And it meets the NRC requirements, the GDC and the IEEE standard. And each system has a single-failure ITAAC to verify the design commitment. And the staff's evaluation is in Section 7.1.4.5 of the SE. Next slide please.

Early this morning or this afternoon, AREVA already presented --

MEMBER BROWN: Question on the single failure ITAAC, is that an analysis or is that an actual physical test?

MR. TRUONG: They will provide a report.

MEMBER BROWN: A report, okay.

MR. TRUONG: That confirms.

MEMBER BROWN: All right. So they're going to drag themselves through the potential single failures and show that it works okay.

MR. TRUONG: Yes, sir. They have -- The

next slide. There is an FMEA in the detail of --

MEMBER BROWN: Is there any hardware testing where you take something out of service when you're trying to shut something down or trip it?

MR. TRUONG: I should let the reviewer answer that question.

MEMBER BROWN: As part of the qualification program?

MR. STACK: Could you repeat the question?

MEMBER BROWN: Yes. You've got redundancy. Do you ever run a test that shows that the redundancy actually performs like it's supposed to? In other words, you introduce a trip into some channel failed or some systems failed or various pieces failed throughout the thing to see that it still does what it's supposed to do.

MR. SHOOK: In terms of the -- Let me just answer the -- Are you talking about during design or during operation?

MEMBER BROWN: Qualification, not during operation. During qualifications.

MEMBER STETKAR: Make sure you're up close to the microphone because that will pick you

up.

MR. SHOOK: So the question is during qualification and testing of the design.

MEMBER BROWN: Qualification of the design. Some place where you check to see that if it's wired up the way it's supposed to.

MR. SHOOK: I can say that we do failure modes and effects analysis which at the system level FMEA has been supplied as part of the FSAR.

MEMBER BROWN: I heard that part.

MR. SHOOK: Okay.

MEMBER BROWN: I was asking about actual --

MR. SHOOK: But during the qualification testing.

MEMBER BROWN: Yes. Something failed high or low and one of the other channels at the same time you get trips. Does it still process it as a trip in other words?

MR. SHOOK: Yes. As part of the FATT testing they'll run through those various checks.

MEMBER BROWN: Hardware testing.

MR. SHOOK: Well, we call it -- It's FATT or system integration testing. So you start

off and do the software testing. Just the software. Then we'll integrate it with the hardware that's built. And then you'll do a system integrated test or a FATT test. And that's when you're checking -- You're essentially treating the protection system as a black box at that point. So you're looking at your inputs and then looking at the outputs. And you'll be failing measurements high and low and making sure the system responds the way you design the two.

MEMBER BROWN: Okay. Go ahead.

MR. DOYEL: This is Chris Doyel for AREVA. And I can't specifically recall, but I do believe that in the development of the topical report for the TXS platform that in the qualification process in Germany that those types of tests were done.

MEMBER BROWN: That's the platform itself, not the whole multiple division stuff.

MR. DOYEL: Okay.

MEMBER BROWN: I mean it's a matter of making sure your two-out-of-four actually work when something shorted or whatever on the input to the voting units. Does it really work that way? That's

a failure. That's a single failure that can happen depending on -- It could be a logic unit. It can be software. It can be whatever. I'm just curious if you did that. And the answer is don't know.

MR. ZHAO: It should be done in the integration testing.

MEMBER BROWN: I presume. I just ask if they did it.

MR. FREGONESE: I'll make a comment. This is Vic Fregonese with AREVA. I personally witnessed testing of this type in Europe both our Acony systems that's installed there and the system we're deploying at the EPR's worldwide have an extensive hardware and software integration test.

The functional requirements for the system rolled down into the test plan. And we have an independent verification and validation group that conducts that test independently. And they validate all the functional requirements of the system that include the failure modes that are assumed, hardware failure, software failure, power supply, power up, power down, all of those tests. And in fact the NRC for the Acony system witnesses those and we have independent witnessing by quality

assurance personnel.

MEMBER BROWN: It's actual tests, not just on paper.

MR. FREGONESE: Absolutely.

MEMBER BROWN: Okay. All right.

MR. FREGONESE: Full integrated test in the test field.

MEMBER BROWN: That's all I ask.

MR. FREGONESE: Completely wired up.

MEMBER BROWN: That's fine.

MR. FREGONESE: Thank you.

MEMBER BROWN: That's all I needed. The answer was yes. It was hard to get to, but the answer is yes.

MR. TRUONG: Okay. For the protection system, that's the integrated reactor trip system and ESF systems. They are four redundant, independent PS divisions with redundant power supplies and early on represented redundancy at the APL/AOU level. And again there's an FMEA for the PS system.

And for the PACS there the redundancy mirrors the mechanical train system. For example, the emergency feedwater is four trains and for each

there's an associated PACS module. And again this is also describing in the PS FMEA. Next slide.

For the other safety systems, like the SICS, in-core, ex-core, the boron concentration and so on, there are sufficient level of redundancy and there's also ITAACs for each as well. And there are some questions that the staff has asked AREVA and that's just pending.

And for the SAS system, there are four, redundant, independent divisions and currently there are a couple open items which my colleague will speak to about later to address later on. And that's it for redundancy.

CHAIR POWER: At this point, I'm going to interrupt and avoid a rebellion on my Committee and take a break until 3:30 p.m. Off the record.

(Whereupon, a brief recess was taken.)

CHAIR POWER: On the record. Let's come back into session. I'm sorry to interrupt.

MS. ZHANG: No problem.

CHAIR POWER: But I was facing rebellion here. Mutiny is so abashing in public.

MS. ZHANG: Hope everyone had a good break. I really like the bathrooms on this floor.

They have these fu-fu soaps that make your hands smell so good.

MEMBER STETKAR: Maybe in your bathroom.

MS. ZHANG: Before I go into independence, my name is Deanna Zhang. I graduated from the University of Maryland with both my undergraduate degree in electrical engineering as well as my graduate degree in electrical engineering. I study in the area of magneto-optics and also semi-conductor physics. Nothing to do with I&C.

I had my heart set out on going to Intel and being a process engineer there. Well, one life event changed that. I got engaged and then married. So I think it's actually two life events.

Then to find a job very quickly, I got a job at BoozAllenHamilton as a consultant for the DoD. I worked there for a couple of years mainly on satellite communication systems. Then I got a job here at the U.S. Nuclear Regulatory Commission and I've been working as a technical reviewer in the area of I&C for the past five years.

My presentation today focuses on two topics. The first topic is independence. The

second topic is determinism. On this slide -- Before I begin, I want to start by discussing that my presentation is my only focus on communications independence. Physical separation and electrical isolation of safety systems was in the U.S. EPR design. Relatively straightforward. They are designing with IEEE Standard 603 and IEEE Standard 384. So I know Charlie may disagree.

MEMBER BROWN: I'm just listening.

MS. ZHANG: Okay. So for the evaluation against data communications independence or for conformance to data communications independence, I evaluate each of the major safety systems against the 20 criteria within digital I&C ISG 04.

For those of you who are not familiar it was the interim staff guidance. It was developed under the digital I&C subcommittee working groups 04 and it provides -- it has three sections. The first section provides 20 criteria on communications independence between safety divisions and between safety and non-safety systems. The second section discusses priority functions. And the last section discusses multi-divisional control and display functions.

Some of the other systems that I did not evaluate for data communications independence are SICS and the SCDS systems. They do not use microprocess servers and they do not perform any data communications.

For the safety automation system, that finds that SAS conforms with most of the 20 criteria which was in ISG 04. Specifically the staff found that only information that enhances or is used in safety system functions is accepted from outside its safety division. And although the slide says i.e., voting logic, it should really be e.g., voting logic because of the cross train functions that were introduced earlier for interlocks.

CHAIR POWER: That's okay. We're not good at Latin here anyway.

MS. ZHANG: In addition, only discrete data is sent between divisions. And that's only for the cross train functions also.

The staff also found the use of dual port RAM between processors and the separation between safety processors and the communications processors meets the criteria within ISG 04. And that only predefined data messages with fixed length

and headers are generated and accepted by each safety functions processor.

The staff does have one open item regarding how invalid signals from outside the division is handled? As was discussed this morning for the Protection System, they do voting logic modification for invalid signals that come in. There is one invalid signal and it modifies the voting to two out of three. It's unclear how in the SAS that's handled whether there is any voting logic modification. Next slide.

For the Protection System, with the exception of the use of SPNDs, The staff finds that the Protection System complies with all 20 criteria within ISG 04, Section 1 or provides an acceptable deviation from the guidance. And similar to the SAS, the use of only pre-defined data messages with fixed length and headers that are accepted by the function processors as one way of ensuring that only valid data is accepted and the use of error detection to ensure erroneous messages are not processed by the function processors. And invalid signals are accommodated through identifying invalid signals and modifying the voting logic to

accommodate.

MEMBER BROWN: You all agree that corrupted information will 100 percent be detected and rejected and not utilized in any processors.

MS. ZHANG: It's portions of it. The staff will later discuss about the washed-out timer functions.

MEMBER BROWN: Okay.

MS. ZHANG: Next slide.

MEMBER BROWN: I couldn't let you get away without saying that.

MS. ZHANG: I know. It's the way these slides are organized. We could jump ahead, but I don't think so.

(Laughter.)

MS. ZHANG: Next slide.

MR. TESFAYE: There is a problem. I don't think we put the last email I sent. It's not just you.

MR. WIDMAYER: Actually I did use the last one.

MR. CANOVA: This is actually what should be presented on that slide.

MS. ZHANG: You know what? I don't

think we really need to go through a diagram. It's very similar to the one that AREVA showed this morning. So I think we can skip this.

MEMBER BROWN: Yours is a little clearer.

MS. ZHANG: Yes. Mine's a little prettier. I actually hand-drew that.

CHAIR POWER: Let's move ahead.

MS. ZHANG: The next slide. So the next couple slides I want to talk about the alternative request for The SPNDs. As had been mentioned before, The LDMBR and The HLPD reactor trip functions are based on the 72 SPND measurements. Each division of the Protection Systems received all 72 measurements for evaluating core conditions.

Each SPND sensor occupies a unique location within the core and that's multiple redundant SPNDs can't be co-located. As such, these 72 SPNDs must be shared among all four divisions of the Protection System.

Thus, The SPNDs do not meet the traditional redundancy and independence requirements as required by 603-1991, Clause 5.6.1. However, The SPNDs provides a more localized reading of the core

conditions over traditional ex-core detectors. Next slide.

In the original design, as we had mentioned before, the 72 SPND measurements were divided into four sets of 18 that were sent to each Protection System division. Each division processes the received SPND signal and then shares the process signals among all four divisions through various ring networks and point-to-point networks. The staff found that this design did not demonstrate compliance with independence requirements.

In the new design, analog hardware components are used to amplify and multiply The SPND signals and 72 electrically isolated signals are provided to APUs in each Protection System division via The SCDS. And they are electrically isolated I believe through our OPAMPS. During an audit, we had looked at some of the components for that distribution and multiplication components for The SPNDs.

MEMBER BROWN: What do you mean by multiplication? I mean, or isolation? You've got 72 detectors independently coming in and they go to

72 different scaling and conversion.

MS. ZHANG: When they come out of the core since there's only one set of them and each division needs it.

MEMBER BROWN: One set of what?

MS. ZHANG: One set of 72 SPNDs. So there's no duplicates.

MEMBER BROWN: They split them out.

MS. ZHANG: So they have to split it. They have to multiply the signal, each of The SPND signals four times so that each division gets them.

MEMBER BROWN: Okay. Terminology issue.

MS. ZHANG: Yes.

MEMBER BROWN: We didn't multiply in my program. We split the signal.

MR. CANOVA: Seventy-two times four channels.

MEMBER BROWN: I got that.

MS. ZHANG: That's why not an I&C.

MEMBER BROWN: Only terminology, Deanna. I didn't understand what you meant by that. Thank you.

MS. ZHANG: After acquisition, by The APUs, each division of The Protection System

independently performs The HLPD and The LDNBR calculations and downstream voting logic. Therefore, the two reactor trip functions exhibit traditional redundancy and independence from The APU acquisition of the SPND measurements through the reactor trip breaker. So treat them like other sensors from that point on.

However, the staff finds that a single failure in the upstream of the SPND input channel does impact all four divisions of the Protection System. So the staff requested the Applicant provide more information as far as how an undetected failure in range can be accommodated by the Protection System.

The Applicant included in their alternative request a description of the conservative setpoint selection that will accommodate this single, in-range, undetected failure.

Based on the information provided, the staff finds that the alternative request is acceptable pending submittal of necessary revisions to Chapter 15 accident analysis. Specifically, the staff finds the use of the 72 SPNDs relative to ex-

core detectors provided more direct measurement of core conditions and provides a reduction in the level of uncertainty in the assumptions made.

And the staff finds the use of the 72 SPNDs shared by the Protection System divisions to divisional approach provides an acceptable design that can enhance plant safety by accommodating multiple SPND failures. Since it's 72 SPNDs, they can accommodate up to six failed SPNDs before initiating a reactor trip.

MEMBER SKILLMAN: Question please.

MS. ZHANG: Yes.

MEMBER SKILLMAN: You talk at ease about 72. But as I understand it, it's really 12 fingers of six detectors each.

MS. ZHANG: Yes.

MEMBER SKILLMAN: And I'm presuming that those 12 fingers are somewhat geometrically representative of the flux in the core.

MS. ZHANG: Yes.

MEMBER SKILLMAN: My question is for a particular finger or a particular detector in finger how one knows the heat flux based on the neutron flux is accurate for that location.

MS. ZHANG: I'm not an expert on that, but there is also a separate system that validates The SPNDs through -- There is Aeroball System that get sent in every 15 days that basically it's like an aero track to make sure that The SPNDs are calibrated correctly. But I could defer to AREVA if you want it explained further.

MEMBER SKILLMAN: I would if we could just -- I would like just a brief explanation so that I can become comfortable of the degree of attention that's been given to knowing that The SPNDs that are being used for reactor trip are doing so properly.

MR. ROYAL: This is Mark Royal for AREVA. I'll try and address your question. We have provided a lot of information in Chapter 4 previously about SPNDs and Aeroball system.

MEMBER SKILLMAN: Okay.

MR. ROYAL: Also there is a technical report about the in-core system and also a topical report about The Powertrax system which also encompasses information provided about SPNDs and Aeroball system. Both of those have been provided to the staff for review.

MEMBER SKILLMAN: Thank you. I think I'd better take the action and look at Chapter 4 and look at that information.

MR. ROYAL: Okay. Specific RAIs that I think you would get really good information for are RAI Set 194 and RAI Set 205 from Chapter 5.

MEMBER SKILLMAN: Yes, sir. Thank you.

MR. ROYAL: Thank you.

MS. SLOAN: This is Sandra Sloan from AREVA. One other place that might be a condensed way to look at the information and save you having to look at that is our Chapter 4 presentation to ACRS. I think that had a lot of good pictorial diagrams and puts it in one place. It saves you having to look in like six different places.

MEMBER SKILLMAN: Thank you. Deanna, thank you.

MS. ZHANG: Okay. Next slide. Next I'll move onto the evaluation for independence between safety and non-safety control and display systems. The staff also used ISG 04 for this evaluation. Particularly the staff evaluated communications links between the Protection System and SAS with the PICS. And other non-safety systems

and links between the Protection System and SAS with the non-safety QDS was in the SICS and the interface between the PACS and non-safety systems.

The staff finds the communication link demonstrates compliance to ISG 04 or provided an acceptable alternative. Particularly, the staff found that since no data is received from non-safety control systems to the SAS and Protection System through the uni-directional communication link from the Protection System SAS out to the plant data network. Any failure from the non-safety control network or the non-safety control systems connected to that network will not be able to virtually impact the Protection System or the SAS. That was described in detail earlier by Jeremy.

Also the isolation is achieved through a Class 1E device that enforces uni-directional data flow from the Protection System/SAS to the control systems. Those are those EOCs, electrical optical converters.

And for the PACS, the staff finds that only the non-safety communication module that PACS receives data from the non-safety system and that non-safety system data is translated to discrete

hard-wire signals before it's sent to the actual priority module. Next slide.

The staff also evaluated the data communications between the Protection System and SAS with the service unit. The staff finds the interface between the Protection System and SAS with the service unit is acceptable through demonstrating compliance to ISG 04 or providing an acceptable alternative. Specifically, the staff finds that the communications path between the service unit and the divisional MSIs for the Protection System and SAS is normally disconnected through a hardwired disconnect.

This is achieved through isolation switches which ensure that only the one division can be connected at a time between the Protection System or SAS with the service unit. The MSI provides authentication and error detection for messages sent between the service unit and the Protection System/SAS while they are connected.

The staff does have one open item to ask for clarification on how isolation is achieved between the RPMS and the service unit. Next.

MEMBER BROWN: Before you do that, there

was a question I forgot to ask and I'm trying to figure out which slide this applies to. I guess it was 32. I forgot to ask this question earlier and this relates to my later observation of the way the PICS data network server bus is configured.

There's a gateway shown in the Figure 7.1.2 coming off the Protection System from each division. And it said it feeds the PICS. And I presume it's that data bus of some kind through that gateway.

MS. ZHANG: Yes.

MEMBER BROWN: And the gateway, I tried to find some discussion of how that gateway is configured. Is that a --

MS. ZHANG: It's just like a server.

MEMBER BROWN: No, the gateway. The gateway, not the server server. But the gateway itself.

MS. ZHANG: It's essentially a computer. It's --

MEMBER BROWN: Okay. Now wait for a minute. It's supposed to be one-way device. But how is it configured as a one-way device?

MS. ZHANG: The gateway itself is not

configured --

MEMBER BROWN: There is data that goes from the Protection System to the gateway.

MS. ZHANG: The device that's enforcing the one-way communication is the electrical optical convertors. That's before the gateway. So it's between the --

MEMBER BROWN: That's out of the Protection System.

MS. ZHANG: Out of the Protection System and then to the gateway before it gets fed to the data network.

MEMBER BROWN: Okay. So that's -- Is that where they talk about the only the send fiber optic is attached.

MS. ZHANG: Yes.

MEMBER BROWN: And the receipt is not.

MS. ZHANG: So my next figure will show that.

MEMBER BROWN: Okay. That's fine.

MS. ZHANG: Can you go back to -- That's kind of why I wanted to go to the next figure. Can you?

MR. CANOVA: Which one?

MS. ZHANG: Whatever slide I was at before.

MEMBER BROWN: Thirty-four.

MS. ZHANG: Thirty-four. So you see how there is two electrical optical convertors there between the safety side and non-safety side. Those two sets between the first one and the second one is what enforces the uni-directional communication. So that's fiber optic out.

After the second --

MEMBER BROWN: Is that like two OLMs on this picture?

MS. ZHANG: Similar but they're only one way. So you're not connecting the one back.

MEMBER BROWN: I understand that.

MS. ZHANG: Yes.

MEMBER BROWN: Okay.

MS. ZHANG: Then on the other side there's a gateway. And the difference between The EOCS and The OLMs, The OLMs are configured to talk pro feed bus. These are not I don't think.

MEMBER BROWN: No. So these are the ones you're talking about that just have the one way fiber. They don't connect the receipt, only the

transmit.

MS. ZHANG: Yes.

MEMBER BROWN: Okay.

MR. MOTT: This is also on AREVA Slide 21 where they were showing this uni-directional signal only coming out of the first CLC coming out of the safety system from the MSI that we're discussing right now.

MEMBER BROWN: Okay. Got it. Thank you.

MS. ZHANG: It's the same type of connection.

MEMBER BROWN: Shows you how long I remember stuff.

MS. ZHANG: This is the same type of connection going between the Protection System and SAS with The QDS also since The QDS is non-safety related.

MEMBER BROWN: Okay. Thank you.

MS. ZHANG: Next slide. So the next few slides we're going to talk about determinism as well as the TXS features that support deterministic operation. The staff finds that The TXS system operates and communicates in a deterministic manner.

This includes the use of pre-determined fixed cycle times for all TXS with the same sequence of processing steps in each cycle.

MEMBER BROWN: Before you go any farther because it's another question I forgot to ask when AREVA was up here when they were showing the picture of the execution cycle which is what you're talking about here. Is that execution cycle and a description of it actually contained in the topical report?

MS. ZHANG: It's actually --

MEMBER BROWN: The picture.

MS. ZHANG: Yes, it's part of The TXS topical.

MEMBER BROWN: The TelePerm topical.

MS. ZHANG: Yes.

MEMBER BROWN: I just wanted to make sure it was in there and wasn't just a paraphrasing of how it's supposed to work. That's all.

MS. ZHANG: No. It's same exact.

MEMBER BROWN: Okay. Thank you.

MS. ZHANG: The staff also finds that through The use of constant message sizes and communication rates will result in constant

communication loads under all circumstances and that The communications protocols used in The TXS system do not require acknowledgment of The transmitted message by The receiver as well as no process-driven interrupts. And The use of The hardwired watchdog timer triggered by self-test features in The run-time environment. These are all features that contribute to The deterministic operation of The U.S. EPR safety systems.

In addition, The Applicant provided a response time analysis for The Protection System and an ITAAC to verify that response time. Next slide.

This is about The watchdog timer, Charlie.

MEMBER BROWN: Are you trying to get my attention as I'm writing The answer down from The previous question?

MS. ZHANG: I'll give you time.

MEMBER BROWN: You can go ahead. I'm listening.

CHAIR POWER: Keep going. It's his job to keep up.

MS. ZHANG: Actually, I just wanted to make a note before we begin talking about this

slide. There's a typo here on The second main bullet or second submain bullet. It should read "does not trigger" instead of "does."

MEMBER BROWN: Which bullet?

MS. ZHANG: So the second sub.

CHAIR POWER: The second dash.

MS. ZHANG: Yes. Should read "does not."

MEMBER BROWN: Okay.

MS. ZHANG: It makes more sense that way.

MEMBER BROWN: After the fourth word.

MS. ZHANG: Yes.

MEMBER BROWN: Thank you.

MS. ZHANG: So as described by Jeremy earlier, each TXS function processor is equipped with a hardware watchdog timer.

If the run-time environment does not 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 also switches off the I/O module power supply placing the processor and puts it in a defined failure state. For reactor trip functions,

switching off the I/O module power will result in a zero-voltage output which initiates a reactor trip signal. It's different for these.

MEMBER BROWN: Okay. So there is four ALUs of subsystem A and subsystem B. Does it only take one watchdog timer to not operate in order to trigger that or does it require a watchdog timer in both subsystems. It should be just one because they process different variables.

MS. ZHANG: Since it's an Or function, it's just one. So the outputs on subsystem A and subsystem B don't work together. Therefore it only takes one. But if it's just one ALU since both ALUs are and-ed together it would not result in a reactor trip. Only both ALUs were in one subsystem.

MEMBER BROWN: Yes. I'm looking at the picture now.

MS. ZHANG: Yes. So these actions are actually independent of the inherent self-monitoring software. So this is hardware based. Next slide.

A response time analysis was also provided for the microprocessor based portion of the Protection System. And the microprocessor based portion is defined as the time from the sensor

conditioning output, SCDS, to the reactor trip breaker terminals for the reactor trip functions or to the input terminals of the PACS for the ESF actuation functions.

This analysis is based on the fixed cycle times of The TXS processor and certain timing assumptions are made to calculate the response time. The response times for typical Protection System functions are calculated and based on the assumptions the longest theoretical response time calculated is about 0.25 seconds. The final response time is verified through an ITAAC. Next slide.

That finishes my portion. I'll turn it over to Mr. Kenneth Mott.

MR. MOTT: Hey. How are you doing today? My name is Ken Mott. Background, I have a bachelors of science in electrical engineering from Howard University. I have a masters of science and system engineering from George Mason University. I also was a former Naval nuclear reactor operator aboard the USS Enterprise CVN-65, the world's first nuclear powered aircraft carrier.

And upon leaving and getting my

honorable discharge and getting out, I swore I would never do anything on the planet that deals with nuclear power.

(Laughter.)

Of course, it's the highest paying job coming out of the Navy was at the Byron Nuclear Generating Station in Byron, Illinois. That's a Westinghouse PWR. It's a sister plant of Braidwood. Back then when I worked there it was owned by Commonwealth Edison which was ComEd.

