Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
US-APWR Subcommittee: Open Session

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, April 25, 2013

Work Order No.: NRC-4166 Pages 1-334

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

US-APWR SUBCOMMITTEE

+ + + + +

THURSDAY

APRIL 25, 2013

+ + + + +

OPEN SESSION

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

COMMITTEE MEMBERS:

JOHN W. STETKAR, Chairman

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR. Member

JOY REMPE, Member

WILLIAM J. SHACK, Member

NRC STAFF PRESENT:

GIRIJA S. SHUKLA, Designated Federal Official
JOE ASHCRAFT
TOM BERGMAN
JEFF CIOCCO
IAN JUNG
ERICK MARTINEZ
LYNN MROWCA
KHOI NGUYEN
DINESH TANEJA

ALSO PRESENT:

HIROSHI HAMAMOTO
KEVIN LYNN
RICHARD SAMPLES
KEN SCAROLA
RYAN SPRENGEL
MAKOTO TAKASHIMA

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

P-R-O-C-E-E-D-I-NG-S

(8:34 a.m.)

CHAIR STETKAR: The meeting will now come to order. This is a meeting of the United States Advanced Pressurized Water Reactor Subcommittee. I'm John Stetkar, Chairman of the Subcommittee meeting.

ACRS members in attendance are, Dennis Bley, Bill Shack, Charles Brown and Joy Rempe. Mr. Girija Shukla of the ACRS Staff is the designated federal official.

Subcommittee will discuss the US-APWR Design Certification Document and Comanche Peak Combined License Application Chapter 7, Instrumentation Controls and Sections 2.0 through 2.3 of the Combined License Application Chapter 2, Site Characteristics.

We will hear presentations from Mitsubishi Heavy Industries, Luminant Generation Company and the NRC Staff. Mr. Royce Beacom of the NRC staff has requested to make a brief presentation on the US-APWR Chapter 7. His presentation is scheduled today at 1:00 p.m. and it will be closed for external participants.

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

Rules for participation in today's meeting have been announced as part of this notice of this meeting previously published in the Federal Register. Parts of this meeting may need to be closed to the public to protect information proprietary to MHI or other parties.

I'm asking the NRC Staff and the Applicant to identify the need for closing the meeting before we enter into such discussions and to verify that only people with the required clearance and need to know are present.

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

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

The telephone bridge line has also been established for this meeting. To preclude interruption of the meeting the phone will be placed in a listen-in-mode during the presentations and Committee discussions.

Please silence your cell phones, anything else you have during the meeting. And we will now proceed and call upon Jeff Ciocco.

MR. CIOCCO: Yes, good morning everybody. My name is Jeff Ciocco, I'm the lead project manager for the US-APWR Design Certification.

We'd like to thank the ACRS Subcommittee for having us here today to present Chapter 7 on Instrumentation and Controls, as we progressed through the remaining chapters of the US-APWR Design Certification in our Phase 3 licensing review.

We do have technical staff here this morning, of the NRC Staff, available for any questions. And we'll do our introductions this afternoon before we begin the NRC presentation.

And we find it particular helpfully, John, as you have always done, is to recapitulate at the end of the session any specific action items or questions that you have so we can write them down and we certainly peruse the transcripts whenever they become available. So thank you very much.

CHAIR STETKAR: Great, thanks a lot, Jeff. And with that, well turn it over to MHI.

MR. SPRENGEL: I'm still over here.

CHAIR STETKAR: Ryan.

MR. SPRENGEL: This is Ryan Sprengel with MNES. Good morning again and I guess it's been about two weeks since we've seen each other, so glad to see you again.

We will be picking back up with our Subcommittee meetings on Chapter 7, as you're all aware. And one thing I'd like to point out, we have received previous questions and discussion topics throughout our Subcommittee meetings that we try to integrate those into our presentation. And so we do plan to cover those and then have any need of discussion on those specific topics.

CHAIR STETKAR: Great.

MR. SPRENGEL: So they'll be throughout the presentation. So now I'll go ahead and turn it over to Makoto Takashima.

MR. TAKASHIMA: My name is Makoto Takashima from MHI. I have a responsibility for the US-APWR I&C Design.

First I would direct a thank you very much to the vast opportunity to present our key design features of the US-APWR I&C Design. And the main presentation will be provided by Mr. Richard Samples.

MR. SAMPLES: Good morning.

CHAIR STETKAR: Before we start, let me

just alert you. Essentially all of the technical reports are proprietary information. So if the questioning gets into enough details where you feel that we are treading on proprietary information, just alert us.

I don't know how that will transpire. If we're kind of going in and out of public information quite bit, what I'd like to do is kind of hold all the proprietary discussion to a block of time. So I'll let you alert us to situations where we're getting to deep into the details, if you will, and we'll organize kind of closing the meeting for a block of time to discuss those.

MR. SAMPLES: Okay.

CHAIR STETKAR: Just wanted to alert you to that.

MR. SAMPLES: That's good. Well then good morning, my name Richard Samples. I'm a Instrumentation and Control Engineer with Mitsubishi. I'll be the main presenter today with Mr. Makoto Takashima, Mr. Ken Scarola and several Mitsubishi engineers supporting me.

This is the US-APWR Chapter 7 presentation for the advisory Committee for Reactor safeguards. Due to limited time I can't cover every detail that's in the draft safety evaluation so I'll cover the main points.

The safety evaluation does run over 300 pages. I'll cover the safety related, non-safety and diverse instrumentation and control systems of the US-APWR as well as their conforments to sense of safety criteria and covering opening items and will summary at the end.

Mitsubishi does have experts present today if you have questions. These are the topics I'll cover in the introduction.

In this figure you see how the various topical and technical reports are associated with the different chapters, different sections of DCD Chapter 7. These topical and technical reports refine key details that support the information in DCD Chapter 7.

CHAIR STETKAR: Richard, before you click off that slide, you'll find you haven't been here before so you don't get a chance to string together more then about 30 seconds of continuous thought without us interrupting you. Topical reports, it's only one topical report on this list, 7006, correct?

MR. SAMPLES: Yes.

CHAIR STETKAR: Are you going to reissue that topical report? You've changed the design of DAS and that topical report has outdated, incorrect design information.

MR. SAMPLES: I'll let Mr. Takashima answer that.

MEMBER BROWN: Can I, you say pink means it's outdated?

CHAIR STETKAR: No, pink is the only, that's the only topical report.

MEMBER BROWN: Oh --

CHAIR STETKAR: The other technical, technical --

MEMBER BROWN: I got it.

(Crosstalk)

CHAIR STETKAR: Technical reports I don't care about, topical reports I do. There's an SER and more importantly, the ACRS has written a letter endorsing that topical report.

MEMBER BROWN: I'm aware of that, okay. I just didn't --

CHAIR STETKAR: But it's my understanding that you've changed the DAS design from, to digital actuation to control cabinets, whatever you call DACs.

MEMBER BROWN: I guess.

CHAIR STETKAR: To four and change the coincidence logic. And that topical report report actually describes the old, it has information with the old design. Two cabinets and super coincidence logic. So that is now outdated.

MR. SCAROLA: We understand. This Ken Scarola. And I'm going to give you some background and then we'll basically explain where we're going.

When we had originally submitted all of these topical reports, they were all topical reports, okay. And they were intended to be applicable to both operating clients as well as the US-APWR.

But overtime it was recognized that that was going to be a difficult review process. So the subsequent topical report, the first one that got approved as topical report was 07006. The others we were able to changed the technical reports before hand.

So although 07006 is a topical report, whatever needed to be superceded in 07006 has been superceded by DCD information. So within Chapter 7.8 it supercedes, it references 07006, but it identifies where there are changes.

So at this point in time there is probably no need to --

CHAIR STETKAR: Okay.

MR. SCAROLA: -- update 07006 for the US-APWR, however, as Mitsubishi thinks about their strategy for operating plants, it may be appropriate to update it. But that decision has not been made.

CHAIR STETKAR: Okay, thanks.

MEMBER BROWN: Can I ask one question relative to that because in the existing, because I had to read a good bit of 06, the output of the DAS actually feeds over in the output section of the SLS into the I/O, the PIF, whatever you want to call it.

Is that combination of things different than what it was before? Although it only indicates only two channels --

CHAIR STETKAR: I'm sure we'll talk about DAS, more of the details.

MEMBER BROWN: No, I just wanted to --

CHAIR STETKAR: This is kind of administrative --

MEMBER BROWN: No, I understand that.

CHAIR STETKAR: -- legal thing that I wanted to get on the record.

MEMBER BROWN: I just wanted to know how much that fed over into the output of the SLS as it goes and feeds down to the ESFAS function?

MR. SCAROLA: The simple answer is it's all the same. We have slides, we'll show them later.

MEMBER BROWN: Okay, that's fine. Thank

you. Well let me ask one other question. I keep forgetting the nuance between topicals and technicals.

You referenced technical reports in the DCD as well as the one topical. To me that meant those also get brought under as part of the licensing basis when it gets approved.

So even though there's a nuance as to whether you get and SER on them or not or whether you do or don't, it's irrelevant relative to its applicability in terms of other design detail. Okay.

CHAIR STETKAR: Just for the record, everything that's referenced in the DCD is part of the basis. The only difference between topical and technical reports is, a topical report receives its own separate review by the staff and they write a Safety Evaluation so that in principle the information in a topical report can be used for other applications.

MEMBER BROWN: Without review.

CHAIR STETKAR: Without review, unless the staff, SER, restricts it to a particular application. Technical reports are strictly for this application and only this application. So it's a nuance but it's sort of the way the world works.

MEMBER BROWN: And how come the MELTAC technical report is not a topical report since it has multiple applications?

CHAIR STETKAR: Because there's a long history to this and MHI may want to speak to it. But it's my understanding, they decided it was more expedient for this particular licensing activity to not try to have that reviewed as a topical report. It originally was a topical report --

MR. SPRENGEL: Right.

CHAIR STETKAR: -- back --

MR. SPRENGEL: This is Ryan Sprengel, just a, it's not the potential use of it but it's the intended use. So right now we've accepted that the intended use is specifically for US-APWR and that's the kind of the genesis of the switch from topical to technical.

So we do agree that in general it could be applied broader, but for right now we're focusing that submittal and review for the reason stated. And that's why we switched it to a technical report.

MEMBER BROWN: Did that have some bearing on whether it was, what do you call it, a commercial-grade --

MR. SPRENGEL: Dedication.

MEMBER BROWN: --dedication process vice a formal acceptance of the qualification -

MR. SPRENGEL: No.

MEMBER BROWN: Did that play into this at all or?

MR. SPRENGEL: No.

MEMBER BROWN: I expected that answer.

MR. SPRENGEL: And if the staff want to contribute anything?

MEMBER BROWN: All right, I just was curious.

MR. SPRENGEL: Okay.

MEMBER BROWN: Thank you.

CHAIR STETKAR: You're starting, Richard, you're starting to get a flavor of this now.

MR. SAMPLES: Yes, I have to.

CHAIR STETKAR: Oh, the other thing is, if you haven't been here before, interpret silence as expediently go to the next slide.

MEMBER BROWN: If we want you to come back we'll tell you. Excuse me, unless you're a glutten.

MR. SAMPLES: Okay, the instrumentation and control systems of the US-APWR, they're the Protection and Safety and Monitoring System or PSMS, the Plant Control and Monitoring System or PCMS, the Diverse Actuation System or DAS, the main control board or as we'll refer to it at the later slides, the Human-System Interface or HSI and the data communication systems.

In this picture you see a picture of the main control room of the US-APWR. This picture actually comes from the US basic HSI simulator in Pittsburgh, Pennsylvania.

Now the point of view you have is the view of someone standing in the very back of the simulator.

MEMBER BLEY: We were up there several years ago.

MEMBER BROWN: It was 2009 or something like that.

MEMBER BLEY: Have there been any substantial changes in the way the displays are setup and the way it's organized?

MR. SCAROLA: No, there are not.

MR. SAMPLES: It's essentially the same now for all of this. But what you see in the front of the room is a large display panel. It shows different plant parameters and indications on a ref or representation of plant systems for easy comprehension of data.

Directly in front is the operator console where the Reactor Operator will sit. On the left side over here you have conventional switches. These are part, the large display panel is part of the PCMS, by the way.

The conventional switches here for system level actuation of safety systems are part of the PSMS. Over here on the right you have four VDUs, visual display units. VDUs are touch computer screens. There are four of these, one for each safety train.

In the middle you have different non-safety VDUs. Alarm VDUs, operational VDUs, procedural VDUs.

MEMBER SHACK: Are those four the only safety VDUs?

MR. SAMPLES: Yes. In the current design these four you see here, we have four, but there are also two other ones for, these basically do control. We'll take about this later in the slide, but there's four that do control and two you can monitor everything. But we'll go into that more later.

MEMBER REMPE: So commands are entered, as I think you said, with touch screens?

MR. SAMPLES: Yes.

MEMBER REMPE: I wasn't at your tour that you had previously, but is that how you can enter commands?

MR. SAMPLES: Yes, that's the normal way from the operational VDU here in the middle. It's a normal way the operator will control all the plant systems.

MEMBER REMPE: And are there a feedback that it says, is this what you really mean or how does it work?

MR. SAMPLES: Well you have to select the component. Say a valve you want to open or shut then you have a signal and then, I'm kind of getting past my information here --

MR. SCAROLA: There's a later slide where we actually show the pop-ups. I think it would be better --

MR. SAMPLES: Yes, we could probably explain it better --

MEMBER REMPE: Again, if I had been on the tour, this is for my time --

MEMBER BROWN: Yes, but my memory is --

MR. SCAROLA: But you're invited come anytime in the future if you'd like. We'd love to have --

MEMBER REMPE: Oh, I'd love another trip right now. I'll keep that in mind.

MEMBER BROWN: The main operator position is in the center?

MR. SAMPLES: Yes, it is. Right in the center.

MEMBER BROWN: And so he doesn't really

have to slide to the other side in order to perform any of his operational control functions?

MR. SAMPLES: For normal operations he can sit at one VDU and control everything in the plant.

MEMBER BROWN: Okay. When does he slide over to the other ones? Is that going to be answered at some point or does he have to or --

CHAIR STETKAR: This will come up.

MEMBER BROWN: All right. So you're prepared to attack on --

CHAIR STETKAR: This will --

MEMBER BROWN: Okay. All right, I'll --

CHAIR STETKAR: We'll either hear about this from MHI or the staff later.

MEMBER BROWN: Okay, all right.

MR. SAMPLES: We'll go into more depth about how each of these work later --

MEMBER BROWN: Okay, I was just trying to help Joy out here a little bit.

MR. SAMPLES: I think we've made it to the back of the room here. On the left side the shift technical advisors console, some more VDUs and the main control room supervisor on the right. These again are part of the PCMS.

Now over in the right, it's a little hard to see, that's the diverse HSI panel. That's were you would do manual initiation of the diverse actuation system components.

CHAIR STETKAR: Where's that, Richard, because I don't think they had that in the mockup when we were there?

MEMBER BLEY: Are you sure, I thought it was there.

MR. SCAROLA: Hey, John, when you were there we had a blank cabinet --

CHAIR STETKAR: That's right, you had a blank cabinet.

(Crosstalk)

CHAIR STETKAR: Okay.

MR. SAMPLES: Take a look at the --

MR. SCAROLA: We actual have a cabinet that had indicators and switches on it now.

MR. SAMPLES: It's kind of hidden in the right, it's kind of like --

MR. SCAROLA: We have to update our picture.

MR. SAMPLES: Behind the safety VDUs. So if you're not used to seeing it, it maybe kind of hard to see.

MEMBER BROWN: Now there's also a remote

shutdown room in addition to this, correct?

MR. SAMPLES: Yes.

MEMBER BROWN: Or is that's two different things? The DAS is in the main control room if I remember, with the other things you have to abandon ship --

MR. SAMPLES: The diverse HSI panel, yes, is in the main control room right over here. Here's overall architecture of the I&C systems. The general logic here is, on the top you have the HSI while controller is on the bottom.

Okay, starting with the protection and safety monitoring system on the left, this is a four-train redundant fully digital system that, for all safety related I&C. You can see we just talked about the previous slide, the conventional push-buttons.

Conventional switches, excuse me, the safety VDUs. Now you can also see the four trains, the Reactor Protection System.

Down here it's showing the engineered safety featured system, a safety logic system and behind me there are four other trains. You see one train of those down there.

Over on the right you have the plant control and monitoring system. It's a redundant fully digital system for all non-safety I&C.

The DAS is over here on the left. It's an analog system. It's hardwired for diverse and independent control.

You see the HSI system up here and the largest wave panel, the operator console, supervisor console, the Shift Technical Officer console.

Also shown on this picture are the data communications systems. First of all the multi-drop networks or the unit bus that connects all I&C.

Then you're showing one of four safety buses. Also a multi-drop network.

Throughout here, a little bit hard to see on this diagram, are point-to-point data links. And also if you look, these black dotted lines show hardwired connections directly, for instance, from direct protection straight to the reactor trip breakers.

MEMBER BROWN: One question that I couldn't get out of the DCD. The safety bus that's specified, that is contained totally within that division?

MR. SAMPLES: Yes, sir.

MEMBER BROWN: That doesn't have access, it only takes the internal for that division from its RPSA and feeds off to ESFAS functions and all, okay. So that's replicated --

MR. SAMPLES: One for each --

MEMBER BROWN: -- from one and so it's isolated, it has no other connections to the outside? There's no inter-divisional communications or anything like that on that safety bus?

MR. SAMPLES: Yes, sir.

MEMBER BROWN: Okay.

MR. SAMPLES: That is correct. Now the protection safety monitoring system is implemented using the Mitsubishi electric total vas control or MELTAC.

MELTAC is a fully digital distributed control system platform produced by Mitsubishi Electric Company.

Now we use MELTAC to implement, not only the controllers for the protection safety monitoring system, but also the HSI for the protection safety monitoring system, the controllers for the protection plant controller monitoring system.

We use Mitsubishi real-time computers for the various VDU computers. Such as alarm operational and operating procedure of the large display computer, alarm logic computer, the different ones you see here.

Also over here, just a little harder to see, for the technical support center we also have operation

VDUs and a large display and the computers that run them. So those are actually apart of the PCMS. And all of this here is also part of the PCMS or the HSI.

For the unit bus and the safety buses we have multi-divisional, multi-bidirectional communication. However, we do transmit one-way-only information from the unit bus through the unit management computer out to the station bus.

And I'll talk about that for a moment here. For data flow, again, it's one direction data flow to external networks.

So we give data to the station bus, the station provides information to plant corporate personnel to the emergency operating facility to the emergency response data system. Receives its information from the data communication systems via the unit management computer.

The unit management computer provides a firewall interface, allows only outbound communication. There's no other connections from those data communications systems of the control systems to any outside network.

MEMBER BROWN: Are you going to talk about that firewall now or later.

MR. SAMPLES: We have kind of a surprise

for you in the next slide.

MEMBER BROWN: Okay.

MR. SAMPLES: I think you'll like.

CHAIR STETKAR: Charlie likes surprises.

MR. SAMPLES: Let's take a picture of this and, well you're not going to see this in DCD Rev 3, we have done it yet, but we're going to add a hardware based unidirectional device to this system.

If you see the data communication system, unit management computer station bus, right there between the unit management computer and the station bus we're going to add this hardware device.

MEMBER BROWN: It's going to be on the output of the unit management computer as opposed to, I'm not arguing whether ones better then the other, I'm just saying it's on the output not the input from the unit --

MR. SAMPLES: Again, you see it right here, this big green box, the big red arrow, here's the current unit management computer, here's the station bus, we're putting it right in between. Now this device is not going to rely on any kind of software to ensure unidirectional data flow.

You have design concept, you know, kind of optical fiber with a transmitter on one side and a receiver on the other. And you can only transmit data one way through that optical fiber. So that's what we've used to ensure one-way data flow.

MEMBER BLEY: And that will make the next revision within DCD?

MR. SAMPLES: We're planing for DCD Rev 4.

MEMBER BLEY: Okay.

MR. SAMPLES: So again, this is not in yet we're adding this and we should have this to you by DCD Rev 4.

CHAIR STETKAR: Just out of curiosity, what's the schedule on Rev 4?

MR. SPRENGEL: It will be August.

CHAIR STETKAR: August, thanks. I forgot.

MEMBER BROWN: When you issue that, will there be some identification to the changes? I mean I know I'm going to want to look at it, but I don't want to try to have to read the whole thing, divine what has, word by word what's been changed.

I've seen a revision blocks in some of them, but they weren't real crisp in terms of what was changed. I'm not talking about the nits and lice, I'm only talking about the fundamental design features that change. For instance, this.

MR. SPRENGEL: The changes are identified.

And I guess to go, to give a little extra detail, in the actual DC revision that's submitted, it will just be a rev bar identification.

But separately with changes that are not submitted in kind of complete markups with RAI responses, we also submit tracking reports. And that includes a, like a red-line strike-out version. It gives a little more detail in terms of specifically what words are being removed and what are being added.

MEMBER BROWN: Yes, sometimes words make a difference.

MR. SPRENGEL: Agreed.

MEMBER BROWN: Even with the pictures.

MR. SPRENGEL: Usually they do. So there's a tracking report that will contain this and then there will also be the DC revision. But that will just have the rev bars indicating what portions are, what areas are changing but not the specific details.

MEMBER BROWN: And they're rev bars from Rev 2 to Rev 3 will have been canned by then, right?

MR. SPRENGEL: That's correct.

MEMBER BROWN: They will not be there, okay.

MR. SPRENGEL: That's correct.

MEMBER BLEY: So before you leave that, I see another one of those boxes with the big red arrow, is that another one-way hardware device?

MR. SPRENGEL: Yes.

MR. SAMPLES: Yes.

MEMBER BLEY: Okay. Good, thank you.

MEMBER BROWN: Yes, so let me make sure I, you bet me to the punch, Dennis thank you. So you're really kind of, the way I look at this is kind of a double-ended set of backstops.

The station bus is a plant station, I presume that's a generating station?

MR. SAMPLES: It is a plant IT network.

MEMBER BROWN: Okay. And the stuff that runs off the folks who are uncontrolled from an information technology standpoint, the corporate LAN, et cetera, will be further isolated, but yet the EOF and other stuff will have, just be fed right off the station bus?

MEMBER BLEY: Maybe uncontrolled is not the right word.

MEMBER BROWN: Not controlled --

MEMBER BLEY: Well in any case, all that stuff is isolated.

MEMBER BROWN: Yes, well my point being is it's the second red box. Downstream of that is where the internet gets connected in someplace.

MEMBER BLEY: Well no, even further then that.

MEMBER BROWN: I understand that you go to the corporate --

MEMBER BLEY: I just didn't want our record to say that's an open access box hooked to the internet.

MEMBER BROWN: You didn't like my phraseology, but that's okay.

MEMBER BLEY: I didn't like the concept. But go ahead, Charlie.

MEMBER BROWN: It's just that EOF and ER, what's the ERDS anyway? Emergency Response --

MR. SAMPLES: Emergency Response Data System.

MEMBER BROWN: -- Data System, okay.

MR. SAMPLES: Yes, sir.

MEMBER BROWN: Is that transferred to the NRC via the internet?

MR. SCAROLA: No.

MEMBER BROWN: Or is that via a dedicated --

MR. SCAROLA: It is typically a dedicated interface.

MEMBER BROWN: Dedicated, okay.

MR. SCAROLA: I misspoke.

MEMBER BROWN: Okay, I had know idea what those look like, but okay.

CHAIR STETKAR: Richard, the --

MR. SAMPLES: Yes, sir.

CHAIR STETKAR: The station bus, you characterized it as a plant system. And I know the EOF is shared among all four units, if I am correct? I'm looking over to Luminant, but I believe I read that the EOF was going to be shared among all four units.

Which means there will be communications, at least in the simple cartoon, on the station bus coming over from Units 1 and 2. Which in principle have the same practice, communicate with the outside world.

Are there protections, similar protections installed over on the Unit 1 and 2 side?

I know that the Unit 3 and 4 folks can't really control that in terms of the design and licensing of Units 3 and 4, but it's another potential communications pathway. Unless there's an actual break and you have a Unit 3, 4 station bus and a Unit 1, 2 station bus.

So do you have that level of information or is that something we should ask --

MR. SAMPLES: I don't think we have --

MR. SPRENGEL: I guess I would request that we delay that discussion.

CHAIR STETKAR: Okay.

MR. SPRENGEL: Until the COLA portion.

CHAIR STETKAR: Okay.

MR. SCAROLA: It's important to understand that the scope of the US-APWR DCD ends at that picture that you see right there.

CHAIR STETKAR: Understand.

MR. SCAROLA: So the responsibility is, we define the information that goes to the station bus.

CHAIR STETKAR: Understand.

MR. SCAROLA: The design of the EOF is a COLA item.

CHAIR STETKAR: Is a COLA, okay, thanks. We'll hold it till then. Don, be ready.

MR. SAMPLES: Okay, now we'll start discussing the safety related I&C systems, the protection and safety monitoring system. And these are the topics we will cover.

Now the PSMS consist of five digital subsystems. These are the reactor protection system or RPS, the engineered safety featured actuation system or ESFAs, the safety logic system or SLS, and the communication subsystem of the PSMS and also the safety related portion of the human-system interface system.

Now all safety, I&C safety functions of the US-APWR are implementing using either one or more of these subsystems. Here you see a figure that shows configuration of the reactor protection system.

You see first of all we have four different trains of reactor protection system. Within each train we have two different groups.

And we'll explain why we have those two different groups later. But first we'll just walk through and show you how signals are generated for protection actions in the RPS.

Starting with the sensor on the left, we sense a condition to the pressurizer pressure, high or low. Goes in through one of the groups, there's analog signals converted to digital, they send signal process.

Here in the middle we have a bistable that senses that we're exceeding a set point. If we do we get a signal. This signal is combined with signals from the other three trains over here, two-of-four logic.

This is one parameter of being monitoring, there's several others being monitored. So here and over here several others are being also combined together.

Then through digital output through the

hardwire connections straight down to the reactor trip breakers for a trip. That's the automatic path. Now --

MEMBER BROWN: Before you leave that definition I wanted to make sure I understood.

MR. SAMPLES: Yes.

MEMBER BROWN: Right in that CPU Group 1 Box.

MR. SAMPLES: This one?

MEMBER BROWN: There's two-out-of-four showing the stuff coming from the other trains and there's a little dotted line to the two-out-of-four, and the way I interpreted that there's, this is a redundant parallel, redundant controllers in the CPU, Group 1 and Group 2.

I mean you got the Group 1 and Group 2 stuff. Two different controllers, right?

MR. SCAROLA: But they're not redundant.

MEMBER BROWN: I understand they've got different parameters that they monitor.

MR. SCAROLA: They have different parameters.

MEMBER BROWN: Functionally they are redundant, I understand. You all refer, if you look at the MELTAC report it says, redundant parallel controllers configuration.

My understanding of that is the Group 1 one has, and you listed them in one of your tables, a series of protection or plant parameters that you monitor. All of those, that one sensor that you show coming in is represented by, there will be nine, for Group 1 there will be eight or nine other ones or whatever the right number is.