Like I said once again, I left nuclear power, went to telecommunications. I was a project manager specialist for the Northern Virginia region. Verizon Telecommunications for the outside plant engineering group which was doing a fiber to the premise project which the public knows as FiOS. Left there once they snatched our pension. And came here to the NRC back to nuclear power. Thank you very much.

(Laughter.)

Two things we've been talking about electrical isolation all day. Electrical isolation BTP 7-11 provides guidance for this and it talks about Reg Guide 1.75 which also endorses are IEEE

384. And what BTP 7-11 is stating is that you have your maximum creditable voltage. You're going to increase it to some percentage above the maximum creditable voltage and for some time period you're going to apply that voltage, whatever percentage above that, to the electrical isolation device for a particular amount of time. If the failure of this voltage -- if the isolation device is able to prevent the voltage at fault from coming over, then it would be considered a qualified isolation device in addition to meeting the other guidance of the reg guide as well as --

MEMBER BROWN: Just electrical isolation.

MR. MOTT: That's just electrical isolation. But I know we've been talking all around it and AREVA has committed to all three BTP 7-11, Reg Guide 1.75 and IEEE 384 in their -- I think it's Table 7.1 for the design requirements. They've committed to all three of those for their credited, qualified isolation devices.

Another thing we were talking about earlier was the Protection System self-system signal diversity. And I want to say the signal diversity

that's credited between the two subsystems, subsystem A and subsystem B, is specific to reactor trip functions, only not just SFAS functions.

And what this is saying as Jeremy was explaining we'll take whatever the primary plant parameter is and it can be pressurized to pressure and we will put that in protective system alpha. And then we'll put a secondary reactor trip function. And it can be T hot or something and Protective System Subsystem B such that if a failure of your original Protection System pressure, pressurized pressure, would have failed it would not affect the secondary reactor trip functional protection system subsystem B. So therefore that would be the signal diversity. One signal could not prevent a particular division subsystem from failing. So that's what's described and the rules for doing that are within the digital protection system technical report. And we do have an RAI open item waiting on an ITAAC to verify that this set-up is going to be as such as built.

I'm Ken Mott. I will comment on this D3 defense-in-depth and diversity. These are the diversity categories after reviewing and evaluating

the design that the staff has approved. These are diversity attributes right out of The NUREG 6303.

For the software one, we have an open item on that on how the software that's with the credited DAS. Is it sufficiently diverse from the software that's in the Protection System?

I think they just sent a draft RAI response in last Thursday or Friday. And I have not had a chance to look at it to update this. So that response is in. And we will discuss with them to make sure it's sufficient and adequate. We can go to the next slide.

There are other systems that make up the D3 mitigation systems and once again we're talking about D3. We're looking at it as Charlie was alluding to it earlier. I have an APU that sends a corrupted data signal to all three ALUs and it corrupts all four ALUs. It corrupts.

Essentially the Protection System does not work. What happens in that case. And as Jeremy was alluding to, we have a DAS system such that that same failure cannot also fail the DAS system. And these are other systems that a postulated software failed. The Protection System cannot fail as well.

So the PACS would not be failed by that same software common cause failure. And we also have one and the same common cause testing to address software common cause failure to PACs as well as The SCDS. Obviously, we don't want these to fail in any way because these are inputs to the systems. But their functions are not performed by microprocessors and there is no software running in SCDS with the exception of the temperature compensation that Jeremy was discussing.

The SICS uses the hardwired panel, uses discrete and analog buttons and switches. It is not a computer on the SICS that's doing a particular function or that could be failed by the same software common cause failure that would fail the Protection System. We can go to the next slide.

And this is the one I say this is where all the marbles are right here. What I do when I do my evaluations, I build myself a simplified design such that I would know what I'm looking at and what I'm talking about. And then I go back and make sure that this is equivalent to what they're demonstrating.

What we have in red, the red-lettered

items are the things that will be credited if there is a failure in the Protection System and the related Protection Systems.. So these are things that are going to protect us in D3 space. The red lines are the lines and the signals that will be credited once again if the Protection System were to be failed by a software common cause failure.

All of the lines are hardwired with the exception of the PAS. If you notice the PAS is a data network signal coming from the PAS going to the non-safety related communication module in the PACS.

So in the Chapter 15 space we're on the left side of the page and we're crediting the Protection System. We receive sensor inputs from The SCDS going to the Protection System. It senses an input and The setpoint is actuated. It will either wind up as an SAS actuation with sent signal to the PAS module. Or if it needs a turbine generator trip, we go to the turbine generator as well as shown by Jeremy. We go to the reactor trip on the voltage coils or the control rod drive control system trip contactors.

Now in D4 the diversity requirement is, the main one, is 10 CFR 50.62 ATWS where you need a

diverse way to actuate emergency feedwater system and turbine trip as well as depending on your plant built and the diverse reactor trip system. At the bottom three boxes on the right side, these are what's going to meet your diversity for 10 CFR 50.62 where we have a diverse way to trip the turbine generator I&C.

And as well as the reactor trip breakers, we go to the SHUNT trip coils from the DAS as well as the control rod drive control system. And like I say they placed a more detailed design up on the board. The rod control units will go from the DAS.

On the right side the DAS is what is the main actuation system up on a failure, software common cause failure protection system. Since we do have -- We were talking -- As Jeremy mentioned, he was talking about IEC goes over to items that are necessary for a triggering event for a software common cause failure, a latent software failure as well as a common triggering event.

Since we're receiving the same input from the -- Essentially what he's saying is he's talking about The SCDS system we can say that we

have a common triggering event. So therefore that's why the software open item was very important. But the selection of a technology that does not use non microprocessor based technology and no running software to make a decision, we can say that the DAS is sufficiently or adequately diverse for the Protection System once the open item question -- We do state as adequate. That was just in last week Thursday or Friday.

So therefore even though we have a common triggering event, we can say that the two systems are diverse enough such that both systems won't be taken out by the same failure.

Looking at the PACS module with a lot of the talk about the PACS module. As you can see, not only do we have safety related systems signals going into the PACS module. We also have PAS coming in, non-safety related. We also have manual controls coming into the PACS as well as non-safety related controls coming into the PACS.

From the staff one of the items that was brought up was does the PACS itself on a pre-event basis and we're considering the logic built into there. Chapter 7 we don't really get into that.

The explanation we have is a priority set-up and Rev 2 priority was that the Protection System had the highest priority such that no matter what was coming into the PACS, the manual controls, non-safety related controls from the PAS. If a Protection System signal came into the PACS, that one would be honored and that would end up going to the actuator, the SAS actuator. So that was a priority.

The Rev 3, the one that has just come in is that the DAS being a functional substitute for the Protection System, has the same already as the Protection System. Therefore if we had normal operating with the PAS controlling some functions and the Protection System should be failed, then the DAS would take the next priority and it would override other systems in order to effectuate taking the plant to a safe and subcritical shutdown.

MEMBER STETKAR: Kenneth.

MR. MOTT: Yes, sir.

MEMBER STETKAR: Let me interrupt you for just a second. You just mentioned things. I think I heard you say that in Chapter 7 you simply accept the priorities as they're set and make sure that the system implements those priorities. Is

that right?

MR. MOTT: That is not correct.

MEMBER STETKAR: Okay.

MR. MOTT: Don't accept anything. What I'm saying is Chapter 15 is what deals with on a pre-event basis. For this event, show me and demonstrate what systems you have to protect this event. But next event show me what happens to protect this event.

MEMBER STETKAR: Well, let me interrupt you for a second. I understand Chapter 15 analyses. I'm asking if I have a choice between an open signal and a closed signal for a valve, a particular valve, in a safety system having the higher priority signal, who in the staff during the integrated review of this design looks at that portion of the design and determines that there is indeed an adequate technical basis for determining that, for example, the closed signal ought to have higher priority?

MR. MOTT: I know in Chapter 15 they're going to list the systems that are going to come to play in actuation such that if they need isolation I'm pretty sure they would say the PACS module would

--

MEMBER STETKAR: But I don't want to rely on pretty sure and I don't want to rely on deterministic single event analyses that performed in Chapter 15. I'm talking about who in the staff steps back and says, "Yes, I understand the full spectrum of events that can occur in this plant. And it makes sense that for this particular valve the priority signal is to close this valve because that's the best thing that can happen for the full spectrum of events that can happen to the plant."

Chapter 15 simply looks at single failure criteria, deterministic design basis accident analyses, one by one and says, "Yes, I can mitigate this event if these things happen." Some of those events require this valve to close. Some of those events require this valve to open.

The Chapter 15 analyses don't care about the integrated effects. That's the problem with Chapter 15, the chapter deterministic design basis accident analyses.

Now the question is who in the staff looks at the technical justification for why the closed signal has higher priority than the opened

signal. It's obviously not Chapter 7 people. It's obviously not Chapter 15 people. Who does it?

MR. JACKSON: This is Terry Jackson. I would say because the priority logic is described in Chapter 7 of the application we would take the primary role in addressing that in their chapter. Now we will work with the Chapter 15 folks to understand what accidents are being addressed because some accidents may progress slower than others. And so you may want to give priority to one mitigation versus the other.

Also we will work with the human factors branch as well. Because if, for example, an open or a close is given priority, the operator would need to be able to address the other situation. And that may be a manual action that they have to deal with.

I think that the staff has an open item with regards to priority. So we're still working on the application with regards to that.

MEMBER STETKAR: But some of the issues are priority of how it's achieved. It's sort of the electronics of the system. I'm talking more in terms of integrated safety functions.

MR. JACKSON: Yes. And that's our

intent. It's an integrated review in that case. We'll take the lead on that in Chapter 7.

MEMBER STETKAR: Okay. And it is under Chapter 7.

MR. JACKSON: Yes.

MEMBER STETKAR: So I ought to see those kind of questions coming out of that part of the review.

MR. JACKSON: Yes.

MEMBER STETKAR: Okay. Thanks.

MR. MOTT: Okay. And also within the SICS the non-safety -- NSR stands for non-safety related. The non-safety related controls that are credited for DAS on the SICS, those are the ones that are credited. And that gives the operator in D3 space for the Protection System coming in with the Protection System in a common cause failure state, these, either one, go directly to the component, the PAS module, or go directly to the DAS bypassing the failed Protection System. And that would meet 0.4 of the staff's requirements memorandum for SECY 93-07.4 If there are no questions, we can go to the next slide.

MS. SPAULDING-YEOMAN: Good afternoon.

My name is Dierdre Spaulding-Yeoman. I have a bachelor of science degree in electrical engineering and a doctor of science degree in engineering management.

I first began my career at the Potomac Electric Power Company designing the underground electrical distribution system to commercial buildings in downtown D.C. I then came to the NRC and I worked in a diversity of areas, special inspections branch, instrumentation and controls, division of reactor projects, office of enforcement. I then left the NRC and worked for two years in the intelligence community, returning to the NRC and the Office of New Reactors in the Instrumentation and Control branch.

I'm going to speak on the staff's position and review concerning simplicity. As mentioned earlier in the staff presentation by my colleague, Jack Zhao, the NRC staff concern of complexity of the Applicant's design are rather the lack of simplicity existed. A lack of simplicity in design will contribute to the design's inability to meet NRC requirements and guidance and it would be unlikely that the staff review of the design would

be completed or found acceptable in the time frame desired by the Applicant or the combined license/applicant's referencing this design.

In regard to the contents of the technical information in applications, the Code of Federal Regulations stipulates that the system description shall permit understanding of the system designs. Additionally, the staff guidance indicates that a more complex system increases the likelihood of failures and errors and that a complex design should be avoided.

The staff guidance discusses the need for 100 percent testing and manual verification of test results such that the demonstration and achievement of this would ensure that a design is not overly complex. In other words, keep it simple.

One example in using staff guidance addresses the staff concerns of the service unit being continuously connected. And this led to the service unit being disconnected in instances where the service unit was not being used for maintenance or testing.

Based on staff guidance and throughout the course of the staff's review and interaction

with the Applicant, the NRC staff indicated that the complexity of the design is not necessary to provide the required safety functions and that the lack of simplicity would require substantially more information to be submitted by the Applicant and reviewed by the NRC staff.

During the staff's review and its interaction with the Applicant, it was found, for example, that (1) extensive interconnections existed between redundant safety divisions and between safety systems and non-safety equipment and that (2) most of these interconnections did not directly support or enhance the performance of safety functions and created unnecessary complexity that outweighed any benefit from using bi-directional communication. The increased complexity could generate additional faults and failure modes in the design.

The NRC staff would have needed detailed design information potentially including associated software to be submitted on the docket in order to determine the acceptability of these interconnections. Such a review would require extensive resources and time to be completed both

during initial certification and throughout the life of licenses issued for such a design. Subsequently, the Applicant proposed a less complex and therefore a simpler design. Next slide please.

The following design changes were provided.

(1) Reduced inter-divisional communication;

(2) Elimination of inter-divisional communication SICS'

(3) Implementation of physical uni-directional communication;

(4) Changes regarding DAS.

The staff reviewed the Applicant's changes to reduce the design complexity and thus make the design simpler. The staff's review of these design changes found that to address the concerns of data communication between the safety divisions, the Applicant remove functions for which there was no inherent safety benefit versus keeping them which would have caused the introduction of potential data communication hazards.

The Applicant also implemented the SICS using hardwired controls and indications which

reduced inter-divisional communication. The changes to minimize inter-divisional communication also simplified the overall I&C design. In addition, the Applicant made the diverse actuation system to be non-microprocessor based technology. Also the Applicant redesigned The QDS from safety related to non-safety related and this simplified the need to demonstrate adequate diversity and qualification of The QDS.

As mentioned previously, the Applicant proposed to disconnect the service unit except for maintenance and surveillance testing. Furthermore, the Applicant proposed the use of physically limited, uni-directional data communication from safety related to non-safety related systems.

This concludes the staff's discussion on simplicity and how the complexity was reduced by the Applicant and reviewed by the staff. Next my colleague, Wendell Morton, will discuss self-testing.

MR. MORTON: All right. Good afternoon, everyone. I'll be batting clean-up for the staff presentation today. My name is Wendell Morton and just a little bit of background about myself.

I graduated from the University of Delaware where I have a degree in electrical engineering, specializing in semiconductor devices and materials. I also have an undergraduate degree from Delaware State University in physics.

Upon graduation, I started work at Exelon at the Limerick Generating Station in Pottstown, Pennsylvania, where I was the system engineer in charge of RPS radiation monitoring both process area as well as a number of back-up functions for the electrical systems at that plant. After a few years there, I started work at Bechtel where I worked with my colleague, Jack Zhao, for a couple of years before I started here with the Agency. And I am in the IS-1 branch working with Terry Jackson.

So today I'll be covering a number of topics that AREVA has previously touched on earlier in its presentation as well as some of my other colleagues. I just want to touch on a few more points just to kind of give you a source or a better feel for some of the significance of some of the issues that we touched briefly earlier. To the staff, they're a little more significant.

For my first topic, I'll be talking about the automated self-testing features that are documented in ANP 10315. That's the self-testing feature and surveillance testing philosophy technical report. That report has been talked about earlier today in terms of self-testing. But the report is actually the entire maintenance and surveillance philosophy for the entire U.S. EPR design.

One-half of that report specifically touches on the self-testing features. The other half is for surveillance testing. Right now, I'll just focus on the self-testing features.

For the self-testing features, they are part of the qualified TXS platform. So they are safety related. AREVA is taking credit for these features to meet certain surveillances to obviate the need for them such as the channel checks operators perform in the control room and, for example, the quarterly functional test that a lot of I&C teams to go out and perform on a regular basis. Now I know that's particularly fair and dear to my heart since I worked a lot of I&C teams performing those kinds of surveillances.

And with this design by taking credit for it AREVA is basically stating that those types of surveillances will no longer be needed. So within this testing report, the 10315, essentially you're only going to see testing intended for the 24 month surveillances. You're not going to see anything designated strictly for anything of a shorter time frame than that. You can go to the next slide.

This next slide just summarizes some of the features for the automated self-testing features documented in the 10315. Essentially the self-testing features are split up into two halves according to AREVA. You have the inherent self-testing features which are part of the standard TXS features that exist on every TXS function processor from production. And then you have the engineered self-testing features that are designed as part of another COL applicant's design.

You can see if you read through the list that we've talked about the watchdog timers. And that particular device is spoken about in detail in 10315.

Just want to touch on with one

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

that are part of the self-testing regiment that are also then performed at a two year internal? Or is that just --

MR. MORTON: There are two considerations with that. Per our guidance in BTP-17, it's stated that the self-test feature should be verified on a periodic basis. And that's something we're working with AREVA to determine what that basis is if that's going to be performed along with the surveillance testing for individual function processors such as ALUs or CUs, things of that nature. The self-tests themselves have to be periodic or it's stressed to be periodically verified.

MEMBER BROWN: Who tests the self-tests?

MR. MORTON: It would have to be the plant personnel at that point. But how that's done is still an open item. It would have an RAI on it because it's still an open question.

MEMBER BROWN: I guess my question is I'm trying to get this phrased properly. When we address we utilized self-test in the program that I came from. And at first we continued to do our weekly or biweekly manual, turn-the-switches type

stuff. And then after a while, we said, "Okay. We're getting good results from that." And this was before we had the automatic self-testing. So we were trying to look at every time you operate a switch you break them.

MR. MORTON: Right.

MEMBER BROWN: A lot of maintenance associated with broken switches.

MR. MORTON: Right.

MEMBER BROWN: And if you got reliable systems particularly the integrated circuit, solid state stuff was much more reliable than the old mag-amp or discrete transistorized stuff. So we started looking early at trying to extend that one weekly calibration check to a long term based on experience.

Then once we went to the microprocessor based stuff, we said, "Okay. What can we do?" But we didn't go out to two years. And then the other thing we incorporated was a periodic check of the self-test to make sure that a datapoint that you were using to do the self-test.

For instance, say, you put in whatever. If you've got RTDs for temperature, you put in some

fixed resistor, high precision plate 0000001 type percent resistors to check that. So we did some of those manually. I retired 12 years ago. So I have no idea what they're doing now.

But I guess my question is I don't have any problem with self-testing. But is there a point at which you check that your self-test regiment is still performing satisfactorily with external, you know, some type of external, actual stimulus such as an RTD or a pressure simulated pressure signal or level of whatever? I guess I didn't think of that earlier.

CHAIR POWER: I think that's what you're talking about.

MR. MORTON: Yes.

CHAIR POWER: That's where you have an open item right now.

MR. MORTON: Yes. The open item basically is the verification of are you making sure that your self-testing features are doing what you say that they're doing on a periodic basis per the information you find.

MEMBER BROWN: All right. If there's an open item on it, I'll wait until you get the thing.

We don't have to resolve it. I just feel it ought to be addressed. And Jeremy looks like he wants to talk. But you're going to talk, talk into the mike.

MR. SHOOK: So just to follow up on Wendell's point, we are working with the staff on clearing that open item. But I would point to the testing strategy that's been laid out. And if you look on slide --

MEMBER BROWN: Forty-five?

MR. SHOOK: For reactor trip, it would be slide 28.

MEMBER BROWN: Twenty-eight. Yes, I've got the --

MR. SHOOK: And so you can --

MEMBER BROWN: That's what I was looking at. They're both roughly the same.

MR. SHOOK: And you can see that the sensor operational test will test functionally through the ALU. And then The ADOT test will test a portion of the ALU on out. So then you have -- Then you're looking at the self-test, the continuous self-test and the extended self-test, to test the portions in the middle that aren't tested by the sensor operational test in The ADOT.

The point I wanted to make is that a good portion of this system including the microprocessors are going to be tested through a periodic testing program.

MEMBER BROWN: With humans?

MR. SHOOK: With humans. But there is a portion of the system that's not tested and that's the part that we're working with the staff on.

MEMBER BROWN: Okay. I guess I didn't read the -- When I looked at the sensor operational test, I thought that meant you had an automatic signal being produced as opposed to an external check that that was actually out right periodically. This tech spec will refer to something.

MR. SHOOK: That's correct. That sensor operational test is basically functional similar to what we would call the trip point calibration.

MEMBER BROWN: Yes, but you still need -- At some point, there is still some processing stuff in terms of the calibration of your software that it's taking the data and producing the desired result from whatever the input is from the analog signals you get from the sensors.

MR. SHOOK: That's correct.

MEMBER BROWN: Okay. All right. So that's being addressed. The pieces that haven't been nibbled on are being addressed.

MR. SHOOK: That's correct.

MEMBER STETKAR: Jeremy, while you're there, let me ask you or I could ask Wendell.

MR. SHOOK: All right.

MEMBER STETKAR: Response time test which is the only one that I'll use the term end-to-end tests, the only true end-to-end test, through the whole function is performed according to tech specs once every 24 months on a staggered test basis. Does that mean division one is tested once every eight years?

MR. SHOOK: I don't know the answer to that.

MR. PHAN: The staggered test basis is referring to is because for the response time testing it's not one test that goes from your sensor all the way down to your actuator. It's made up of overlapped tests between.

Say, for instance, your sensor operational tests, that also functions as a response time test. And there's also a response time test

for your APU and AOU and those processing components. But that overlaps with --

MEMBER STETKAR: I guess that discussion is somewhat contrary to the little cartoon that we see in slide 28 from AREVA which would indicate to me anyway that the response time test is a fully integrated sensor to output device tests.

MR. SHOOK: I think one of the -- a piece that's sort of not clear what this picture is that these are actually referring to The surveillances. And so when we actually do the testing we may piece different parts of the test to satisfy different pieces of surveillances.

MEMBER STETKAR: That's like stroking a valve and making sure that the valve strokes and then testing the pump and making sure the pump works. And never making sure that when the pump works, you actually get flow through the valve. Is that right?

MR. SHOOK: Yes, you're essentially testing --

MEMBER STETKAR: It's a problem that we've had in the nuclear industry for not doing integrated tests of fluid systems. Because people

find out that when the pump starts, the DP across the valve is too high and the valve doesn't open.

MR. SHOOK: Right.

MEMBER STETKAR: That has happened. That's why in mechanical systems there's a strong advocacy for doing full end-to-end tests verifying that the entire function works when you initiate the function that you don't piece together and assert that the system will function because all the little bits and pieces worked individually.

My interpretation of what I thought you had here was that the 24 month test was indeed an end-to-end test. You actually tripped the input and verified that the output behaved according to the way it was supposed to behave. And from what I hear you say that's not true. Is that?

MR. PHAN: This is Duc Phan again. It's all described within our ANP 10315 document. We describe why it's impractical for us to end-to-end test and take out a whole division.

MEMBER STETKAR: Excuse me. Why is it impractical for you to do that? I worked in a nuclear plant that had relays that sparked and we used to do it. Why is it impractical with these

wonderful software driven things that you can't do it?

MR. PHAN: Some functions such as your low DNBR function, you have all 72 SPNDs that feed into the system each division.

MEMBER STETKAR: I'll give you that one. What about all of the other ones? Reactor protection and safeguards?

MR. PHAN: If you would like, I can go and I'll point out the section because there's page full of bullets.

MEMBER STETKAR: Okay.

CHAIR POWER: Let's do just that.

MR. PHAN: Okay. And I'll point to them.

MEMBER STETKAR: Okay. Thanks. I'd appreciate to see that. Thanks.

MR. MORTON: All right. So just to tie up this slide as far as that open item, it's just that we're working with AREVA still to determine how the automatic self-testing features in TXS are going to periodically verified.

Secondly, there is the question of operability for the self-test features. The

operability comes in two different steps for the staff's review. How is The operability addressed for a TXS component that's actually been found by self-testing features to be faulted, failed, locked up or any one of those terms to describe a device that is no longer functioning as designed? That's one aspect of it.

The second aspect of operability that the staff is looking for is how is operability of a TXS function processor or affected when the self-testing feature fails to a certain degree. And we touched on that earlier with the locked function processor and the hardware watchdog timer. But specifically if you do have a failed self-testing feature when it's not specifically covered in ANP 103 what steps the operator would take upon a failed self-test run? So the staff has an open item on that.