MR. SCAROLA: Yes, there's a couple of groups.

MEMBER BROWN: For Group 2 there will be another seven or eight, whatever that is, to repopulate the remaining of the parameters.

MR. SCAROLA: Different parameters.

MEMBER BROWN: Different parameters. And then that's replicate, that functionality is replicated in each other train?

MR. SCAROLA: Yes.

MR. SAMPLES: Correct.

MEMBER BROWN: Okay. So there's multiple, within each group there's multiple two-out-of-four of like functions in each of those. And that's to separate on a functional basis, the protection parameters. It gives you some functional diversity.

MR. SAMPLES: That's correct.

CHAIR STETKAR: Are you planning to discuss that in --

MR. SCAROLA: We have a later slide about --

CHAIR STETKAR: You do, okay, thanks.

MEMBER BROWN: And the thing to note is that out of either Group 1 or Group 2, you come down to that little circle with a flat bar on it, that's a Or gate. And so either one of those producing a trip, sends a trip down to the reactor trip breaker functionalities?

MR. SAMPLES: That is correct.

MEMBER BROWN: Okay. And that's replicated also? Okay, thank you.

MR. SAMPLES: They're also --

MEMBER BROWN: Just want to make sure I understood.

MR. SAMPLES: Yes, that's correct. I think you understand it. There's also a shunt here on the bottom, the system level conventional switch is on the far left side of the reactor operator console in the main control room where you can manually initiate with those conventional switches, trip the reactor breaker that way.

MEMBER BROWN: The detail of that was not shown. If I actually have it, do they actually, presume these breakers have undervoltage or shunt trip coils or both? I guess they have both?

MR. SAMPLES: Both.

MEMBER BROWN: Do they --

MR. SCAROLA: The detail --

MEMBER BROWN: -- note switches, pardon?

MR. SCAROLA: I'm sorry, the detail is actually in one of the technical reports. 07004, there's a figure that shows the detail of the interface to the shunt trip and the undercurrent.

MEMBER BROWN: Oh, I missed that. Okay, I apologize for that. Seven-hundred pages later I was starting to phase out.

MEMBER BLEY: Is that all you read?

MR. SCAROLA: Are you --

MEMBER BLEY: I had my eyes open that long.

MR. SCAROLA: And it's hardwired, it's completely hardwired.

MEMBER BROWN: Yes, that was my next question, my memory was that you all said it was and that's why I wanted to see if that functionality was stated. And it is in 04 so that's fine.

MR. SCAROLA: There's a figure that shows the details of that and how it's tested.

MEMBER BROWN: Okay, thank you.

CHAIR STETKAR: Are you, I haven't had a chance to study all of your slides because I was reading 702 pages.

MEMBER BROWN: He beats me every time.

CHAIR STETKAR: Are you going to talk, in any of your slides anymore about the so called conventional switches and the hardwired connections? Or is this an appropriate place to ask you about things?

MR. SCAROLA: Well this is the appropriate place to ask about the switches for reactor trip. Later we will talk about the switches for the engineered safety features actuation.

CHAIR STETKAR: I'll wait for that, thank you.

MR. SAMPLES: Yes, this showed you one way to manually trip the reactor breakers. The other way is through the safety VDUs on the right side of the operator console.

So there's actually soft switches on the safety VDUs. Push those, a signal will be transmitted through a safety VDU processor down on a safety bus. For instance, say Safety Bus A since we're talking about Train A, into the two different groups inside Train A.

Then you get reactor trip signal that way. Also, output down in through straight to the hardwire connection, to the reactor trip breakers.

But the reactor trip breakers themselves, these range from four different divisions such that you trip any two breakers you'll get a reactor trip. So basically, two of these different divisions give you a trip.

Okay, hold on. For some monitor variables --

MEMBER BROWN: Oh, one other question before you run off. I apologize.

MR. SAMPLES: Okay.

MEMBER BROWN: In your legend you talk about E/O, which are electrical to optical convertors.

MR. SAMPLES: Yes.

MEMBER BROWN: In your diagrams you frequently have the words, D/O, and that's not defined anywhere. And so I took it upon myself, someplace you didn't, a D/O was a digital output and I didn't know whether D/O was equal or was that with digital to optical or --

MR. SCAROLA: Digital output.

MEMBER BROWN: It's the same, okay. Have to just, small --

MR. SCAROLA: We'll fix that in Rev 4.

MEMBER BROWN: Okay.

MR. SAMPLES: Now for some parameters we measure if we exceed the set point. We don't just want a reactor trip, we may want it, we need to generate a signal to initiate the emergency safety features.

So the signal path through the sensor, through the analog to digital, through the bistable, through the combining of logic. We went right for the reactor trip, now we go left through the electrical optical output down through the engineering safety feature system. Now --

MEMBER BROWN: Before you shift, go back again. From your first picture of the overall, you show the diverse actuation system output for reactor trip functions going and tripping the M/G set.

But yet there is no connection via the diverse system, the automatic part of the diverse system, to tripping the reactor trip breakers. At least the way the dotted lines show that. Is that correct?

MR. SAMPLES: Correct.

MEMBER BROWN: So you use a different functionality for, and instead of doing both you just do one?

MR. SCAROLA: Correct.

MEMBER BROWN: Is there some thought process of why you do just one of them vice sending the signals off to the screen breakers as well?

MR. SCAROLA: 10 CFR 50.62 says, the reactor trip must be completely diverse. Including the hardware, not just the software.

MEMBER BROWN: Well there's no software in the DAS.

MR. SCAROLA: Right. But the hardware can't be the same, so we can't use the reactor trip breakers. We have to have a diverse mechanism for tripping. Completely diverse. So that's why we use the M/G sets.

MR. SAMPLES: So we trip, the motor generate sets that feed director trip breakers.

MEMBER BROWN: Well the director trip breakers are not exactly software. No, but, so.

MR. SCAROLA: So that's my point. Is that in the old rule for ATWS, there was no distinction between hardware and software. It just requires complete diversity. Including all the hardware.

There are some exceptions. That the ATWS rule allows us to use the same sensors, the same power supplies. But all the active devices must be completely diverse.

So we don't use the breakers for the backup for the DAS. We use the M/G set tripping. It's completely diverse.

MEMBER BROWN: Does that meet your analysis requirement, only M/G sets require that they take, the electromagnetic fields require sometimes to collapse and all that type of stuff.

MR. SCAROLA: We trip the outputs, not the motor side.

MEMBER BROWN: Not the motor side, okay.

MR. SCAROLA: We trip the generator side.

MEMBER BROWN: All right, I just wanted to understand your thought process.

MR. SAMPLES: So we have the signal for the engineered safety features leaving the reactor protection system, going into ESFAS and the SLS. So basically we saw, down here we see four trains to the RPS.

And it's also, we're showing only one train, ESFAS and SLS here. There are four of them, there's four different ones.

So the automatic signal, again, it comes from the reactor protection system, goes into ESF Actuation System. Inside the ESF there's two different subsystems. The ESF Subsystem 1 and 2.

These are identical modules all work the same way, work in parallel. If either one detects a condition where you need to actuate engineered safety features, it will transmit it to safety logic system which is on component level actuation of pumps, valves, different components of the plant.

Again, there is two different subsystems inside SLS. Now what happens is, inside ESFAS, Subsystem 1 will send itself a signal to Subsystem 1 inside the SLS. Subsystem 2 to Subsystem 2. They operate in parallel.

Then the signals are combined at the bottom and then sent to the component that needs to be actuated.

MEMBER BROWN: But only then require a coincidence of the two subsystems in the SLS. All your coincidence is done up in the CPU subsystems of the ESFAS, ESF functionality, similar functionality that you have in the reactor protection system?

MR. SAMPLES: It's just voting logic inside the systems and then down here it's combined --

MEMBER BROWN: Yes, the SLS is a hard combination of logic. Is it FPGAs or is it, it's not microprocessor based?

MR. SCAROLA: No, it is microprocessor based.

MEMBER BROWN: Oh it is? The SLS part is?

MR. SCAROLA: It's the same MELTAC --

MEMBER BROWN: Oh, yes, I'm sorry. I see that, too late.

MR. SCAROLA: The part that is hardwired, and we'll talk about later, is the final output in the PIF module. We'll talk about that later.

MEMBER BROWN: All right, thank you.

MR. SCAROLA: There very bottom here, that's hardwired.

MR. SAMPLES: Okay, that's the automatic signal for ESFAS.

MEMBER BROWN: Before you leave, what's a Group 2, 3, out to N? You show these multiple groups but they're all still on the same safety bus.

MR. SAMPLES: Different groups and safety logic system grouped together to control different components. Also discuss that a little bit later.

MEMBER BROWN: Okay.

MR. SCAROLA: There might be up to 200 components in a safety train.

MEMBER BROWN: I understand that.

MR. SCAROLA: Maybe even 300. I don't even know what the exact number is, so we --

MEMBER BROWN: Okay so what that is, is --

MR. SCAROLA: -- distribute them.

MEMBER BROWN: Okay. So you don't use the output of priority of logic to do that, you've got to distribute it amongst the other functions to ensure that you have, I don't know, to ensure I guess, just to pick up the power.

MR. SCAROLA: Well there are two constraints. There is a response-time constraint, so we want to make sure that one controller group pair is not overloaded and running in excessive response-time because we have to trip these things in 300 milliseconds, or get them actuated in 300 milliseconds.

And then you have the issue of functional distribution to make sure that if one group were to spuriously actuate, we wouldn't get an unusual event in the plant that's not bounded by the safety analysis.

MEMBER BROWN: All right.

MR. SCAROLA: So we distribute for two reasons. The performance reason and safety reason.

MEMBER BROWN: Okay, thank you.

CHAIR STETKAR: You said you're going to talk a little bit more about that distribution later or?

MR. SCAROLA: Not that, we don't have any more slides on that distribution. What I pointed out before was the RPFs distribution.

CHAIR STETKAR: Okay, let me ask you then a question I had about the distribution. I don't want to go into individual components, but there is a section of the DCD, I don't remember whether it's a DCD or technical report, it doesn't make any difference, that talks about, a bit about the distribution in particular to prevent spurious actuation.

And I'll use one particular function as an example. There's a list of, I don't know, seven or eight different functions that are addressed. One function, for example, main steam insolation.

As I understand it, and I might be wrong, the main steam isolation valves receive signals to close from SLS Trains A and D.

MR. SAMPLES: Correct.

CHAIR STETKAR: And the description in the DCD, there's a little cartoon, if you will, shows that external to what we can see here, you require a signal from both SLS A and SLS D to close the MSIVs?

MR. SAMPLES: No.

MR. SCAROLA: No, either one.

CHAIR STETKAR: Okay.

MR. SCAROLA: Either A or D.

CHAIR STETKAR: That's what I was curios about. Because I looked at, there's a little logic drawing in the DCD, it might be in the technical report of the DCD that shows A and D out to the MSIVs.

MR. SCAROLA: Right.

CHAIR STETKAR: And I was given the impression that that and logic was somehow out, was out in the plant.

MR. SCAROLA: The A and D trains are completely independent --

CHAIR STETKAR: Yes.

MR. SCAROLA: -- from both an I&C signal path right to the different solenoids. There are two sets of solenoids on those valves.

CHAIR STETKAR: Yes.

MR. SCAROLA: A solenoids and D solenoids. So everything is completely independent and the actuation of either the A solenoids or the Ds will result in MSIV closure.

CHAIR STETKAR: That's what I wanted to hear.

MR. SCAROLA: Correct.

CHAIR STETKAR: Okay.

MR. SCAROLA: Now --

CHAIR STETKAR: Now how, if that's the case, what is all this stuff about preventing spurious actuation from a signal from A or D?

MR. SCAROLA: You can't prevent spurious

actuation.

CHAIR STETKAR: Okay.

MR. SCAROLA: What you can do is accommodate spurious actuation. So one of our design basis is we don't want any signal failure to trip the plant.

CHAIR STETKAR: Right.

MR. SCAROLA: Now since A or D can shut those valves, you could say, well then if you have an A spurious failure, you can get a plant trip. So what we do to prevent that, the MSIVs are actually controlled from two groups in this picture that you see here. And the coincidence of both groups has to happen before the A train to close those valves.

CHAIR STETKAR: Okay.

MR. SCAROLA: And then A signal has a two out of two coincidence from both groups.

CHAIR STETKAR: Oh, okay. Okay, I got it. Thank you.

MR. SCAROLA: That's how we deal with preventing spurious plant trip. It's not a safety issue, has nothing to do with safety --

CHAIR STETKAR: No, no, your right. I was just trying to get straight in my mind about this prevention of single failures and how it was actually implemented out to the valve.

MR. SCAROLA: There's a whole technical report entitled SLS Functional Assignments that gets into all the philosophy behind the distribution of the groups. And the few components, like MSIVs, that we actually control from two groups.

CHAIR STETKAR: I didn't read the whole --

MR. SCAROLA: If there's a bunch of, there's a handful of components that we do to double control.

CHAIR STETKAR: We have it, it's MUAP-09020.

MR. SCAROLA: Correct.

CHAIR STETKAR: I read part of it, I didn't read every word. Thank you.

MEMBER BLEY: Ah, yes, okay.

MR. SAMPLES: Well we just talked about how we generate automatic signals for engineered safety features actuation. Several different ways to manually initiate ESFAS.

First of all, from the system of a conventional switches on the operator console from the main control room. The ones on the left side, there's a switch hardwired directly to the DSF systems. Push the switch you initiate and then the signal through there is the same as fully automatic.

MEMBER BROWN: Does the switch go to both subsystems within that train?

MR. SCAROLA: Yes.

MR. SAMPLES: Yes.

MEMBER BROWN: Logically it should, I just was making you read up to that push. One switch, okay.

MR. SAMPLES: One switch.

MR. SCAROLA: There are two contacts on one switch.

MEMBER BROWN: Okay.

MR. SAMPLES: Now the second way is from down the safety VDUs in the main control room. And say we push a soft switch on the safety VDUs, it will go through a safe VDU processors down to the safety bus and to the ESFS subsystems and then actuate a signal that way.

Okay. Now the third way is from the operation VDUs in the middle of director console. Go through, push a soft switch again, go through VDU computer on to the unit bus and then down through the communication subsystem of the PSMS, onto the safety bus and then from there it's the same as it was from the safety VDU to the ESFS subsystems down to the SLS to the components.

You could also initiate ESFS from the remote shutdown console. Again, through safety VDUs, processor down through safety bus onto ESFS subsystems.

MR. SCAROLA: I want to point out, before you asked about sliding, you know the operator sliding his chair left and right, this is the first place where we show that the non-safety operational VDUs have the ability to control all the safety components in the plant. So there is no requirement for any kind of chair-sliding at all.

And well hit this again in several places in the presentation. This is the first one where we show it.

MEMBER BROWN: You also show the remote shutdown console, a line going over. Which way does that line go from the operational VDUs?

MR. SAMPLES: Well the signal starts from the remote shutdown --

MEMBER BROWN: So there's two paths. If you operate something from the remote shutdown, it will try two things. One going back to the operational VDU, that's what the impression is, as well as going to the safety VDU processors.

MR. SCAROLA: The figure is not perfectly clear. Those words remote shutdown console, are intended to simply represent the same thing that's in the main control room.

So at the remote shutdown room, we have safety VDUs and we have non-safety operational VDUs. So it's the same signal paths from separate VDUS.

So that picture is trying to depict that there are safety VDUs in the main control room and also at the remote shutdown room. We have operational VDUs in the main control room and also in the remote shutdown room. I know the picture is not perfect.

MEMBER BROWN: You ought to delete the line. They mean different things. I was totally confused on that. Go ahead.

MR. SAMPLES: Essentially, just to reiterate what Ken just said, the remote shutdown room, safety VDU, you can go through the same path we did from the safety VDU in the main control room. And also there's operational VDUs to go through the same path you did through operational VDUs in the main control room to initiate engineering safety features.

CHAIR STETKAR: I was writing and I can't write and listen at the same time. Did you talk about the conventual switches?

MR. SAMPLES: Yes, I did.

CHAIR STETKAR: You did, okay. Like I just said, I can't listen and write at the same time. I had a question, why in the reactor trip logic you pay a lot of attention to making sure that those conventional switches go directly to the reactor trip breakers that they're hardwired to the endstate.

In ESFAS, they only bypass the reactor trip logic. Those signals are still processed through a heck of a lot of software before they finally get to starting an EFW pump, for example. Why is that? I mean there must be a reason.

MR. SCAROLA: Right. They are several reasons. The simplest one to understand is reactor trip.

The switch has to go to two breakers. Engineered safety feature, the signal for the A train has to go maybe 50 components for safety injection. Another 30 components for containment isolation. So there is a much broader distribution of those signals.

The second reason is, all of those components have interlocks in the SLS for things like equipment protection. So all those interlocks still remain active. You don't want to bypass all those component-level interlocking.

MEMBER BROWN: Also meaning that it's a sequence here.

MR. SCAROLA: In sequence. The last reason is, when you initiate safety injection, since there are some many components, including HVAC things that have to align, chillers, ventilating, there's a lot of stuff, things have to be sequenced. They can't just go.

And all the sequencing logic is in the ESFAS boxes that you see there. So there's a lot of different reasons why we can't just go right to the final components.

CHAIR STETKAR: Good answer.

MEMBER BROWN: But, okay, I understand your point, but except if I look at the diverse actuation system it shows going right into the priority logic in the I/O as opposed to up into all the sequencing logic.

So at some point people are just actuating stuff based on their knowledge of when things ought to be sequenced. Is that, that's the presumption I would, or the assumption that I would make.

And I'm not disagreeing with, I'm just saying that's there's a nuance on your comment relative to why the other things are done, that at some point you've got to have human intervention, via the DAS, and there you're using the priority logic directly and therefore the mind, people have to determine what goes on and when.

MR. SCAROLA: But the DAS actuates a fraction of the components.

MEMBER BROWN: I understand that, but it's just a difference. I'm not disagreeing with it.

MR. SCAROLA: It's kind of a significant difference because then it doesn't require sequencing and we just don't have some much signal distribution.

MEMBER BROWN: Okay, I got it. It's just a difference relative to the discussion.

MR. SCAROLA: It's clearly a difference. Realize the purpose of manual actuation. This thing that bypasses the RPS. It's really not intended to be a backup function. Because we have four trains.

The purpose of manual actuation is to give the operators the ability to take preemptive action so that they can initiate the same functions that would have been initiated by the reactor protection system. We really do not take credit for it as any kind of a backup.

DAS is backup. DAS is clearly a backup. This is really, and it's not intended by IEEE-603 to be a backup either. It's a preemptive initiation.

MEMBER SHACK: Just on this operational VDU, I thought there was a one way communication from the safety systems to the non-safety systems? But somehow now I've got a two-way communication going on.

MR. SCAROLA: Well spend a lot of time talking about that. There is definitely two-way communication, we'll explain how we maintain communication independence and the benefits of that two-way communication.

MEMBER BROWN: It's also why that data diode is important from the external sources.

CHAIR STETKAR: Ken, you're a great straight man. In passing, when I'm listening I actually pick up on words. You mentioned that one of the reasons that you need to inject the manual signals where you do is that the SLS contains all the equipment protective signals.

MR. SCAROLA: Not all, some. Some, not all.

CHAIR STETKAR: Okay. I'll use the word some then, you didn't use the word all you said, whatever. The question I had, and I don't know how these things work, is suppose that I have a motor overload or a torque switch or thermal overload device or something like that.

Do those protective signals block everything coming out of the SLS? In other words, do the equipment protection signals override the output of the PIF?

MR. SCAROLA: In general, yes.

CHAIR STETKAR: Okay.

MR. SCAROLA: For example, on a motor-operated valve, torque switches stop the valve regardless of any demand from the SLS. Those are outside the SLS. It varies depending upon the protective interlock as to how significant that interlock is.

For example, we bypass thermal overloads on motors by the engineered, when you have an accident signal, the thermal overloads are bypassed.

CHAIR STETKAR: So there's a smart logic in the SLS that looks at particulate protective --

MR. SCAROLA: Well some functions are in the SLS and some functions are actually in the motor control centers.

CHAIR STETKAR: Yes.

MR. SCAROLA: For example, torque switches on motor-operated valves are in the motor control, not in the SLS.

CHAIR STETKAR: Well often thermal overloads are also. That's why I was asking.

MR. SCAROLA: Indeed they are. But

because they need to be bypassed, you feed them back up after they get feed back.

CHAIR STETKAR: Okay.

MR. SCAROLA: It depends on the protective type.

CHAIR STETKAR: Okay.

MR. SCAROLA: For example, in switchgear, there's a lot of fault protection in the switchgear. Phase imbalances, overload faults, those are all still in the switchgear.

CHAIR STETKAR: Yes.

MR. SCAROLA: Because --

CHAIR STETKAR: But for example, on a pump, I don't know how the pumps are protected, but some sophisticated pumps have high winding temperature or high lube oil temperature or bearing vibration or you name it.

MR. SCAROLA: Those things are typically brought back into the SLS. Because we say, well even though we have a high winding, we're going to run that pump.

CHAIR STETKAR: Yes, okay.

MR. SCAROLA: A high winding temperature or a high thermal overload. Things that you know that the equipment can't run if that happens.

CHAIR STETKAR: I didn't look, is there something anywhere that describes which of things are bypassed and which are, remain enabled? I didn't particularly go look for it, so.

MR. SCAROLA: There is an MHI documentation. There's something we call a Component Control Design Guide that identifies.

MR. TAKASHIMA: There's a discussion in Chapter 8.

MR. SCAROLA: In Chapter 8?

MR. TAKASHIMA: In Chapter 8.

MR. SCAROLA: Okay. I'm not sure.

CHAIR STETKAR: I read Chapter 8.

MR. SCAROLA: I think the detail you're looking for may not be in Chapter 8.

CHAIR STETKAR: No, it's not.

MR. SCAROLA: But no, it is --

CHAIR STETKAR: Chapter 8 does give you the protection signals, for example, for circuit breakers and things. But it doesn't give this level of detail in terms of which ones are bypassed on, which actuation signals.

MR. SCAROLA: Correct.

CHAIR STETKAR: I mean it will tell you phase differential over current, you know, all of that kind of stuff for the electrical protection, but not what I'm asking about. Okay, thanks.

MR. SAMPLES: Now the PSMS interfaces with safety sensors and safety actuators, such as valves and pumps, PSMS interfaces with non-safety I&C systems. First of all, the non-safety portion of the human system interface system, reactor control system, turbine protection system, the balance of plant control system and the diverse actuation system.

These interfaces from the PSMS to the non-safety systems, they don't negatively impact the safety functions of the PSMS do to the PSMS independence. And as we progress through this presentation, we'll talk about how these interfaces enhance the safety function.

MEMBER BLEY: This isn't really a safety issue, but the discussion you and John just had leaves me wondering what are the folks in the plant going to have? Will they have logic diagrams in detail on all of this stuff so that they can troubleshoot and figure out where the heck these signals are tied up?

MR. SCAROLA: They'll have both logic diagrams as well as electrical wiring diagrams. As I said, some functions are in logic, some functions are in motor control centers so they will actually have both.

MEMBER BLEY: Okay. And those will be of the kind we've seen before?

MR. SCAROLA: The electrical part.

MEMBER BLEY: Yes.

MR. SCAROLA: Oh, yes, even the logic part. Yes.

MEMBER BLEY: Okay.

MR. SCAROLA: Because you've seen logical --

MEMBER BLEY: Two of their logic diagrams, but, yes.

MR. SCAROLA: In fact later we will show you a picture of software base logic that they can actually see on the screen.

MEMBER BLEY: Okay.

MR. SCAROLA: That's coming up later.

MR. SAMPLES: There are only two types of inter-divisional. Inter-divisional, between division, data communication, interface methods apply to the PSMS. There's point to point datalink and a multi-drop network.

With point to point datalink, the interface between the, communicate information between the different RPS trains for partial trip, between the RPS and the ESFAS for partial ESF actuation and between the multi-divisional safety VDU trains. We'll discuss those in a moment for monitoring information.

The multi-drop networks communicate between the PSMS and non-safety systems, via the unit bus, for both monitoring control information to non-safety and for manual control commands from the operational VDUs.

The PSMS safety function is assured by functional and communication indecence such that the failure of one PSMS division doesn't negatively impact other functions of the other PSMS divisions. And the failure of a non-safety system does not negatively impact the functions of any PSMS division.

Now normal shutdown can be achieved and maintained using the operation controls from either the main control room or the remote shutdown room. Safe shutdown, both hot and cold, can be achieved and maintained using only the PSMS from either the main control room or the remote shutdown room.

Safety VDUs or operational VDUs can be used with the PSMS to achieve safe shutdown from either main control room or remote shutdown room. There are master transfer switches for transferring control from the main control room to the remote shutdown.

One for each PSMS train and one for the PCMS.

They're in two different locations. One location is just, it's on the pathway between the main control room and the remote shutdown room. And the other one is inside the remote shutdown room.

You need two-of-two actuations to transfer control. If you want to transfer to control, for instance, from PSMS Train A from the main control room to the remote shutdown room, you have to push that corresponding switch both, at both locations before you transfer.

Pushing only one will not do it. So you have to push all ten of those switches to transfer control.

And we'll talk about the safety visual display unit, the VDU. Again, this is a computer touch screen. It is an alphanumerical display because it has the graphical display.

It's kept very simple to meet Class 1E quality assurance requirements. Especially the software quality assurance requirements for --

CHAIR STETKAR: I'll ask now, you hesitated. Don't ever make eye contact.

MEMBER BLEY: First mistake.

CHAIR STETKAR: You mentioned a couple of times using a touch screen controls.

MR. SAMPLES: Yes, sir.

CHAIR STETKAR: Are they only touch screen controls or you have mice? The reason I'm going to ask about this rather then, because of time, just recently somewhere I read about a problem that had occurred because someone was using touch screen controls and indeed the controls for adjacent components were really close on the touch screen.

And I have fat fingers, and basically somebody operated the wrong equipment and it was traced back to the fact because of the proximity on the touch screen of those components were so close, that it was really, really difficult to distinguish between them. And they're solution was, well oh gee, that's right, we'll install mice because they give you a much more precise click and select.

MR. SAMPLES: We don't have, we don't use a mouse, it's just touch screen.

CHAIR STETKAR: It's only touch screen.

MR. SAMPLES: I think Mr. Scarola can explain better.

MR. SCAROLA: Someday we'll have an opportunity to come in here and talk to you about Chapter 18, where we will address all the human factors designs of touch screen.

CHAIR STETKAR: I knew you were going to say that. I just wanted to ask.

MR. SCAROLA: And I'm saying someday. I mean I hope I'm still here. But 0700, no, there is a NUREG-0700 that has very strong requirements for things like touch screen separation and, so we'll talk about that in Chapter 18. I was being facetious, that's mean, but.

CHAIR STETKAR: Okay.

MEMBER BLEY: Well this is a diversion, but all the touch screens I've played with, depending on moisture and that sort of thing, sometimes they work great, sometimes they don't recognize you're touching. Is there something in these designs that gets around that problem?

MR. SCAROLA: Well there are many different types of touch screen technology. We use what's called surface acoustic wave technology. And its been extremely reliable.

MEMBER BLEY: Okay.

MR. SCAROLA: We haven't had any issues.

MEMBER BLEY: I mean we were only up there one day, it looked that way, but.

MR. SCAROLA: Yes.

MEMBER BLEY: I wondered if on a dry day

or something like that you run into trouble?

MR. SCAROLA: Very honestly I was, when I first got involved with this program I was skeptical about the touch screens. But we've had 13 operating crews, senior reactor operators and the reactor operators through our US basic HSI test facility, the one that you saw, and they loved the touch screens.

MEMBER BLEY: Okay.

MR. SCAROLA: So that made me a believer.

MEMBER BROWN: That's because they're paying with their smart phones all the time.

MR. SCAROLA: Well this was actually a few years ago before smart phones were --

MEMBER BROWN: No, I'm just going to make one observation. The program I was in before, we looked extensively at touch screens and we avoided them like the plague because they had so many problems.

And we ended up with stationary screens and put a whole level of little pushbuttons down below where you had touch, you had tactical feel for the buttons as well. Even if you had soft keys where you could use them multiple times.

MEMBER BLEY: What year was that?

MEMBER BROWN: It was a couple years ago. I mean you seen how much, it was like ten years.

MEMBER BLEY: But very frankly, ten years ago --

(Crosstalk)

MR. SCAROLA: One of the problems with screens years ago is screens had curvatures to them. So it was very difficult to make touch screens function because the actual glass of the screen curved. But now with flat screens, it's just much more reliable.

MEMBER REMPE: We can come back and confirm and so you have to double indicate, is what you told me earlier, is it really faster if you're in the middle of something? I mean you said you'll take about human-factors later, but is it just expedient as switches?

MR. SCAROLA: Yes, it's very expedient. It's what we call soft covers on switches. Where it's kind of like lifting up a hinge cover on a button, we have soft covers on our switches. So you hit something, it removes the soft cover and then you take the action necessary.

CHAIR STETKAR: There are a lot of designs in Europe, even hardware based, where you have a confirm switch. And once the operators get use to using it, it's no more then, you need two hands instead of one.

MR. SCAROLA: Well this is not two-hand

operation. But, no, we'll show you a picture later. I think it will help.

MEMBER REMPE: Okay.

MR. SAMPLES: Now these safety VDUs consist of both the safety VDU processor and a safe VDU panel. There's two different kinds of safety VDUs.

Single additional safety VDUs that we saw in the main control room, the four-train redundant. Each one of these controls and monitors all the safety related functions of a safety train.

Or safety Train A, the lead safety train. VDU for safety Train A controls all the equipment in Train A. The VDU for Train B, all the safety functions in Train B and so forth.

We also have multi-divisional safety VDUs, which we didn't show in that picture. These are two-train redundant, two different ones.

These do not have any control capability, but each one can monitor all of the information, all the parameter from all four of the safety trains at one time. So each can monitor all for the multi-divisional safety VDUs.

The type two VDUs consist, are implemented by the same digital platform as the PSMS. That's the MELTAC platform. And they set aside all safety criteria and the requirements.

Interlocks important to safety. The interlocks are implemented in the PSMS. These are the ones credited for DCD Chapter 15 to prevent accidents and help to ensure the availability of the safety systems. You see a list here of all the various interlocks important to safety for the US-APWR.

CHAIR STETKAR: Now that third one from the bottom doesn't exists anymore, is that correct?

MR. SAMPLES: Component --

CHAIR STETKAR: CCW supply line isolation. Interim Revision DCD Rev 4, at least in Chapter 9 eliminated that.

MR. SAMPLES: Mr. Hamamoto?

MR. HAMAMOTO: This is Hiroshi Hamamoto. I believe this interlock is Rev 4. We don't change that part, somebody else return line. I believe this exists in --

CHAIR STETKAR: Okay, that's a disconnect between the information we got when we review Chapter 9. So this is in particular, the interlocks on MOV-020 A, B, C, D and 007 A, B, C ,D.

And we were told that that interlock was going to be removed because we had questions about how it was working. It's important because it supplies cooling water to the reactor cooling pumps.

So if the Chapter 7 folks think the interlock is still there and the Chapter 9 folks think it's not there, somebody has to get the story straight.

I'm just going to make that observation, because we have it on the record that it was changed, that it was removed in, at least interim Revision 4 of the DCD. Now if it's back in place --

MR. LYNN: This is Kevin Lynn. I recall the thing that you're asking about, but the isolation interlock that you are talking about is actually a different one that was removed. This is one that was not changed.

If you look at DCD Chapter 7, you can see the section that talked about the interlock. Removing the interlock that you're thinking of that was removed, that's shown in redline strikeout, but then that same section is then where this other interlock was discussed and you can see the valve numbers that you're talking about were taken out.

But this is referring to different valve numbers. I don't have them in front of me right now, but you can see it in Chapter 7.

MEMBER BLEY: Different valves in the same system?

MR. LYNN: Yes.

CHAIR STETKAR: Well take a look at that because when I read Chapter 7 they were the same valve numbers. I referred back to Chapter 9, so.

MR. SCAROLA: Okay, we'll look at that.

CHAIR STETKAR: I'm not sure which interlocks we're talking about now, but they seem to talk about the same valve numbers. Anyway, go on.

MR. SCAROLA: Okay, I don't know if this helps, but this section --

MR. HAMAMOTO: We will check it after the break.

CHAIR STETKAR: Check it after the break, we'll never finish.

MR. LYNN: This is Kevin Lynn again, I just want to clarify. So you're asking about the interlock that was for Valve 7 and 20?

CHAIR STETKAR: That's correct.

MR. LYNN: That has been deleted.

CHAIR STETKAR: And that's --

MR. LYNN: The interlock that is showing on that screen is for Valves 57 and 58.

CHAIR STETKAR: Somebody ought to change --

MR. LYNN: They're different valves.

CHAIR STETKAR: I found Valve Number 7 and 20 in the DCD.

MR. SCAROLA: According to Chapter 7, we use to have interlocks on both the supply line and the return line. Now we only have interlocks on the supply line. The return line interlocks have been deleted from Chapter 7.

CHAIR STETKAR: Let's leave this for the break, I'll look up the section that I referred to and see what numbers are listed there and so we can keep going here.

MEMBER BROWN: Ken, before you go on, I meant to ask a question back about five slides ago, but this is an easy answer. All the intra-divisional communication for train-to-train voting, those are dedicated communications, know of those go up to the unit bus or require --

MR. SCAROLA: Yes, point to point data link --

MEMBER BROWN: I saw the point to point, I just wanted to make sure it covered that plethora of items for both the ESFAS as well as RTS. Thank you.

MR. SAMPLES: Now for the information --

CHAIR STETKAR: I'll refer you to DCD Section 7.6.1.5 where they explicitly list Valve 7 and

20. I'm done.

MR. LYNN: This is Kevin Lynn again. You're looking at DCD Revision 3, right?

MR. SCAROLA: That's correct.

CHAIR STETKAR: It's the only I have.

MR. LYNN: In the change from the Chapter 9 RAI it included a markup to that section which eliminated the Valve 7 and 20.

CHAIR STETKAR: Okay.

MR. LYNN: So in the DCD Revision 4 it will look different then what you're looking at.

CHAIR STETKAR: Thank you. I'm sorry I just get, when things are changing, one of the things that we do by the way, one of the functions the ACRS has is to try to make sure that bits and pieces tie together because we only see individual chapters at a time.

But we're also responsible for overall safety review for the entire integrated design. So that's one of the reasons why we try to pick up on these things, if they are discrepancies.

MR. SAMPLES: Okay.

CHAIR STETKAR: That sort of explains a little bit about why I brought that up. Thank you.

MR. SAMPLES: Makes perfect sense. So

I'll move on to discussing the information systems importance to safety. Specifically the post-accident monitoring system.

Post-accident monitoring system monitors all five types of PAM variables from Type A through Type E. With the Type A parameters, excuse me, the Type A and B parameters, these have spatially dedicated and continuously visible displays above safety VDUs and the large display panel.

Types A, B and C parameters have Class 1E power. They're processed by the PSMS and they are displayed on the safety VDUS.

The performance of the PAM variables such as range, accuracy, response time, required duration, reliability, these have been selected in accordance with IEEE-497.

You see there is an open time related to this. Related to the selection basis for PAM variables to demonstrate complete accident coverage. We're preparing a response to that.

CHAIR STETKAR: Curiosity been submitted. Are you going to talk anymore about PAM variables or is this the time to ask about PAM?

MR. SCAROLA: This is the time.

CHAIR STETKAR: Okay. This is more of a

curiosity but sort of a, may I ask about a few things? Were never going to finish on time so I'm giving up on that.

Reactor vessel water level, I found a couple of different reference points for that. One place it said it's from the bottom of the hot leg to the top of vessel. The other place it said it's from the top of the fuel alignment plate, which I'm assuming is the top of the upper core plate.

There's a substantial difference between those two elevations. It would seem to make sense that it's the top of the core plate.

MR. SCAROLA: Where are you seeing this information? I don't think --

CHAIR STETKAR: DCD 7.5.1.1.3.2 says it's from the top of the fuel alignment plate. Table 7.5-3 says it's from the bottom of the hot leg. So I'm just curious where it came from. You may want to check that?

MR. SCAROLA: Okay. It sounds like we need to take the action. We'll move on.

CHAIR STETKAR: Here's a, I understand the, I know about the open item, about selection of the variables. One of the things in the DCD is it discusses that the PAM variables are displayed on both the safety VDUs and the operational VDUs.

The operational VDUs, the way it's cast is, it says that recoding and trending are available on PCMS. And only the actual value displays are available on the safety VDUs.

Why didn't you provide the trending capability over on the safety VDU side? The reason I'm interested is the PCMS is non-safety related.

In a complete Station Blackout, after an hour it's gone. So if I'm now an operator in the control room, it's gone.

Station Blackout, in my words, means no ac power. Not a legal Station Blackout, a real Station Blackout.

MR. SCAROLA: So you're essentially discrediting the alternate ac sources that --

CHAIR STETKAR: That's my definition of Station Blackout, is no ac power.

MR. SCAROLA: Okay.

CHAIR STETKAR: The non-safety batteries have a rated life of an hour. The trending information is often very important to operators because it tells me how things are changing, the direction they're changing and how fast they're changing, rather then just looking at an individual value.

And to understand the trajectory of the

plant, that trending information can be really important. And we have a lot of experience with operators, not operators, people in general not doing well about looking at individual point values and remembering which way they're going and how fast they're going.

So that's the reason I bring up the question about why the trending information isn't available over on the safety side of the plant.

MR. SCAROLA: Well if it were determined to be needed, it would be on the safety side.

CHAIR STETKAR: You're going to kick me back to Chapter 18.

MR. SCAROLA: Well no, because IEEE-497, which we follow, says that if the emergency procedures require trending, then that is a Type A or Type B variable.

CHAIR STETKAR: Okay.

MR. SCAROLA: But right now, that has not been the case. And we have been through, not all accidents, but many accidents with operators in our facility and they have not requested any kind of trending on the safety VDU.

CHAIR STETKAR: Okay.

MR. SCAROLA: So my point is, it is a

Chapter 18 issue, but it's also a Chapter 7 issue. But if they are required we will add trends, but right now we have not seen any need for it.

CHAIR STETKAR: They're not required and you haven't had any feedback from the operators that they feel that they're missing.

MR. SCAROLA: Okay, thanks.

MEMBER SHACK: Even if you blacked out the operational VDUs after an hour?

CHAIR STETKAR: That's a good question.

MR. SCAROLA: Well I'm not an operator, but I, clearly an operator can look at a value on the safety VDU and he can see if something is increasing or decreasing. And he can see the rate of increase and decrease for short term decisions.

Now if there was something that the EOP said go back and look at an hour ago, then of course we would have to put some type of historical data. But we have not seen that.

MEMBER BLEY: I'm just curious. We'll get to this at Chapter 18, but did you specifically ask the operators about this or they just never talked about it?

And the reason I ask is there's only one plant that I know of that's operating today, had one of those unfortunate things. They had their operating crew on hand for several years before they got to start up. It was while everything was delayed back in the late '70's.

And they completely redesigned their control panels the way they wanted them. And they actually, one of the key things they used, they preset in a number of trends that depending on what's going on, they can pop up this set of four or a different set of four and they love them.

And they actually designed that into their system. It wasn't there when it started, so.

MR. SCAROLA: Well we have that same functionality in the PCMS.

MEMBER BLEY: Yes.

MR. SCAROLA: There are many preconfigured trends, but the operators also have the ability to --

MEMBER BLEY: Setup their own.

MR. SCAROLA: -- configure their own trends on the fly during any shift and they can save them so they're available on the next shift. But here we're talking specifically about the safety VDUs --

MEMBER BLEY: Right, and it's not there.

MR. SCAROLA: -- and those, the way we test, we blackout or freeze, depending upon the scenario, some are blackout some are freezes, all the non-safety VDUs --

CHAIR STETKAR: So they essentially simulate --

MR. SCAROLA: -- and we force the operators to manage accidents and achieve safe shutdown with just the safety VDU. Now we haven't done every accident and we will never do ever accident in the V&V part.

We do a broad sampling of that cross section, but the operators are not shy about given us feedback on what they want. And this has never come up.

MEMBER BLEY: That's interesting. It surprises me.

CHAIR STETKAR: Continue, we'll try to get through the safety related stuff before we take a break here.

MR. SAMPLES: Okay, there was a question at a previous meeting about the reactor trip on turbine trip function. Specifically to it's reliability.

First of all, unless we have a diagram of how the signal for reactor trip on turbine trip is generated. If you're above ten percent power the P7 interlock is satisfied. Then if you have either one of two different conditions.

One, all four of your main turbine stop valves are closed. Because if you had any one of them your turbine could still be operating.

Or, you have two of four the turbine emergency trip oil pressure switches indicated low. So either one of those conditions and you're above ten percent power, you'll get your reactor trip on turbine trip.

Now this trip is, it's an anticipatory trip function. It's not credited in the Chapter 15 analysis.

Now while it can't be Class 1E due to the turbine being non-safety and the turbine building is in a non-seismic location, is a non-seismic location, but it is designed to be highly reliable by seismically and environmental qualified sensors, uses Class 1E power sources, diverse redundant sensors, separation of sensors and cables and the function is maintained by the tactical specifications including periodic surveillance tests.

There's also question about the turbine trip on reactor trip function. Now the way we trip the turbine is the main turbine stop valves are held open by high pressure hydraulic oil. So you trip them, you vent that off.

These turbine trip solenoid valves in the bottom, once you operate these, that allows the venting of the high pressure hydraulic oil go off and you get a trip.

So what this is showing you is the PSMS on the left and the PCMS on the right with the turbine protection system and the separate turbine control system.

Now just from, we have a reactor trip we detect, the reactor trip breakers opening, the CPU would generate a signal through the power interface module down to actuate these turbine trip solenoid valves, vent the pressure trip to the turbines.

The turbine protection system, see it's a dedicated system, it has four redundant digital subsystems. Two for A, two for D. And it too generates a signal.

Whereas the PSMS, when it's given a turbine trip on a reactor trip, is given this trip to protect the plant from unsafe condition. The turbine protection system, when it gives a trip, it's doing that trip to protect the turbine itself. So these two will all come together and protect power interface module.

The turbine control system you see is totally separate system. It's also dedicated as duplex-independent digital subsystems.

Our independent sensors, including speed sensors for these two different turbine protection system, turbine control system and also whereas the main control, excuse me, the turbine control system controls the main turbine control valves, throttle valves, it actuates those to control the Turbine E. The turbine protection system in PSMS control the main turbine stop valves.

Okay, now we'll move onto the non-safety systems. The plant controls --

CHAIR STETKAR: Let's, I'll stop you here. Let's take a break, it's a convenient time, and reconvene at 10:20.

(Whereupon, the foregoing matter went off the record at 10:04 a.m. and went back on the record at 10:20 a.m.)

CHAIR STETKAR: We are back in session. Let the fun continue.

MR. SAMPLES: Okay, we'll move on now to the non-safety I&C systems. The plant control and monitoring systems and we'll discuss the topics you see here.

Starting with the plant control systems. The non-safety systems are controlled by the PCMS. The control and functions are distributed to multiply

PCMS controller groups to ensure that transients due to experience signals from one control group are bounded by the DCD Chapter 15, AOO analysis.

The controller redundancy and the distribution of functions to multiple controller groups minimizes the potential for single or complete controller function failure. The input and output redundancy apply to the components, for example, feedwater regulation valves that could cause plant trip.

There is an open item associated with this. The spurious actuations caused by PCMS failures, including software design defects, they're being examined or plant effects as part of this open item.

The PCMS shares sensors with the reactor protection systems for many control functions. The reason being that sensor-sharing reduces pressure boundary penetrations and local maintenance work in accordance with ALARA principles.

The PCMS avoids adverse control and/or protection interaction by using multiple redundant sensors and the signal selection algorithm. Essentially the signal selection algorithm works by selecting the highest of four sensors, if there's available.

Once sensors failed it selects the highest of the three. If another sensor fails and you only have two, we transition into a failure state because with two you don't really know which one is going to be correct in that case.

MEMBER BROWN: I guess I missed that, the selection of the second highest, where does this come into, I'm trying to think in the PCMS where this even comes into play sense the sensors that actuate things of interest are all feed up through the RPS and then over to the ESFAS. And what shared, I have no problem with shared sensors so I'm not asking a question relative to that, what part of PCMS actually makes this decision process as opposed to what sensor it uses?

MR. SAMPLES: You mean where is the function implemented in the PCMS?

MEMBER BROWN: Yes, what function? I mean I looked back at the PCMS I've got rod control, I get a switch actuation, you know if somebody wants to move the rods from the main control room.

CHAIR STETKAR: Charlie, think about pressurizer level control pressurizes, pressure control, main feedwater control.

MR. SCAROLA: Even rod control, T-average.

CHAIR STETKAR: T-ave for rod control.

MEMBER BROWN: But how many channels, I

agree, I don't understand all of that. I don't have the knowledge that you all have of the balance of plant or the other systems. You know, the plant systems, from that standpoint.

MR. SCAROLA: Well every reactor control system --

MEMBER BROWN: Pressurizer level moves up and down, pressurizer pressure is controlled by heaters or I presume it is.

MR. SCAROLA: Right.

MEMBER BROWN: This is a PWR.

MR. SCAROLA: So those are the same sensors that we use in the RPS.

MEMBER BROWN: Right.

MR. SCAROLA: The sensors are used in the RPS and in their digitized form, the sensor values are sent to the PCMS from each of the four RPS divisions. They're sent separately.

And then inside the PCMS in the specific group controller where that function is needed, we have an SSA algorithm block. The signal selection algorithm block.

So we take all four signal sensors, put it into the SSA block and the SSA spits out the output, which is the second highest. And the reason we do that is so we don't have any spurious control system actions based on a single sensor failure.

So you got one sensor deviating, yes, that might make the D division of the RPS out of service because it's deviating non-conservatively, but it won't result in a spurious control system action. Because of this SSA algorithm. Signal Selection Algorithm.

So this applies to rod control, because we move rods automatically based on T-average. So we look at hot leg and cold leg temperatures, turbine bypass control. Every control, just about every NSSS control system.

MEMBER BROWN: Okay, go ahead.

MR. SAMPLES: Now the sensor failure does not cause an adverse control systems action while the PSMS is in degraded state from that very same sensor failure for IEEE-603. And the signal selection algorithm as augmented quality.

CHAIR STETKAR: God, I hate to keep doing this, but it's okay. I read someplace where SSA kind of marches down the daisychain if I have four, three, two, one. And it knows if the monitored parameters are out of range.

So for example, if one monitored parameter is out of range it takes the second highest of the remaining three, if two are out of range it takes the second highest of the remaining two, if three are out of range it takes the second highest of the remaining one. That's at least the way I read, I can look up the reference.

MR. SCAROLA: You're making it more complicated. It always takes the second highest.

CHAIR STETKAR: Okay.

MR. SCAROLA: It doesn't matter whether they're drifting or not, it just always, it's very simple. It just always uses the second highest.

CHAIR STETKAR: Second highest, okay. So if three of them are all failed high and it's right, it's going to control on the wrong one?

MR. SCAROLA: Right. Yes, if three of them are all failed high, one of those three is the second highest.

CHAIR STETKAR: Is one of those three the second highest --

MR. SCAROLA: Well sure.

MEMBER BROWN: They're all the second highest.

MR. SCAROLA: Oh, you mean they all fail like right out of range?

CHAIR STETKAR: They're all pegged?

MR. SCAROLA: It's different. Then they're taken out of the equation completely. If they --

CHAIR STETKAR: That's what I was saying.

MEMBER BROWN: That's where --

CHAIR STETKAR: But that's what I was saying. If they're out of range, there was a discussion in there --

MR. SCAROLA: Yes, I'm sorry, your right.

CHAIR STETKAR: -- it's the second highest as long as they're in range.

MR. SCAROLA: Correct.

CHAIR STETKAR: Now if three of the four are out of range, it's going to control on the one-of-one that is in range.

MR. SCAROLA: Right.

CHAIR STETKAR: Even though it might be wrong?

MR. SCAROLA: That's all tech-spec controlled. As soon as you get down to two, you're in a LCO condition.

CHAIR STETKAR: I understand. I understand that from the lawyers. I'm trying to understand, if things happen in the plant that the ranges that were set in the SSA didn't anticipate all of my potential transient conditions, such that the one that I'm controlling on indeed --

MR. SCAROLA: Is the failed one.

CHAIR STETKAR: -- is the wrong one. Because it didn't respond correctly.

MR. SCAROLA: About this, if the sensors have failed out of range, let's take pressurizer pressure, at that point you have a plant trip because you've got two out of four sensors that have failed --

CHAIR STETKAR: That's a good point.

MR. SCAROLA: -- out of range and you have a trip.

CHAIR STETKAR: Thanks, that's a good point.

MR. SCAROLA: And the same thing would apply for most low range sensors.

CHAIR STETKAR: Yes.

MR. SCAROLA: Pressurizer level, pressurizer level has a high trip and a low trip. Pressurizer pressure got's a high trip and a low trip. So in most cases you can never --

(Crosstalk)

CHAIR STETKAR: You're right, Ken. You're right, Ken. I didn't think over on the protection side of the equation what would be happening over there.

I was just focusing on the description of the SSA. Thanks.

MR. SCAROLA: You're right.

MR. SAMPLES: Okay, now we're ready to discuss the second information system of the I&C system. These are the alarms for credited manual actions.

Now in accordance with the SECY letter, SECY-93-087, the reliability of alarms to prompt manual actions credited to the safety valves is assured by these design features. First, redundancy is provided for all HSI alarm components, the separation between redundant segments, their testability is provided from self diagnostics of the, PSMS, PCMS and the HSI computers.

These alarm functions have augmented quality. In addition to these alarms, there's abnormal indications for these same credited manual operator actions, are provided on the safety VDUS.

Here we see a simplified block diagram with the PSMS and PCMS. It shows how these alarms indications and abnormal indications are going to be generated.

Senors. Both the safety sensor and the non-safety on the left and the location where the alarm indication is given to you.

So first of all, on the top for the PSMS, signals received from a safety sensor, that safety sensor goes, is processed with a safety VDU processor that's shown, that's abnormal indication on the safety VDU. The same signal, raw sensor data, also transferred through the unit bus to the PCMS.

The non-safety sensor here receive input into the alarm logic computer which will then generate an alarm. It will generate the audible alarm, the alarm indications of the alarm VDU and the alarm indication on the large display panel.

And again, the signal is also shared with the PSMS. So for shared signals, a safety signal will come down, also into the PCMS and to the same alarm logic computer, which will then generate alarms on the large display panel alarm VDU and the audible alarms.

Whereas an input from the safety sensor will be transmitted to the PSMS and then the safety VDU would also generate the abnormal indication on the safety VDU.

MEMBER BROWN: One question, just to make sure I, the little thing that says ISO, you mentioned this earlier. Is that a one way isolation, I mean it's a optical coupling into the unit bus or is it a bidirectional, but electrically isolated? I mean I'm just trying to differentiate it.

MR. SCAROLA: The circle that says ISO is representing fiberoptic cable of which it is bidirectional.

MEMBER BROWN: It's electrical isolation --

MR. SCAROLA: Well no, it's a fiberoptic cable.

MEMBER BROWN: So by that's it's electrically isolated also?

MR. SCAROLA: Oh, yes, it's electrically isolated. But it is bidirectional. Any interface that you see here with the unit bus is a bidirectional interface.

The data is one direction. The interface is a bidirectional. So for example in the case, we're showing that safety sensor data is going from the reactor protection system to the unit bus.

Non-safety sensors are coming from the reactor control system via the unit bus back to the safety system for display on the safety VDUs. So the data is going one way or the other, depending upon where the data is actually originating. But the unit bus itself is a bidirectional media.

MEMBER BROWN: I understand that.

MR. SCAROLA: Yes.

MEMBER BROWN: I understand the unit bus

is a bidirectional. It's just my question was relative to the information that gets onto it is unidirectional from the PCMS to all these other displays.

Obviously you got to be able to monitor everything, but yet you can't put information into the reactor protection system A from the unit bus?

MR. SCAROLA: Not directly.

MEMBER BROWN: Not directly.

MR. SCAROLA: If you recall the earlier slide --

MEMBER BROWN: Yes, I'm old, I forget a lot of stuff.

MR. SCAROLA: -- we talked about safety, the operational VDUs, these non-safety VDUs. They can do things like initiate reactor trip. So that's done via the unit bus but through what we call a COM interface, communication module interface. And we'll be talking about that more.

MEMBER BROWN: It doesn't go through the functional calculation part and the tripping and voting units. There's a separate set of communications, I remember seeing that in the diagram.

MR. SCAROLA: Correct.

MEMBER BROWN: So you're going to talk about that later, okay.

MR. SAMPLES: Now for the non-safety data communication system. The data communication system is non-safety and consists of the unit bus and the station bus.

The unit bus interfaces with all I&C systems, including information controls for the main control room and remote shutdown room and technical support center. The unit bus interfaces with the station bus and the station bus is a plant information technology network.

It provides information to the NRC via the emergency response data system to the emergency operating facility and to plant personnel. And it contains systems that you see here, such as work order management, for example.

Okay, we talked about D, PAM and the alarms previously. Now the two remaining information systems are, the safety parameter display systems and the bypass and inoperable status indication.

The safety parameter display system displays keep parameters for critical safety functions and also dynamic safety functions trees used by the operators for procedures. Including emergency operating procedures.

It displays key parameters for performance of normal and emergency systems used to maintain or restore critical safety functions. The bypass an inoperable status indication gives you availability status of emergency systems for all the critical safety functions.

Both of these parameters are displayed in the main control room, remote shutdown room, technical support center and emergency operating facility.