Specifically, for ANP-10315 we just touched on some of the testing that AREVA has talked about, the actuating device operational test, the sensor operational test. One of the concerns the staff has is that these tests aren't necessarily a one-stop shop for testing or performing

surveillances on every TXS safety system.

Right in the preface of 10315, the surveillance testing portion of this report really only applies to the Protection System specifically. So the staff has an open item working with AREVA to determine whether the actuating device operational test and other tests mentioned inside there how those tests would be applied to the other TXS safety systems. In staff's determination, they're not quite a one-stop, one-shoe-fits-all type approach.

Secondly, and I touched on this earlier, other TXS safety systems that utilize credit self-testing features are still not quite clear to the staff. So we have an open item on that as well. If there are no questions.

Now the next topic I'll be touching on and AREVA has touched on it briefly and the staff has as well are the service units and the U.S. EPR design as was -- I believe AREVA had it on a slide previously, the non-safety related computers which serve as the primary means of performing surveillances and trouble-shooting activities specifically for the Protection System, SAS and RPMS.

Within The EPR design, AREVA does not specifically state that the service units will only be used for those three systems. This is what the staff has gleaned from our review of the available drawings and documentation. The service unit is spoken about in detail within Section 7.1, also partially within 10315 and also in digital protection system technical report. I believe that number is 10309 where it talks about service unit functionality.

I just wanted to impress upon the Committee that the service units are the main ways in which a team of technicians on a future EPR plant would actually perform maintenance on those systems. Next slide.

So forgive the graininess of this drawing. This is just another sort of simplified version of what we're dealing with with The service unit. And Deanna touched on this before. If you look at -- You have the service unit to the left. That next blue box is the credited hard disconnect switch per ISG 04 that AREVA is taking credit for to provide the isolation from the divisions.

The next block right there is the MSI,

divisional MSI. The other blocks right there are the CPU state switches. For the service unit function you have two steps in order to perform maintenance on a particular function processor. You have the hard disconnect switch which must be turned to a specific protection system/SAS RPMS division.

And then when you've done that you have to turn the CPU state switch for a specific function processor to enable. That enables you to change the state of the CPU of the function processor from a service unit to perform whatever type of maintenance activities you want to perform. If there are no questions, I'll just go to the next slide.

Here are some of the major open items the staff has for concerning the service unit. Once again, we'll touch upon the topic of operability when it comes to the service unit. There is still open questions on what is the baseline operability for using an NSR piece of equipment when performing maintenance on a safety related piece of equipment. There is open questions about that.

There's questions on when you are performing certain surveillances according to AREVA a function processor may have to be in multiple

operating states in order to perform that particular surveillance. Each one of those operating states of a function processor has an operability designation attached to it. So how would a team of individuals performing a surveillance task? How would an operations team determine operability of a function processor when you're dealing with multiple operating states while you're plugged into the service unit?

I apologize. That's a little bit of a convoluted explanation. But it's sort of the issues that we're trying to work through with AREVA to determine The operability status while using the service unit.

And I touched on earlier the service unit usage for the other TXS safety systems. I'm still trying to pin down how specifically the service unit will be used in the same manner as the Protection System.

At this time, we have an okay idea of how it will be used for the Protection System. But still for the other TXS safety systems, SAS, RPMS, even RMS, other safety systems, we're not quite sure where we stand on that yet based upon The AREVA

available design documentation. No questions. Go to the next slide.

Another open item we have -- I'm sorry. We're going to jump to SAS right now. So we've touched on SAS a number of times already in the presentation earlier, both AREVA and the staff. Just to bring a little more emphasis to some of the points my colleagues had made. Tung Truong had talked about The FMEA for SAS. I believe AREVA has said that's going be coming down the pipeline some time soon.

This is significant for the staff's evaluation because it will give us more of an ability to determine whether SAS meets single failure criterion number one. And I know from a number of questions that the Committee has had earlier just The FMEA should provide information on the effects of SAS failures on plant operations which is significant for those systems such as CCW, ESW and all The HVAC systems in which SAS is performing those safety related interlocks for.

And that particular document has already been provided for the Protection System. So we're looking for the same level of detail for the SAS

FMEA.

Generally, just to make a point about SAS, given that it's safety significance and a number of safety related functions and protective actions SAS performs, the staff is looking for information for SAS comparable to what AREVA has already provided for the Protection System since all the regulations essentially apply to the same system as well. For The FMEA, that would be 603, Cause 5.1, for that one.

As my colleague, Deanna, talked about earlier, we have another RAI specifically requesting more information on SAS voting logic. What SAS functions actually perform voting as we understand it and what SAS functions do not? Or a specific place where they're going to put that. So we have an open item on that. Because obviously some of the conversation we've had earlier today, it's still sort of an open issue as far as SAS voting taking place. There are no questions. Next slide.

For SAS system integrity, this is based upon guidance from SRP 71-C. So the staff is looking for some further information on the failsafe configurations for SAS. I know that was a topic

that came up a little earlier today. We specifically pointed to a loss of power condition, but this is a question that generally covers what AREVA feel are the failsafe configurations for SAS because SAS is utilizing the PAC modules. So that's an important question for the staff to resolve.

And as I said that's a significant issue based upon the number of interactions that SAS has with all the various mechanical systems. As one of my colleagues stated earlier, there is a PAC module for every mechanical actuating device whether it's emergency feedwater pumps, valves, something to that extent. If there are no questions, next slide.

Now this is a question that come up just for the staff just trying to inquire whether SAS has any response time timing attached to it. Based upon the applicable regulations and guidance the staff is looking for something definitive when the design documentation SAS either does have requirements or does not.

There are certain SAS functions that are performed that potentially affect Chapter 15 operations. Specifically, the DCB does not particularly go into any detail as far as what kind

of requirements it may or may not have. So we have an open item covering that. If there are no questions, we'll go to the next slide.

Lastly, for SAS D3, this has been touched on a little bit previously. I also won't belabor this point. But essentially the Applicant has not provided a D3 analysis for SAS. We've touched on a number of the safety related functions that SAS performs, the ESF controls, the continuous loops that it performs for emergency feedwater pump protection. Some of the safety related interlocks it performs for CCW and ESW, some of those systems.

Given the fact that SAS has both actuation -- It is actuated from the Protection System and it also has continuous operation capabilities. The staff is looking for some definitive analysis from a diversity standpoint based upon the guidance and rules concerning SAS. If there are no other questions, that's it.

MEMBER BROWN: I believe that terminates.

CHAIR POWER: Let's see. I have -- You have raised quite a number of open items here. And each of them seems they're worthwhile to pursue.

The question that I have is do you see a path forward on these or do they represent a major hurdle in the drafting of this SER?

MR. MORTON: I will say to that question that we've been working with AREVA pretty closely on all of these topics. We're making progress on many of them. So I guess from that standpoint we do have a path forward on many of these.

On some of them, they're going to be a little bit more of a challenge to deal with. But we are making progress in working with the Applicant on many of these issues.

MEMBER BROWN: By challenge, you mean you have disagreements on whether anything needs to be done at all. Is that correct?

MR. MORTON: By challenge, it means we haven't received a response yet. When we do, we'll get to that.

MR. TESFAYE: I guess the question is are there solutions to these questions and the answer is yes. Otherwise, the staff would not leave --

CHAIR POWER: That's the question I have.

MR. TESFAYE: Absolutely.

CHAIR POWER: Right now, I'm looking at all this and saying, "Gee, it looks like we could move Section 7 forward." I mean I don't see things fundamentally, philosophically, hardware-wise barring moving this forward.

I asked Mr. Morton because he's raised a number of RAIs that I think are worthwhile and certainly speak to many of the questions that have been raised by the Subcommittee if he has a path forward on these things. And you're saying you think there is.

MR. TESFAYE: Yes.

CHAIR POWER: Very good. Very good. Do any of the members of the Subcommittee had additional questions for the staff on these particular items?

MEMBER STETKAR: No, sir.

MEMBER BROWN: Other than I would like to hear on the open-ended stuff.

CHAIR POWER: Right. We've identified many things.

MEMBER BROWN: End-to-end testing and then the items he raised. The basis and I didn't

realize the staggered thing when John mentioned that. That was interesting.

CHAIR POWER: Yes. I think there are several items that need to be worked out yet. But our criterion is we don't see anything that's fundamentally blocking here. We see a path resolution.

MEMBER BROWN: I'm going to look at the watchdog timer stuff in the text in spite of people giving good answers and I understand them. But I just --

CHAIR POWER: There can be lots of questions and indeed what send forward into the next phase is an SER with open items. What we don't want to do is send forward an open item that says the plant can't be built.

(Laughter.)

But I don't see anything there. And you give me assurance that you don't see that either.

MR. MORTON: For the time being.

MR. CANOVA: At this time.

MR. MORTON: At this time.

CHAIR POWER: Okay. Thank you.

You're done.

MR. TESFAYE: I'm done.

CHAIR POWER: Okay. I think at this point we move back to COLA. And I think we have Mark Finley.

Michael, did you want to say anything to begin this section or do we just start with Finley and then get back to you?

MR. CANOVA: No, I'll come in afterwards with Dierdre actually to do the staff presentation.

CHAIR POWER: Okay. I guess the floor is yours. Did you have an opening comment to make, Surinder?

MR. ARORA: Yes, sir.

CHAIR POWER: Please make your opening comment.

MR. ARORA: Good afternoon. My name is Surinder Arora. I'm the lead PM for Calvert Cliffs, Unit 3 COL Application review by the NRC. And today we are here to present Chapter 7, Instrumentation and Control as it applies to the COL application.

I had given the project overview yesterday and I don't believe there's anything I need to add. So in the interest of time we'll get started with The Unistar presentation and with that

I turn it over to Mr. Finley to introduce his team and let's start the presentation.

MR. FINLEY: Thank you, Surinder. So again, my name is Mark Finley. I think most of the members of the Subcommittee here know me.

CHAIR POWER: We're spending way too much time together. There's no question about it.

(Laughter.)

MR. FINLEY: For Dr. Brown here, my career has been with Constellation 27 years. I'm with Unistar five years. I'm a mechanical engineer by training. Recently taken over both engineering and regulatory affairs at Unistar and I'm taking the place of Greg Gibson who was our Senior Vice President of Regulatory Affairs. Also nuclear power, Navy.

Thank you first of all for staying late and considering The Calvert Cliffs FSAR.

CHAIR POWER: We're right on schedule as a matter of fact. In fact, we're ten minutes ahead of the schedule.

MEMBER BROWN: Given the schedule was an extended schedule based on the normal schedule, I just wanted to make sure the Chairman understood

that.

CHAIR POWER: The Chairman understands that the schedules in the past have been lax and loose.

MEMBER BROWN: If we don't have this interchange it's not interesting.

(Laughter.)

MEMBER STETKAR: For those of us who weren't here yesterday.

MEMBER BROWN: In the short session, right?

MR. WIDMAYER: I'll have you know that the Chairman had nothing to do with the establishment of the schedule.

CHAIR POWER: The Chairman is responsible for all that occurs in the Subcommittee. And he'll take responsibility for the schedule and point out that it's still lax and loose.

MR. FINLEY: Okay. So slide 2 should be a short and sweet presentation on our part. We essentially have incorporated the U.S. EPR FSAR by reference in terms of Chapter 7. We will discuss two COL information items and one supplemental information item. Other than that, we're very

consistent with what AREVA presented today.

Slide 3, supporting me today is Cyril Roden. You met him yesterday. He's our manager of instrumentation controls and electrical engineering. And we have other members of The AREVA team that have stayed behind to support us as well. Steve Paul from Bechtel in case we need some support from any experts. And again we'll focus on site specific information that supplements that information in the U.S. EPR FSAR.

So with that I'll introduce Cyril Roden for slide 4.

MR. RODEN: Thank you, Mark. Good afternoon. So my name is Cyril Roden. I'm still French from yesterday.

(Laughter.)

MEMBER BROWN: I would have never guessed.

CHAIR POWER: We're going to start taking away your French.

MR. RODEN: I joined UniStar in August 2010 from EDF where I worked for 11 years in I&C and electrical topic both for operating fleet and new-build. And I've got French engineering degree on

electrical design, signal processing and automation.

And as Mark said we will get through as we did yesterday for Chapter 18 through the different COL items we have on Chapter 7. Next slide.

In Slide 5, the first one concerning the accident monitoring communication, we have the list of PAM variables in U.S. EPR Table 7.5-1 which will be confirmed upon completion of the emergency operating and abnormal operating procedures. And this would be done prior to fuel load. Next slide.

This COL item is a new one that appears in the Rev 3 of The DCD. It refers to the reactor power limitation with respect to thermal power. Our commitment is 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 calculated and the calculation will be completed using an NRC-acceptable method and shall confirm that the safety analysis primary power calorimetric uncertainty bounds the calculated values. Next slide.

On the next slide we have our supplemental information which in fact we supplemented the inventory of the PAM variables table we have in the DC with the tower basin level indication of The ESWS and also with The meteorological parameters, wind speed, wind directions and the temperature information.

CHAIR POWER: That's to get your chi/q values.

MR. RODEN: I'm sorry.

CHAIR POWER: Get your chi/q values for the site.

MR. RODEN: That's correct.

MR. FINLEY: Yes.

MR. RODEN: That's all we have in Chapter 7. I don't know if you have any questions with that.

CHAIR POWER: I don't. I know what you're doing. Not much you can do to get farther along.

MR. RODEN: Thank you for your time.

MEMBER BROWN: Are you all finished?

MR. FINLEY: Yes.

MEMBER BROWN: Figured that when I saw

the conclusion slide. I do have -- and everybody is going to hose me -- But I did have -- Where's my crib sheet? The concern that I voiced relative to the communication of data to The TSC and out to the business.

I made mention of that. I realize that I'm not supposed to talk about that. But I'm going to anyway. And if that configuration is not a very -- It's a very vulnerable configuration depending on how that's done. I can't tell you what to do or how to do it.

AREVA was very mushy relative to it can be anything that the licensee would like to do as long as the NRC agrees. But the way it's set up right now you can trash everything in the PICS if it gets compromised.

MR. FINLEY: I'm sorry. I wasn't here all day today. Maybe --

MEMBER BROWN: If you look at the diagram, right off the PICS server lines there's a firewall that feeds the business network. That's their conception of the setup. And what that does is somebody hacks in. They can take out everything.

MR. FINLEY: So the concern if I can

paraphrase is the communication between the business information system --

MEMBER BROWN: And all the rest.

MR. FINLEY: And?

MEMBER BROWN: And the fixed system. And the main control and TSC and all those.

MR. FINLEY: And TSC.

MEMBER BROWN: Yes. I said if there's a firewall noted right there and they send all the PICS data gets out to the business system for whatever use people want. I'm not objecting to data going out. That's not the point. It's where and how it's executed.

And they were saying that the firewall could be a software configured firewall in terms of a firewall. In other words, where it's easily hackable as opposed to a hardware, one-way, hard core analog data diode per se how it's done. It might be a little slower, but you're much less vulnerable.

I can't tell you. I'm just saying that's -- Brought it up. I was told to pound sand in the last meeting.

MR. FINLEY: Certainly understand the

concern.

MEMBER BROWN: I will suggest that you all look at that closely. That's all. It comes under The cyber plan and all that other kind of stuff which is not covered under the auspices of this design certification I guess.

MR. FINLEY: Chapter 7.

MEMBER BROWN: So other than as a plan.

MR. FINLEY: So I can say we certainly understand the concern. We share the concern. We haven't done any detailed design of the firewall at this point.

MEMBER BROWN: I understand that. I just thought I'd bring it up.

MR. FINLEY: We have that as an action certainly.

MEMBER BROWN: Thank you. That's all I had, Dana. Thank you.

CHAIR POWER: At this point, I think we can move to the staff presentation.

MR. ARORA: Mike knows what happens to the Chapter -- for Calvert Cliffs also. He has already been introduced.

CHAIR POWER: Yes. They told us he was

doing double duty here. But he has a tremendous team supporting him. So I'm not feeling so sorry for him. I started out saying, "Boy, this guy is having to work hard."

MR. CANOVA: I have actually the easily job in the whole world.

CHAIR POWER: And then I saw his team and I said that I don't feel so sorry for him.

MR. CANOVA: We'll go through this really quick. This is our presentation on Chapter 7 for Calvert Cliffs, Units 3 and 4.

We've met. The Applicant has already been here.

MR. ARORA: We skipped these slides.

MR. CANOVA: We did these slides yesterday. So I don't think we need to them.

MR. ARORA: They're the same as yesterday's.

MR. CANOVA: Dierdre Spaulding-Yeoman sits to my right. I talked to Terry and Terry's not going to make any remarks on this presentation. It's just a quick overview. There were only questions asked in 7.1, 7.5, 7.7 and 7.9. A total of six questions. There are three questions

outstanding, two of them in one RAI set. So that's two RAIs they're discussing.

This looks familiar. Dierdre, if you'd like to address it.

MS. SPAULDING-YEOMAN: As you've heard, the Safety Evaluation Report for the Chapter 7 U.S. EPR does have several existing open items. The staff will update its safety evaluation for Calvert Cliffs Unit 3 to reflect the final disposition of those open items in the safety evaluation in regard to how they impact The Calvert Cliffs Unit 3 staff evaluation.

With the exception of the open items to Calvert Cliffs which are discussed in the following three slides, all other Chapter 7 information has been incorporated by reference. In regard to site specific post-accident monitoring variables, the Applicant identified the site specific PAM variables: essential service water system cooling tower basin level, meteorological monitoring system wind speed at 10 meters and 60 meters, meteorological monitoring system wind direction at 10 meters and 60 meters and meteorological monitoring system vertical temperature difference

between 10 and 60 meters. These site specific variables provide indication in order to provide data for radiological release assessment. Next slide please.

The staff found that The Calvert Cliffs ITAAC as provided in its FSAR contain instrumentation and control design information for which there was no information or details within the Chapter 7. For example, the staff found that The ITAAC mentioned site specific systems such as the ultimate heat sink, makeup water system and the ultimate heat sink makeup water intake structure ventilation system. Again, the staff did not find any information that identified the safety related I&C systems controlling these site specific systems.

These systems may be controlled by the safety automation system which is described in the U.S. EPR FSAR. Or they may be controlled by standalone I&C systems. If they are controlled by standalone I&C systems, The FSAR should address how these standalone I&C systems meet applicable I&C requirements.

Additionally, the staff was not able to identify any automatic and/or manual functions

associated with these site specific systems. Therefore, in request for additional information, 325 Question 07.75-01 the staff requested that the Applicant address the identified I&C issues. This is being tracked as an open item. Next slide please.

The staff concluded that the Applicant appropriately incorporate by reference U.S. EPR FSAR Tier 2, Section 7.5. However, the staff issued an RAI to the Applicant, U.S. EPR, which retain to the U.S. EPR FSAR Section 7.5 that questions the necessity for a COL item.

The staff finds that the post-accident monitoring instrumentation in U.S. EPR FSAR, Tier 2, Section 7.5 needs to be a complete list with the exception of site specific instrumentation. Therefore, there does not appear to a need to update the post-accident monitoring instrumentation list.

The staff issued RAI 325 Question 07.05-2 to track coordination of the applicable changes in the U.S. EPR FSAR regarding post-accident monitoring in regard to the site specific Calvert Cliffs Unit 3. Next slide please.

In regard to Section 7.7 for The Calvert

Cliffs application, the staff issued RAI 326 Question 07.07-1. The staff did not find where the Applicant addressed the COL item related to primary power calorimetric uncertainty.

In its review of the U.S. EPR design certification, the staff identified the following information from Section 7.7.2.3.5, Interim Revision 3 markups. The information states in part "a COL applicant that references the U.S. EPR design certification will following selection of the actual plant operating instrumentation and calculation of the instrumentation uncertainties of the operating plant parameters prior to fuel load calculate the primary power calorimetric uncertainty."

And RAI 326 Question 07.07-1 the staff requested that the Applicant provide design information that addresses this COL information item. If the COL information is address in another part of The SER, information should be provided in Section 7.7 that acknowledges the COL information item and points to the applicable location where the design information is provided. This question is being tracked as an open item.

This concludes the staff presentation,

technical presentation on Calvert Cliffs Unit 3. Thank you.

CHAIR POWER: There does not appear to be any barrier to resolving these issues since the Applicant just said he was going to do. So it looks like this is moving right forward.

MR. ARORA: And just for the record, we also have the generic open item on this chapter as well. That's the DC reviews.

CHAIR POWER: Yes. That's right.

Do members have any additional questions on this?

MEMBER BROWN: I don't.

CHAIR POWER: I would like, Mr. Stetkar, you had two items that you spoke on heavily if you would give me a note on those.

MEMBER STETKAR: I'd be happy to, but I don't remember which two.

CHAIR POWER: I have them in my notes.

MEMBER STETKAR: Thank you. I would appreciate that.

CHAIR POWER: I would like to thank everybody that participated in this meeting. I certainly learned a lot. I can tell you it is very

evident that a heroic amount of work has been done both by the Applicants and by the NRC staff in this regard. And I come away much more confident than I came into the meeting on the progress being made in this direction.

And with that I'm going to adjourn this Subcommittee meeting. Off the record.

(Whereupon, at 5:08 p.m., the above-entitled matter was concluded.)