CHAIR STETKAR: Richard --

MEMBER BROWN: Can you, I'm sorry, go ahead.

CHAIR STETKAR: Why is the bypass inoperable status indication not available on the safety VDUs?

MR. SCAROLA: It is but not at the system level. For example, if you think about a conventional plant, you can see that a pump is not available because the lights go out on the hand switch. The lights are powered by the same power supply that powers the pump.

So at the component level, you can see on the safety VDU if any particular pump or valve is not available. What BISI is, is a system-level algorithm that looks at the entire system.

For example, safety injection system looks at the required pumps, require valves and it says, in aggregate, are all the components lined up correctly and it gives a system level indication.

CHAIR STETKAR: But if I bypassed Train A for example, all of Train A, I'll get a Train A bypass indication on BISI, right?

MR. SCAROLA: Up on the LDP.

CHAIR STETKAR: Right.

MR. SCAROLA: Right.

CHAIR STETKAR: I'll get a yellow light?

MR. SCAROLA: You'll get a component level on the O-VDU and the safety VDU. Just component level.

CHAIR STETKAR: But it will show component level?

MR. SCAROLA: Yes.

CHAIR STETKAR: Okay.

MR. SCAROLA: It's really --

CHAIR STETKAR: Yes, it's --

MR. SCAROLA: It's a matter --

CHAIR STETKAR: Okay.

MR. SCAROLA: It's kind of a philosophy that safety HSI is kept as simple as possible so we can achieve all the Class 1E software requirements. All the complexity in the HSI is put in the non-safety systems where we can have nice user friendly graphic displays.

CHAIR STETKAR: Okay, I'm just --

MR. SCAROLA: BISI is just an example.

CHAIR STETKAR: -- thinking the operators are operators, lawyers or lawyers. And the operators who need to understand what they have and what they don't have in extremis --

MR. SCAROLA: Same philosophy --

CHAIR STETKAR: -- as long as they do have that indication available somehow so they're not struggling to operate a pump that's bypassed and they don't recognize the fact that that whole train is bypassed.

MR. SCAROLA: This whole philosophy is really consistent with the philosophy of post accident monitoring variables. On the safety VDUs we show all the type B's and the C variables and the A's, but on an indication by indication basis, single parameters.

But here on the safety parameter display system, we so the integration of variables in a format that mimics the safety function status tree. So it's easier for operators to see it.

CHAIR STETKAR: I didn't ask about SBDS because somebody lost the battle about making SBDS safety-related a long time ago.

MR. SCAROLA: A long time ago.

CHAIR STETKAR: But at least I could ask

about BISI here.

MR. SCAROLA: But even though the battle was lost on SBDS, you still have the PAM variables for as the backup for SBDS. That's my whole point. It's the same correlation.

CHAIR STETKAR: Okay.

MR. SCAROLA: Component level, component level.

CHAIR STETKAR: Thank you.

MEMBER BROWN: Can you go back a slide?

MR. SAMPLES: Sure can.

MEMBER BROWN: I didn't know whether this was the right place to ask a question. The unit buses is an important bus because it kind of puts everything from PCMS, PSMS up into the main control room and all control functions, etcetera, go back down through it. Normal control functions, okay.

But yet there's no real discussion, or at least I didn't see any, talking about the details of how that bus operates or is managed. And my vague memory is that I read a statement that said it is not evaluated from a safety basis, it's a non-safety bus or non-safety component or subsystem or whatever.

What does that look like? I mean, what manages that bus, how does it operate, how does it obtain real-time transmission of data?

Because if it's a LAN it sounds like it's operated by a server, which has an executive which decides what information is going where and when. So who do you ensure real-time data presentation to the operators in both the NCR and any of the other places?

MR. SCAROLA: You're familiar with the technology that's used for the safety bus, correct?

MEMBER BROWN: No.

MR. SCAROLA: Okay.

MEMBER BROWN: A bus is a bus is a bus.

MR. SCAROLA: Well okay.

MEMBER BROWN: I mean there's no real discussion of the safety bus, because it's within a division, I wasn't worried as much about a single failure of a safety bus from train to train to train. My biggest concern was the unit bus is the bus.

MR. SCAROLA: Right.

MEMBER BROWN: There's only one, its got to be managed. And it looked to me like it was a local area network type bus which has to have servers and other things managing it.

MR. SCAROLA: In the DCD we refer to the MELTAC technical report. The MELTAC technical report describes what's called control network.

That network technology, and it is described in exhausted detail --

MEMBER BROWN: I remember there were pages on that.

MR. SCAROLA: That network technology is used for the safety bus and the unit bus. There's only one technology used in both places. It's this dual ring that we'll talk about later, this resilient packet ring --

MEMBER BROWN: We are going to talk about it then?

MR. SCAROLA: We will talk about it.

CHAIR STETKAR: It's the section later.

MR. SCAROLA: The unit, to make you feel a little bit better, is exactly the same technology as the safety bus. Same design, it is same modules, everything's the same. So we'll talk about that.

And I agree with you, it's an extremely important bus. And that's why its been, that's why we adopted the safety technology for the unit bus.

MEMBER BROWN: Okay, you will be explaining why failures of, the certain failures of that bus are components or parts of that bus design will still allow complete, as well as why you have real-time communications? Because I'll have to admit to you that

I didn't try to read all of that.

MR. SCAROLA: We'll get there.

MEMBER BROWN: I would have never been able to do it within a 24 hour, three day period.

MR. SCAROLA: Control network technology is completely redundant and self healing and very high speed. Gigabit speed.

So we'll talk about that a little bit later. It's actually, I like to call it very elegant technology, but it's --

MEMBER BROWN: Well my computer is gigabit speed also, but every now and then I'm sitting there watching the little hourglass and it just never changes. It just happened to me and I just went and say, sorry, this whole program is now not responding.

MR. SCAROLA: We'll get there.

MEMBER BROWN: Thank you.

MR. SCAROLA: I ask for your patient.

MEMBER BROWN: I'll take a deep breath.

MR. SAMPLES: Now we'll discuss the operational VDUs. Non-safety components and safety components in all divisions can be operated from the non-safety operational VDUs.

The PSMS protects itself from any adverse interaction from these O-VDUs based on compliance with

IEEE-603 independence criteria. Including physical and electrical independence, communication independence and functional independence. It also says that priority for all safety functions, including the safety VDUs.

The operational VDUs enhanced plant safety by, one, reducing operator task burden. This results in reduced time for operator actions and improved margin to safety. And two, there's more mental resources available to the operator for plant wide situational awareness. And it reduces a potential for human-performance errors.

Now these safety enhancements have been validated through full scope simulator testing suing 13 crews of US senior reactor operators and reactor operators. Now --

CHAIR STETKAR: Before --

MR. SAMPLES: Uh-oh.

CHAIR STETKAR: You notice we do interrupt quickly. The only reason I want to interrupt here is there's a drawing in the DCD, it's Figure 7.1-7, that shows electrical power supplies for PCMS.

And it shows that there are two, there's two non-Class 1E UPSs feed PCMS. And there are several functions, there's one controller, it's listed as Control A comes from UPS 1 and Controller B, which is backup, comes from the backup.

The input/output modules have a diode --

MR. SCAROLA: Auctioneering.

CHAIR STETKAR: -- auctioneering. The VDUs are shown as only from one of the two. Why?

MR. SCAROLA: Well --

CHAIR STETKAR: Since they're really importantly for the operators.

MR. SCAROLA: But there are multiply VDUs. So half the VDUs are on one and half the VDUs are on the other.

CHAIR STETKAR: Thank you.

MR. SCAROLA: Good question.

MR. SAMPLES: Now --

CHAIR STETKAR: It's a good story anyway.

MR. SAMPLES: One of the core features of the Operational-VDUs is the hyperlinks. These hyperlinks among those non-safety human system interfaces reduce operator task burden, potential for human errors, the time required for safety action responses.

And how this works is, you see the picture of the alarm VDU, operational-VDU and a procedure VDU, and the blue lines are like indicating these hyperlinks. The way this works is, for instance, you get an alarm on the alarm VDU, or some parameter, operator selects that.

And when he does, on the operational-VDU the page that shows that valve component or other part of the system of interest pulls up. Also on the procedure VDU you'll pull up a procedure, an emergency procedure, a normal procedure, abnormal procedure associated with that.

So instead of having to go get the alarm, see what it is and then go dig for it on the O-VDU, then also dig for the procedure, basically push one button and it pulls up what you need to see. Also when you have the procedure VDU and you're working through a procedure to operate, a plant evolution, for instance, as you get to the point in the procedure it will pull up on the O-VDU, the system and the valve components you would need to operate.

Now each of these just pulls up the screen that you'd be interested on the operational-VDU. All operations still has to be done from the operational-VDU itself. Hyperlinks don't cause any kind of operation from these other VDUs.

See an example screen of an operational-VDU. You see that it has a graphical user interface. You can see the different system, some valves, different things shown here. You see that if the operator wants to operate you touch on a component and a screen pops up, if you have such as a shut and close for a certain valve.

This graphical user interface reduces the mental processing time for both monitoring and control actions. It reduces the potential for operator selecting the wrong components. It's a lot easier to see what you're looking for here than just try to pick from conventional operating switches.

And by using the same screen, a single operator, one operator can control safety and non-safety success paths more than having two separate operators with two separate consoles, with one having to talk to the other to make sure they're doing things in sequence and the right way.

So one can actually control everything, such that safety is enhanced when operator time for operator action is reduced, potential for errors is reduced, and the task is simplified. There is an open item associated with this, and MHI is in the process of quantitatively evaluating the safety advantages of operational-VDU in response to this open item.

CHAIR STETKAR: This is not for the U.S. Safety WR, is it?

MR. SCAROLA: You mean this pressurizer, that pressure picture?

CHAIR STETKAR: Because I'm looking at three relief valves in the parallel, and you guys only have two -- okay, thanks.

MR. SAMPLES: I do believe this just must be an example.

MR. SCAROLA: This is just an example.

CHAIR STETKAR: Thanks.

MR. SAMPLES: Okay. With the turbine bypass valves interlock, erroneous turbine bypass control signals are prevented by the PSMS. The PSMS controls redundant non-Class 1E permissive solenoids from the SLS trains both A and D. These are the valves over here. The turbine bypass control function output signals are provided by the reactor control system in the PCMS through current to pressure converters and the trip open solenoids over here.

What you see here is the logic for generating the block turbine bypass valve signal. This is the signal that blocks the opening of these turbine bypass valves. The block turbine bypass valve signal is generated under these conditions.

First of all, you have two of the four average coolant temperature low-low or two of the four reactor coolant loops. You see this on the other side over here. Or the turbine inlet pressure is low, actually it does not indicate a rate of decrease in the turbine load, or you don't have your condenser available. And your hot full power conditions you have would be established.

The turbine inlet pressure is not indicating a rate of decrease in the load. When you have this, you have the block turbine bypass valve signal and you're generating both your trains A and D.

CHAIR STETKAR: I'm trying to look forward and I'm not seeing it, but you guys know the slides better than I do. You ever talk about the load rejection at any time?

MR. SCAROLA: Only here.

CHAIR STETKAR: Only here, okay, let me ask about that. And this is a curiosity, it's not necessarily a safety question, I don't think. If I read the discussion of the load rejection, and I understand you're capable of withstanding a 100 percent load rejection without lifting any secondary relief valves, without lifting any primary relief valves. Everything works, works fine.

There is a statement in there that says, "In this scenario, the main turbine control valve is immediately fully closed and four banks of turbine bypass valves are tripped open to fully dump excess steam to the condenser." I understand that.

My question is, if the load rejection signal closes all of the turbine -- and then it goes on to discuss a lot of things. For in the interest of time, it says eventually, you know, the rods go in, turbine bypass starts to modulate closed so you eventually get a stable state where reactor power matches turbine power.

Is the plant designed to go into what I call "island mode operation," where if you have a load rejection the reactor remains at power, the turbine remains at power, and you're supplying in-house loads from the main generator?

And if that's the question, what does the load rejection thing do to turbine control? Because if the load rejection signal slams the turbine control valves all the way closed, what reopens them? It's got to do something to turbine load control.

MR. SCAROLA: The position of the turbine modulating valves is controlled by the turbine control system based on the load demand or the significant step change in the load demand.

CHAIR STETKAR: But this says they go all the way closed. It doesn't say it modulates according to turbine load, it says they go all the way closed. So what reopens them and when?

MR. TAKASHIMA: Maybe the module open?

CHAIR STETKAR: The thing I'm interested in, if at some point I start to get, for example, frequency deviations and voltage and reverse power on my generator and, for example, the thing doesn't recover, if indeed the turbine control valves are all the way fully closed, as this says.

I've seen these systems in the past. I'm not familiar with this design. And that caught my eye because other systems run back the turbine, they don't close the valves completely.

MR. SCAROLA: In my mind, I'm questioning whether that wording's correct.

CHAIR STETKAR: You may want to look it up. It's in section, and just in the interest of time, it's in section -- oh crap, it's on the record too, huh -- DCD section 7.7.1.1.11.3. You just may want to look that up. Because I didn't understand, I couldn't see the signal that came in.

The reason I asked about this is I look at the schematics and I don't see a load rejection signal specifically that opens all of the turbine bypass valves, all four banks. And the only way I could see that happening is a huge difference between Tref and Tave, where Tref falls to zero because you've got no steam pressure in the steam chest.

MR. SCAROLA: You will see that signal in section 7.2 in the logic diagrams. There's a set of logic diagrams in 7.2, and I realize 7.2 is RPFs. But those logic diagrams also show the interface between the safety instruments and the control systems. And in one of those figures you'll see the load rejection signal.

CHAIR STETKAR: But it still comes from a Tave/Tref deviation. It's not a load rejection at least in what I was looking at. I looked at that drawing. It didn't show a load rejection signal that says open all four banks, boom. It showed a load rejection controller that's got a ramp with Tave and Tref, I believe, into it.

It's a lot of detail, and I thought I could make it work if I got all four of the turbine control valves all the way closed, because my Tref would then go to zero because I have no steam pressure and --

MR. SCAROLA: On the break we'll look at that diagram. My recollection is that it relates to the turbine inlet pressure signal that you're seeing on this drawing. This turbine inlet pressure signal not only removes the block, but it also initiates this trip open of those valves.

CHAIR STETKAR: Let's look at it on the break, because that's a lot of detail. But I'm still curious about that statement about the turbine control valves going fully closed, because I'm not sure how you recover from that in enough time to save the electrical side of the plan.

MR. SPRENGEL: So real quick, can you summarize the question?

CHAIR STETKAR: There's a couple of questions. One question is, if the plant is designed to withstand the full load rejection with the main generator supplying in-house loads, which I'll call island operation, if that's the design philosophy, and if the load rejection signal causes all four of the turbine control valves to close fully, meaning no steam going into the turbine, it's difficult for that system to recover, for the main generator to keep supplying in-house loads in a stable condition. Because power is going to start to decrease immediately, and you're going to get into, you know, voltage or frequency or reverse power or some sort of protective trips on the electrical side that you won't survive.

So I'm questioning, first of all, the

statement in the DCD about the full closure on the turbine control valves in terms of the overall design philosophy. The second thing that Ken and I were going back and forth is, maybe we'll work that out during the break so we'll just take a look at that later.

MR. SAMPLES: Okay, now for the diverse I&C systems, the diverse actuation system. We'll discuss these topics starting with the basic architecture of the DAS. You see here the starting of the sensor, its distribution.

The same sensor signal goes to the RPS and also into the DAS, diverse automatic actuation cabinets through an isolation device. There's four diverse automatic actuation cabinets, within each bistable, logic and output.

And the DAS is implemented with conventional discrete logic, relays, latches and other conventional analog electronic devices. Nothing requiring software. So you see the bistable, logic and output, and then the output of each cabinet is combined within the safety logic system and then is sent to a component for actuation.

MEMBER BROWN: This is where I asked the question before about how does, you're using a common part. There's this diverse actuation system and yet we're using a common part of the, the PIF is located within the overall SLS envelope.

And I guess my normal thought process on a diverse system would have bypassed anything associated with the normal path. I mean what is the argument for saying, well, I can depend on these last little parts of the output logic not being, that it's the same technology for either the automatic or the diverse trip and they're not even separate units, they're the same units?

MR. SAMPLES: Well, the same unit, it's the same for ESF --

MEMBER BROWN: That question's the same.

MR. SAMPLES: For reactor trip we do use two different actuations.

MEMBER BROWN: The reactor trip part I don't disagree with, but it's for the ESF DAS --

(Crosstalk)

MR. SAMPLES: -- interface module for DAS.

Mr. Scarola, do you --

MR. SCAROLA: I'll be happy to answer. The PIF module is conventional binary digital devices, CMOS logic, no software.

MEMBER BROWN: I understand that.

MR. SCAROLA: So simply based on BTP 7-19 which says you have to take a common cause failure in digital devices, this is not a digital device. But then beyond that this device --

MEMBER BROWN: Well, it is a digital, I mean it's a combinational logic is what you're doing to trigger these things. It's manual. It's like we had the old-time computers where they were all transistor, or transistor logic or whatever you want to call it, or CMOS logic all on a single chip. It's still a digital device.

MR. SCAROLA: Well, let me continue. This is so simple for this device. It has no timers, no latches. It has very few inputs because it's only control of one component. So it's so simple that we can actually test every combination of inputs and outputs and ensure it's 100 percent tested during the design phase. So therefore we can say there is no potential for common cause failure of that device that would impact both PSMS and DAS.

MR. TAKASHIMA: That is the common motivating factor of these kind of devices also evaluated in a PRA.

MR. SCAROLA: Yes, there is a deterministic side and a PRA side. On the deterministic side --

CHAIR STETKAR: Okay, and before you do

that I'm going to rant later on this afternoon about the PRA. The fact of the matter is, it is not evaluated in the PRA, because the PRA does not consistently and completely include the SLS modules. That is a statement of fact. That is not a question. You can go look it up. Go look at the emergency feedwater system, the SLS is not in there. The only place that I could find it is in high-head injection in the PRA models. A fact, not open to discussion. It's on the record. If you want to dispute me, that's fine, but I can show you the --

MR. SCAROLA: What the PRA says is that the high-head injection model is representative of all the other ESFAS signal caps.

CHAIR STETKAR: I don't care what the words say. I can tell you what the fault trees are, and the high-head injection model does indeed have the SLS modules in it. I couldn't find them anywhere else.

MR. SCAROLA: Okay. All right, I understand.

CHAIR STETKAR: Now you can continue on deterministic stuff.

MEMBER BLEY: But were you linking this to the PRA or you were talking about probabilistic --

MR. SCAROLA: No, what I was trying to say is there are two parts to this. There is the deterministic compliance, the BTP 7-19. And 7-19 says if it's 100 percent testable then we do not have to consider it as a common cause failure point. So that's what we have done.

But then what you're saying is in some method, and I'm not going to argue with you, I thought we covered this in the PRA on the probabilistic side.

CHAIR STETKAR: I think you should put your eggs in your deterministic basket for the moment.

MEMBER BROWN: Okay, you used the words 100 percent tested in the design phase. Now I mean, is there a process where this is, you've got all this auto-testing and diagnostic stuff going on.

This is a single point where all this stuff comes in. It's one set of little voting logic. There's not multiple, multiple units. Okay, it's for one particular, it comes down right to these combinational logic, CMOS, whatever it is, integrated circuits, which I like, okay.

But is there a part of you that the end-process test routine that where this gets tested either manually or automatically on a periodic, manually if it's a periodic basis, or is it part of the auto testing? I was unable to find a discussion, and it's easy not to find this stuff.

MR. SCAROLA: There are two parts to the tech specs. There is the part of the tech specs that covers the DAS, and in those tech specs we have surveillance requirements that ensure the DAS signals propagate all the way to the PIF and are received by the PIF. There's actually feedback from the PIF.

MEMBER BROWN: What about the output of the PIF?

MR. SCAROLA: Then we have, whenever you control the pump or valve, the safety related pump or valve which is part of like a 90-day test for every ESF component, you send the signal through the PIF module in an overlap with the signal from the DAS. So there's an overlap point where both signals come together. So the PIF is fully tested.

For the DAS interface every 24 months, but for the normal pump and valve interface control every 90 days for in-service testing of the pumps and valves. Because that PIF is the only way that you can reposition a pump or valve is through that PIF module. There is no way around it.

When you control a pump or a valve from the main control room, the signal goes from the O-VDU or the S-VDU all the way through all these networks, and finally generates an output from that PIF. So the PIF is the common point, but it's frequently tested.

MEMBER BROWN: Somebody could have designed in an alternate way of initiating the action on those. It's just you didn't, therefore it is a common point. It's not that it couldn't have been done, it's just that it was not done. You're using a common point. I just was looking for an answer as what you all considered satisfactory --

MR. SCAROLA: Okay, so let me explain why we have to have a common point. If you've got two systems that are trying to control the same valve --

MEMBER BROWN: I understand that point.

MR. SCAROLA: -- you've got to have a common point somewhere.

MEMBER BROWN: Well, the valve is the common point.

MR. SCAROLA: Well, no, because you can have one system saying open the valve and the other system saying shut the valve. So someplace you need to combine those logic signals and establish which one is going to have priority. So you can't just send both signals to the valve because the valve's a mechanical device.

MEMBER BROWN: This is part of the DAS. There could have been a way to block, if the DAS is calling for it that takes precedence. I mean there are ways to do that, just you chose this way. And I just wanted a discussion of why and you've given it to me. I'm not telling you whether I agree or disagree, I'm just saying you've given it to me. Thank you.

MR. SCAROLA: I'm never satisfied until you agree.

MR. SAMPLES: Now you can actuate. You just saw this signal path for automatic actuation of DAS, but you can also manually initiate it from the diverse HSI panel. This bypasses the DAAC panels and go to the safety logic system.

And just to state again that the reactor trip for DAS trips the motor generator set while the PSMS trips the reactor trip breaker so there's a diversity of actuation for those components. This is how the DAS functions. The DAS does it immediately --

(Crosstalk)

MR. SAMPLES: -- acuate components. So it actuates if it detects an accident and the safety components are not actuated successfully. So you see logic here. Down here you see DAS monitoring several parameters. We'll discuss those in a minute.

You see signal trip statuses from the PSMS. DAS says it looks like there's an accident. It looks like PSMS should do something, and it monitors whether it does it or not. And it waits for a short amount of time, and after that time if it doesn't see that its, for instance, reactor trip breakers have been tripped, then it takes action to trip those breakers. In this case, for the diverse reactor trip.

MEMBER BROWN: Before you change that, the key words in here are "and safety components are not actuated successfully."

MR. SAMPLES: Yes.

MEMBER BROWN: And this is discussed in a couple places, the prevention of diverse reactor trip, turbine trip --

(Crosstalk)

MEMBER BROWN: I mean you're using the actual auxiliary contacts on the reactor trip breakers to do this, so that's good.

But fires and other stuff could contaminate switch contacts such that they did not provide the closure such that you get an indication of it, or they might show give you closure when you really haven't activated it due to contamination. And now because of that I have blocked myself from using the DAS system to actually complete the actuation.

So I don't know that I'm out to lunch or not. I just didn't like the idea of having something tell the DAS not, that it's annulled and cannot control that safety function. And that just kind of went against the grain.

And I understand the thought process a little bit, but to me the diverse actuation system should always be there and not be prevented. Are we smart enough to always consider all the circumstances under which that prevention signal would not prevent it when we don't want it to prevent it.

(Crosstalk)

MR. SCAROLA: Well, a couple of issues. First of all, the operator can manually actuate all these components completely around the automation of DAS, so there is a diverse manual method of actuating everything in the diverse actuation system.

It's shown in the previous figures if you want to go back to that. So if, in fact, the automated part of DAS does not work, there is a backup manual part that has its own signal path. That's the first point. Second --

MEMBER BROWN: Okay. Well, let me then --

MR. SCAROLA: Look at it here.

MEMBER BROWN: I'm trying to relate where this reactor trip breaker functionality that you show on the next page is reflected in the previous page.

MR. SCAROLA: Okay. So all this logic that you see in this page, if we now go back to the previous page, is what you see in bistable and logic blocks and the output block on the first page. That's the automated function.

MEMBER BROWN: Okay, so the other switch you show, permissive switch that actuates a relay, which closes a contact which, so that's your fallback from that.

MR. SCAROLA: That's your final fallback. The other point I wanted to make is that all these interfaces are under tech spec control, so they are all periodically tested. All these manual inputs into DAS, everything is tested as part of the DAS tech specs, periodic tech specs.

So you're right. I mean over time you can get random failures in auxiliary breaker contacts, but they would be picked up during the periodic surveillance tests.

MEMBER BROWN: I'm more comfortable with, I recognize this. I mean I saw this and I looked at that, I just didn't connect the dots between my discussions. So sorry about that. I appreciate your patience with me.

MR. SCAROLA: No problem.

MR. SAMPLES: This table shows you the different components that are actuated by the DAS. You can see on the right side that all of them can be manually actuated from the main control room, and several have automatic actuations.

These are the variables monitored by DAS. If you take a look at the pressurizer pressure and steam generator water level, the asterisks are telling you that these are the two different variables monitored to initiate automatic actuation.

Now DAS has three automatic diverse reactor trip and ESF actuation signals. These are the high pressurizer pressure, low pressurizer pressure, and low steam generator water level. These signals were selected to be the minimum set required to mitigate occurrence of a Chapter 15 AOO or postulated accident concurrent with a common cause failure.

The adequacy of these three reactor trip and ESF actuation signals for the DAS is demonstrated by the defense-in-depth and diversity, D3, coping analysis. Now the D3 coping analysis demonstrates pressure boundary integrity, core coolability and offsite dose limits are maintained for Chapter 15 events with concurrent common cause failures.

The analysis considers both partial actuation and failure to actuate with false indications. With partial actuations, the AOOs and postulate accidents are analyzed with the failure of both the PSMS and the PCMS and a failure of only the PSMS.

What we're concerned with is failures that partially, partial failures that block the DAS which could occur if you have conflicting commands, erroneous blocking signals, or erroneous actuation of components not monitored by the DAS.

The failure to actuate with false indications that the actuation has actually occurred, the analysis demonstrates this would actually require a common cause failure of multiple software blocks which is beyond the scope of Branch Technical Position 7-19. There's an open item associated with this, and MHI is justifying the inputs and assumptions of the D3 coping analysis in response to this open item.

The DAS has augmented quality. It's an augmented quality, non-safety system as defined by Generic Letter 85-06. The attributes of the augmented quality program for the DAS are, it's designed using a nuclear quality program that meets the US-APWR quality assurance program descriptions and the guidance of the Generic Letter 85-06; uses components with a history of successful operation; uses components commonly used in conventional non-digital safety systems; the design process includes an independent review; and the seismic testing method is equivalent to that for seismic category 1.

Now we're going to move into how the I&C systems conform to the essential safety criteria. These different safety criteria have been aggregated from multiple sources such as regulatory guides and IEEE standards.