1

2

3

4

U.S. EPR Chapter 7 Presentation for ACRS

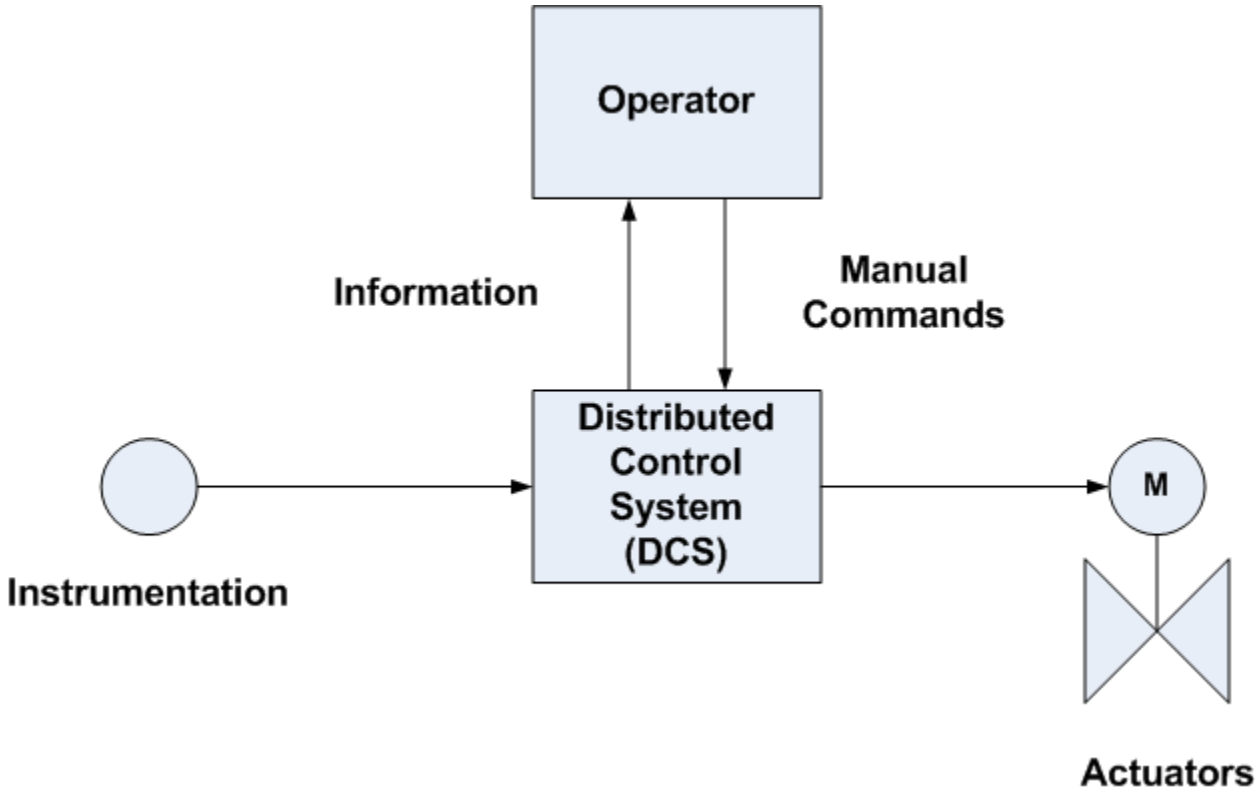
Jeremy Shook, I&C Engineering Discipline Lead

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

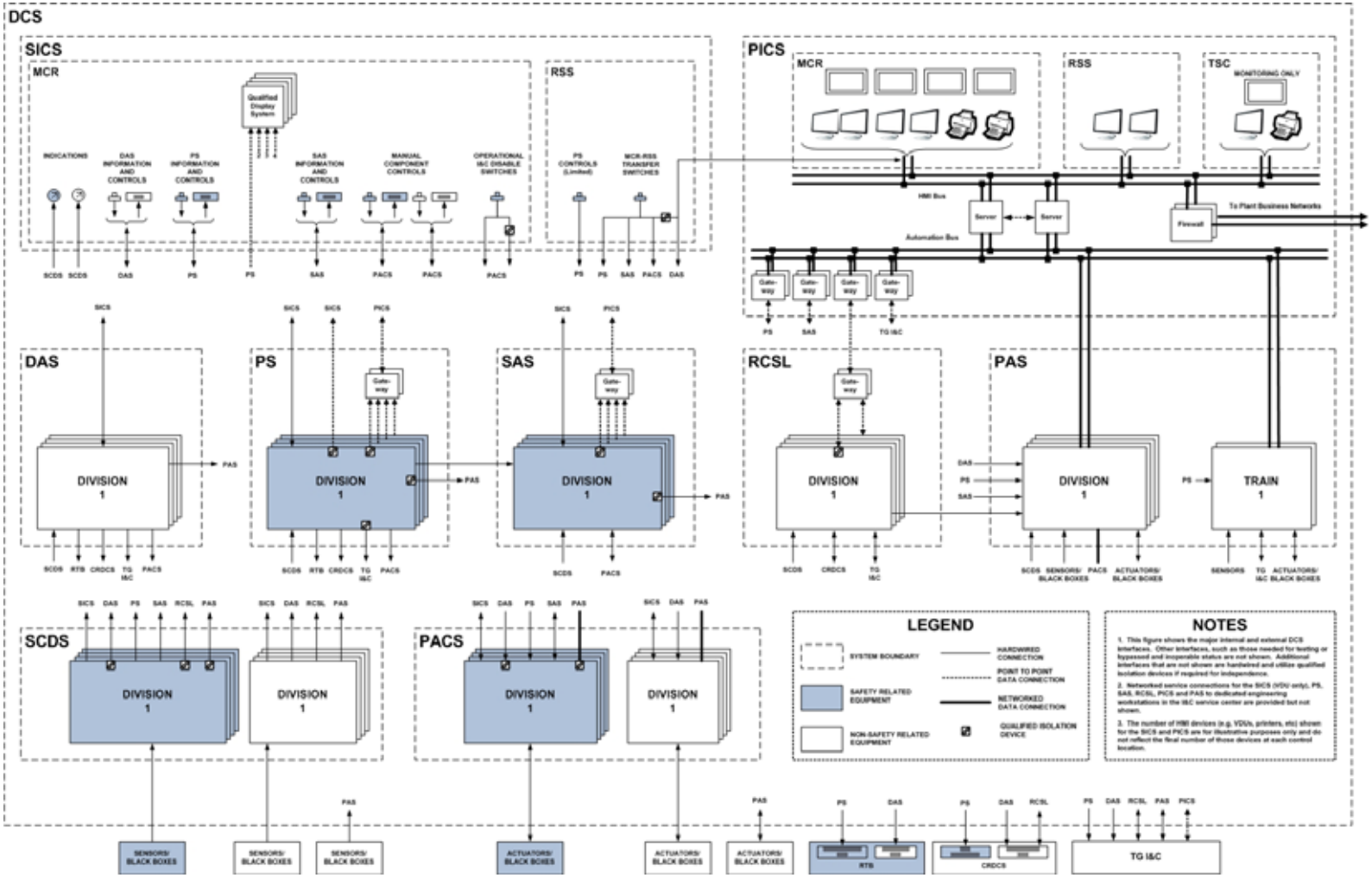
Basic I&C Concept



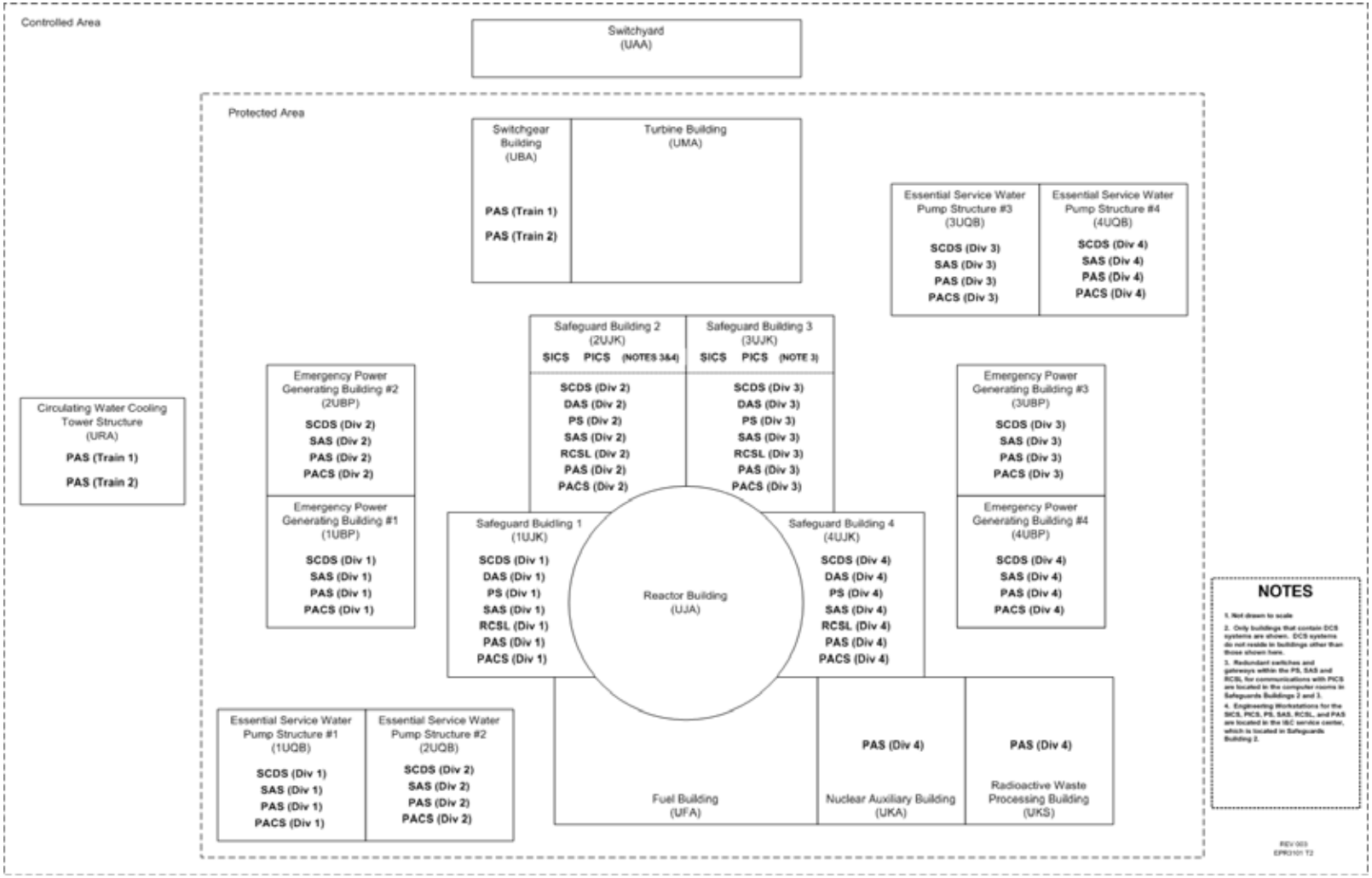
Instrumentation Systems

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



Actuator Systems

SYSTEM
Process, HVAC, Electrical Systems
Control Rod Drive Control System
Turbine Generator I&C

SECTION 7.2:
REACTOR TRIP SYSTEM

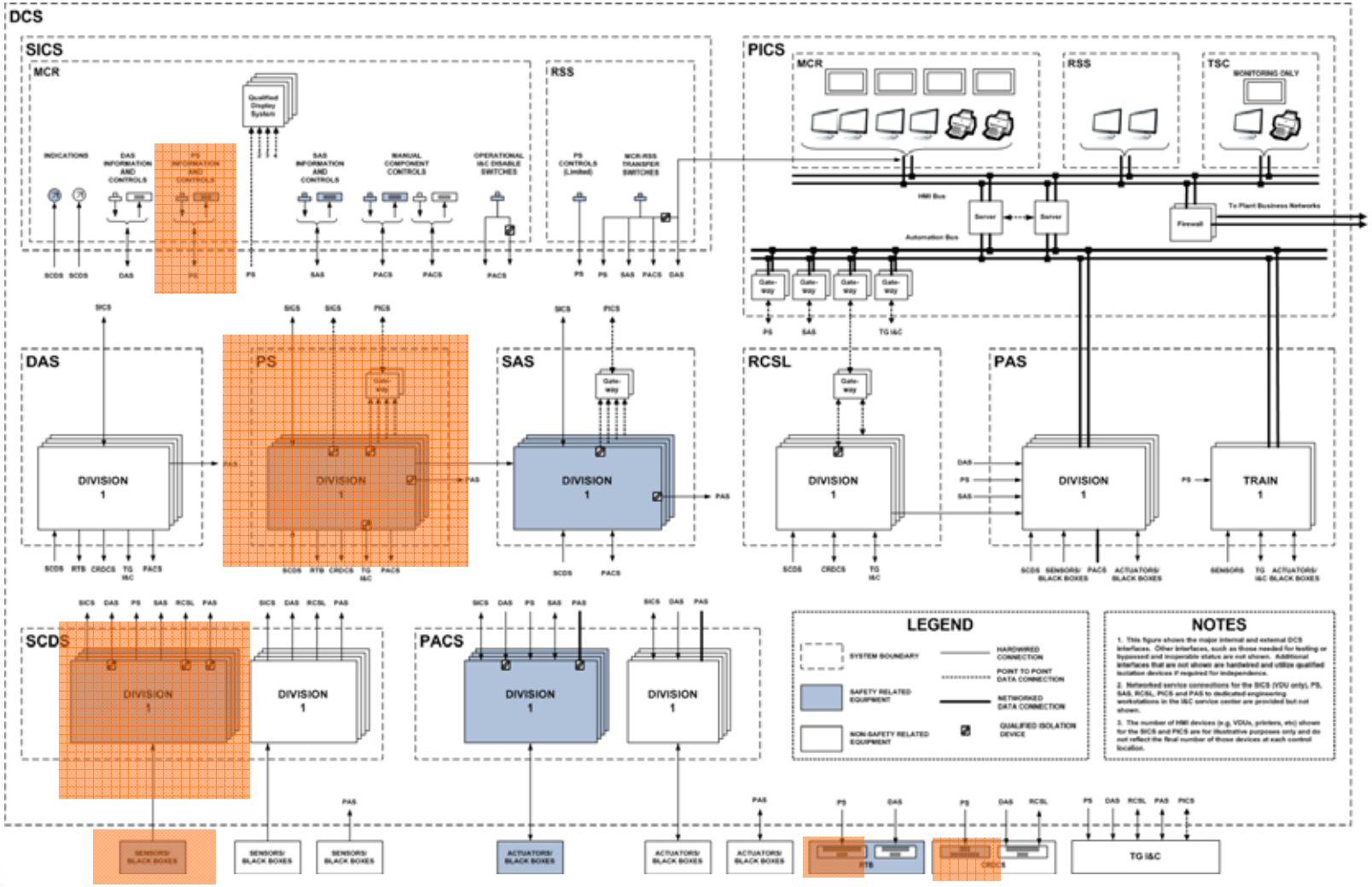
Topics

- Functions
- Design
- Redundancy
- Independence
- Deterministic Response Time
- Fail-Safe Behavior
- Testing

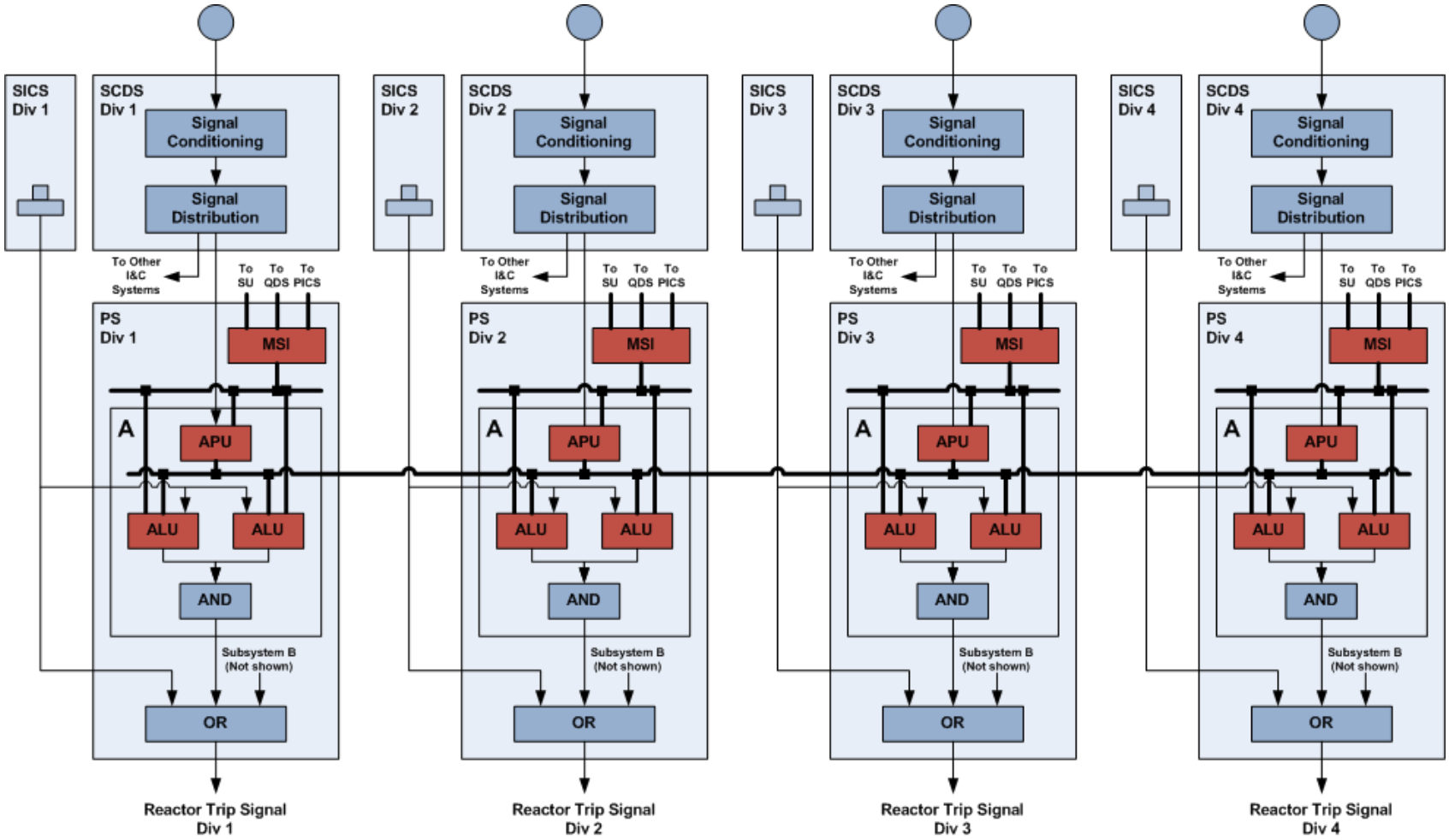
Functions

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	

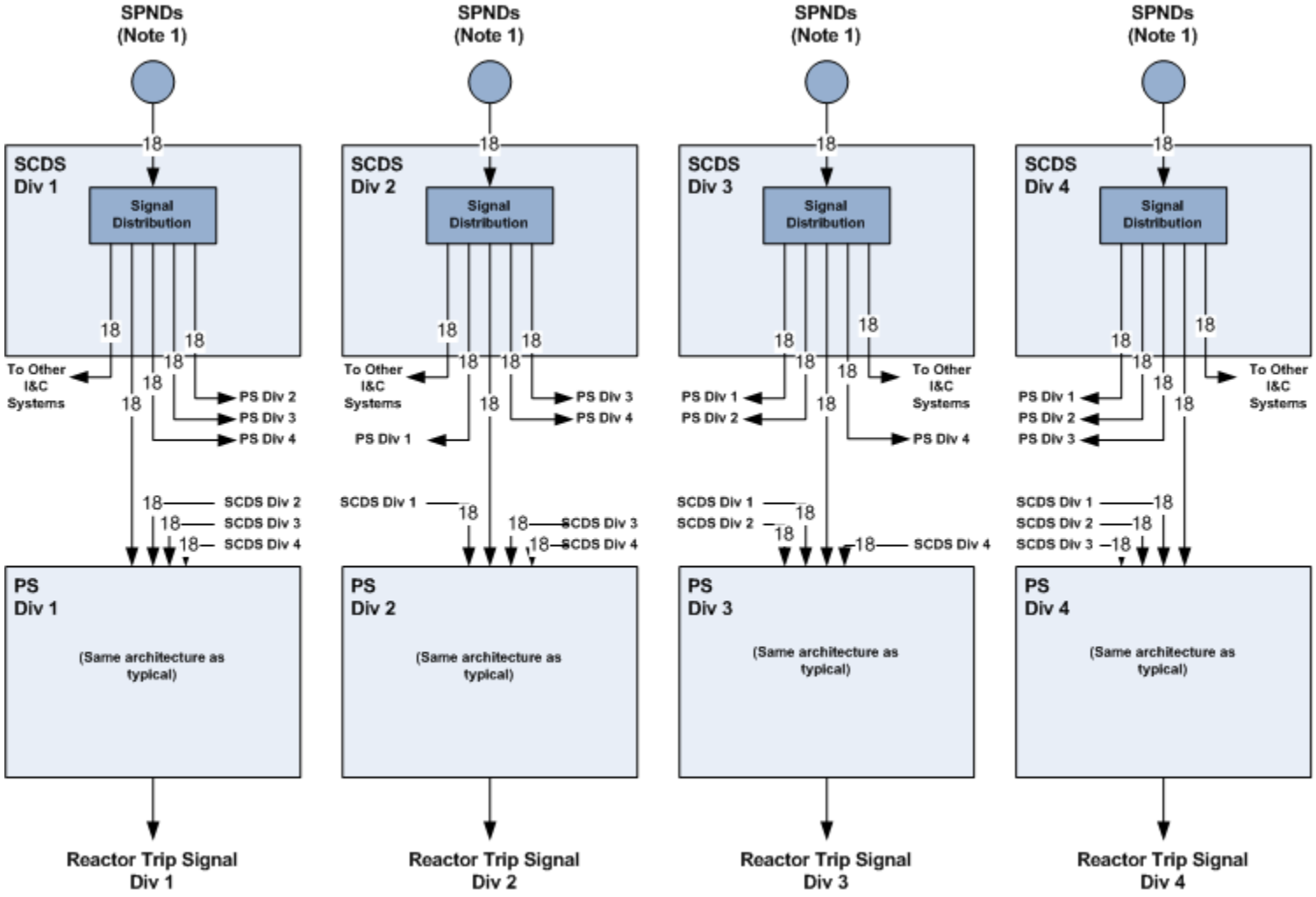
Design: Allocation within DCS



Design: Standard Reactor Trips

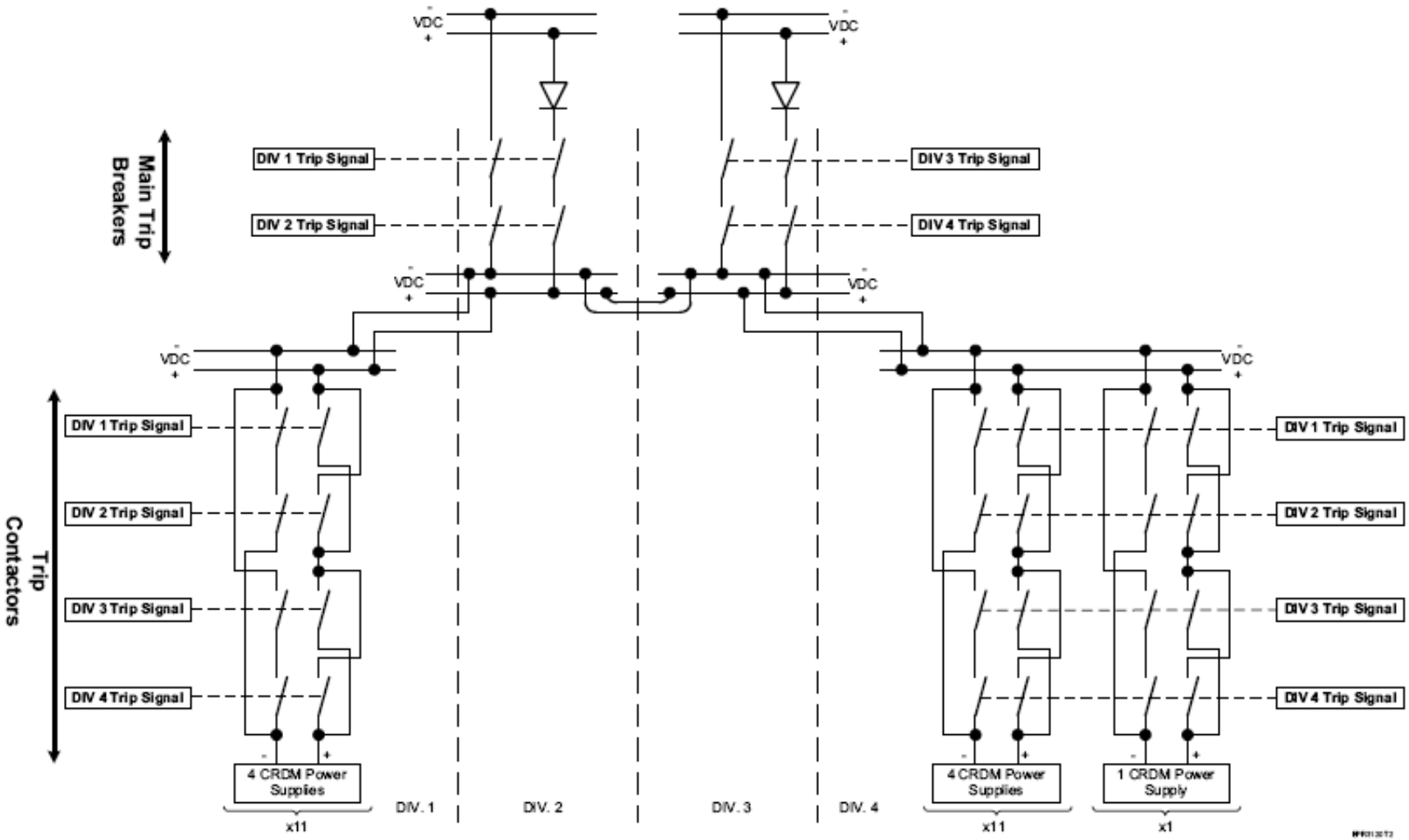


Design: SPND Reactor Trips



Note 1 – Includes SPNDs and signal conditioning cabinets that are part of the Incore Instrumentation System

Design: Reactor Trip Devices



Redundancy: Standard Reactor Trips

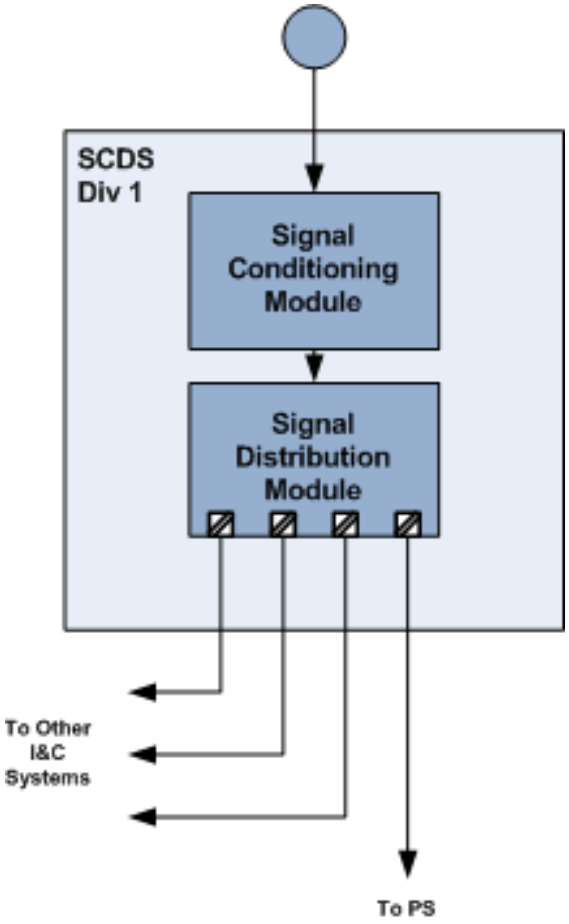
- **Sensors/signal conditioning/APU (setpoint comparator)**
  - **4-fold redundant for each process variable**
- **Manual actuation**
  - **4 reactor trip buttons (1 per I&C division)**
- **ALU (Voting)**
  - **8-fold redundant**
    - 4 divisions => meet single failure
    - 2 ALU per division => improve 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

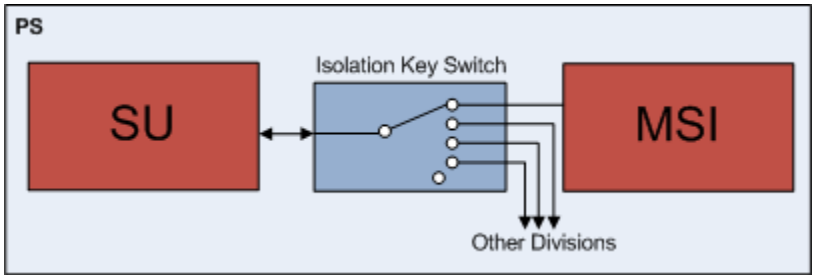
Independence: SCDS Output to Other I&C Systems

- **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



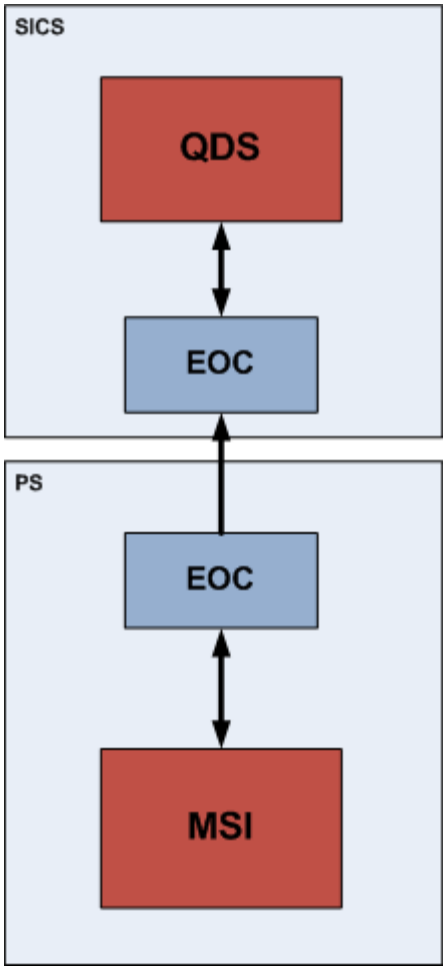
Independence: Service Unit Interface

- 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



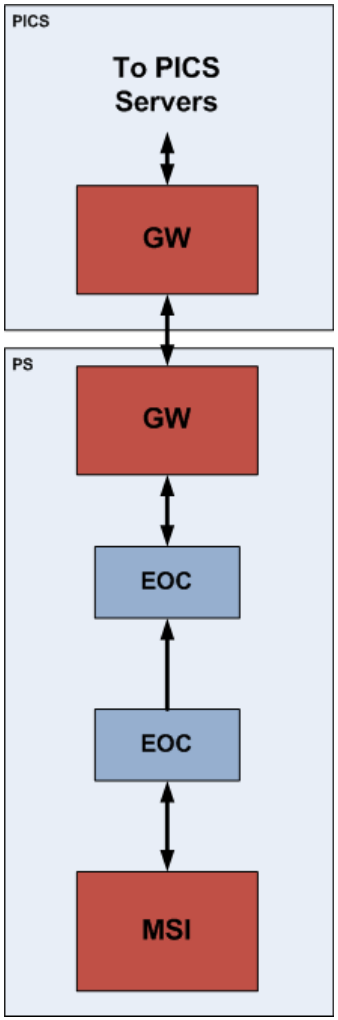
Independence: QDS Interface

- **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



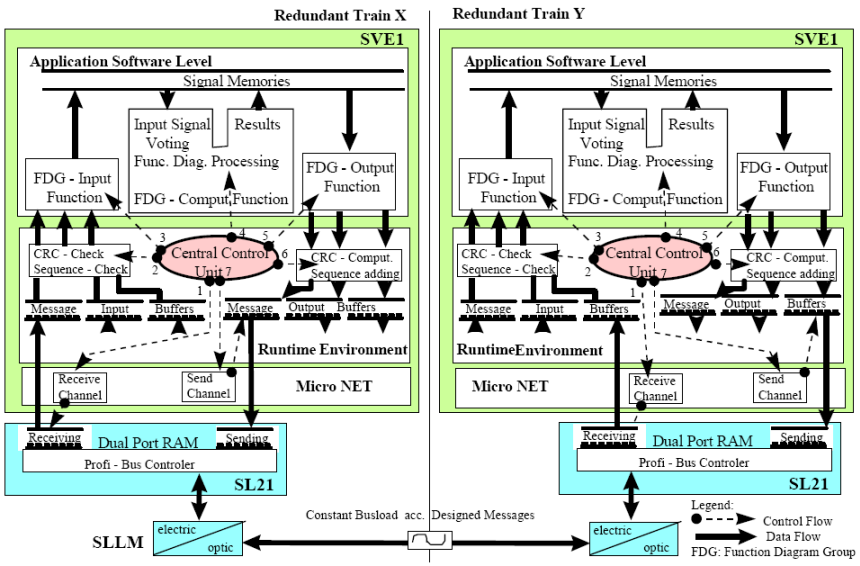
Independence: PICS Interface

- **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



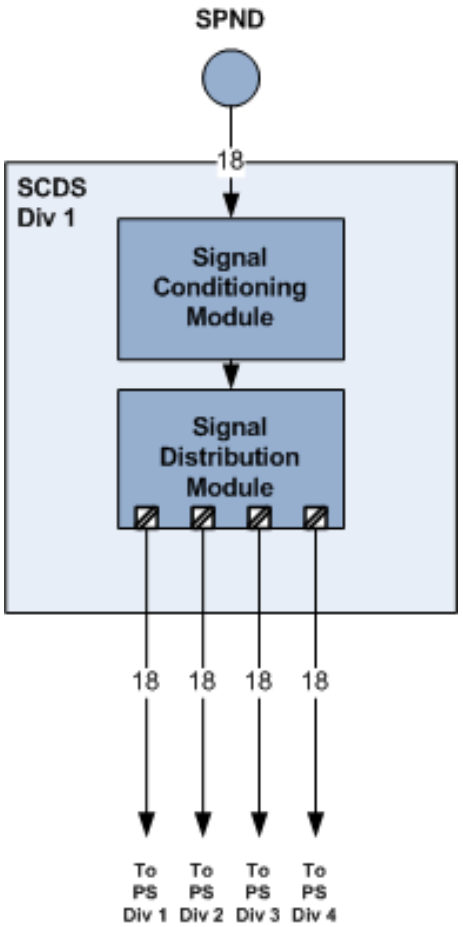
Independence: APU-ALU Interface

- **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



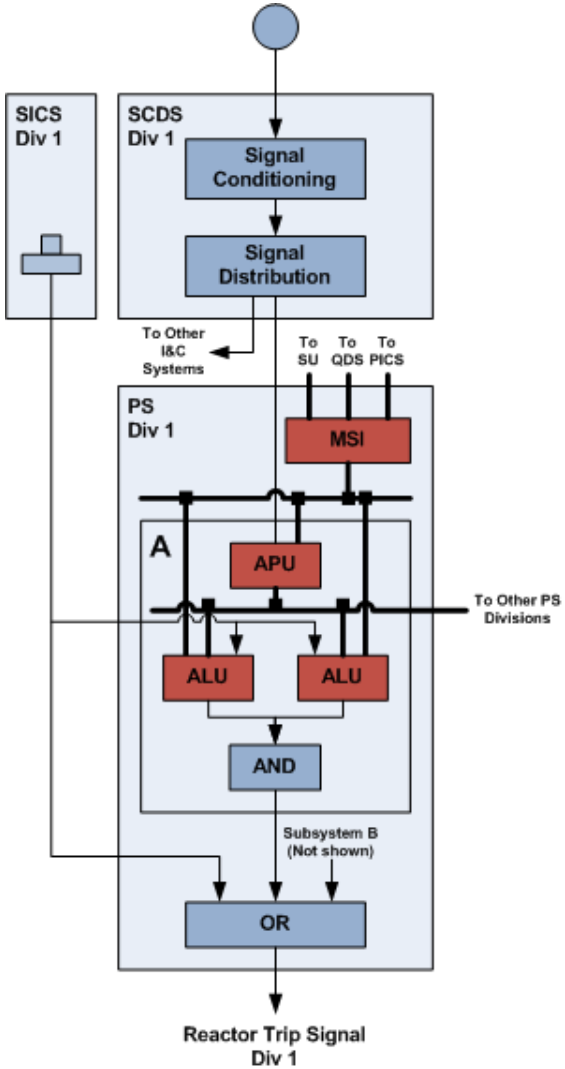
Independence: SPND Outputs from SCDS to PS

- **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

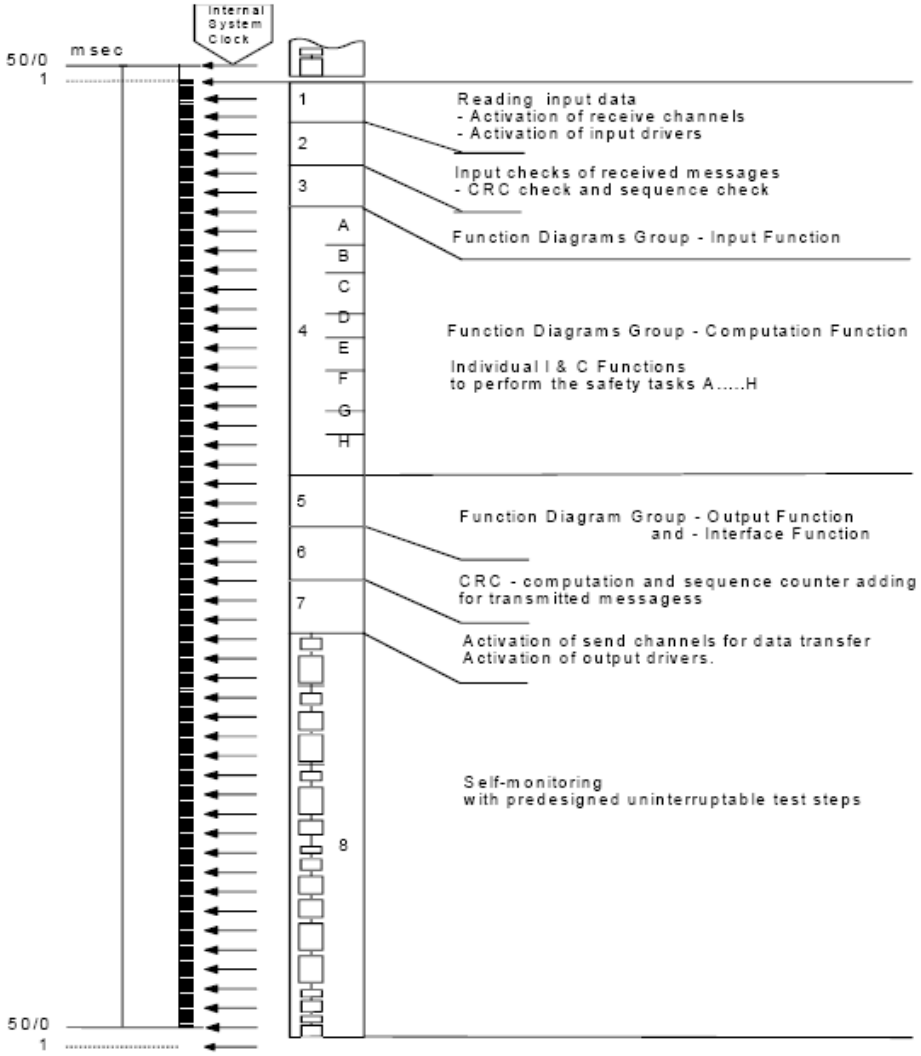


Deterministic Response Time: System Design

- 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

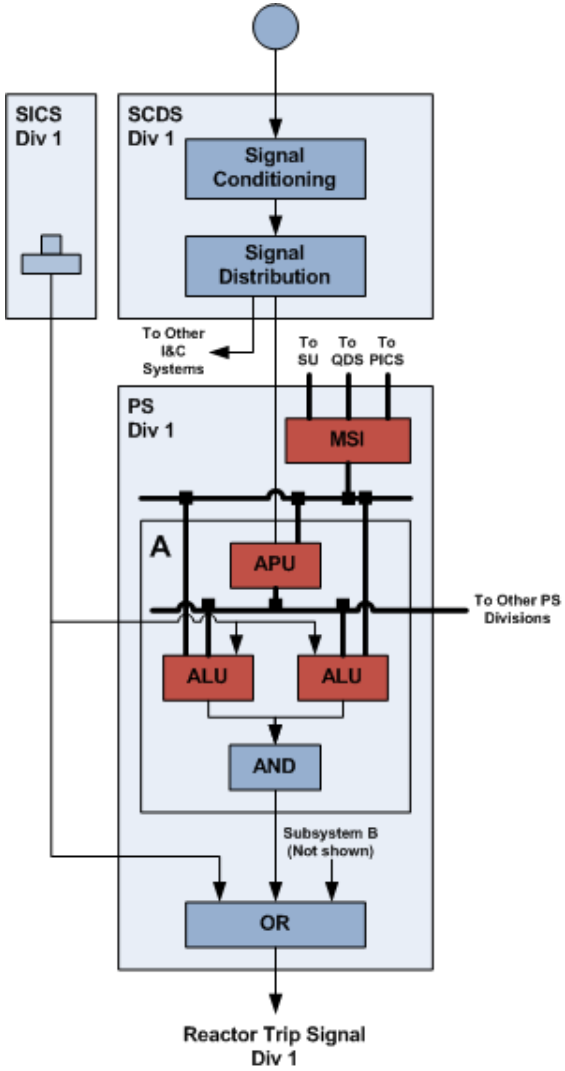


Deterministic Response Time: Cyclic TXS Processor Execution



Fail Safe Behaviour: System Design

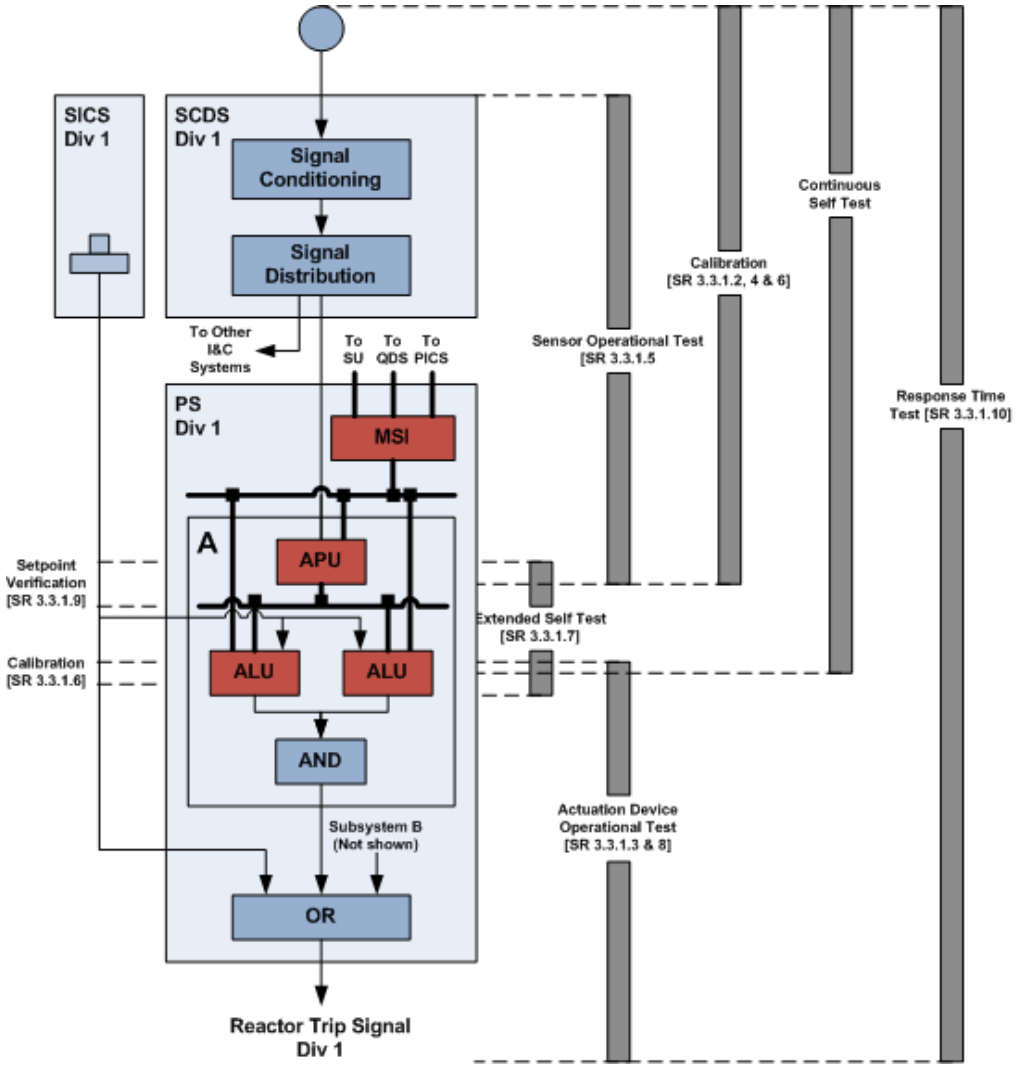
- **Sensor, signal conditioning and distribution failures**
  - **Out of range failure => detected by APU and flag signal, modify voting in ALU**
    - 1 sensor to 2/3 logic
    - 2 sensors to 1/2 logic
    - 3 or more sensors => reactor trip actuated
  - **In range failure => not detected**
- **APU 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


SICS
Div 1
SCDS
Div 1
Signal
Conditioning
Signal
Distribution
To Other
I&C
Systems
To
SU
To
QDS
To
PICS
PS
Div 1
MSI
A
APU
ALU
ALU
AND
Subsystem B
(Not shown)
OR
Reactor Trip Signal
Div 1
Setpoint
Verification
[SR 3.3.1.9]
Calibration
[SR 3.3.1.6]
Sensor Operational Test
[SR 3.3.1.5
Extended Self Test
[SR 3.3.1.7]
Actuation Device
Operational Test
[SR 3.3.1.3 & 8]
Calibration
[SR 3.3.1.2, 4 & 6]
Continuous
Self Test
Response Time
Test [SR 3.3.1.10]

SECTION 7.3: ENGINEERED SAFETY FEATURES SYSTEMS

Topics

- Functions
- Design
- Redundancy
- Independence
- Deterministic Response Time
- Fail-Safe Behavior
- Testing