Now the DCD and the related I&C reports demonstrate the PSMS design conformance to the essential safety criteria. The overall conformance to the essential safety criteria is described in DCD Chapter 7. That's in Section 7.1.4. And the detailed conformance is described in the technical report, Safety I&C System Description and Design Process," and Section 3 in the appendices listed here.

PSMS or redundancy of the PSMS, PSMS consists of four redundant and independent trains, A through D. The RPS performs its function with any two out of four trains tripped. The ESFAS, SLS, the communication subsystem of the PSMS, and the human system interface perform their function by any two out of four trains to actuate safety systems, or one out of two trains depending on how the mechanical system is designed. Essentially we'll use two out of four if we need to actuate an active component. For isolation we use one out of two.

Now for independence. The independence of the redundant PSMS divisions is achieved through four different methods. Physical independence, electrical independence, communication independence and functional independence. The methods for ensuring physical, electrical and communication independence are common throughout the entire PSMS. The functional independence on the other hand is application dependent. It's done different ways for each application.

Now for physical independence, this provides protection, for instance, against things, flood, fire. Also provides, just meets some operational environment requirements. You see that the four PMS trains, these are A, B, C, and D, are separated into four separate I&C rooms around the main control room. Four reactor trip breaker trains are separated into two separate trip breaker rooms, 1 and 2.

MEMBER BROWN: Are they adjacent to each other, physically, in the plant design?

MR. TAKASHIMA: Yes.

MEMBER BROWN: Okay. The way you laid out the other I presumed that that meant the same thing. When you saw a wall between the two they weren't separated, so I presumed they were in the same, just adjacent to each other.

MR. SCAROLA: But with a firewall between --

MEMBER BROWN: Yes, I understand that. I'm just saying they're adjacent to each other, with a firewall or whatever.

MR. SAMPLES: The motor generator sets are in the rooms, motor generator set rooms, separate from both reactor trip breaker rooms. And finally, the non-safety, the PCMS is located in the non-safety I&C room.

For electrical independence, each PSMS train is electrically independent from each other and from the non-safety system. I see three different types of electrical isolators here in the red, the green, and the blue.

Starting with the red, these electrical independence between the PSMS trains, between the PSMS and the PCMS, and between main control room, remote shutdown room, and I&C equipment rooms, is maintained through the qualified fiber optic data cables. These are again the red lines you see in different places, here.

For the green lines, for instance, here and here, electrical independence between the PSMS and the DAS is maintained through qualified conventional electrical signal isolation devices.

Following the blue lines, there's one up here. The electrical independence between the PSMS power sources is maintained through conventional electrical power isolation devices.

Here you see a figure of optical fiber isolation. The optical fiber is used for the digital interfaces in the PSMS. This is for the, sustains just the data links and the control networks. You see, you have an optic cable in the middle. You have a transmitter on one side and receiver on the other.

You go from electrical to optical through the cable then back from optical to electrical with physical separation. Now these fiber optic cables are constructed using only non-conducting materials, and that provides inherent blocking of any electrical faults.

Conventional isolation modules used for hardwired interfaces for the DAS and to and from the PSMS, these isolation modules are qualified for non-safety side faults for both the AC and DC, the value you see, and for both transverse and for most common modes by the isolation tests.

On the left you'll see an analog isolation module. This is used for safety side and non-safety side, the isolation amplifier and current limiter.

MEMBER BROWN: That would be the green?

MR. SCAROLA: On the previous slide.

MR. SAMPLES: Now on the other side we have a digital isolation module essentially going the other way from the non-safety side back to the safety side, photo coupler and an over voltage protection design.

Now for communication independence, the data is communicated between PSMS divisions, and between the PSMS and the PCMS. Communication independence allows two different digital systems to exchange data while ensuring that there's no potential for one of these digital systems to alter the execution of the other one in any way.

The PSMS meets all the communication independence guidance of ISG-04. Now there's only two types of on-line inter-division communication interface methods used in the PSMS. There's the point-to-point data link. It's for communication between the RPS trains, between the RPS, the ESFAS, and multi-drop networks used by the unit bus interface to the PSMS.

Both types of communication assure independence using two-port memory, separate communication processors separate from the functional processors, and unalterable memory.

What you're seeing in this figure on the top here is a picture of one computer sending data to another one. The one on the left goes through an optical fiber into a data communication interface module, and then there's a CPU module on the right.

Now all communications --

MEMBER BROWN: May I ask one, I just want to clarify something to make sure I understand it. Go back to your previous slide.

MR. SAMPLES: This one.

MEMBER BROWN: Point-to-point data link between RPS trains.

MR. SAMPLES: Yes.

MEMBER BROWN: Okay, I got that. That's where you're sending trip data from one to the other, and between RPS and ESFAS. Now that's within a train. On your diagrams, I did not see with external, from train to train communications from an ESFAS CPU unit to another train anywhere.

MR. SCAROLA: Go to Slide 12.

MEMBER BROWN: That's what I was looking

at. I don't see anything going from the safety buses within Train A, the ESF is, there's no, it's not like if I go back and look at the RPS block where there's communication between Train A and Train B from the ESF subsystems A1 and A2.

MR. SCAROLA: Okay. If you look at this figure you see four divisions of the RPS, right?

MEMBER BROWN: Yes.

MR. SCAROLA: Each one of those divisions is sending data links out to the A-train of the ESF.

MEMBER BROWN: I got that.

MR. SCAROLA: And to the B-train and to the C-train and to the D-train.

MEMBER BROWN: I understand that. That's coming from the RPS to Train A, B, C, and D, of the ESFAS.

MR. SCAROLA: I think part of the inter-division that we're talking about --

CHAIR STETKAR: I think part of the confusion is, RPS here is not reactor trip. One function of RPS is reactor trip.

MEMBER BROWN: No, I understand that. I got that John, okay. I'm looking at this from a, where do I have to look for data communications? They go through all this laundry list, and I'm not going to talk about it because they cover it on Slide 67.

CHAIR STETKAR: But my understanding, let me make sure I understand it, because my understanding is the only inter-train communication A, B, C, D, is at the RPS level.

MEMBER BROWN: That's what I was saying.

CHAIR STETKAR: Is that correct?

MR. SCAROLA: That's not correct.

CHAIR STETKAR: That's not correct?

MR. SCAROLA: In this picture, that's what I'm trying to point out. What you said is right for the parameter voting. If I want to vote on pressurizer pressure I do that in the RPS.

But once an RPS decides it needs to actuate an engineered safety feature, that RPS signal now goes down to the ESFAS which you see in this drawing. And the ESFAS does a second layer of voting, two out of four voting, from all four RPS trains.

CHAIR STETKAR: So each RPS train goes to all four.

MR. SCAROLA: These are all data links but from RPS to ESF.

CHAIR STETKAR: Okay, thanks. I'm sorry. Yes, now I get it. I'm sorry, Charlie.

MEMBER BROWN: I understand this. This is still RPS trains feeding the ESFs.

MR. SCAROLA: Correct.

MEMBER BROWN: There's no links, ESF subsystem to ESF subsystem, they come from the RPS. I understand. That's the point I was trying to make sure I understood.

MR. SCAROLA: Correct.

MEMBER BLEY: But there's no intercommunication at the ESF --

MEMBER BROWN: There's no intercommunications at the ESF submodule level. It all comes from RPS. That's all I was trying to make sure I understood. I understand the voting point. It's a matter of where I'm going to pay attention to later which you cover on Slide 67. So I'll wait until I get there instead of interrupting this conversation. You've been very patient. Okay, where are we?

CHAIR STETKAR: We're at 49 or 50.

MEMBER BROWN: We're not at 67.

CHAIR STETKAR: We're not on 67.

MR. SAMPLES: I think we just moved past 49 into 50. I was explaining that this figure is, again, it's one computer talking to another and the data was going across the fiber optic cable. Data communication interface module here is separate from the CPU module.

Now all communication uses a two-port

memory. The two-port memory, you can see it here. There's a separate communication controller. It has its own processors here in this module. There's a separate CPU function process, it's over here in the CPU module.

Now the functional processor and the communication processor accesses its two-port memory asynchronously. What's going to happen is, this data is going to be coming into the communication module. It's in the buffer. The communication controller is going to write it to the two-port memory.

Now going on asynchronously, whenever the CPU module needs information it will go over here and read the information out and pull it into the CPU module and use it as it is necessary. Now these signals are transmitted. They have a predefined format, length, and message content. And anytime a signal doesn't meet those requirements it's just ignored.

If you want to know more about the control network, these control networks are the multi-drive networks, the ones for the unit box and the four different safety buses.

MEMBER BROWN: Let me ask, let me go back a slide again. And I think I got this out of the reading of it, I just want to confirm my understanding.

The F-ROM is where you actually operate and control the, you don't download your basic, your operational application code into a faster, more speedy RAM or anything like that. I thought I saw the words "operate out of ROM." So my thinking is correct?

MR. SCAROLA: Correct.

MR. SAMPLES: Yes. Yes. So the control network, this is the multi-drop networks, the ones we use for running across the safety bus. They use the IEEE standard 802.17 Resilient Packet Ring protocol.

So what you're going to see her on the left side is the network operating normal conditions. There are several nodes. For each node you have communication, control network interface module here with communications going on. You have a controller.

You notice there's a two-port network in the interface module. They're showing six different of these nodes. Each of these nodes through communication control are going through an optical switch. We have the equivalent of point-to-point data links so, for instance, this node here on the bottom, a point-to-point link to the one up here. The same link here.

They're connected redundantly in the sense, you know, not just going clockwise, you also have counterclockwise connections. The signal is transmitted continuously regardless of what the data change is.

And what each node is going to do is it maintains an entire memory map of the entire network. And then when they transmit it, they transmit that whole memory map to the next, and each node updates the information as necessary. Memory information goes into the two-port network and it's there, so when the controller needs to access it, they access it again asynchronously and just reads out what it needs.

To the right you see an example of what happens when the node fails, say, the bottom middle one fails. In this case the network will adjust, bypass the failed node to ensure that you have data communication continuing.

In a case where you have, say, a failure of another module, a switch, a cable, some other component of the network, then the network will adjust using the IEEE Resilient Packet Ring protocol.

MEMBER BROWN: So the redundant paths are both bypassed so that you don't use the redundant path for the data flows?

MR. SAMPLES: They're transmitting the same information back and forth both clockwise and counterclockwise all the time.

MEMBER BROWN: Even though that node has been lost?

MR. SAMPLES: Yes. It just automatically, the switch automatically adjusts to bypass, with this example.

MEMBER BROWN: Is that an active switch or a default, loss of power?

MR. SCAROLA: It's a passive optical prism, where a spring holds the prism in one position and if it loses power, or if the node tells it that it's not being powered any more, then it's like a relay. It just springs back to a alternate position.

MEMBER BROWN: An optical relay function?

MR. SCAROLA: Basically an optical relay. So when it springs back it self-heals as you see in that other picture. Normally --

MEMBER BROWN: Well, it doesn't heal, it just bypasses the node.

MR. SCAROLA: That's healing. That's self-healing. It self-bypasses that node.

MEMBER BROWN: That's fine.

MR. SCAROLA: Now we also have the ability to manage a completely broken optical cable, or if the optical switch completely fails, because you have a bi-directional data path counterclockwise as well as clockwise. So if a node can't send data via the clockwise direction because the cable actually broke, it'll send it the counterclockwise direction.

MEMBER BROWN: If a prism didn't switch properly, then you'd break both paths.

MR. SCAROLA: That's effectively a broken cable. That's the same as a broken cable. So if the prism doesn't switch, now you have a signal path to another node via the opposite direction on the ring. Because you can get from any node to any other node via two paths, counterclockwise or clockwise.

MEMBER BROWN: It's just you don't have a circular path any more.

MR. SCAROLA: You don't have a circular path any more. You just have a point-to-point path.

CHAIR STETKAR: Ken, do the operators know when those contingencies have been invoked? I mean do they get some sort of trouble alarm in the control room? I mean obviously, you know, there must be LEDs or something on the individual cards --

MR. SCAROLA: Well, they'll get alarms in the control room if there is any self-diagnostic detected failures. The extent that operators will actually repair these versus technicians --

CHAIR STETKAR: Operators will not do this. It's just so that they're aware of that they might be in a degraded condition, that's all.

MR. SCAROLA: One nice thing about this, that design, is it's a handful of parts that's used everywhere in the whole plant. So it's not inconceivable that we can train operators to go get the spare part and replace Module XYZ. It's not inconceivable. We're not there yet, but --

CHAIR STETKAR: It's not inconceivable, but I wouldn't bet the farm on it.

MEMBER BROWN: Well, aren't these A, B, C, D, E, and F, aren't those equivalent of a pull-out card in your card rack?

MR. SCAROLA: Well, yes.

CHAIR STETKAR: That's okay. Operators typically in nuclear power plants don't go fool with that stuff.

MEMBER BROWN: Well, that's fine. I'm just saying from the ability to recover at some point, it's not a major deal to do it.

CHAIR STETKAR: No.

MR. SCAROLA: Self-diagnostics are going to tell them Cabinet 4, Rack 3, Module 6 has failed, and there is only about six different modules in the whole system. Not beyond comprehension, I mean, maybe. Maybe. We're not there yet.

MR. SAMPLES: Okay, I'll move on down.

MEMBER BROWN: You didn't talk about the real-time performance of this network. You said you were going to talk about it at some point.

MR. SCAROLA: Yes, this is probably the best place to talk about it. This is a one-gigabit network, which means all data is updated every 100 milliseconds on this network at the maximum node capacity of 256 nodes. We won't have 256 nodes, but if we did, it's 100 millisecond update time for all data every cycle.

And as Pat said, the entire memory map is transmitted from node to node and it's a fixed memory map. So each node knows where its data is in that memory map, and when it gets the map it updates its data, and then passes the whole map on to the next node.

MEMBER BROWN: So what you're telling me is the safety bus, is that the one I'm talking about? It's within this, is this the internal CPU communications? I asked a little while ago about bus mechanics, you know, the server, the unit bus, and the safety bus. You said the unit bus is the same as the safety bus. Is this the safety bus?

MR. SCAROLA: This is the control network technology. It's used for both the safety bus and the unit bus. It's only one MELTAC technology for multi-drop data communication that we call a control network in the MELTAC language. In US-APWR, we call it one application of this control network is the safety bus. Another application of this same network technology is the unit bus.

MEMBER BROWN: Okay, you said but the refresh is every 100 milliseconds.

MR. SCAROLA: Correct.

MEMBER BROWN: That's a long time.

MR. SCAROLA: Come on.

MEMBER BROWN: Well, I mean you're processing data. I mean when I look at your complete input to output data processing, I think the number you mentioned a little awhile ago is somewhere, it's like 300 milliseconds from input to output. That means 100 milliseconds is eaten up on this data transmission path to refresh all of your plant parameters. And then if you look at the ten-bucket sample period, that for application code, I'm trying to figure out where all that works into your, does that become involved in the time response?

MR. SCAROLA: It's all considered in the

time response --

MEMBER BROWN: Yes, I understand that. But now the MELTAC processing for application code said it could be anywhere from 20 milliseconds to 100, to one second, excuse me, 1,000 milliseconds. So somewhere you're getting data in, and I'm trying to figure out how often you're getting data that gets into the calculations, the functional calculations for your parameters.

MR. SCAROLA: Okay. Why don't we discuss that when we show you the slide on response time propagation.

MEMBER BROWN: That's fine. I'm just bringing the point up, that's all.

MR. SCAROLA: It's a better place to talk about it.

MEMBER BROWN: Okay.

MR. SCAROLA: We have a slide specifically on response time.

MR. SAMPLES: It's several slides ahead, but yes, we do get to it.

Some more communication independence, this time independence from signals coming from outside that could reprogram. Now the on-line Flash-ROM is protected from alteration in this way. See here, the on-line chassis? When the CPU module is inside this, the write enable signal is not enabled. You can't write to it. You can't write to it if it's inside. In order to write to the F-ROM you have to actually pull it out, put it inside a dedicated reprogramming chassis. In this chassis there's connection made that enables the write enable signal, and allows you to reprogram it using the MELTAC engineering tool.

Similarly, the ROM and the FPGA is only reprogrammable outside of the module chassis but only at the factory. There is no reprogramming chassis for them. So essentially these features are ensuring there's no potential for inter-divisional data communication to alter the software either basic software or application software inside these CPU modules on-line.

MEMBER BROWN: Okay, let me ask one question. I don't have any problem with what you're telling me here, it's just I mean these are flash electrically erasable, read-only memory, at least that's according to the words, which electrically erasable means electrically erasable. You can change it.

And I guess if I'm in the application mode, I've got it in the normally installed configuration operationally, how have I bypassed or prevented some input coming in and modifying the set points application code, what have you, which are stored in that ROM?

I mean it is electrical erasable so, now there are ways to prevent that but the ones I'm familiar with, and I'm not familiar with all of them, are it's the way it's hardwired to make sure that that input port is not accessible at all, or it's grounded or something like that.

And there was no discussion of that as to why that was, how it just said it couldn't be changed. That's all it said. And sometimes I get just like John. There's a detail that you'd like to have as to how do you, in fact, do that? Is it a hardware or is it a software turn-off of that bit that allows it to be electrically erased?

MR. SAMPLES: No, it's hardware. I may not have explained this clearly, but you do have to have a hardware signal that actually enables you to write to the module to the F-ROM, and it's disabled within the on-line chassis. It just isn't enabled. There's no connection made and you can't make it.

MEMBER BLEY: When it's plugged into the cabinet you can't get to it.

MR. SAMPLES: The on-line chassis, yes.

MEMBER BROWN: The pin is disabled.

MR. SCAROLA: That's what this figure is trying to show. The figure on the left is showing that the write enable pin of the F-ROM is an open circuit.

MEMBER BROWN: So it's physically when you transfer it, you --

MR. SCAROLA: Now we close the circuit when we --

MEMBER BROWN: I just wanted to make sure it wasn't a program when you plug it in now it feeds back and says, okay, you can't write it any more, which can get lost.

MR. SAMPLES: The hardware is open signal. You can't write to it even if you were to connect and try to write to it. You have to pull it out to the dedicated chassis which --

MEMBER BROWN: Yes, I read all that part. When it's in the chassis, the operational chassis, how did you ensure it? You've answered the question. It's an open circuit.

MR. SAMPLES: Okay.

MR. SCAROLA: This was originally an area where we did not fully comply with ISG-04. And this was a design change we made to comply with ISG-04 which strictly says you must have a hardware method of preventing rewriting.

MEMBER BROWN: Good.

CHAIR STETKAR: Now let me -- no, no. Go to the next slide and stop. There are five slides on functional independence. I have a meeting that I must attend at noon. Is there a chance that we can get through these five slides in 15 minutes? I see shaking of heads. I don't want to necessarily break a conceptual topic in the middle because people have to run off for lunch.

So now we have another little bit of a sticky situation is that we have another closed session scheduled at 1 o'clock with the staff. And for a variety of reasons I don't want to interrupt that.

So what I'd like to do now is break for lunch. MHI and company, if you could return from lunch at about 1:00, be outside at 1:15. We have to close the meeting to you at 1:00 for a variety of reasons.

MR. TAKASHIMA: And also for Luminant.

CHAIR STETKAR: And Luminant also, anybody who is not staff.

MEMBER BLEY: But it's on this topic?

CHAIR STETKAR: It's on US-APWR. So just to make it clear, we'll break for lunch now. We'll ask the staff to return at 1 o'clock, and we'll ask everyone else to be available outside at 1:15. We don't know whether it's going to run 15 or 20 minutes. I'm not going to let it run longer than 20 minutes. If I can hold it to 15 we'll reconvene at 1:15. And with that we'll recess for lunch.

(Whereupon, the foregoing matter went off the record at 11:47 a.m. and went back on the record at 1:01 p.m.)

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

(1:37 p.m.)

CHAIRMAN STETKAR: Okay, we're back in session. And this is an open session. So we're continuing where we were this morning. Back to you, Richard.

MR. SAMPLES: Okay, let's move on to functional independence now. Each PCMS division receives data from outside its own division. The data comes from other PSMS divisions, from the PCMS, and from DAS.

Functional independence ensures that the data received from the outside divisions can't adversely affect the safety function being performed within that division.

We explained this functional independence individually for each sub-system of the PSMS, RPS, ESFAS, and SLS, because it's done differently. For detailed conformance, that's described in the Technical Report, Safety I&C System Description and Design Process.

Now, this figure here depicts functional independence as we achieve it in the RPS and the ESFAS. You see that the following signals are received from across the PSMS train boundaries, reactor and ESFAS partial trip status signal for the two-out-of-four trip voting logics.

The ESFAS status signal of each trip parameter for bypass interlocks, bypass allows the channel be tested and allows failed channel to be taken out of service. Now, authenticated messages can have spurius data or frozen data. And each train --

CHAIRMAN STETKAR: Up front, just be careful to not hit your microphones, because our recorder has very, very sensitive things in his ears and it really bothers him. Thank you.

MR. SAMPLES: So authenticated messages can have spurius data or frozen data, and each train protects itself.

Essentially, each PSMS train is assuming that the data coming from another train, it could be wrong, it could be failed. So it protects itself. There's no reliance at all on the data coming from the other division being correct.

And these are some ways that each train protects itself. First of all, for a partial trip the two-out-of-four voting logic prevents a spurius trip and ensures a trip when there are single failures.

And if you have all inter-division data communication to fail, each division will initiate a reactor trip and ESFAS.

Now, the bypasses, there's first-in blocking logic that prevents having more than one bypass channel. So once you have the first one bypassed you can't have bypasses at the others.

CHAIRMAN STETKAR: Something you said, and

I want to make sure I understand it. You said if all inter-division data fails, each division will initiate a reactor trip and ESFAS. Will it initiate an ESFAS signal? I understand it'll initiate a reactor trip. Will it initiate an ESFAS signal?

MR. SAMPLES: It does initiate a reactor trip. It does --

(Off microphone comments)

MR. SAMPLES: In this case it does initiate --

CHAIRMAN STETKAR: If communications fail you get a high output for ESFAS actuation.

MR. SAMPLES: You'll get an actuation signal.

CHAIRMAN STETKAR: Oh, okay.

MR. SAMPLES: Now, the following HSI signals are transmitted to the PSMS from the operational VDUs that are part of the non-safety PCMS. These are component position commands, maintenance bypass commands, operating bypass commands, ESFAS reset commands, and component lock commands.

Now for all of these signals, the unalterable priority logic within the PSMS ensures that each PSMS division protect itself so that safety function can't be adversely affected.

MEMBER BROWN: How do they get there? I've got to go back and look at one of your diagrams.

MR. SAMPLES: You're asking about --

MEMBER BROWN: Yes. You've got all this stuff, I guess this connects a lot of dots, or some dots, ESFAS reset commands, component position commands.

MR. SCAROLA: These are the signals that come from the O-VDUs, the operational VDUs, via the unit bus.

MEMBER BROWN: And then down to the safety bus?

MR. SCAROLA: And then down into the COM, then into the safety bus, and then back to the RPS.

MEMBER BROWN: So in order to do that they go into that safety bus, I'll just refresh my memory. I have to go back to that control network technology. That's the concept that's used, right?

MR. SCAROLA: Well, you can --

MEMBER BROWN: And again, it's been awhile since I looked at this kind of stuff, that's a LAN.

MR. SCAROLA: That was a resilient packet ring.

MEMBER BROWN: I have no idea what the difference is. But you showed six data input devices. I guess there could be more. But they are all dumping information onto that, one going in one direction, the same data going the other direction.

So they're all dumping the information onto those two buses. Something's controlling the timing. Can you saturate that bus in terms of how is that prevented?

MR. SCAROLA: All data's transmitted every cycle. And there's a packet of data where the first section of that packet represents the first node on the network.

The second section of the packet represents the second node all the way up to the nth node on the network, up to 100-and-something nodes.

MEMBER BROWN: You showed six, right?

MR. SCAROLA: Yes. We only showed six. You could have as many as 100-something nodes. But every data map is the same. It's not dynamic. It's a fixed location in memory.

So what happens is when a node needs to update data, when it needs to send data, it puts new data in its section of the packet and then just passes the whole packet onto the next node.

So as the packet of data goes around, each node is updating its piece of the packet. But the packet is the same every time.

MEMBER BROWN: Its' fixed. It's a fixed number of bits, bites, whatever it is. The field length is fixed.

MR. SCAROLA: Fixed, and the data rate is fixed.

MEMBER BROWN: So the only thing that --

MR. SCAROLA: And the destination is fixed. Now remember, if I'm a node, I only send to the guy next to me. That's as far as it goes. It's a point-to-point data link. Then he sends it on to the next guy.

MEMBER BROWN: But he adds his onto it.

MR. SCAROLA: He doesn't add, he updates his piece. He updates his piece. He doesn't add anything. Because that data's always there.

(Crosstalk)

MEMBER BROWN: So he would take whatever part of that packet is his node's territory --

MR. SCAROLA: Correct.

MEMBER BROWN: -- or field length.

MR. SCAROLA: To make it right.

MEMBER BROWN: He updates that field length and it just goes into the -- he replaces the old with the new.

MR. SCAROLA: Right. And it may be exactly the same data. Because a lot of the data, cycle to cycle, will never change.

MEMBER BROWN: Yes, I understand that.

MR. SCAROLA: But he still writes it, no matter what. He still updates it. He still updates with the same data again, over, and over, and over again. So the data transmission is completely deterministic.

MEMBER BROWN: So every node, though, is shifting from one node to the next all the way around. They're all doing that simultaneously --

MR. SCAROLA: All doing it simultaneously.

MEMBER BROWN: -- as they are putting data in. So it's not like a router-based LAN where you can have collisions, and clog up the highway, and you can't get out of one place and into the others.

MR. SCAROLA: That's why we can use this technology for the safety bus, because it's 100 percent deterministic.

MEMBER BLEY: But if there's an interruption anywhere along, the whole train is derailed.

MR. SCAROLA: For some milliseconds, until it reconfigures.

MEMBER BLEY: But if it's still going node to node, if there's a problem, if one node --

MR. SCAROLA: It might never get passed.

MEMBER BLEY: Just a minute.

MR. SCAROLA: Every five milliseconds this network is sending out, in addition to this data packet that we talked about, each node sends around what's called a protective packet. And that packet goes out every five milliseconds to make sure that every node is still there.

MEMBER BLEY: Still there and working.

MR. SCAROLA: And if one node is not there, then that packet reconfigures the network to say, hey, that's a missing node.

MEMBER BROWN: But that's got to be part of each 100 millisecond packet, doesn't it? It's not a different --

MR. SCAROLA: It's actually every five -- that goes out every five milliseconds. The 100 millisecond packet --

MEMBER BROWN: Why didn't it run into the one that's sitting around, hanging around in a node?

MR. SCAROLA: Because it's going on in the spaces in between the 100 millisecond transmission. There's a lot of dead time in this network.

So what's happening is this node is sending out this protection packet every five milliseconds.

But at the 100 millisecond point, now it sends out the data packet. And it sends out the five millisecond packet.

MEMBER BROWN: So the lines are not blocked --

MR. SCAROLA: The lines are never blocked.