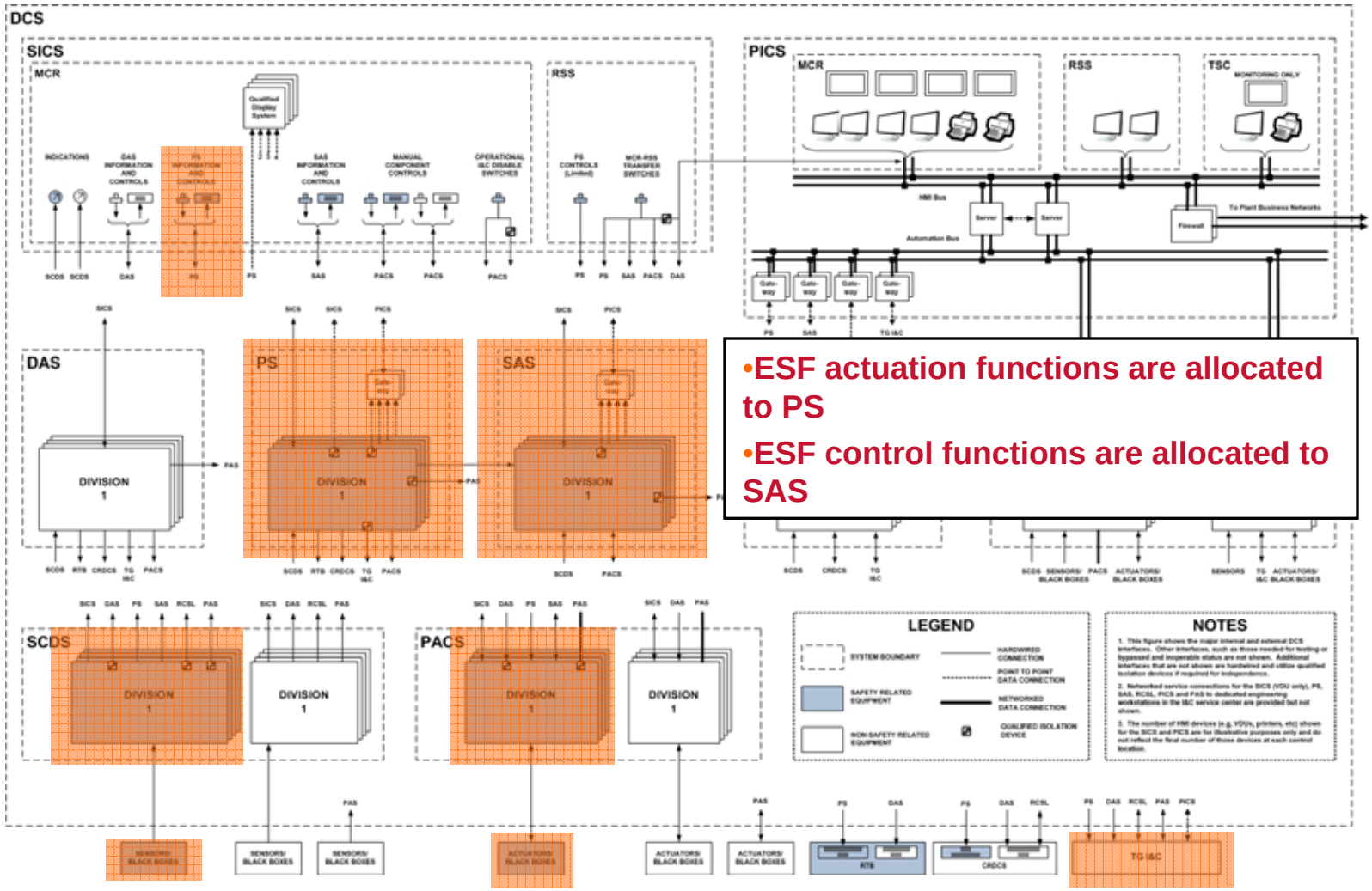
Functions: ESF Actuation

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

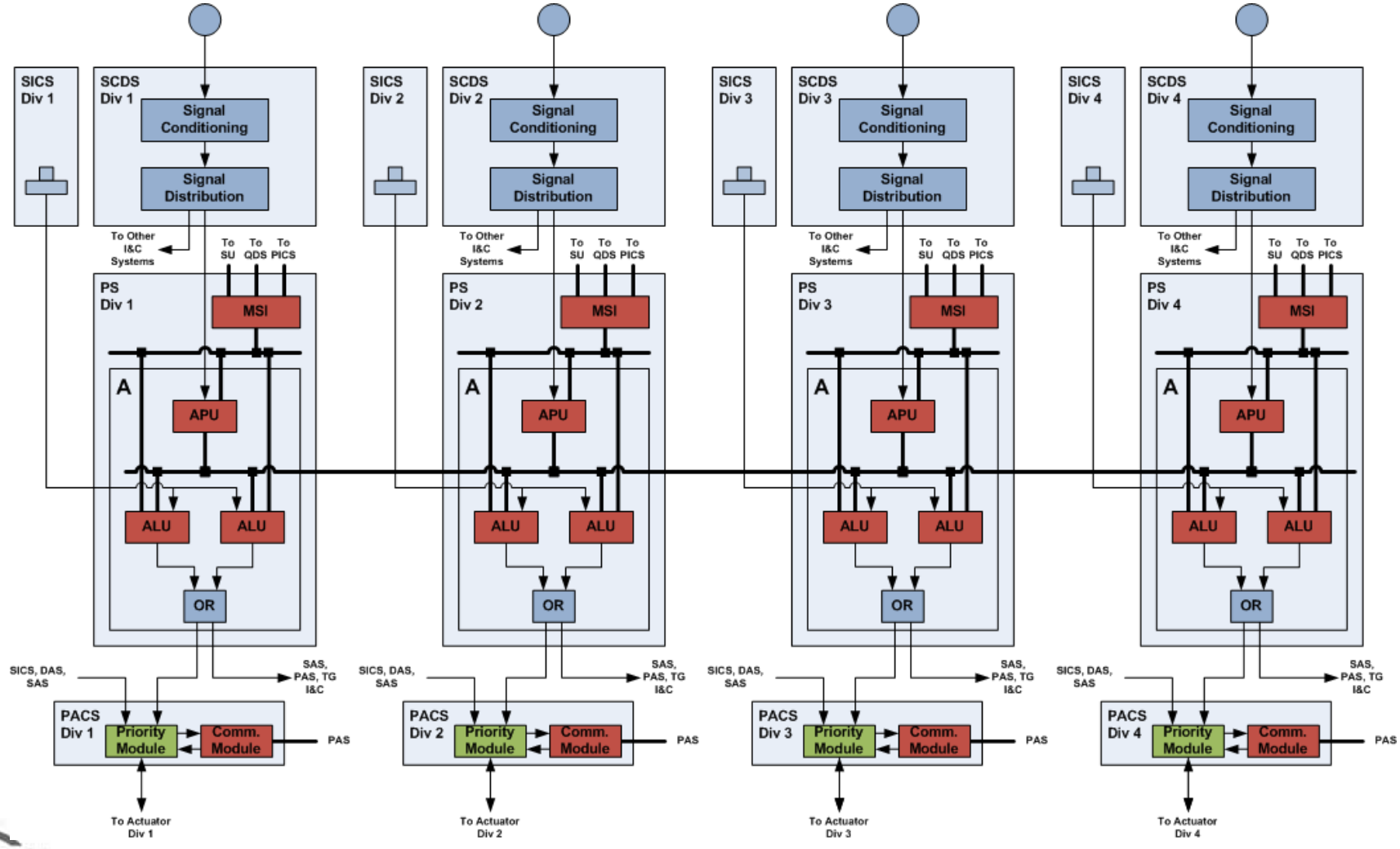
FUNCTION
Emergency Feedwater System: Steam Generator Level Control
Emergency Feedwater System: EFW Pump Flow Protection
Main Steam Relief Control Valve Control

Design: Allocation within the DCS

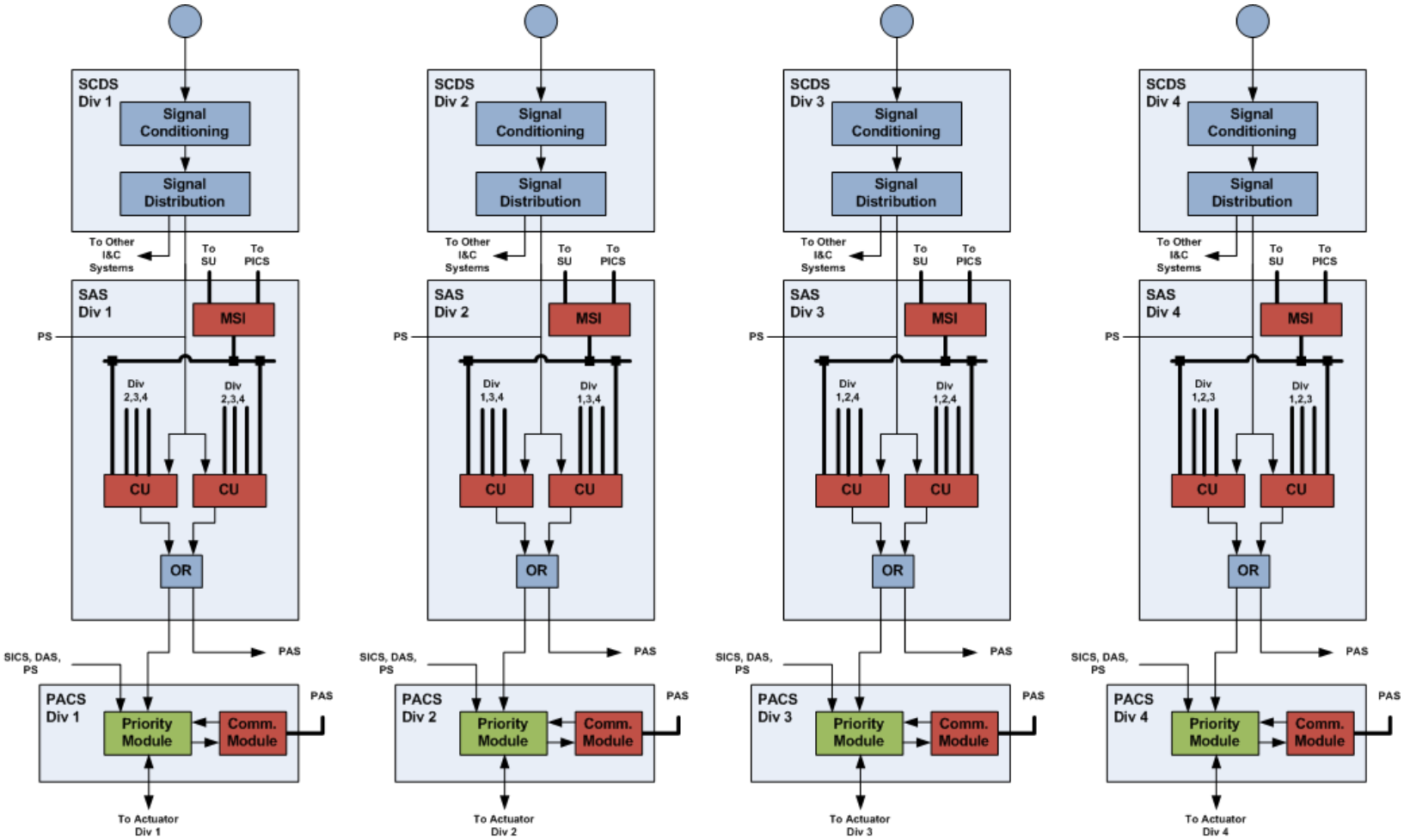


- ESF actuation functions are allocated to PS
- ESF control functions are allocated to SAS

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

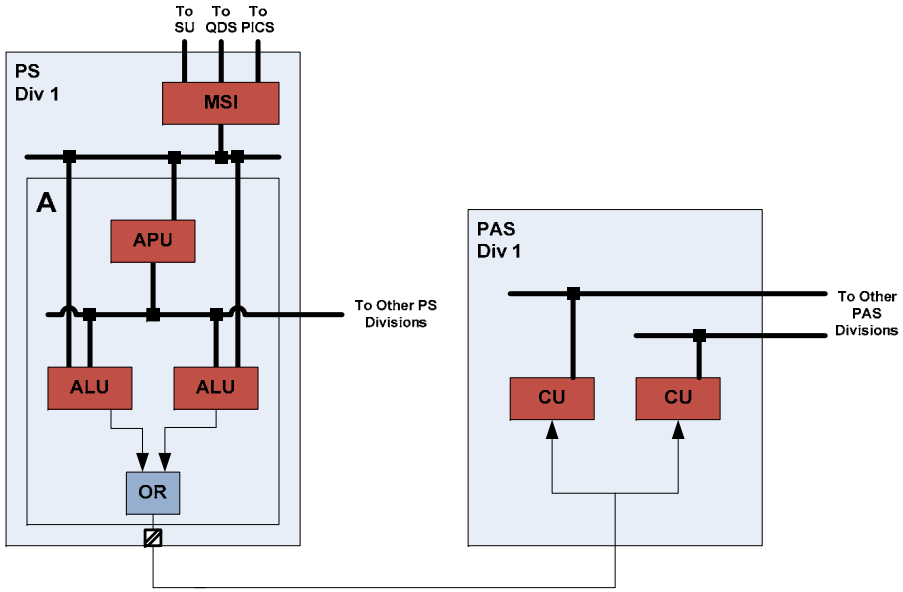
- **ESF control functions follow redundancy of mechanical trains**
  - **EFW => 4 redundant trains**
  - **MSRT => 4 redundant trains**
- **Redundant CU's per SAS division for improved availability**

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

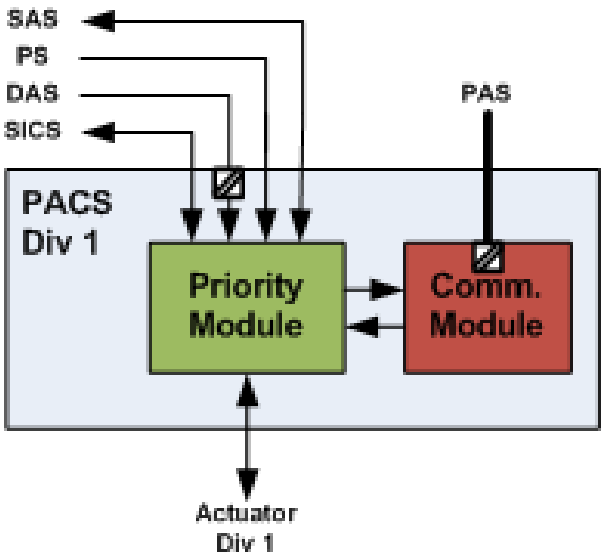


Independence: CU-CU Interdivisional Communication

- **Purpose**
  - **To send signals for voting (MSRT isolation valve position)**
- **Type**
  - **Data**
- **Means of independence**
  - **Same as APU-ALU**

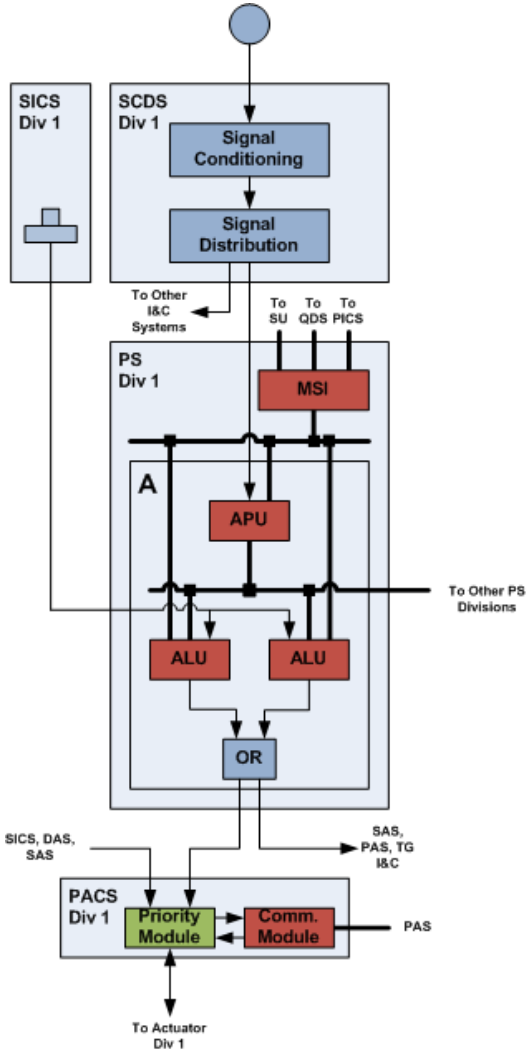
Independence: PACS

- **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



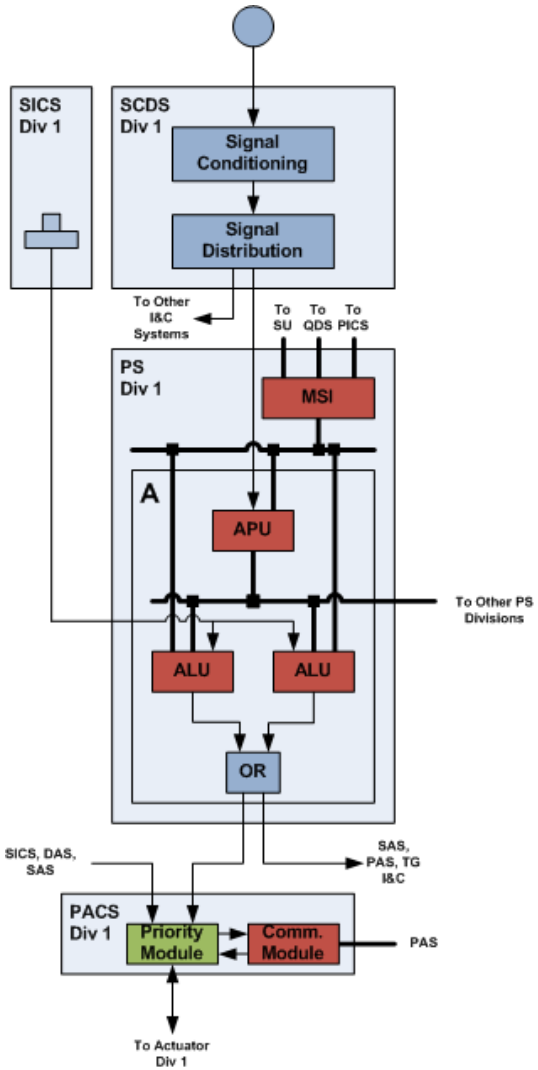
Deterministic Response Time

- 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



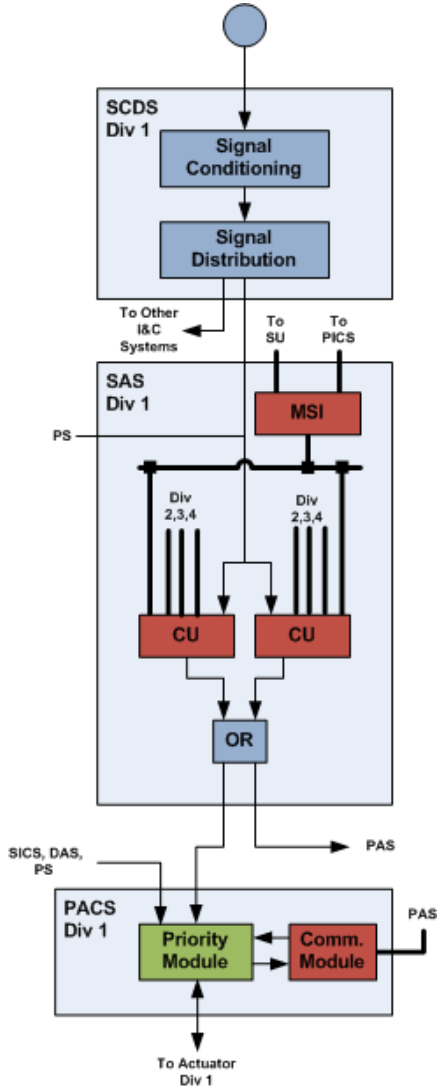
Fail Safe Behaviour: ESF Actuation

- **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**

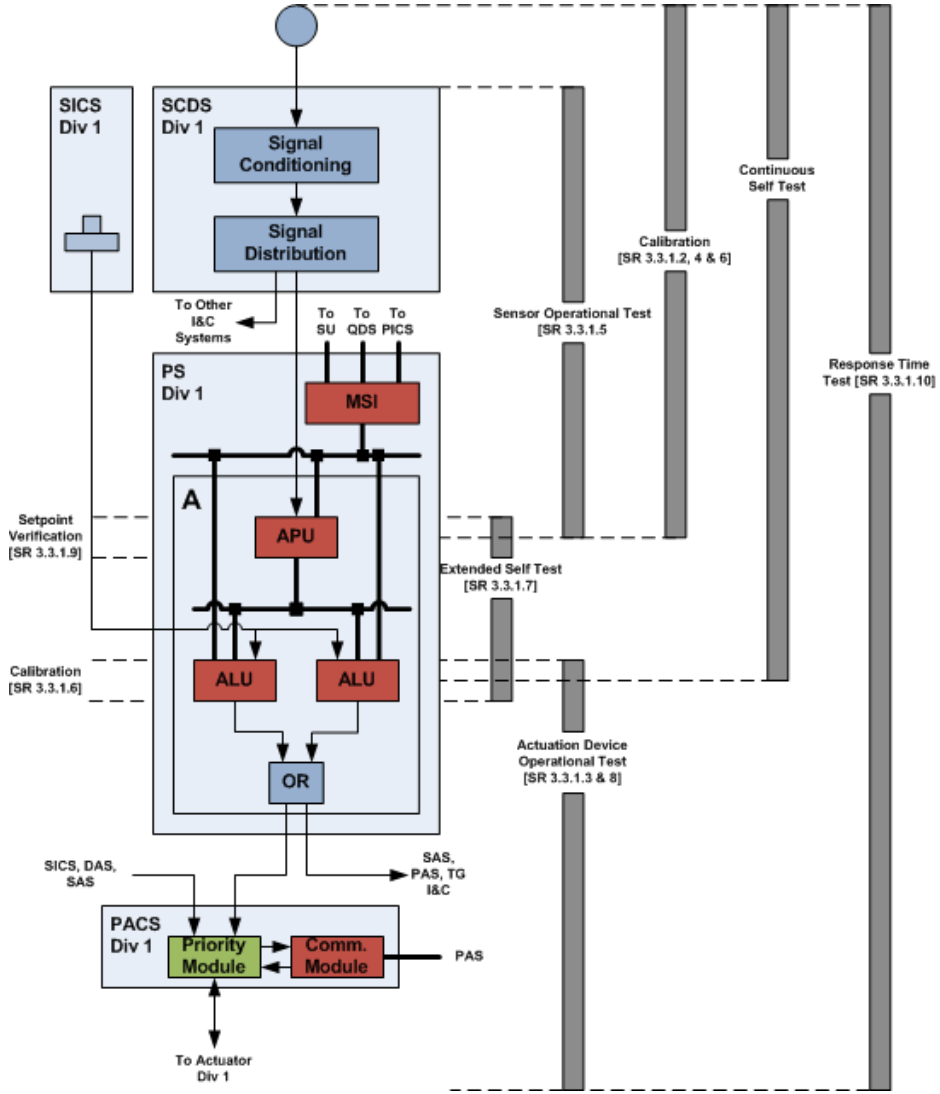


Fail Safe Behaviour: ESF Control

- 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


SICS
Div 1
SCDS
Div 1
Signal Conditioning
Signal Distribution
To Other I&C Systems
To SU
To QDS
To PICS
PS
Div 1
MSI
A
APU
ALU
ALU
OR
Setpoint Verification [SR 3.3.1.9]
Calibration [SR 3.3.1.6]
Sensor Operational Test [SR 3.3.1.5
Calibration [SR 3.3.1.2, 4 & 6]
Continuous Self Test
Response Time Test [SR 3.3.1.10]
Extended Self Test [SR 3.3.1.7]
Actuation Device Operational Test [SR 3.3.1.3 & 8]
SICS, DAS, SAS
SAS, PAS, TG I&C
PACS
Div 1
Priority Module
Comm. Module
PAS
To Actuator Div 1

SECTION 7.4 : SYSTEMS REQUIRED FOR SAFE SHUTDOWN

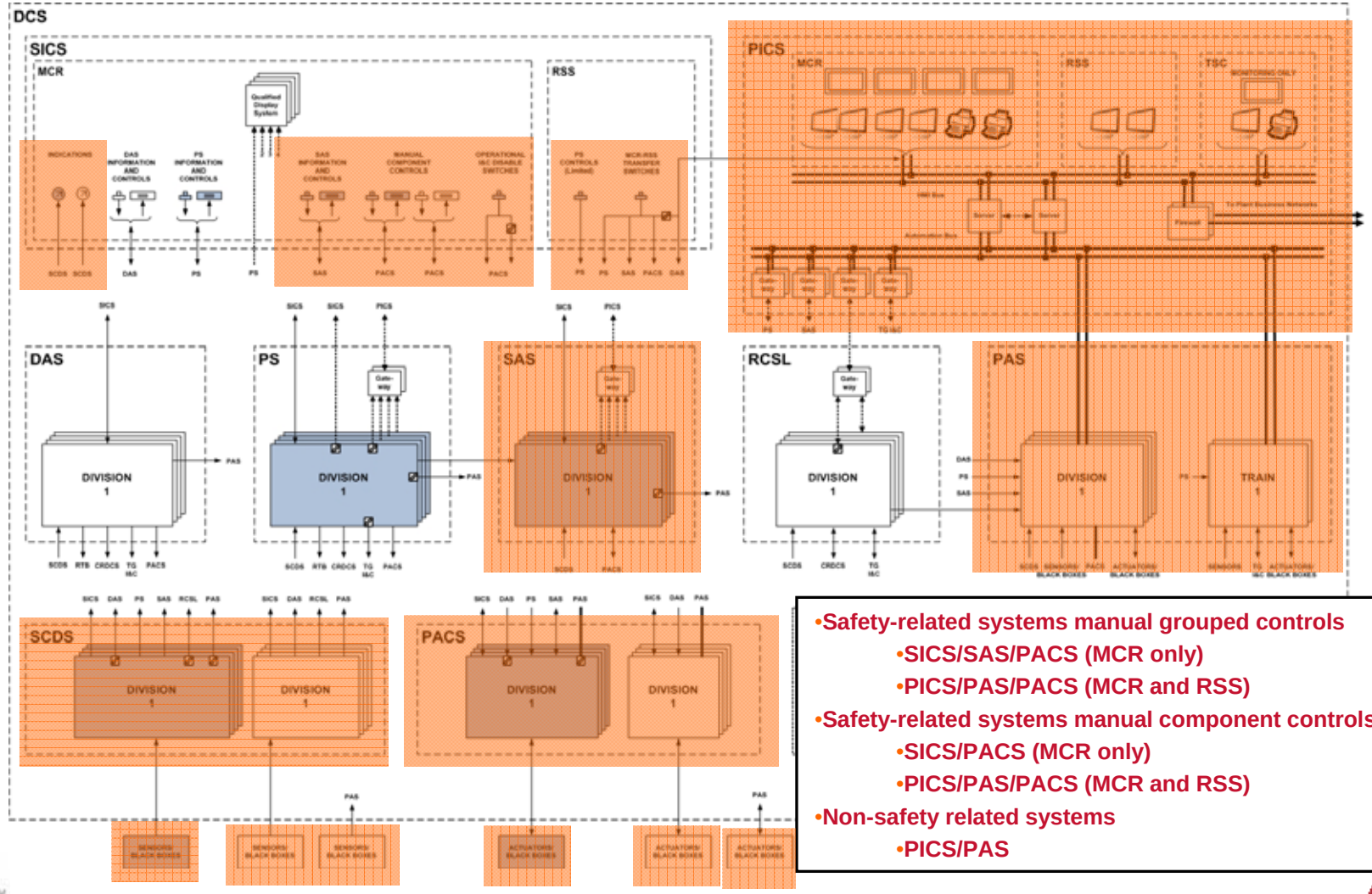
Topics

- 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 phyiscally 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 cablets