MEMBER BROWN: -- in between.

MR. SCAROLA: Correct. They're not blocked.

MEMBER SHACK: But it's bidirectional, so it's sending to this node and to that node.

MR. SCAROLA: To the left and to the right --

MEMBER BROWN: Yes. It goes to the left and the right.

MR. SCAROLA: -- via separate data transmission packs. There's a data buffer to go to the right and a data buffer that goes to the left. So they actually work completely independently as a buffer.

MEMBER BROWN: Now the two directions are controlled by a separate machine to keep that data moving through there?

MR. SCAROLA: Well, it's what we call the communication interface module, which is one of the modules that you saw --

MEMBER BROWN: I don't know why I didn't read this thing.

MR. SCAROLA: -- that's completely separate from the CPU module, which is actually asynchronously running the safety applications.

So you have a CPU that's looking at all the field inputs, looking at all the inputs, and running the bistables, running all the functions for the application, running completely asynchronously from this data communication that's running around the network.

MEMBER BROWN: Yes, I understand that. And that was what was bothering me relative to the asynchronous transmission, because they're all running all trains. All CPUs are running on a different clock, well, the same frequency maybe. But they're not timed. They're not synchronized.

MR. SCAROLA: Nothing's synchronized.

MEMBER BROWN: So everything's just coming in randomly to these based on their particular clock, wherever they are relative to this synchronous performance, asynchronous performance.

MR. SCAROLA: We say it a little differently. All the data is being updated in that two-port memory. You might say that's random, because that's basically going on on this ring.

But if I'm the CPU that wants that data, I fetch it when I want it. It doesn't get pushed to me when the network wants it. The network only puts it in this thing we call a two-port memory.

And when the CPU that's executing the logic functions says it needs the data, it's ready for the data, it goes and gets it. It's a fetch operation, or what we call a read operation.

It's a pull, not a push. There's no data pushed into the CPU. It's pulled from that two-port memory by the CPU. So the CPU controls it 100 percent.

MEMBER BROWN: I'm lost.

MR. SCAROLA: You're lost.

MEMBER BROWN: I understand the difference between fetch and push. But the safety bus is what transmits all that stuff down to the SLS. And that has no pull to it. The data's not there.

MR. SCAROLA: Yes, but --

MEMBER BROWN: It's got to wait for the packet to go through its 100, whatever it is before it gets around. It's got the flags and the tags that says, hey CPU, this is my data. And he pulls it out at that point. He's waiting.

MR. SCAROLA: No. He doesn't wait at all.

He reads that CPU probably five times before the data actually gets refreshed. He might get the same data over and over again.

For example, if the CPU has a 50 millisecond cycle time, but the network has 100 millisecond cycle time, the CPU may read the data, same data, read it again, same data. But, oh, now I read it and it's updated. The CPU has a completely asynchronous cycle.

MEMBER BROWN: So it's pulling from whatever packet happens to be there at the time it asks for information.

MR. SCAROLA: Correct. Only from the sections of the data map that it has any interest in. It may only be interested in the data from Node 3 and Node 7. Well, it doesn't look at any of the other data.

MEMBER BROWN: So it's polling the nodes.

MR. SCAROLA: It pulls the data from that memory, not polling, pulling.

MEMBER BROWN: I understand what you're saying. You're saying it's not the same as polling. But effectively it's looking into its nodes. And there's information there and it pulls it out.

And information may be good information, it may be bad information, or it may be the same information. I don't want to argue about good and bad.

MR. SCAROLA: Right. The only way we can distinguish good and bad is by data at correctness format language.

MEMBER BROWN: I really don't want to get that started, that discussion, right now.

MR. SCAROLA: If a source node is saying the valve should be open, but it's a point in time in the plant, that transient, where the valve should actually be closed, it could be an erroneous signal.

And that's what Pat is trying to explain, that if it is erroneous, the protection system is going to protect itself against that bad data by doing its safety functions in a higher priority than any of this other data may demand.

MR. SAMPLES: I am not sure we've answered your question or not.

CHAIRMAN STETKAR: I'm not sure we have.

MR. SAMPLES: You still have that puzzled look.

MEMBER BROWN: I have a slow integration factor, so --

MR. SAMPLES: Maybe we can move on and --

MEMBER BROWN: Yes, we ought to move on.

CHAIRMAN STETKAR: Move on. He's not shy about going backwards.

MR. SCAROLA: Now we see some typical priority logic. This is for manual operational signals. One example that you're seeing is that the unit shows you safety switches, examples of soft switches and safety VDU, operational VDU. And that's safety VDU over here.

Now on the top here, this priority logic here is going to ensure that signals from these safety VDU switches always have priority over any signal from the operational VDU, so that your safety signals always get more priority than any kind of non-safety signal.

Down here what's going to happen is there's more priority logic. But this priority logic does something a little bit different. It ensures that automatic signals, signals going through automatic actuation such as the ESFAS here, higher priority over manually initiated signals.

The reason that is, these automatic signals are going to be safety, and the manual signals coming from the operational VDU are non-safety. And they could be wrong, could be spurius.

CHAIRMAN STETKAR: Let me ask you a question about that. I tried to think through a lot of stuff, but I'm pretty burned out.

There are some valves in the plant called the emergency feedwater control valves and emergency feedwater isolation valves that have two safety functions. One is to close and one is to open. How does SLS know which one it ought to do? Because they're both safety functions.

MR. SCAROLA: That question is, is it pertinent to the next slide?

MR. SAMPLES: I think it's the next slide.

CHAIRMAN STETKAR: Is it, okay, sorry.

MR. SAMPLES: There is yet one more kind of priority logic. Let's go ahead and talk about it now.

MR. SCAROLA: Now, before we go to that slide, the slide we were on is simply discussing priority of safety signals over non-safety signals. We're not talking about state-based where we have to determine, well, if I've got two safety signals --

CHAIRMAN STETKAR: Well, I mean in some sense it, yes, this thing knows that, in this little cartoon, it knows that it's better to start a pump than to stop a pump.

MR. SAMPLES: In this one, no.

CHAIRMAN STETKAR: In this one?

MR. SAMPLES: It just knows that whatever safety signal you're getting is why that presumably the safety signal would be doing the correct thing for safety. The manual signal could be doing the right thing too. But it just ignores it has a safety signal.

CHAIRMAN STETKAR: Okay. Let's get to the other one. Because I still want to understand how those valves know which way they ought to go.

MEMBER BROWN: Before you leave that, there's the little box. Look at the operational VDU. There's a start and a stop switch. And there's two little boxes below those. Are those supposedly And boxes?

MR. SAMPLES: Yes.

MEMBER BROWN: So in order for the operational VDU to start something it has to have a particular signal from the safety VDU. I know it's got a line coming from it via that little X box, whatever the X box is --

MR. SCAROLA: What it's saying is --

MEMBER BROWN: -- from a start line, which was Ored, from either the start or the stop in the safety VDU.

MR. SCAROLA: All it's saying here is that for the operational VDU to do anything, either start or stop, there must be no signal from the safety VDU. If there's either signal from the safety VDU, then the O-VDU is blocked. That's with that inverter going into the AND gate means.

MEMBER BROWN: Okay, it's a Not then.

MR. SCAROLA: That square is an inverter.

MR. SAMPLES: These squares with the bar, that's an And. Circular, that's Or gates.

CHAIRMAN STETKAR: So all that says, even if you're trying to start it from the safety VDU, you could push start on the operational VDU all you want to. And there will be no output.

MR. SCAROLA: There will be nothing happening. If you are controlling from the safety VDU, the O-VDU will do nothing.

MEMBER BROWN: What's this software switch? That turns off the software and the other one starts the software, or disconnects your processing?

MR. SAMPLES: No. You push a button on the soft switch. Hard switch will be like if you turn the light switch off in a room like this, a hard switch. Push the button on a touch screen, that's a soft switch.

MEMBER BLEY: The software is processing it. It's not hard wired from point to point.

MR. SAMPLES: It's made out of software.

CHAIRMAN STETKAR: They only distinguish that because they have conventional switches that are apparently real switches.

MR. SAMPLES: That's touch screen. This figure shows an interface between the PSMS and the DAS. And what we're interested in here is this green box down in the power interface module.

Down here, these conventional solid state circuits implement a different kind of priority logic. this is state-based priority logic. Now, you notice that we have the DAS on one side and the PSMS over here.

Both are giving signals into the power interface modules to operate a component. When this component, such as a valve, we just select a safe state and a non-safe state. For a valve, oftentimes the safe state is closed, the non-safe is open.

In here, what this priority logic does, regardless of where a signal comes from, either PSMS or DAS, it gives priority to the signal that will acuate it to its safe state.

MEMBER BLEY: Although the two arrows coming out of the CPU look the same, one of them is an arrow that's a safe state signal, and the other one is an arrow that's a non-safe state signal.

MR. SCAROLA: Like an open and a close, or a start and a stop. So this logic then just gives one of them priority. And as you said, John, we do it based on each component state.

But we do have these few components in the plant, like emergency feedwater isolation valves, where it's difficult to determine the safe state. So there what we do is we look at the normal state of the valve.

And we say emergency feedwater isolation valves are normally open. And if they were to ever close spuriously by an erroneous signal, we get an alarm. And we put that up on this BISI thing. Because that disables the emergency feedwater system. So we take credit for the alarms that would spuriously close these things during normal operation. So therefore we can assume that these valves are open all the time. Because if they're ever not open, they're immediately alarmed and the operators can solve the problem.

So for the emergency feedwater isolation valves, we define the safe state as closed. Because that's the state that they need to automatically reposition to if there's an accident.

CHAIRMAN STETKAR: Where is that documented?

MR. SCAROLA: In the D3 coping analysis.

CHAIRMAN STETKAR: In the D3 coping analysis? That's one place I didn't go.

MR. SCAROLA: Because it's dependent upon the accidents. We have to look at the accidents and we've got to say, well, how are we going to protect for that accident.

And what you're talking about is how do we isolate a faulted steam generator, which is the issue. We need to be able to make sure we're not --

CHAIRMAN STETKAR: Well, that's the issue with one sort of philosophy, the philosophy you just described. I'm trying to understand how --

(Crosstalk)

MEMBER BLEY: To have that valve actually shut, and get an open signal and a shut signal, isn't going to happen. It's really unlikely. That valve's going to be open almost all of the time.

MR. SCAROLA: Now, if you're asking where do we document the safe state for every component, the answer is that's part of detailed design. We have not gotten that far yet.

CHAIRMAN STETKAR: There are some statements in the DCD that says for, I don't know, almost all or for something like that, the safe state is, I forgot, is well known, or something.

You want to start and EFW pump for example. But for a few things, the example I used, EFW isolation valves, and I didn't try to think of other things, but --

MR. SCAROLA: It's pretty clear that if the purpose of the engineered safety feature is to get water from Point A to Point B, that we want to have a flow path open, right?

CHAIRMAN STETKAR: Right.

MR. SCAROLA: And it's also very clear that if we are trying to isolate main steam isolation valves, or isolate the containment, the safe state's closed. So those are the easy ones.

CHAIRMAN STETKAR: Those are the easy ones.

MR. SCAROLA: But there are some --

CHAIRMAN STETKAR: A few of the other ones, like safety depressurization valves, EFW isolation valves, where it's not as clear, especially if the safe state is preventing operator intervention.

MR. SCAROLA: But what makes this whole common cause failure thing very difficult to deal with is you have these two systems. And you can never know, at any point in time, which one is wrong and which one is right.

So you can't give the systems themselves priority. You have to look down at the components and say, well, where do we want this component to be. And that's what this little logic does.

Now before, Charles, you had asked about is there a common cause failure in that PIF module. And I said, well, it's so simple we can do 100 percent testing. And this is representative of that logic in that module. That's how simple the logic is.

MEMBER BROWN: What's the X?

MR. SCAROLA: That's an inverter.

MEMBER BROWN: Okay, I think --

MEMBER BLEY: Logically, it's a Not gate

MEMBER BROWN: I missed the definition when they were running through their discourse a minute ago.

MEMBER BLEY: So I think I asked this several years ago. And I think I remember the answer, but I'm not sure.

So should the real world come up with an oddball scenario where our logic isn't working right, and it keeps a valve shut that somehow today I need to open, how can the operator override the signals that are keeping it closed?

And it's not an easy to get to valve with a handwheel on it. Is there any way? My memory was the answer is no. It's going to stay closed.

MR. SCAROLA: He could use a different train.

MEMBER BLEY: But this one valve he can't move. But something happens that generates the logic that says go to the failsafe condition. And just today we really need that valve open, or one of those multiple valves open.

MR. SCAROLA: Let me address it two ways. Let's assume that the spurius signal that's holding that valve closed --

MEMBER BLEY: It might not be spurius.

MR. SCAROLA: Well, whatever the signal is, is coming from the DAS. The operators have a DAS defeat switch.

MEMBER BLEY: That's true.

MR. SCAROLA: They can defeat the DAS and shut off the DAS so the DAS stops sending signals. So for that one, we can defeat it. And now we can let the safety system do whatever it wants to do. On the other hand, on the safety side, we don't have a defeat switch.

MEMBER BLEY: There's just no way we can get that valve open if we need to?

MR. SCAROLA: If the safety signal is keeping --

MEMBER BLEY: Well, without going in --

MR. SCAROLA: Well, if the safety signal is sending the safe state signal, and the operator will ultimately --

MEMBER BLEY: Which all our analysis said will always be the safe state, but today it's not. We're stuck.

MR. SCAROLA: So they have to use a different train.

MEMBER BLEY: Yes. But all the trains are getting the same signal, because it's a condition where we would have generated the safety signal. But we just weren't complete enough in our thermohydraulics analysis, or whatever, to get it right.

MR. SCAROLA: Now, I guess we could make an argument that the operators can pull the module out of the rack. But I know you don't like operators pulling out modules.

MEMBER BLEY: Well, we don't like that. But if you've got no other choice --

MR. SCAROLA: I don't have an answer other than that.

MEMBER BLEY: That would be it, I guess. We used to be able to use --

CHAIRMAN STETKAR: Operators, unless they're really trained differently --

MEMBER BLEY: Are heavily trained not to do this.

CHAIRMAN STETKAR: -- are heavily trained not to mess around with electronic stuff. They don't even like to mess around with electrical things. So I think there would be a very high reluctance among operators, licensed people in the control room, to do that.

MEMBER BROWN: They can call on somebody to go do it that's qualified for that. I presume they have people on the side.

MEMBER BLEY: They can. And within an hour or two they might get --

MEMBER BROWN: Well, that's fine. It's doable. You don't have to wait three months to do it. You can, I guess.

MEMBER BLEY: I don't know for sure if it's even possible.

MR. SCAROLA: Well, yes. If they pull the module, now the safe state signal's going to be gone. And now they can find other ways to manipulate that.

MEMBER BLEY: Then they can turn it on through --

MR. SCAROLA: Then they can manipulate that valve in a different way.

MEMBER BLEY: Of course, can they pull just the PIF module for this one valve?

MR. SCAROLA: Yes. Every component has its own PIF on it.

MEMBER BLEY: And those are accessible, yes. Okay, so there is a way around. But it would be heavily trained against it.

MR. SCAROLA: A little cumbersome.

MEMBER BLEY: That's okay. On the day we're in the SAMGs and we have to come up with a strategy, that might be one we have to do. We used to do stuff like that.

MR. SCAROLA: Now, one thing I will mention is we've done a lot of work in Chapter 18 on risk important human actions, which go down this -- I'm not going to say the P word, because I'll get jumped on -- but it looks like all these special actions that are based on multiple train failures, we do not take credit for the operators doing any of this stuff.

What we do take credit for is the operators find an alternate success path. They don't attempt to open that valve you're talking about. They find another way to get the water in like use component cooling water --

MEMBER BLEY: And they're really good at that.

MR. SCAROLA: -- or a way to inject that. And those kinds of things are probably a lot better success paths than saying, okay, go try and find a way to open this valve.

MEMBER BLEY: I don't have a scenario for that.

MR. SCAROLA: So we do a lot of that evaluation.

MEMBER BLEY: I haven't planned a scenario, but one day Mother Nature might. But I suspect that whenever you get to SAMGs and that sort of thing they'll probably have to deal with this kind of a nightmare. That's my memory of asking this a long, long time ago.

CHAIRMAN STETKAR: Good memory. Let me ask you a question on this. And I actually had a scenario. And it has to do with EFW. And I didn't know I wanted to ask it, so I'll ask it now since we're talking about it.

EFW comes off. I've lost the feedwater. I don't care. The main feedwater goes away. The EFW comes on. All the valves are open. The operators don't do anything.

EFW runs, and runs, and runs, and runs. And the steam generators all fill up, because that's what they will do. EFW doesn't automatically control level, does it?

MR. SCAROLA: Well, EFW turns off at a level setpoint. The valves close at a level setpoint.

CHAIRMAN STETKAR: The valves close from that safety --

MR. SCAROLA: It's not a modulating control, but it is an on --

CHAIRMAN STETKAR: The valves close from that safety signal that isolates the valves.

MR. SCAROLA: Correct.

CHAIRMAN STETKAR: Does that signal seal in, because you say all safety functions seal in.

MR. SCAROLA: No.

CHAIRMAN STETKAR: That one doesn't.

MR. SCAROLA: That does not seal in. That one's a cycling signal. What seals in is the EFW signal that starts the pumps.

CHAIRMAN STETKAR: Okay. Thanks, that helps me. Because I was getting in, there are many, many statements that say all safety signals seal in and can only be reset by manual operator action. That one doesn't.

MR. SCAROLA: Well, the signal --

CHAIRMAN STETKAR: Where I was getting is the priority logic, because if it's sealed in how does the system then know that the valve's got to reopen, because it's got a sealed in safe state signal.

MR. SCAROLA: The EFW actuation signal

seals in at the system level. But the specific signals that go to the valves do not seal in.

CHAIRMAN STETKAR: Okay. Then I understand how it can work. Thanks.

MR. SAMPLES: And I'd like to mention a couple of more things on this slide here before we move on.

In addition to ensuring that the safe state has priority over the non-safe state, this same logic ensures that a failure of either the PSMS or the DAS is not going to block the safety function.

Since we're making the PIF module out of conventional solid state circuits, there's no potential there for software common cause failure.

And if you notice, the isolation module here, the non-safety DAS interface, it's hard wired with this conventional isolator. And there's no digital communication between the PSMS and the DAS.

Move on to the topic of determinism. You're seeing here a CPU module. It's blown up with some internal features shown. You're also seeing a bus master module, which is taking data from plant components and from sensors and pushing it to plant components.

You also see one of the control network interface modules and another bus master module for data link for this case here. All of these functions are executing cyclically with single task processing.

They're operating with a fixed deterministic time cycle in which the predetermined cycle, with the predetermined steps, each step executed in the correct order each time, Step 1 first, Step 2, Step 3, to the end. Every step is executed.

The cycle time is 100 percent reproducible, repeatable every time. There's no change in that sequence at all. So what you're seeing is that the data comes from either the sensors or the control network with the data link.

It's placed here in these little green boxes here. And each of those are two-port networks. That's where the data is placed as it comes in.

MR. SCAROLA: Pat, two-port memory.

MR. SAMPLES: Am I saying two-port network? Two-port memory, I keep saying something else. I'm not sure why. But two-port memory is there and the data is stored there.

Now, you see the CPU module going through its time cycle, the various steps. When it gets to an input cycle, it's going to need data. So what it's going to do is go read data in from each of those two-port memories into its data table.

Now when it's done, it goes to the next step. It's the operations step. We actually use the information in the data table. The next step is just to check it, make sure it's operating properly. And we'll talk about the different checks done there.

The output, in that case, it takes data from the data table and writes it back to the two-port memories. And all of these actions from each of these three here in the CPU module on the top are all done asynchronously.

Again, the CPU module is reading in and writing out. And no data is ever pushed into it. It's controlling its own operation itself. Self- diagnostic features, they're both in a step here. And there's also some other ones in the time remaining section here.

Since they are part of the overall cycle, the self-diagnostics, they don't affect the predetermined fixed cycle at any time. And there are no interrupts here, except by self-diagnostics.

The only time you get an interrupt if one of these blocks senses an error condition, then they'll cause the CPU module to transition to an error state and get a lock.

And this time cycle can't be interrupted by the other trains, or the unit bus, or anything outside of it, just the internal diagnostic --

MEMBER BROWN: Just finish your statement, I'm sorry. I just didn't want you to leave.

MR. SAMPLES: Internal diagnostics. Okay, stay here for something?

MEMBER BROWN: Yes, to try to put a specific event, to make sure I understand this.

MR. SAMPLES: Yes.

MEMBER BROWN: This is executed by every controller, every CPU unit.

MR. SAMPLES: Yes.

MEMBER BROWN: And I'm going to pick an example. I'm just going to take Train A, Controller Group 1, whatever. There's a number of parameters evaluated in that train CPU.

And there are a set of algorithms associated with that process, determinants. Some of them may be simple, numbers higher than this, numbers that are lower than that.

There may be a conglomeration algorithm, which takes other parameters and says you've got to look at it regardless of what it looks like. There are those functions that are evaluated by that controller. Are every one of those functions evaluated on every cycle?

MR. SAMPLES: Yes.

MEMBER BROWN: Okay.

MR. SAMPLES: That's RAM check.

MEMBER BROWN: I'm talking about plant parameter function and recycling. Do I trip, do I not trip, do I operate something, do I turn on a valve, do I whatever.

If those functions are performed every time in that controller, the same applies for the ESFAS controller for the data that gets transmitted to that during that period. Every function is done every time?

MR. SAMPLES: Yes.

MEMBER BROWN: All right. And the output now is at the end of that operation it goes back into to data table where it's then transmitted to whatever other things that need to execute that output, or monitoring, or what-have-you.

It goes out through those other links through the output, the ones you show as output dual port, or two-port memory units, with the bus controller.

MR. SCAROLA: And all completely asynchronously.

MEMBER BROWN: Yes, I got that. And, all right, let's see, I had another question. Where did it go?

Now, you say there are no interrupts. And I'm trying to recall now, at one point in the documents you said there were no external interrupts to this. And I got that.

You did talk about two internal interrupts. And I don't remember the difference. One of them was diagnostics and another one some color peripheral interim map.

I may be saying that wrong, but there were two internal interrupts. And it seems to me you've only talked about one when you've talked about the self-diagnostics. And am I going to have to go find that? That's going to be terrible.

MR. SCAROLA: I actually can't think of any other interrupts --

MEMBER BROWN: But they are internal.

MR. SCAROLA: -- that are not self-diagnostics. But there are two self-diagnostic interrupts.

MEMBER BROWN: All right, that's fine. The fundamental answer I wanted was that this is a single time sample to cycle and that everything is executed in turning, including constant time monitoring in the remaining time, the part of the self- diagnostics that you do in the remaining time you have left over each time.

MR. SAMPLES: Okay. I think the next slide there, similar information on determinism. What you're seeing here is a signal path from a sensor through input modules, CPU modules, other modules in Train A.

And it does pass through a data link into Train B. And the signal eventually reaches the trip breaker for a trip.

The cause of the deterministic cycles of each of the modules that you see here, each of these different blocks, the red and the green, each of these have these deterministic cycles. We can calculate the worst case, the longest time to perform the function in each of them.

Now if you add all these up, the worst case is through here. It's just simple addition. You can see what we'd get worst case for. And this reactor trip function is about 300 milliseconds max.

MEMBER BROWN: So the data link is the transmission from Train B over to Train, and still you're looking at the maximum amount of difference between the asynchronous operations to show those two, the compounding time frames, time steps.

MR. SAMPLES: That's because the data links are deterministic. We can do that.

MEMBER BROWN: Yes. I'm not questioning that.

MR. SCAROLA: And based on the voting logic, no train does anything without voting on data from another train.

MEMBER BROWN: Yes. No, I understand that. I got that. I just wanted to make sure I was totally clear on the picture.

MR. SAMPLES: It's telling us that determinism allows us to calculate worst case, and it's never going to be worse. You can bound, and you can say that 300 millisecond max is the longest time you're going to have for a reactor trip function.

We also have an ITAAC that confirms that the detail design meets these response time requirements as defined in the technical report for a response time on the safety I&C system.

MEMBER BROWN: How does this apply now when you have to then, on a time response for the ESFAS functions, obviously you've got the 300 milliseconds associated with sending the reactor trips.

Now that same signal, in some circumstances, needs to actuate some safeguards equipment. There's another set of processors involved in that. I mean, you're not talking about that time frame. Or is there an analysis for --

MR. SCAROLA: In this same document, there is a document that's entitled PSMS response time. We model the reactor trip response time, and we model the ESFAS response time. This slide only shows reactor trip.

MEMBER BROWN: But they are in series.

MR. SCAROLA: Correct, they are in series. So for the ESFAS, you have another ESFAS CPU section --

MEMBER BROWN: Okay, all right.

MR. SCAROLA: -- that's received from the data link. Then you have the safety bus time, and then you have the SLS time. So for ESFAS, there is a longer signal propagation.

MEMBER BROWN: That's fine. I didn't look at 09021.

MR. SCAROLA: Now, I would like to correct something I said earlier. I had told you that the safety bus, or the control network, has a response time of 100 milliseconds.

The hundred milliseconds is the unit bus response time. Because the unit bus has many, many nodes on it. The safety bus has a much fewer set of nodes. And the response time is 50 milliseconds for the safety bus.

MEMBER BROWN: Okay. That makes more sense now, based on the numbers you all were throwing around. Okay, thank you.

MR. SAMPLES: Now I'll discuss the issue of diversity for software common cause failure. I have the conventional analog DAS provided for Branch Technical Position 7-19 to accommodate beyond design basis common cause failures that could adversely affect the PSMS and the PCMS when you have a concurrent AOO or postulated accident.

The DAS provides automated reactor trip, turbine trip, main feedwater isolation, emergency feedwater actuation, and emergency core cooling actuation.

And the DAS also allows the operator to monitor critical safety functions and manually actuate the safety system to achieve and maintain safe shutdown.

Earlier we talked about the RPS. We talked about the four trains and how, in each of the four trains, there are two different groups. And they monitor different variables.

And now, I'm going to go ahead and talk a little bit more about the RPS functional diversity. You can see it monitors two diverse parameters to detect an event and initiate a protective action.

These are processed in two separate controller groups, two in each train. PRA shows some significant benefits from this functional diversity.

Now, for instance, for the different protection here in the far left column, a good example is loss of heat sink.

You have Group 1 and Group 2. You see that, for Group 1, the group is monitoring the variable of steam generator water level and pressurizer water level. While in Group 2 it's measuring pressurizer pressure. So it's measuring two different sets of variables.

CHAIRMAN STETKAR: Is this table anywhere in the DCD?

MR. SAMPLES: Yes.

CHAIRMAN STETKAR: It is? I think we cut off the piece to it.

MR. SAMPLES: Yes, I've got it right here.

CHAIRMAN STETKAR: The ESFAS signals, I couldn't find them. I had a question. There's a nice comparative table for RPS that shows diversity of signals.

MEMBER BLEY: I thought the ESFAS was up with that one.