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)

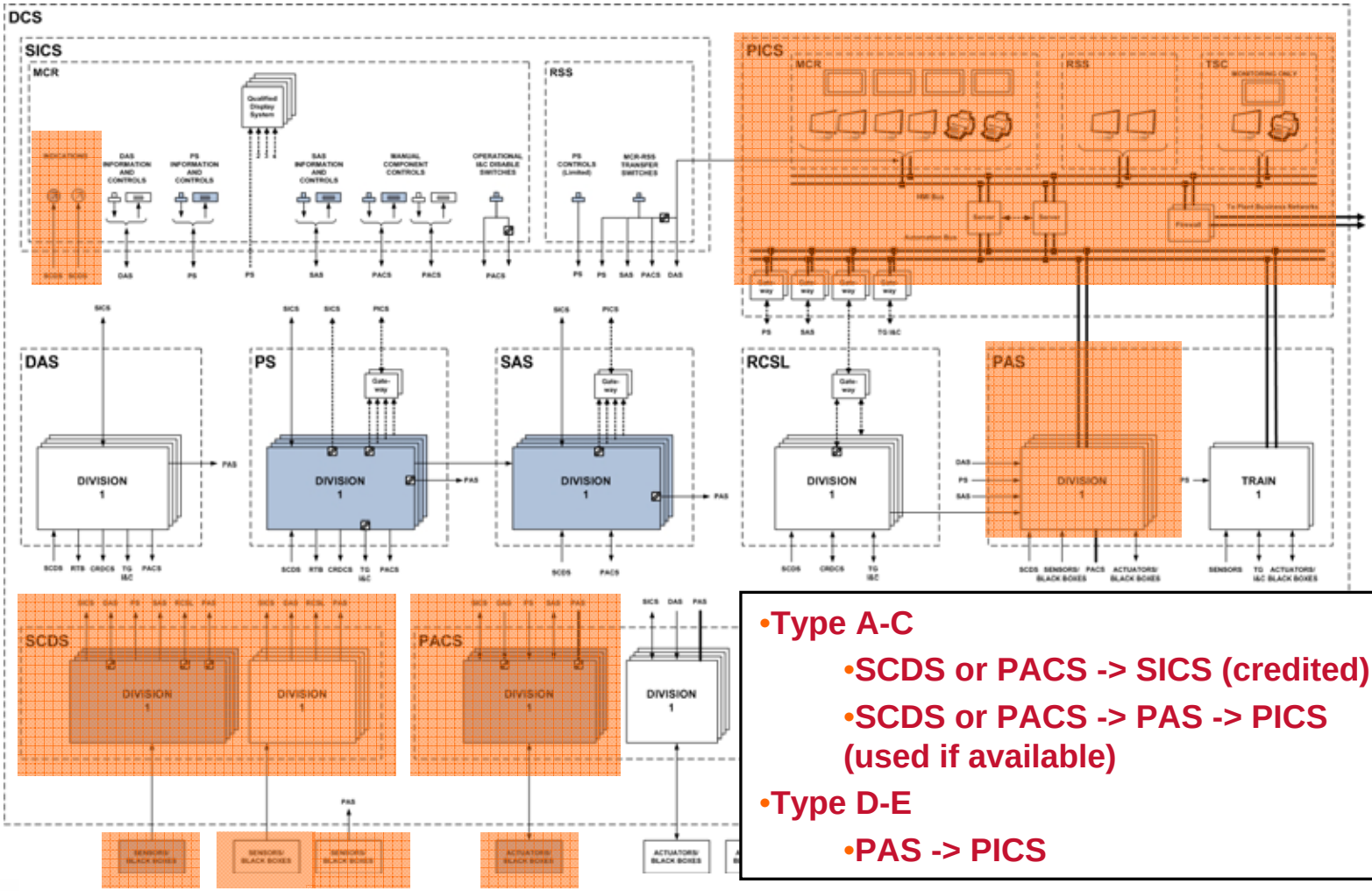
Alarms

- **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

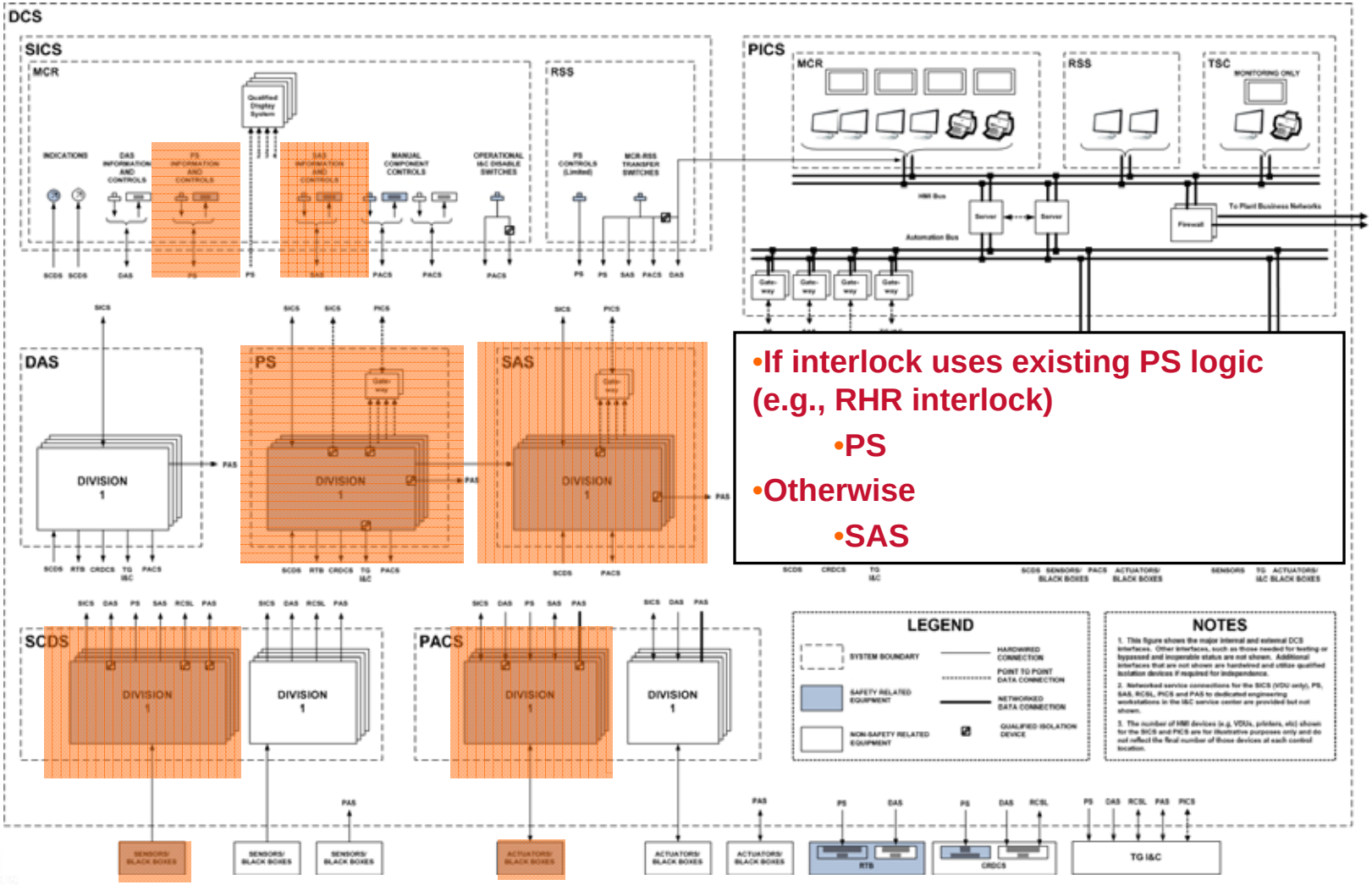
Topics

- 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



- If interlock uses existing PS logic (e.g., RHR interlock)
  - PS
- Otherwise
  - SAS

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

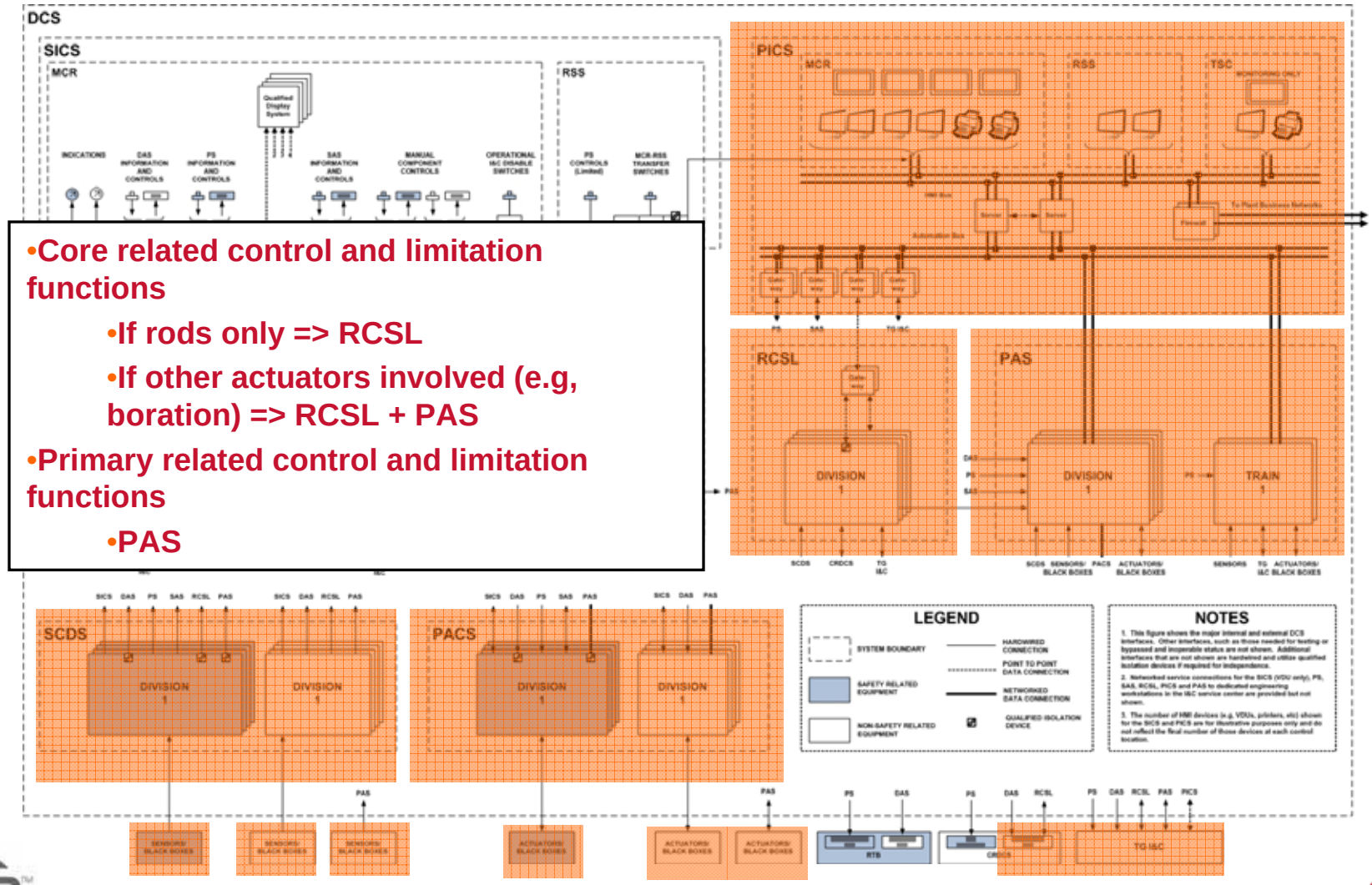
Functions:
Process Control Functions

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)	

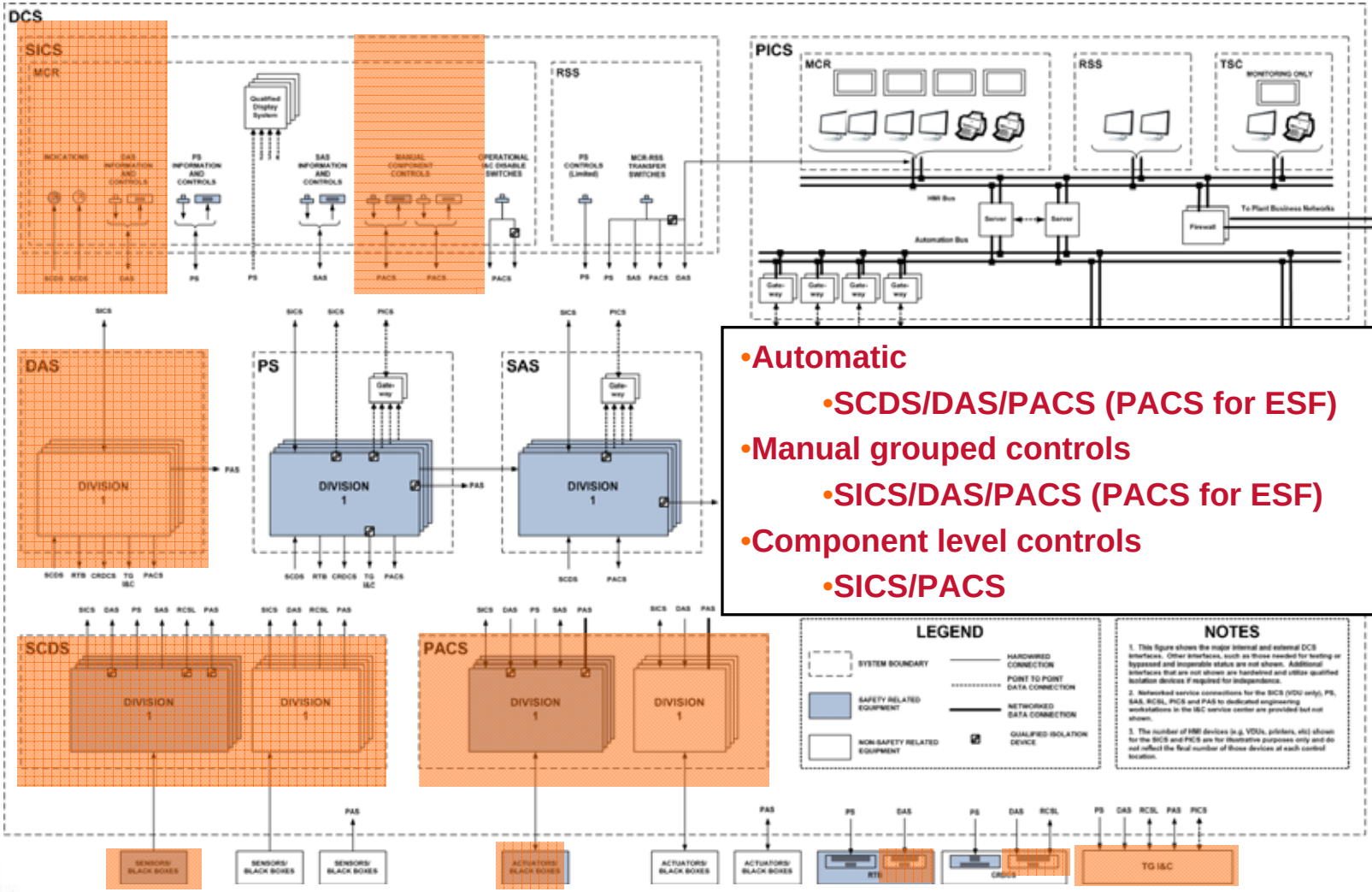
Functions: Diverse ESF

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 Isolaton	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)

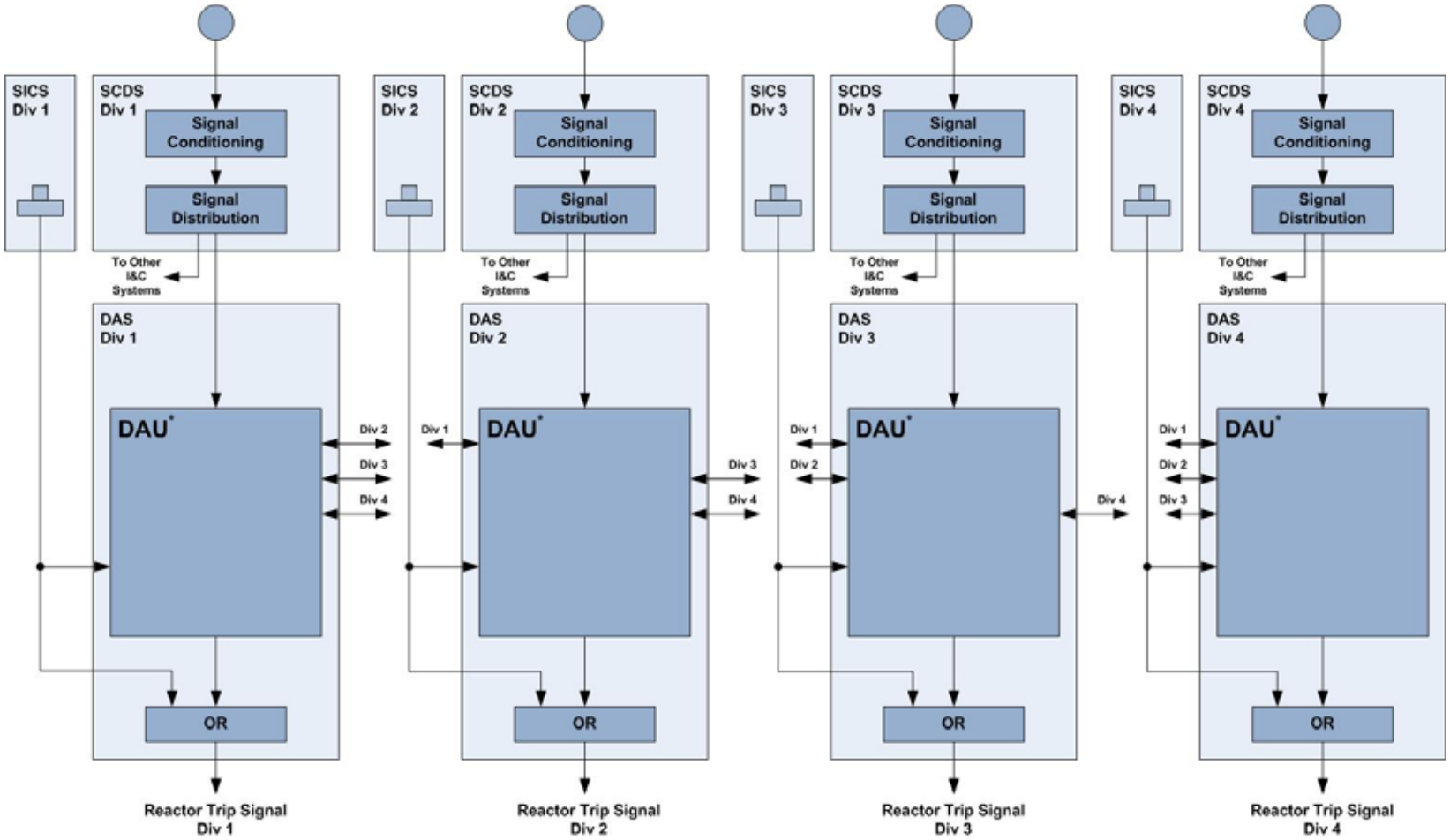
FUNCTION	AUTOMATIC	MANUAL SYSTEM LEVEL	MANUAL COMPONENT LEVEL
Start Emergency Diesel Generators			x
Emergency Diesel Generator Loading			x
Extend Partial Cooldown			x
Safety Injection Switchover to Hot Leg Injection			x
Depressurize Reactor Coolant System with Pressurizer Sprays			x
Extra Borating System 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



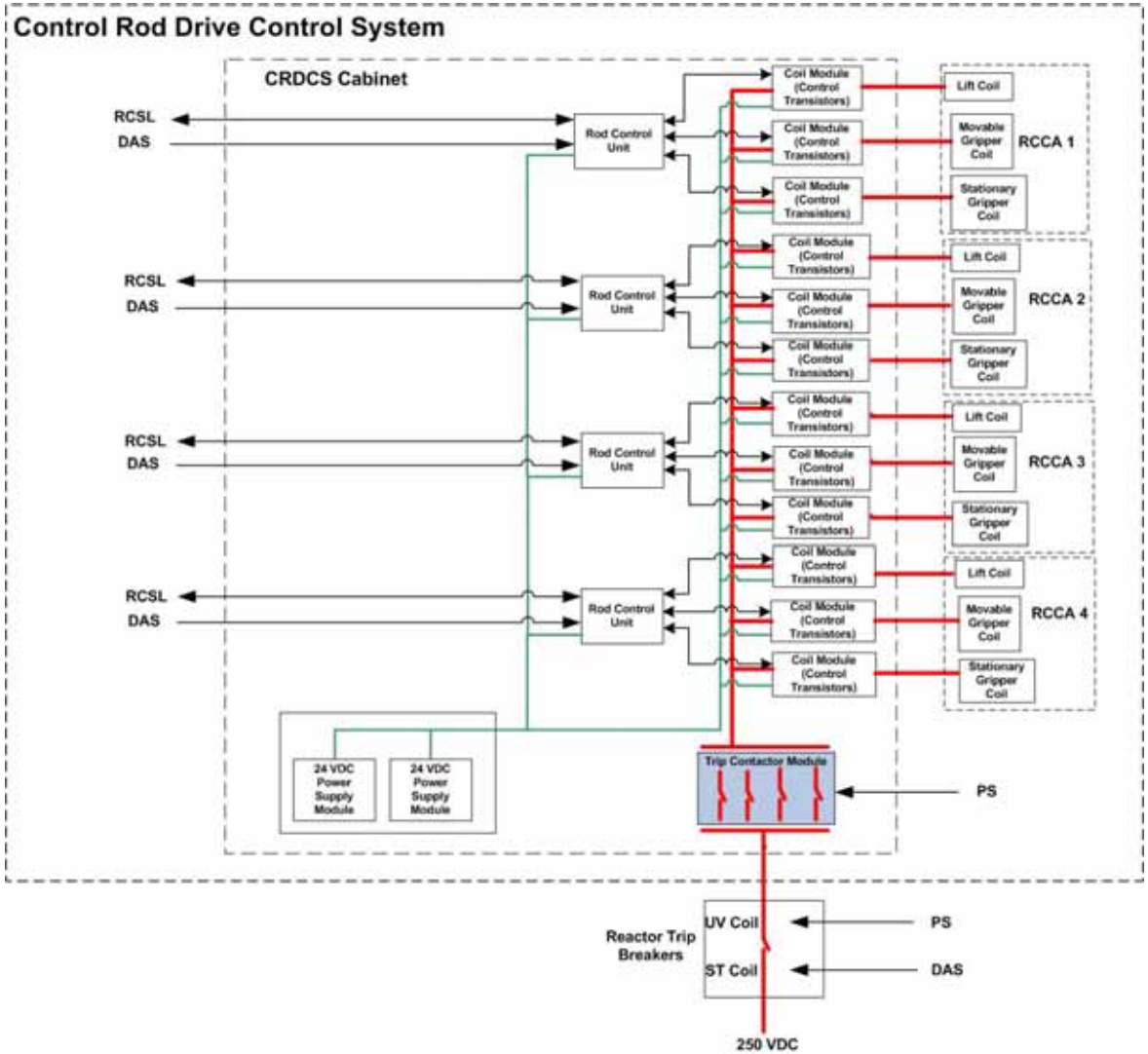
- Automatic
  - SCDS/DAS/PACS (PACS for ESF)
- Manual grouped controls
  - SICS/DAS/PACS (PACS for ESF)
- Component level controls
  - SICS/PACS