CHAIRMAN STETKAR: Was it?

MEMBER BLEY: I thought it was both.

CHAIRMAN STETKAR: Okay, maybe I missed it, thanks.

MEMBER BLEY: But I could be wrong.

CHAIRMAN STETKAR: I can find tables.

MEMBER BROWN: No. I think there's one in the ESFAS section.

CHAIRMAN STETKAR: Fine, I must have missed it, thanks.

MR. SAMPLES: Now for simplicity. The overall plant-wide simplicity is achieved through these different ways.

MEMBER BROWN: Go back just one second please. I did have a question. Okay. Some of these have multiple -- okay, that's fine. I looked and I saw a couple of these were doubled up in terms of pressurizer pressure. No, I guess it'd be on Table 7.2-5. There were two high pressure water levels in that.

CHAIRMAN STETKAR: Well, there was a statement. In some cases where there wasn't functional diversity you do split the same signal between both groups.

MEMBER BROWN: Yes, I know. And that's fine, except that I didn't see it. I didn't see it on this table. There were two high pressure water levels in Group 1, in the Table 7.2-5. And I quickly looked down there. I did not see, oh no, there it is. There are two pressurizers. Okay, never mind, go ahead.

MR. SAMPLES: Okay.

MEMBER BROWN: I understand your point,

John. I remember seeing that also. I just hadn't connected it.

MR. SAMPLES: Back to ways we achieve overall plant wide simplicity. And first of all, oh --

CHAIRMAN STETKAR: Some of them are both, but I was looking for a steam line break, LOCA-type stuff.

MR. SAMPLES: See, first of all we have the one digital platform, the MELTAC platform. It's applied to all safety and non-safety applications. There's one system, the PSMS, provides all the safety functions. One system, the PCMS, provides all non-safety functions.

We have a standard approach to a logical independence but only four common isolators, power, inputs, outputs, fiber optic communications. There's standard approach to data communication using two common interfaces, the data link and control network that we discussed before.

There's a standard approach to communication independence. This is the separate communication controller, separate from the functional controllers, the two-port memory, and the same human system interface in both the main control room and the remote-shutdown valves.

Now as far as simplicity related to software, first of all the basic software and the application software are separated. And what you're seeing here is an example of an application software development display.

The application developer will pull this up, and what you're seeing here is, first of all, the Application Program Interface 4 application software is a set of pre-defined functional blocks, either AND, OR, Timer and Latch, such things in back.

The developer will take these functional blocks, ANDs, ORs, Latch, or whatever you seem to have, connect them together, connect them to inputs and outputs, and that way develop the software. And they do that using the engineering tool offline.

Doing software development this way has some advantages over doing it by writing lines of text code. First of all, it's much easier for a verifier to take a look at the graphical representation of the circuit here and follow through different signal paths to verify that it's correct. There's less likelihood of error when programming.

CHAIRMAN STETKAR: If you're going to do that, I presume each thing in here, such as just pick one box, it says FX, that's a function?

MR. SAMPLES: Yes, function.

CHAIRMAN STETKAR: So I presume that

function is a block of code that is pre-written and defined for input, output --

MR. SAMPLES: I may not have explained that as well. See, each of these AND, and OR, Timer, and the function block you're talking about, you see them. But it's actually the basic software implements them behind the scene.

CHAIRMAN STETKAR: No, I understand that. But when you've taken a block of code that executes that with all its lines, and you've called it something so you can put this into a diagram, when you do that, then it pulls that out when you're programming. And it pulls that code out and sticks it in whatever the appropriate place it's supposed to be executed.

MR. SAMPLES: The basic software does implement the function. I don't think it exactly implements it in the way you describe it. But it is the basic software running to execute the function block, or the ANDs, ORs, other functions.

CHAIRMAN STETKAR: Maybe I'm not making myself clear. If somebody's going to program using that and they go pick that block, someplace there's got to be a set of code that says what's in that block, line by line, what the inputs are, what the outputs are, et cetera.

And so when you do that, then in the background that code is brought in and connected to the other code that's going to interpose with it on the front end and on the back end. Or you presume there's a library that defines every one of these pieces.

MR. SAMPLES: Are you asking if there's a library that defines what an AND gate is, for instance, something that simple --

CHAIRMAN STETKAR: Well, there probably would be if you're going to call for an AND gate itself. But if you've got a function that's going to combine three different parameters under some circumstances, then you'd have to have a block of code that defines what that code looks like.

MR. SCAROLA: Pat, let me in. In the MELTAC technical report, which is one of the documents you have, in the back there's an Appendix B that identifies every library function that's part of this basic software.

So you'll see every type of function, three input AND gates, two input AND gates, latches, One-shots, timers. There's a whole library, several pages.

So the designer, as you say, simply has to select the block he wants graphically. But when he selects that, there's a whole bunch of code, as you said, embedded in that block that he never sees.

MEMBER BROWN: Yes. I've got that.

MR. SCAROLA: The application developer never sees that code.

MEMBER BROWN: But what about a more complex algorithm like your overpower delta T-high, which is more than just an AND gate --

MR. SCAROLA: There's an integral block, there's an integral function block, there's a summer function block, there is --

MEMBER BROWN: But that function would have already been a library developed for that function that combines all those that you would then call up if you were looking for that.

MR. SAMPLES: Those functions would have been designed by the person who developed the basic software. The application software developer ought to have that.

MEMBER BROWN: Who checks all that? Functionally, some of that stuff could change from design application to design application.

MR. SCAROLA: No. I think that's what maybe we're confusing you about. The software code that's inside a block never changes. It's part of the basic software. It's a library function that's encapsulated. It's part of MELTAC. So you get those libraries --

MEMBER BROWN: They know what all the functional applications you're going to need in the US-APWR for protecting the plant.

MR. SCAROLA: Well, I can tell you that the function library has grown over time.

MEMBER BROWN: Okay, that's fine. You've added to it.

MR. SCAROLA: There's 450 MELTAC controllers --

MEMBER BROWN: Okay, that's fine. I'm just saying MELTAC doesn't do that. So the designers have to define what the function is for the plant. And then you develop whatever library piece you need for it.

MR. SCAROLA: What will happen is the application designers will look to build an application with the existing function blocks. They may find that there's not a function block that they really need.

Now they'll go back to MELCO. And MELCO will build a new function block using their basic software methodology, which includes full BTP 7-14 documentation, independent verification --

MEMBER BROWN: A different side from that, the designer tells them what the functionality they need, and what influence --

MR. SCAROLA: Some kind of a specification.

MEMBER BROWN: Some type of a specification that tells them what that function needs to look like.

MR. SCAROLA: And that's how the library has grown so big over time.

MEMBER BROWN: Who checks that MELCO does it right. How do you check that?

MR. SCAROLA: Well, MELCO has an Appendix B software development program.

MR. TAKASHIMA: The function was checked by the designer. The designer may check.

MEMBER BLEY: Well, these are in the library then, so you can check them. So your question is who does that.

MEMBER BROWN: Yes. I understand the designer providing here's the functionality you want.

MEMBER BLEY: Then he gets the package back from MELCO.

MEMBER BROWN: And he gets it back. Somebody needs to recheck it. There ought to be a QA process that does that. And I was just asking a question about if that's part of your overall software program.

MR. SCAROLA: It's part of the software life cycle program, part of the software quality assurance program, which includes not only independent verification and validation within MELCO, but then independent oversight by MHI people as well. So there's multiple layers of independence.

MEMBER BROWN: I'm not objecting. I just want to know what you're doing, that's all. You were doing this when I left my program. So I just wondered how you all were doing it.

MR. SAMPLES: I think we can move on to testability now. I&C systems of the US-VWR, they're tested by a combination of automated self-testing and manual tests.

So the continuous automatic self-testing covers all digital system components. It includes controller memory, inter-controller data communications, all the way from input to output.

All program memory, including memory that holds the self-testing and the setpoints, is confirmed by continuous automatic self-testing.

Now for manual tests, there are diverse manual surveillance tests. These are controlled by tech specs, including the operability of the testing functions that confirm the operability of each PSMS controller, for example, the channel calibration test, trip actuation device, operability test, memory integrity check, and --

MEMBER BROWN: What is TADOT again?

MR. SAMPLES: Trip actuation device operability test.

MR. SCAROLA: It's the test that we run that makes sure when you generate a signal the valve actually moves. So you actually get an output from the system to the valve, or the reactor trip breakers actually open. That's a typical TADOT test.

MEMBER BROWN: Okay, thank you. Just didn't know the acronym.

(Off microphone comments)

CHAIRMAN STETKAR: Keep that up at the moment. I just want to make sure. I think we asked about this once before, but I can't remember whether we asked you or someone else.

As I understand it there's no, what I would call, end-to-end operability test ever performed on this system. In other words, you never inject signals into a sensor and make sure that the valve closes. You rely on all of the overlaps.

MR. SCAROLA: Only through overlaps, correct.

CHAIRMAN STETKAR: Okay, thank you.

MR. SAMPLES: And the figure here, what you're seeing are several hardware elements, a communication interface module, a CPU, Bus Master module, and both an input and output module.

Now the yellow over here, you're seeing the several different automated individual checks, such as for the CPU you see a clock check, a RAM check, a CPU health check, for output module a read back check.

These self-diagnostic functions completely test the hardware and the software. And all the memory and other hardware that affects the safety function are tested directly.

In addition to these individual checks that cover the individual hardware elements, there are two broad tests to detect erroneous function execution, first of all, a watchdog timer.

It's a gross cycle time check by the hardware and a periodic process time check. This is a precise time cycle check by the software. And notice that one of these is the hardware and software, so you have an element of diversity there.

MEMBER BROWN: Are there three watchdog timers in that controller? You use WDT three times between the little arrows, one down in the memory aisle communication circuit, one up in the CPU line, and another one in the output memory concert breakthrough.

MR. SCAROLA: There are watchdog timers in that communication module, watchdog timers?

MEMBER BROWN: There's no box inside that says watchdog timer. It shows a box that's independent. But I presume that is.

If you look at the circuit card or whatever controller card you've got, there would be a hunk of hardware on it somewhere that's independent of all the rest of the circuits. It's just sitting there monitoring, waiting for time pulses, for the reset line to go out back to the CPU.

MR. SAMPLES: I'm not sure I follow you.

MR. SCAROLA: I know your question. We need to ask our MELCO representatives. Are there actually hardware watchdog timers on the communication modules? Yes, separate watchdog timers on the communication modules and the CPU modules.

MEMBER BROWN: And the CPU modules. So the bus master, the COM module, and the CPU all have distinct hardware watchdog timers on them.

MR. SCAROLA: Correct.

MEMBER BROWN: Okay. And you're going to talk about those next, right?

MR. SAMPLES: Yes. I'm going to go next and let's talk about the watchdog timer, how that operates. The watchdog timer itself is a counter. It's for the hardware clock generator.

MEMBER BROWN: Let me ask one question before.

MR. SAMPLES: Sure.

MEMBER BROWN: It's related. You'd have to go backwards, but you said gross time check. Each of those three components, those three units, has a time frame within which they're supposed to be starting and stopping their processes. I'll just pick a number, say it's 50 milliseconds. When you say gross, does it mean --

MR. SCAROLA: Four or five times.

MEMBER BROWN: So it's really gross.

MR. SCAROLA: The hardware watchdog is gross. The software is very precise, the software watchdog. That's why there are two watchdogs.

MEMBER BROWN: Okay. I understand what gross means.

(Off microphone comments)

MR. SAMPLES: Now, the watchdog timer, how it's working here is it's reset at the beginning by the basic software. And then it counts up and counts up as the basic software, as the module performs its function.

Then once the module's done and it's operated correctly it will reset the watchdog timer back to zero. And it'll count up again.

Now, if the basic software doesn't reset the watchdog timer, what's going to happen is it's going to keep counting up. It'll go past, reach its predefined timer value.

And at that point we'll get a fail, a module going to failure mode, and get an alarm. When that happens in the failure state you're going to get a partial reactor trip and a fail as is for the ESFS system.

MEMBER BROWN: How do you get the partial reactor trip? Is that executed by hardware, or is that by you depending on the software that's not operational anymore because it's not completing its -- that's not illustrated as to how you phrased it in the MELTAC.

Its processing is monitored for deterministic cycle time by watchdog timer, enforces a fail safe processing termination. Nice words but how is that executed? It doesn't say, or at least I couldn't find it.

MR. SCAROLA: It depends on the watchdog that's timing out. If a CPU watchdog times out, it's simply going to tell the I/O module that there's no more, the I/O module that's supposed to get the output is just going to recognize that there's nothing else happening from the CPU.

So now the I/O module is eventually going to time out. Now the I/O module watchdog timer is actually a hardware interface to the output that will de-energize, for example, the undervoltage relay going to the reactor trip breaker. So it's an actual hardware interface.

MEMBER BROWN: So I'm effectively looking at the bus master module then, which is the last one in the line if I go back to the previous page. Is that correct?

MR. SCAROLA: Yes.

MEMBER BROWN: Because it's involved in both the input side before you get to the CPU, and somehow it's on the output side, even though it's on the input side.

(Off the record comments)

MR. SCAROLA: So the output module senses that the watchdog timer has timed out in the bus master module.

MEMBER BROWN: It would be nice.

MR. SCAROLA: We don't have a diagram for it.

MEMBER BROWN: Okay. It would be nice if, I'm not suggesting modifying the MELTAC, but if the DCD included --

MR. SCAROLA: A diagram.

MEMBER BROWN: -- a diagram and a discussion of how the reactor trip is actually executed and that it covers the waterfront relative the reactor trip as well as the ESFAS functions.

MR. SCAROLA: I agree.

MEMBER BROWN: The failure modes, in terms of tripping and/or fail as is, that's obviously the direction. That's the fail safe direction for both of those.

The only other thought process is if you have a fail as is in the ESF how do the operators know that you've got that?

I couldn't find anything relative to an alarm signal or a warning signal saying system inoperable, or train inoperable, or something like that, which seems to be lacking. They ought to know if this thing times out.

The other question I had was in the description, and I don't have the right part pulled up, it talked about it terminates at n, and n could be equal to more than one.

In other words, just as you show here, well no, it's not as you show there, I'm sorry. In other words, it implied that the watchdog timer would attempt to reboot the CPU, or the I/O module, or the bus master, or whatever was involved.

And it would try to do that two or three times, or some number of times, before it generated the reactor trip. Personal opinion is one is the only right answer. So that point should be addressed as well. And can we somehow make sure the operators know about it. So those are the three points.

In other words, a figure that shows where it is and how each of them performs, which one generates the reactor trip and why it doesn't need to be done by the other two, wherever they are, because it's important that generation be independent of whatever software is now not operating.

MR. SCAROLA: Good comment.

MR. SAMPLES: It's possible the watchdog timer can fail. And the way you detect a failure of the watchdog timer is by monitoring the counter, the value.

This is the watchdog timer clock check. It's performed by basic software. Again, if the counter stops, becomes askew, this indicates an abnormality of the watchdog timer.

This watchdog timer's clock check is performed periodically by the basic software. And if an error is detected by this clock check, the controller transitions to a failure state.

MEMBER BROWN: Same as the other one?

MR. SAMPLES: Yes.

MEMBER BROWN: I like the feature of checking the checker, or checking the timer. But I didn't see where, when it said failure state, I didn't know what that meant either. So if it generates the same result as a watchdog timer trip it would be a good idea to just expand that to say the same thing.

MR. SCAROLA: But we don't have a good figure that shows it. And I agree with you there. We need to have it.

MEMBER BROWN: Thank you. And the DCD would be a good place. That way you don't have to go back into the technical report if you're going to do a REV. It makes it part of the licensing basis also.

MR. SCAROLA: Well, even if it's --

MEMBER BROWN: I guess all of them, they all do, I'm sorry. You're right. I, yi, yi, come on.

CHAIRMAN STETKAR: Whatever page or whatever document it's on.

MEMBER BROWN: Keep pounding on me. I understand that.

CHAIRMAN STETKAR: Their decision.

MEMBER BROWN: I just like the DCD because it's the precedent document. If you read the DCD it says this takes precedence over everything else.

MR. SAMPLES: Some more information on testability, the self-testing detects hardware and software errors in the PSMS. The logic algorithm setpoints, time constant values, and inter-train communication of the PSMS are self-tested.

Input/output is confirmed by manual periodic tests. The manual periodic I/O test also provides diverse confirmation of each controllers ability to execute multiple diverse software functions.

All the memory that controls basic software and application software is confirmed by the manual initiated software memory integrity check. And that's diverse from the self-tests.

Through the aggregate of all these tests, all the safety function of the PSMS are confirmed. Also the setpoint methodology technical report includes the method of allowable value calculation used for testing.

Moving on to reliability now, the following key features of the PSMS ensure high reliability. First, the MELTAC platform, the digital platform operating history demonstrates a long component mean time between failure. And there are no software common cause failures in the operating history.

The continuous self-testing, high coverage, detect failures there. Periodic surveillance tests ensure 100 percent test coverage. There's redundancy between division and within divisions, including safety bus, diversity within divisions to reduce the PSMS common cause failure potential.

And if we do have a PSMS common cause failure to occur, we have the DAS to mitigate the accidents. The impact of the PSMS reliability is analyzed in DCD Chapter 15 in the PRA.

Now the key elements of the PSMS reliability calculation in the PRA are these, the mean time between failures of the digital I&C components, self-test coverage, the rate to detect failures in the periodic test intervals, common cause failure probabilities, and the digital I&C modeling method.

All modules include the module performed in the safety bus functions, including network interface modules. Optical switches are modeled in the PRA. Safety bus itself, what we'll hear it say, and it's just the actual physical optical cables fiber itself, is not modeled because the failure rate is negligible. Everything else, except the actual physical fiber is modeled.

CHAIRMAN STETKAR: By the way, I'm going to remain silent for this presentation every time you say PRA. I do have several comments on the PRA. I've asked the staff to have their PRA folks available when I talk a little bit about that. So don't cringe every time you say PRA. You'll get to cringe later.

MR. SAMPLES: Okay. As far as the mean time between failures of the digital I&C components, these mean time between failure values for each of these digital I&C components that are used in the PSMS, we calculate these based on the MIL handbook, 217F.

The actual mean time between failure values that would get from the operating experience of the platform are actually longer than the calculated values, the analytical values. So we actually use the analytical values for more conservatism.

The PSMS reliability is assured through the Reliability Assurance Program in both the design and operation phases. And the PSMS digital platform will be included in the Design Reliability Assurance Program.

The self-diagnostic rate is estimated as 100 percent based on the FMEA of the platform. We used the conservative value of 90 percent in the PRA to count for uncertainty. The periodic test intervals used in the PRA, these are provided in the DCD Chapter 16 tech specs.

Now the integral extensions from historical standard technical specification values are shown to have negligible effect on the core damage frequency per the

PRA technical report in Attachment 18A.1 of that.

The summary will be added to the DCD in Chapter 19 and Appendix 19B in DCD REV 4. That will be a new Appendix 19B, new to that report.

The 24-month sensory calibration interval is the basis to channel uncertainly in the setpoint methodology.

Now we use a zero percent self-diagnostic rate for hardware devices not covered by self-diagnostics, such as sensors, breakers, non-digital parts of I/O. Obviously they can't diagnose themselves, so it's zero percent there.

Now for common cause failure probabilities, three different ways for different ones for basic software, application software, and the hardware components.

For basic software, we arrived at a figure of ten to the minus seven per demand. We're assuming one common cause failure through 20 million hours of operating experience, again, even though none has actually happened in the MELTAC platform.

MEMBER BLEY: How much operating experience do we have for operating the platform?

MR. SAMPLES: Well, as you see here, what actually we're talking about here is it's been in operation since 1987. Now we're talking about per controller, for 450 different controllers in 30 different plants.

Now each of those controllers, multiple controllers, to implement any safety system or non-safety system between 2,000, 200,000 hours per, averages out to about eight years per controller.

MEMBER BLEY: Or 30 million.

MR. SAMPLES: When you get to 30 million you just multiply 450 controllers by eight years average per controller, then by 8,760. That's how many hours there is in a year. You get up to about 30 million. But the 20 million value we use --

CHAIRMAN STETKAR: Just because this is a public meeting, you can't have nine women pregnant for one month each and have a child. So saying you haven't had any failures in 20 million hours doesn't mean that you've actually operated anything for close to 20 million hours. Because that's about 2,300 years. You've operated a lot of things for a relatively short period of time.

MEMBER BLEY: On the other hand --

CHAIRMAN STETKAR: Well, I'd say relatively --

MEMBER BLEY: All our other equipment --

CHAIRMAN STETKAR: That's right, that's

right.

MEMBER BLEY: -- we're not looking for a mean time to failure. We're looking at a failure rate.

CHAIRMAN STETKAR: That's right.

MEMBER BLEY: And from the experience they have, this is a pretty conservative treatment.

CHAIRMAN STETKAR: It's pretty --

MEMBER BLEY: It says we've been awfully lucky if that is the case.

MR. SCAROLA: We've been lucky?

MEMBER BLEY: Yes. If that's the failure rate, we should have seen a bunch of failures by now, or at least one. You're happy with what I said, even if you aren't saying a lot.

CHAIRMAN STETKAR: You are. Just nod, yes, he's right.

MR. SCAROLA: It seems like backdoor happenings.

(Laughter)

MR. SCAROLA: I was trying to feel happy.

CHAIRMAN STETKAR: If you're a Bayesian you'd understand.

MR. SAMPLES: Again, we're using the 20 million hour value for conservatism in the calculations for basic software. For application software we have arrived at a value of ten to the minus fifth for demand.

We get there by crediting Class 1E life cycle process management measures and many defensive measures, including strict cyclic operation, constant loading, the different things you see there.

Now for hardware, we start by trimming the failure probability of a single module. And then we consider redundancy and use the multiple Greek letter method to calculate the common cause failure, probably of the system depending on the level of redundancy. And it's different for each module and each configuration of redundancy.

MEMBER BLEY: In the hardware side, have you had common cause failure?

MR. SCAROLA: We've had random failures. That's the MTBF data, but no common cause failures. But probably a better way to say it, no design defects, random failure but no design defects. Because even after random failures we'll look and see if this is possibly a design defect, but no for random failures.

MEMBER BLEY: Back up to that one. You can just help me understand a little bit. I suspect, are all failures of the hardware announced somehow? Can we have a latent failure sitting there of hardware that we don't know until we get a demand on these cards?

MR. SCAROLA: Until you get a test, yes. As we said, self-testing covers everything that's within the digital envelope of the system. But you have the input side of an analog input module, which is an analog signal filtering circuit.

So you can have failures that you don't see until you run a test. So that's why we test, because we don't want to wait for the demand to find out we have a failure. That's why we --

MEMBER BLEY: If you get a failure and it happens to be of that kind, do you check other modules to see if you might have that common condition?

MR. SCAROLA: Absolutely.

MEMBER BLEY: And you've never found that.

MR. SCAROLA: Correct.

MEMBER BLEY: Okay. Now we have found it on some other electronic cars. But you haven't seen any on this.

MR. SCAROLA: We have not.

MEMBER BLEY: So when you use the MGL method you don't have any common cause failures from which to start. Go ahead.

MR. SAMPLES: Okay. Now for quality, first of all discussing the quality of the MELTAC platform.

MEMBER BLEY: I just want to make a point, one more question. You don't have to go back to the other one. But in the software side, we've got to use something, maybe we have to use something.

But counting up hours probably isn't what this is about. Because software doesn't age, it just sits there. And the only way you're going to get a common cause failure is if some event occurs whereby we're getting inputs that aren't within the realm that we've actually tested for. That's my opinion.

So it's only under really weird events where we're going to see them, so that accumulating hours doesn't really improve our confidence. But you're taking care of it through other methods.

CHAIRMAN STETKAR: I didn't think about this PRA thing until we started talking about this. But I decided I'd go look at the model, because I hadn't looked at this part.

You say you use the MGL method. It's not clear to me that you actually do. Because the MGL method looks at if I have a four train system.

You basically subdivide that system into independent failures, and I've got four of those, failures of two with common cause and independent failures of two more, failures of three and an independent failure of one, and then failure of all four.

The parts of the models that I've seen only have a single basic event that says digital I&C hardware failure. Now, it does fail all trains. That's the all four. But it doesn't seem that you're picking up any of the other intermediate parts, which is really the application of the MGL.

MEMBER BLEY: That's right.

CHAIRMAN STETKAR: You do have a single basic event that says all hardware fails. That's all four together. You don't have any of the other logical combinations of three of these and one of those, and there's four of those, and two and two, and those geometric combinations start to get really large really fast. At least I haven't seen that anywhere in the digital I&C.

MR. SCAROLA: Didn't you say you were going to save these questions for the PRA?

(Laughter)

CHAIRMAN STETKAR: Now this is not one of the ones that I was going to say. Because I didn't come across this until we started talking about MGL methods. I have several others. I just wanted to make that statement, because saying you --

MR. SCAROLA: It was developed to be able to do exactly what John said.

CHAIRMAN STETKAR: -- saying you've applied the MGL method implies a certain logic structure to the model. And that model does not seem to have that logic structure.

Now, I'm a little bit hesitant because in real time here in the last 15 minutes I've pulled up a model to try to see that.

MEMBER BLEY: I would offer one other thing. There are some fault tree codes that put this stuff in for you, and you don't see it in the bigger model if you select the option to do that.

CHAIRMAN STETKAR: It does, but they've used that code and it has a separate flag for things where they develop the logic. And this one isn't here. I've seen it in other places. But for pumps and valves --

MEMBER BLEY: It's there.

CHAIRMAN STETKAR: -- you see the developed --

MEMBER BLEY: You're right, the double --

CHAIRMAN STETKAR: -- the double diamond, or double triangle. That's not here. You have to be careful, in PRA in particular. When you say you've done something you have to understand what that means, both numerically and logically.

And saying that you've applied the MGL method implies a certain logic to the models. And I'm not seeing that here. And we'll just leave it there.

MR. SAMPLES: We may need to wait to address that when --

CHAIRMAN STETKAR: Yes. That's fine.

MEMBER BLEY: Now, I'm sorry to divert. But I just went back to look for something. Ken, earlier you said the library of those models is in Appendix B in one of the MELTAC reports. Maybe that's too big and we haven't received it.

MR. SCAROLA: Well, I think you've, O7005 is the MELTAC topical report.

MEMBER BLEY: 005.

CHAIRMAN STETKAR: That's the one that used to be a topical report in the --

MR. SCAROLA: Yes. It's a technical report, excuse me, O7005, Appendix B.

MEMBER BLEY: Okay. I was looking in the wrong one, which had an Appendix A and Appendix C, but no B. But that's a different report. I was in the wrong one.

CHAIRMAN STETKAR: Interpret silence as proceed expeditiously.

MEMBER BLEY: Or we'll think up something else.

(Crosstalk)

MR. SAMPLES: Let's move quickly to quality then and discuss --

MEMBER BROWN: I did, okay --

(Laughter)

MEMBER BROWN: This is easy, okay. In your slide on the watchdog timer you talked about a partial reactor trip. You mean a train trip. You don't really trip the reactor, you mean one of the four. I presume that's what you meant.