Design:
Diverse Reactor Trip

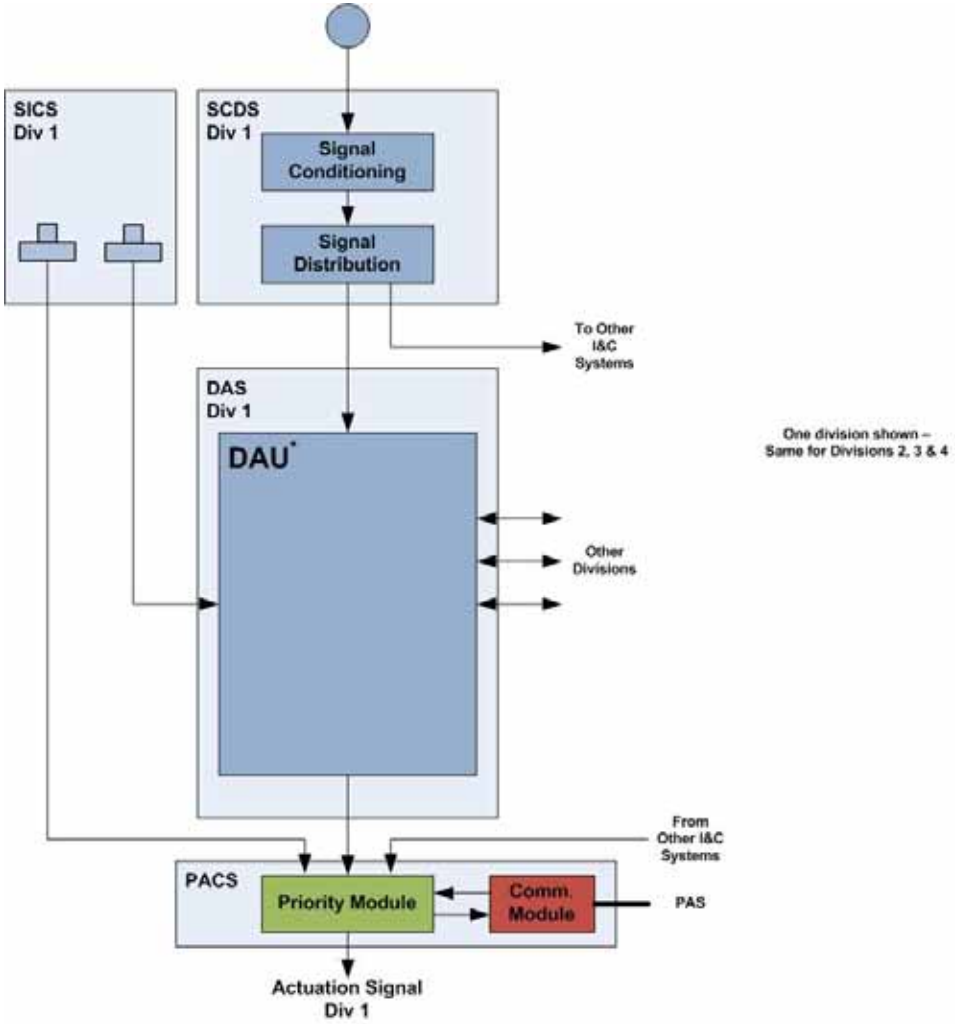


*Technology may be non-microprocessor based programmable electronics also

Design:
Diverse Reactor Trip Devices



Design: Diverse ESF



*Technology may be non-microprocessor based programmable electronics also

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

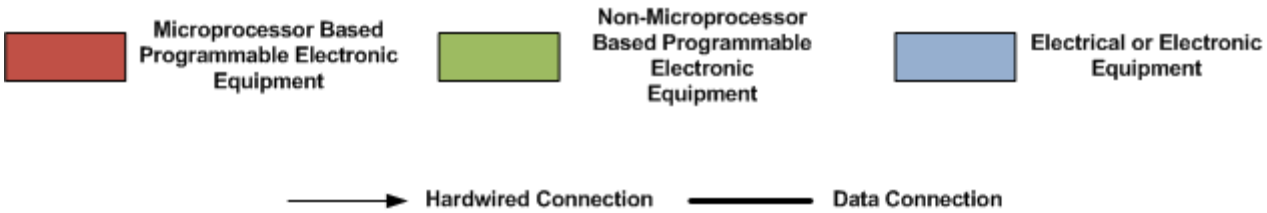
Acronyms

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	Qualfied 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)



AREVA

United States Nuclear Regulatory Commission

Protecting People and the Environment

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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.**

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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 the relate to SAS, especially those that are outside the bounds of the system interaction with PS.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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)

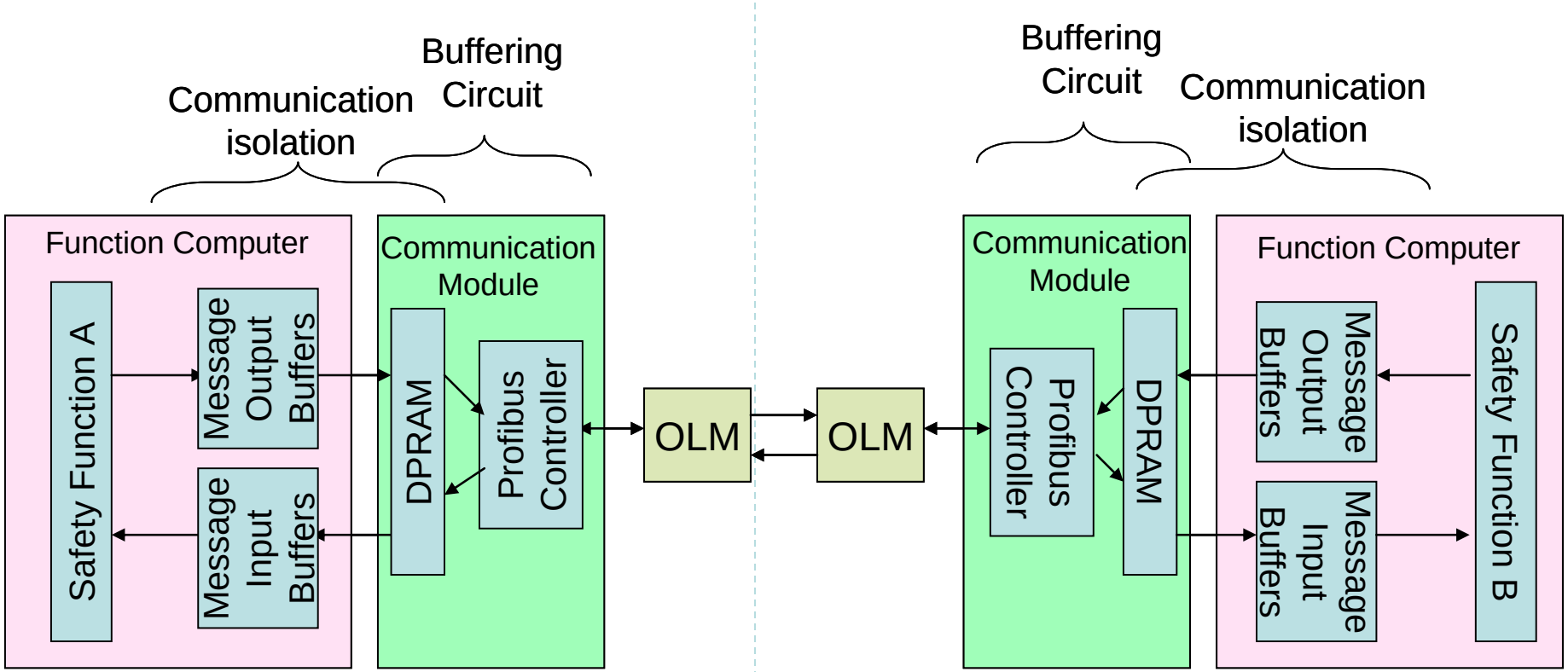
Independence

- **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, <u>undetected</u> 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)

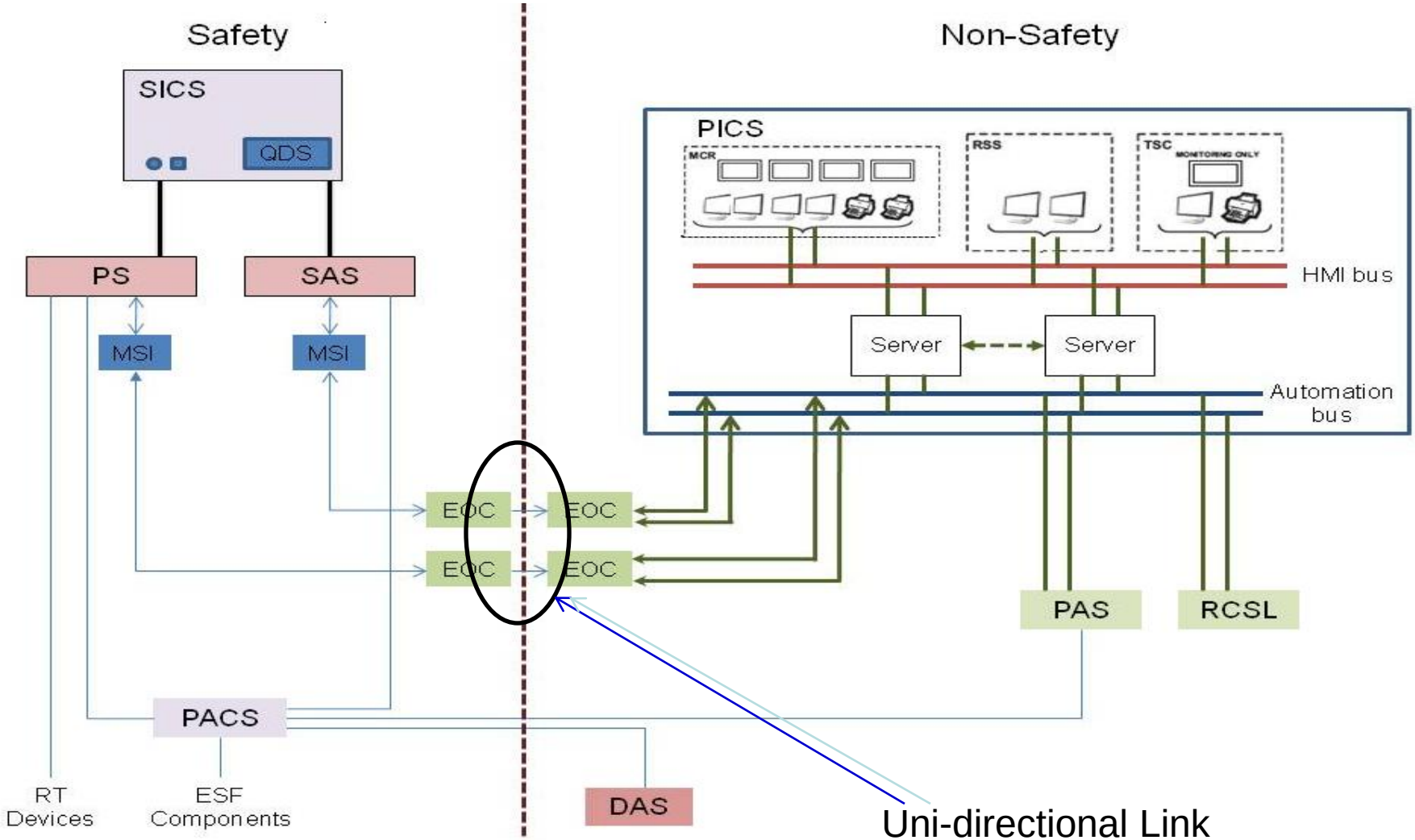
Independence

- **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

Independence

- **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.

Determinism

- **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

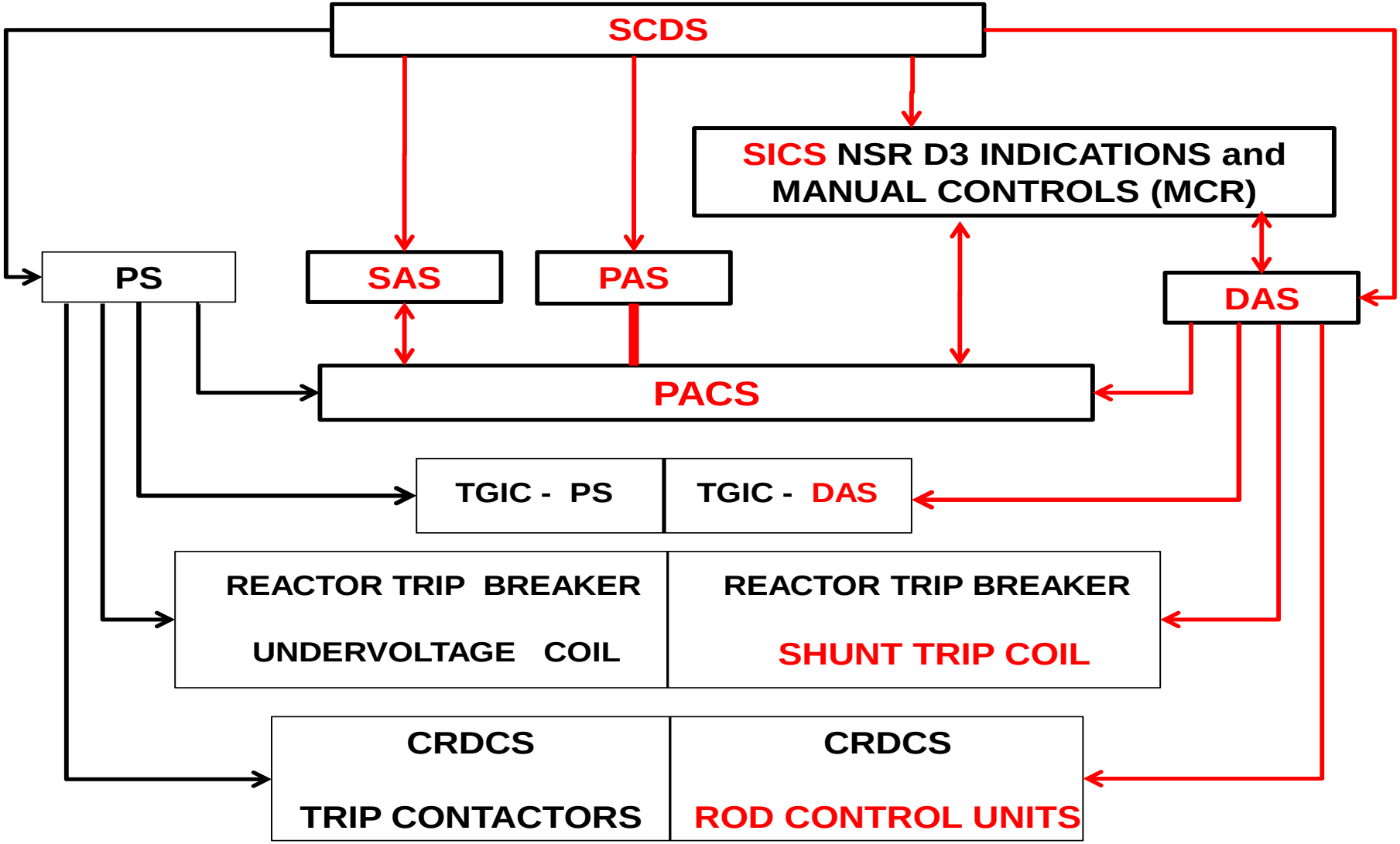
Diversity Attributes	DAS-PS Staff Approved Design Diversity
Design	
different approaches within the a technology	YES
different architecture	YES
Equipment	
same manufacturer of fundamentally different designs	YES
different logic processing equipment architecture	YES
Function	
different purpose, function, 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)

Defense-in-Depth and Diversity

- **Other systems that make up the D3 mitigation systems**
  - PACS: 100% combinatory 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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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)

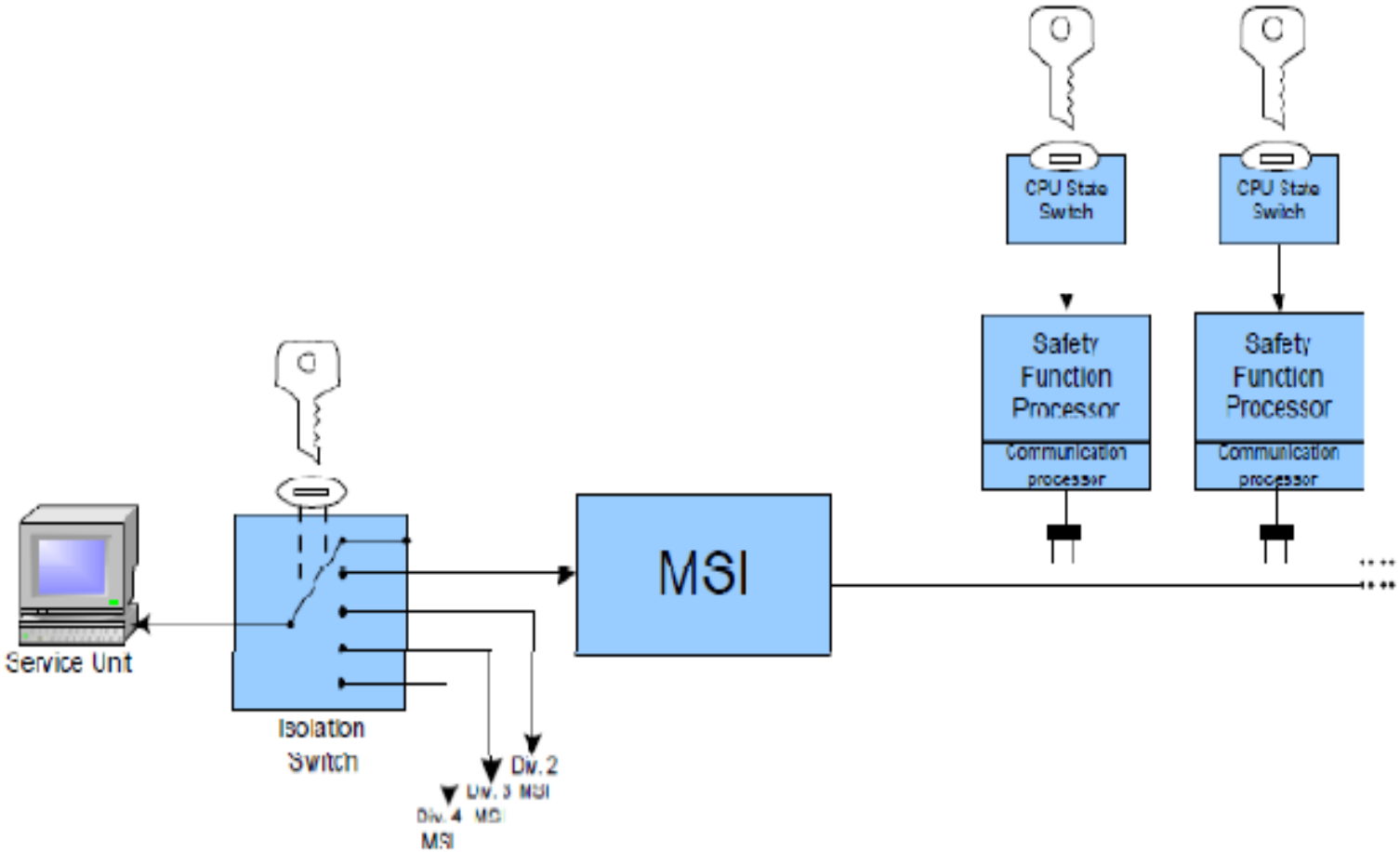
Self-Testing Open Items

- **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

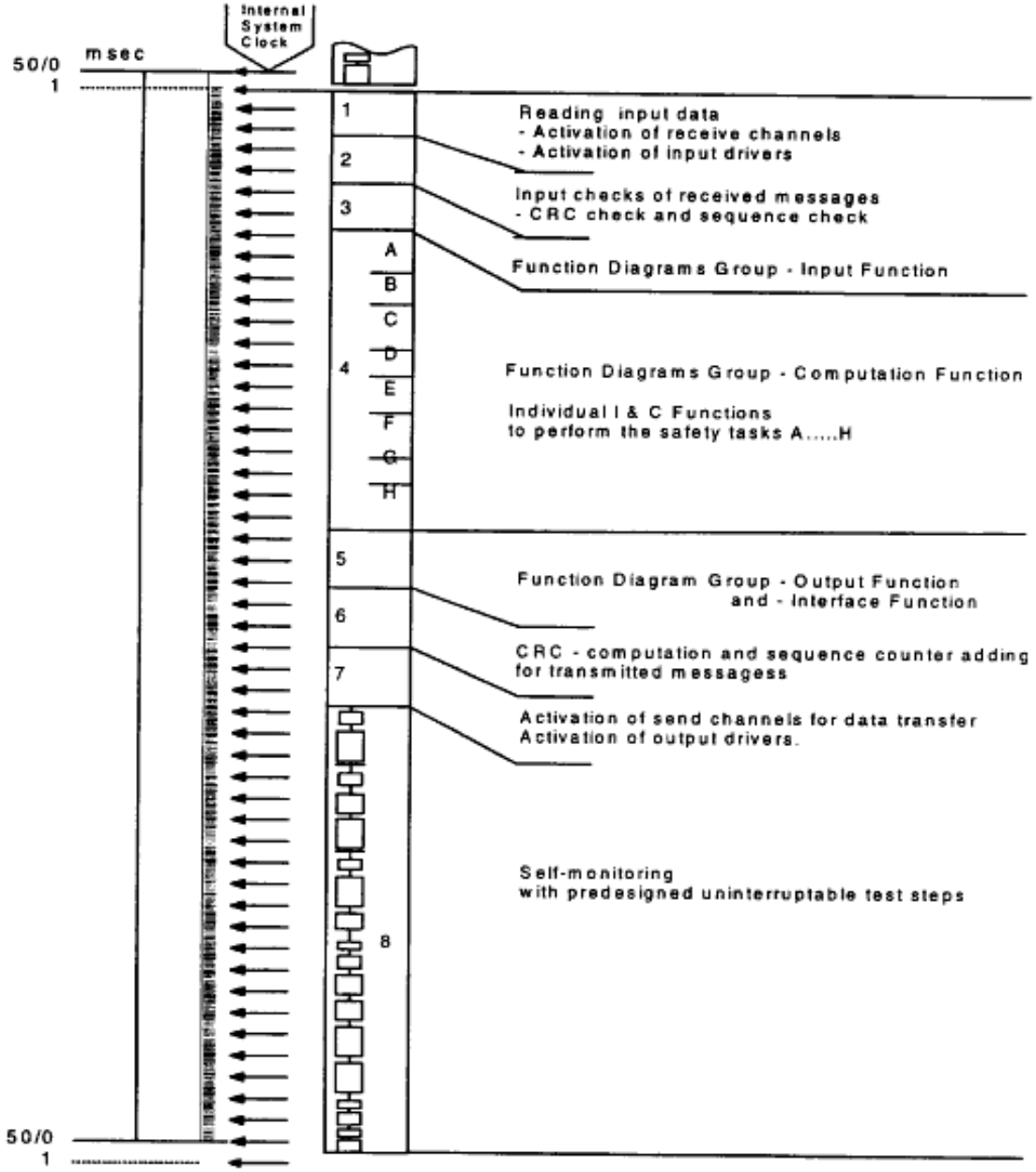
List of Acronyms

- 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



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

- <u>Conformance with RG 1.97, Accident Monitoring Instrumentation</u>
  - 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

- <u>Reactor Power Limitation with Respect to Thermal Power</u>
  - 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

- <u>Site-Specific Post Accident Monitoring (PAM) Variables</u>
  - 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

United States Nuclear Regulatory Commission

Protecting People and the Environment

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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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

U.S.NRC
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 5 12 17 19	3/24/2010 3/22/2010 3/19/2010 3/12/2010 4/19/2010	4/20/2010 4/20/2010 4/20/2010 4/20/2010 5/21/2010
10 11 16	6/11/2010 10/30/2010 10/11/2010	11/30/2010
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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- 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

- 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

United States Nuclear Regulatory Commission
Protecting People and the Environment

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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