MR. SAMPLES: Yes, one of the four signals --

MEMBER BROWN: So that's what you mean by a partial reactor trip. I just --

MR. SAMPLES: Yes. One of the four signals before it goes into the tool kit.

MEMBER BROWN: Yes, that's fine. I just wanted to make sure I understood that point.

MR. SAMPLES: And any of the other trains then, say the A train has --

MEMBER BROWN: They would create one. If one of the other ones went, I'm just saying, when you had one you were referring to that as a partial reactor trip. That's fine.

MR. SAMPLES: Now the MELTAC here, the quality, it says in quality assurance for the MELTAC platform, to begin, issue a criteria of quality.

Just a note, first of all, that the actual model of MELTAC used for implementing the PSMS, the safety related I&C, is the MELTAC Nplus S model of MELTAC. So that's what that's telling you here.

Now for the hardware life cycle, it's the components. The hardware is designed, manufactured, and tested under an Appendix B Quality Assurance Program. This life cycle also includes 30 years of support for proactive obsolescence management and a corrective action program.

For the basic software of the platform, the basic software is developed and tested. All of the basic software configuration items are developed and tested also under an Appendix B Quality Assurance Program.

This Appendix B Quality Assurance Program invokes the MELTAC basic software program manual. And that manual satisfies the requirements of Branch Technical Position 7-14 and complies with Reg Guide 1.152 and other applicable IEEE standards.

You see there is an open item for this. And MHI is to address how to flow down these requirements to suppliers and to share this life cycle process of the MELTAC platform.

Now moving to quality for the application software, you see the design process for the application software is governed by the software program manual. It specifies pretty much standard software life cycle processes.

All independent V&V activities are performed by MHI in accordance with this SPM. The process includes integration of a complete system that's hardware, basic software, and application software, all together. And there's an ITAAC that demonstrates compliance with the SPM.

Now augmented quality is applied to certain non-safety systems that have specific requirements. You can see the different items, which are listed to have augmented quality.

And you see the specific requirements listed over here. For instance, safety function control by the operational VDUs, they have the requirements of ISG-04.

MEMBER BROWN: What does augmented mean?

MR. SAMPLES: Essentially these are non-safety systems, and the baseline is a non-safety QA program. Then there's non-specific regulatory requirement, that addition. But they don't go all the way up to a full safety related program.

So for instance, if you look through this Generic Letter 85-06, it gives specific additional things you need to do above the normal non-safety program, to do that, to meet requirements for that.

MEMBER BROWN: I'm just not familiar. Define a non-safety program, non-safety QA program.

MR. SAMPLES: One which I use is ISO 9001. It's the basis of the non-safety. So that would become the baseline for the non-safety, again, these additional specific requirements that we get from regulations and different industry standards.

MEMBER BROWN: Okay. No, I was just asking. We don't have to beat this dead horse. I'll try to get a better understanding of that.

MR. SCAROLA: Maybe to elaborate just a little bit, augmented quality has really two aspects. One aspect, for example, is that we apply an independent review process to the design that you don't normally do to non-safety systems.

Then beyond that, each one of these systems has specific design attributes that are typically safety system attributes. But we apply them to non-safety systems.

For example, we talked about diverse actuation system being tested to an equivalent level of Seismic Category 1. Well, you don't normally do that for non-safety systems. So it's a special requirement for this non-safety system. So we refer to it as augmented.

MEMBER BROWN: I didn't know what preceded that. There's a non-safety system QA program somewhere.

MR. SCAROLA: That's the foundation.

MEMBER BROWN: And I was wondering where the foundation was and how these are just adders to it. That was where my question came from.

MEMBER BLEY: But just thinking about it though, I know there are people who worry about having some of this being non-safety. And this is, well, you're better than non-safety or somewhere in between on the quality.

MR. SCAROLA: But there is a lot of precedence for this that came out of the ATWS rule originally.

MEMBER BROWN: Yes, that's true.

MR. SCAROLA: Because ATWS systems are, in fact, augmented quality. Because they have certain safety attributes, but they're really non-safety systems.

Same thing with the SPDS that came out of Three Mile Island, it has some safety significance, but it's a non-safety system. So we apply augmented quality. So there's nothing that doesn't have a lot of history here.

MEMBER BROWN: And the treatment you're

putting here for augmented quality is consistent with that history.

MR. SCAROLA: With that history, correct.

CHAIRMAN STETKAR: It's the same as the fifth line item down there. It's the stuff that's on the DRAP list. In passive plants it's the --

MEMBER BROWN: Yes. I know some of it, but I didn't know the whole package was a standard approach.

MR. SPRENGEL: One clarification, it is not a genesis from a non-safety program. It's starting from a non-safety classification and adding to it.

But we're not implying that there's a separate non-safety program out there that we work on and then switch it. We have one QA program that we follow. And it's just a classification of the systems or equipment.

MR. SCAROLA: That's a good point.

MR. SPRENGEL: So there was some phrasing --

CHAIRMAN STETKAR: As if you had two different quality assurance programs.

MEMBER BROWN: Yes, you've created new confusion. You've got a QA program that applies, that you use for safety systems, and then you augment it with these. That's the average --

MR. SPRENGEL: No. We have one QA system that we apply for our work.

MEMBER BLEY: Some systems are safety, some are augmented?

MR. SPRENGEL: One QA program. From another time.

MEMBER BROWN: So you've got one QA program that's a huge QA program that covers safety systems as well, that you subtract stuff from to do non-safety systems.

MR. SAMPLES: No, it's not that way. It's basically we have one QA program. Then it's different requirements for different levels, safety, augmented, non-safety.

MEMBER BLEY: People with infinite budgets require everything of everything. But not everybody has that.

MEMBER BROWN: Our budgets were not infinite.

CHAIRMAN STETKAR: Continue, I want to get through two slides before we take a break. There's an incentive here.

MR. SAMPLES: We'll move on to equipment qualification now. Now the PSMS and the other safety related components are qualified by type test to generic environmental seismic conditions that are expected to envelope all potential sites.

Testing is performed in accordance with applicable industry standards, such as the IEEE standards there, and regulatory requirements. There's an ITAAC that verifies that qualification test results envelope actual site specific conditions.

For instrument sensing lines, these are qualified to verify they comply with Reg Guide 1.151, which endorses the ANSI standard, also including freeze protection.

Lines that are connected to ASME Class 1 or Class 2, process piping or vessels, these are designed as ASME Class 2 and Seismic Category 1.

For the MELTAC platform, for the environmental test, the stats are for a mild environment, for the temperature and humidity parameters that we expect there.

For seismic it's tested for operating basis, earthquake, safe shutdown, earthquake requirements. It's also tested for conformance to IEEE Standard 344.

Also for electromagnetic capability it's tested for conformance to Reg Guide 1.80. What you're actually seeing in the picture over here, you see a MELTAC cabinet. The door is open and it's undergoing an electromagnetic capability test.

CHAIRMAN STETKAR: Now, what I'd like to do is, I know we're getting close to the end. But I had some rumbling among the members here. So I'd like to take a break now.

MR. SAMPLES: We have two sub-sections before the end. So we still --

CHAIRMAN STETKAR: Yes. And I'm expecting perhaps a little discussion on this. So what I'd like to do is take a break and we'll reconvene at 3:30, grudgingly.

(Whereupon, the meeting in the above-entitled matter was concluded at 3:14 p.m. and went back on the record at 3:30 p.m.)

CHAIR STETKAR: We're back in session. Let's see if we can finish up MHI here anyway.

MR. SAMPLES: Okay, now for secure development and operational environment. The security of all PSMS software complies with SDOE requirements of RG 1.152.

Complies during development by independent V&V and configuration control processes defined in the Software Program Manual, which also encompasses the MELTAC Basic Software.

Complies during operation by system design features such as locked doors, alarms, module reprogramming restrictions and the Memory Integrity Checks.

Compliance to the SDOE requirements of the RG 1.152 assures, one, that unintended functions haven't been introduced at any point in development of the PSMS software and, two, compliance assures that the system contains design features that prevent and detect unintended alterations during its operation.

MEMBER BROWN: Has the staff accepted that your Software Program Manual is suitable? I mean, is there an evaluation of that independently or is it just a line item?

MEMBER BLEY: No.

MR. SCAROLA: It's a technical report that the staff has reviewed.

(Crosstalk)

MR. SAMPLES: 07017. And the MELTAC Software Program Manual is --

MEMBER BROWN: Did they review this or did they just receive it?

MR. SPRENGEL: That's a question for the staff.

(Crosstalk)

MR. TANEJA: I can answer it now.

(Crosstalk)

CHAIR STETKAR: We'll ask you when you get up.

MR. TANEJA: Okay.

MEMBER BLEY: Yes, I had that on my list earlier.

MEMBER BROWN: Okay, good. All right, good.

MR. SAMPLES: Now, all safety functions of the PSMS are installed in non-volatile memory that can't be altered in any manner, excuse me, while operating.

If you did want to change this PSMS software, this is what you have to do. You have to get access to the equipment room. There's a lock that prevents that. There's an alarm that says if you do that without authorization.

Got to get cabinet access. The cabinet's locked and there's alarm on the cabinet. You have to remove the module. Again, this is alarmed and it's controlled by tech specs.

You have to place the module into the external chassis to reprogram it so you had to have the chassis and you had to be able to put it in there.

MEMBER BROWN: That's in the maintenance cabinet, right? Is that where that stuff is?

MR. SAMPLES: It's the dedicated reprogramming chassis.

MEMBER BROWN: Is that part of the maintenance cabinet that's on the maintenance network or is that just separate box that exists as a standalone?

MR. SCAROLA: A level of detail that has not been defined.

MEMBER BROWN: Yes, I was going to ask that because -- I can't remember if it was the DCD or the 07004 talked about the maintenance bus being independent and having no external connections.

Are there internal connections or is it something where something has to be moved from/to or can you connect the maintenance bus to the safety bus or the unit bus?

MR. SCAROLA: You cannot connect the maintenance bus to any other busses. What you do is you connect individual controllers to the maintenance bus to diagnose --

MEMBER BROWN: You take them out of their cabinet and stick them in or you --

MR. SCAROLA: No. I think we're confusing two things. The maintenance bus is used for diagnosing. If you have failures, you can now connect a controller to the maintenance bus.

MEMBER BROWN: How do you connect it is what I'm saying. Is there a switch that you switch it from out of its cabinet to the maintenance bus and then diagnostically attack it or do you remove the controller and put it into a cabinet where it gets --

MR. SCAROLA: No. No, there's no removal.

MEMBER BROWN: Well, but the reprogramming involves removal and that's what I'm trying --

MEMBER BLEY: That's a different thing.

MR. SCAROLA: And that's what I'm trying to say.

MEMBER BROWN: But that's what I'm trying to differentiate when --

MR. SCAROLA: Reprogramming and maintenance are two different things.

MEMBER BROWN: That's what I thought from reading the stuff but I couldn't find a definition of what the maintenance bus is. Where does it exist? Is it a bunch of wires that run around the plant that somebody take a switch and they connect this controller off to the bus and therefore there's all these diagnostic tools they -- what is it? There was just no definition, not a clear definition. There's a picture somewhere that showed the maintenance bus and some little modules but --

MR. SCAROLA: Do we want to bring up the

back-up slide on the maintenance bus? Maybe this is a good time. Can you get to it?

MEMBER BROWN: I didn't see anyplace else to talk about it --

MR. SCAROLA: Do we have a back-up slide for the maintenance bus?

MEMBER BLEY: Well, while you're getting the slide, is this something you do in at the cabinet?

(Crosstalk)

MEMBER BLEY: Technician goes into that room into the cabinet and --

MR. SCAROLA: Yes, he goes into the equipment room. So it's locked and alarmed. He goes into the cabinet, locked and alarmed. Now he connects a single controller to the maintenance bus typically.

MEMBER BROWN: By turning a switch? That's what we're trying --

MR. SCAROLA: I don't know that we've ever defined --

MEMBER BLEY: Hooking up a cable to it or --

MEMBER BROWN: That's what I've been asking. How does it happen?

MR. SCAROLA: Have we decided how we're going to make the maintenance bus connection, whether we're going to plug a TCP/IP cable into the controller or whether it's switched?

MR. SAMPLES: Yes, it's not showing on this.

MEMBER BLEY: And while everybody's looking for stuff, are these requirements for being locked and alarmed and all this, is this in Chapter 7? I don't remember.

MEMBER BLEY: It is. Okay. Except for the tech specs which are in the tech spec.

CHAIR STETKAR: Well, the tech specs, I think the implication on the tech specs is the bypass inoperable is controlled by the, you know, bitrain and things like that. Tech specs don't specify alarmed and locked.

MEMBER BLEY: No, no. But module removal is controlled by tech specs.

CHAIR STETKAR: Yes. It says you can't have multiple trains bypass --

MEMBER BLEY: That's the kind of control we're talking about.

CHAIR STETKAR: That's administrative control.

MR. SCAROLA: When you take something out of service and now you're entering an LCO.

MEMBER BROWN: In the MELTAC there's a

Figure 4.3-23, the maintenance network configuration.

MR. SCAROLA: Yes, that's the one he's trying to find for a back-up slide.

MR. SAMPLES: Can we switch the monitor over to my personal machine, away from the main presentation?

CHAIR STETKAR: That's difficult to do.

MR. SAMPLES: Okay.

(Crosstalk)

MR. SCAROLA: So at least talk from that figure then since you're -- while you're looking at it in the MELTAC --

MEMBER BLEY: What's the figure number, Charlie? We can all look -

MEMBER BROWN: It's Figure 4.3-23.

MR. SHUKLA: I think there is a switch you can change.

MEMBER BROWN: No. There's a box called a switching hub and that has --

MALE PARTICIPANT: You're talking about different things.

(Laughter)

MALE PARTICIPANT: He's talking about getting the picture up on the screen.

MEMBER BROWN: Oh, I'm talking about the actual figure.

MEMBER BLEY: Say the number again.

MEMBER BROWN: 4.3-23.

MEMBER BLEY: 4.3-23.

MEMBER BROWN: Yes, I'm in the 07005, 4.3-23. Page 137.

MEMBER BLEY: Oh, well that's easier. Yes, there it is. Well, that ain't much. I could have drawn that.

MR. SCAROLA: This figure 4.3-23 shows wire connections into every controller.

MEMBER BROWN: It shows a box called a switching hub.

MR. SCAROLA: Switching hub, right.

MEMBER BROWN: And then it shows below it three controllers with a dot, dot, dot going to the last one. Line going into the switching hub and calling things optical cables that go over to the switching hub.

And above that's got the MELTAC engineering tool with another twisted-pair cable, ten megabit/half duplex and then another engineering tool dot, dot, dot, dot to another engineering tool.

MR. SCAROLA: So MELTAC engineering tools are permanently in place. The hub is permanently in place. The wires going from the hub to the controllers are permanently in place but are disconnected from the controller normally, so --

MEMBER BROWN: Through the switching hub?

MR. SCAROLA: No. That's what I'm trying to ask MELCO, if they've decided if the wire's just going to be hanging there and you have to plug it in under administrative control.

You know, this is a TCP/IP cable like you have on the back of your computer. So it could be the wire's just sitting there unplugged and when you want to plug it in you temporarily plug it in under administrative tech spec control. But I don't think we've made a decision whether or not we have a switch --

(Crosstalk)

MEMBER BROWN: There's a box that says, "Note, the connection of the maintenance network and the engineering tool to the controllers is normally disconnected." Somehow.

MR. SCAROLA: But the disconnect, my point is at the controller end, right where it goes into the controller.

MEMBER BROWN: I would have imagined that but it's whether it's a plug-in or a switch or -

MEMBER BLEY: We don't know yet.

MEMBER BROWN: Okay, it's undefined.

MEMBER BLEY: They don't know yet.

MR. SCAROLA: Well, my photo's telling me it's just a plug. It's normally unplugged. You have cables --

MEMBER BROWN: So you run around and you see a bunch of plugs hanging out from the cabinet and laying down across the front of the cabinet, right? I'm being facetious but control of access is a little difficult if they're just hanging there. That's --

MR. SCAROLA: But, see, they're inside the locked cabinet.

MEMBER BROWN: Okay.

MEMBER BLEY: Inside the locked room. But that's a mystery story you remember.

MR. SCAROLA: The plug and the socket are inside the locked cabinet. Normally the plug is not engaged in the socket.

MEMBER BROWN: Okay. I guess my next question is how long is the cable to plug into the, I mean, does it have to go ten feet -- I'm just. It's late, okay?

MALE PARTICIPANT: Just like the wire on the little -

CHAIR STETKAR: Not as late as it's going to be.

MALE PARTICIPANT: -- truck we used to take around.

MEMBER BROWN: I'm feeling open right now.

MR. SCAROLA: But so as not to get confused, this has nothing to do with reprogramming --

MEMBER BROWN: I got that.

MR. SCAROLA: -- because you can't reprogram through this. Okay.

MEMBER BROWN: You've got to take stuff out and put it in something else to get the reprogram, yes, and that's somewhere, whether they carry it outside the plant or whatever they do with it. You haven't defined that either.

MR. SCAROLA: We haven't defined. Very frankly we don't expect a lot of reprogramming of safety systems. It's not a common thing. Safety systems are typically installed and, you know, safety systems, they're very simple. The logic is simple and it is typically stable, not like non-safety things where you tend to optimize and tune and --

MEMBER BROWN: They're saying there's never any software things, glitches that show up at some point? Oh, we didn't expect that thing to happen and such, therefore you have to go reprogram based on experience in about 400 software changes.

MR. SPRENGEL: No, we're not saying that.

MEMBER BROWN: Okay, go on.

MR. SPRENGEL: Pat, carry on.

MEMBER BROWN: You can get on. I'm finished. You've answered my question.

MALE PARTICIPANT: Thank you.

MEMBER BROWN: It's somewhat undefined yet.

MR. SAMPLES: If you do manage to get through all these different locks and alarms to change the software, realize that you have to do this in four separate I&C equipment rooms because these divisions, you know, they're separated as we said before.

If you are successful in making some changes, these unintended software changes are detectable by periodic memory integrity check.

MEMBER BLEY: Are those automatic?

MR. SAMPLES: The periodic? No, that's the manual initiated one. It's a diverse check initiated by an operator using a MELTAC engineering tool.

Here you see some of the features of the MHI development environment. It's talking about the Corporate Electronic Archive System, essentially stores basic software and application software.

It's password protected, physically secured. Now, the system doesn't allow you to delete or change. It's write-only and there's periodic backup.

Development environment itself, again, it's access controlled. There is access control to development machine by a password. You got to have a password.

Just to get in and out there is controls to control who can get in and out of it physically to the development area, and this development environment and computers and systems there are isolated from the corporate network.

I believe this brings us up to a brief overview of the status of open items for the draft safety evaluation.

Now, for RAI 568, the topic is selection of PAM criteria. That's selection criteria for the PAM should be refined.

For RAI 753 the topic is the basis for the inputs and the assumptions used in the D3 coping analysis. Currently RAI response is under review by the NRC.

For 992 there was, one, sufficient evidence to demonstrate that the use of the O-VDUs enhances the performance of the safety system and that there is an ITAAC that adequately verifies testing for normal and abnormal data transmission conditions for all non-safety to safety interfaces. MHI is still preparing this response.

For RAI 995 the concern is the process flow down requirements for MELTAC to suppliers. For 993 it's the process to ensure the vendor's safety software development process. For 988 the question is the basis of the inputs and assumptions used in the D3 coping analysis. For all three of these, this response is under review by the NRC.

Now, for RAI 996 the concern is how the plant would be adequately protected from PCMS failures, including single failures, design defects including common cause failures of software. MHI is still preparing this response.

In summary, the digital I&C system provides significant advancements over conventional analog plants in that there's higher availability, higher accuracy, a lower potential for human error, better performance, improved operator command and control capability, a reduction of maintenance workload and resources.

Now, the US-APWR, it employs proven digital designs and many years' experience, of many years of demonstrated reliability in Japan.

We have a conventional DAS that ensures plant safety is maintained even if digital systems fail. We are working closely with the NRC to complete U.S. licensing.

MEMBER BROWN: You want to go back to Slide 81?

MR. SAMPLES: We can.

MEMBER REMPE: That means he doesn't want to.

MEMBER BROWN: Pardon?

MEMBER REMPE: It means he doesn't really want to. He said he could.

MEMBER BROWN: No.

MR. SAMPLES: We're here to answer your questions, so.

MEMBER BROWN: You call it this Corporate Electronic Archive System.

MR. SAMPLES: Yes, sir.

MEMBER BROWN: And then you talk about the development environment and then down in the development environment you say it's isolated from the corporate network yet it's connected up in the pictures to the Corporate Electronic Archive System, which I presume is part of the relative, has access from the corporate network which it's not clear that this CEAS is isolated from the corporate network and, if so, what does isolated mean? Not connected at all?

MR. SCAROLA: No connection.

MALE PARTICIPANT: There's no connection in this picture to the corporate network.

MEMBER BROWN: I understand that but if it's a Corporate Electronic Archive System --

(Crosstalk)

MEMBER BROWN: -- it gives a very clear connotation that there's other stuff from the corporation that is stored in this archiving system.

So I guess I would question the fact that is it really isolated from access by anybody if it's in this particular overall corporate archiving system? Since I hear dead silence, could that be answered at some point?

MR. TAKASHIMA: No, no. This system is completely isolated from the corporate network.

MR. SCAROLA: Presume he is saying yes.

MR. TAKASHIMA: Yes, yes.

MR. SCAROLA: This is only used for software development. It's not used for other corporate functions.

MALE PARTICIPANT: You have a case of a confusing name.

MEMBER BROWN: You know, I just see the word corporate in two different places which implies that somebody else can use it. If it's dedicated only for the development of US-APWR --

MR. SCAROLA: No, no, no, no. That's, I think, where we have a misunderstanding. It is used for all software development activities in MELCO or MHI.

But it's for software development. That's why it's called corporate. It's not only used for this one project. It's used for software development. MELCO does a lot of other types of software development.

MEMBER BROWN: Oh, other people have access to this stuff if it's in this that are not associated with the APWR program?

MR. SCAROLA: Correct, correct.

MEMBER BLEY: But it's not that the licensee is corporate?

MEMBER BROWN: Pardon? Regardless, it still has access by other people that aren't part of an APWR --

MR. SCAROLA: Well, developers.

MEMBER BROWN: Well, developers for what? Commercial plants?

MR. SPRENGEL: It would be under the Appendix B QA Program though, so if there were other plants being sort of developed it would be under a completely different QA system and would have completely separate information and storage requirements.

So other developers would have access to it just as they do for all of our codes. I mean, the codes are available within MHI under the MHI Appendix B QA

Program.

But if you're working on a separate, you know, completely separate project within MHI unrelated to US-APWR, you do not have access to that information so it is still controlled.

MEMBER BLEY: Do they have separate code libraries, that Appendix B set of modules that you can paste together? If not, could we get some funny logic injected somehow along the way?

MEMBER BROWN: It's a control of access thing. I mean, if it's in the same overall memory bank system that other people's stuff is stored, then those memory banks are accessible and you're depending on some type of password protection and/or software as opposed to a hard, open circuit. That's all I'm looking for.

MR. SPRENGEL: Okay. Okay, we'll get some clarification on that and we'll follow up on that.

MEMBER BROWN: I mean, it's a location where somebody could muck around with the application code.

MR. SPRENGEL: Yes, right, I do. Yes, I understand the question. It should be pretty straightforward to answer, how we separate and control I guess not only the access but also the potential interactions.

MEMBER BROWN: Yes, that's it.

MR. SPRENGEL: Okay.

MALE PARTICIPANT: Okay? Good. Thank you.

MR. SAMPLES: Again, we're at the end of the presentation, the list of acronyms. I think we did actually have one question but we might have answered that earlier. Is any other general questions or anywhere you want to go back? Again, we're here to answer your questions.

CHAIR STETKAR: Do any of the members have any more questions for -

MEMBER SHACK: Well, this RAI 99-7024 you have listed as flow down here. In the SER there's also a comment there that it's essentially dropping everything about commercial dedication. That's part of this RAI? That's part of your response?

MR. TAKASHIMA: Yes.

MEMBER SHACK: In the SER I see RAI 995-7024, remove any reference to commercial grade dedication of the MELTAC platform. Is that part of that response or is that --

MR. TAKASHIMA: Yes.

MEMBER SHACK: Well, it's the staff since they're asking them to address this in the RAI, and I guess the next question is if they have prepared a response I'm sort of wondering what the answer is.

MR. SCAROLA: But he's just asking what the answer is. Are we going to remove all reference to --

CHAIR STETKAR: Anything else for MHI? If not, I'd like to thank you all. You covered a tremendous amount of material. We're obviously way over-scheduled.

But I think it's really, really important for the Subcommittee Members to get all the questions out on the table, understand all of this. It's one of the places where everything in the plant comes together so it's really important that we understand it.

And kind of in closing before we let you off the hook, sort of an observation that you received a lot of detailed questions from us here and I know it's difficult to field all of those questions.

From our perspective, we're able to ask the detailed questions because you've actually presented a real design in detail, which the ACRS has weighed in on other design certifications that don't nearly have this amount of detail, finality in the design and we really appreciate this.

I know it's difficult to field all of these questions about specificity, but you have a real design that we can actually look at and gain some confidence and sort of probe into little nooks and crannies.

And my personal opinion anyway, it's a much, much better situation than some of the other designs where everything is left to DAC, ITAAC and DAC, after the plant is built.

So I know it's difficult for you to hear all of the probing but we really appreciate being able to look at some engineering.

MR. TAKASHIMA: Thank you very much.

MR. SCAROLA: We appreciate your comments. I just want to say it's actually not difficult to field your questions because we have a detailed design. It makes it much more difficult to answer your questions when we don't have a detailed design.

CHAIR STETKAR: Good.

MEMBER BROWN: Some of us have noticed that.

CHAIR STETKAR: Thank you, and what we'll do is --

MR. SPRENGEL: Real quick procedural question.

CHAIR STETKAR: Yes.

MR. SPRENGEL: I think we have a few things outstanding so obviously we're going to go through with the staff's presentation but are we planning to kind of revisit any topics tomorrow?

CHAIR STETKAR: Yes, yes.

MR. SPRENGEL: Okay.

CHAIR STETKAR: Yes, I mean, we're going to run over into tomorrow so if you jotted down a few notes we can address them.

MR. SPRENGEL: Okay, so we'll plan to try and follow up on a couple items tomorrow morning.

MR. SHUKLA: Yes, that's also on the agenda.

MR. SPRENGEL: Okay, just confirming.

MR. SHUKLA: It's on the agenda.

CHAIR STETKAR: No, we're not going to let you hang.

MEMBER BLEY: We're only three hours behind.

CHAIR STETKAR: Yes, that's fine. I'm trying to get the staff up here so we'll see if we can bring the staff up and start that.

(Off microphone discussion)

CHAIR STETKAR: While we're shifting here, since we're still on the record, let me float a couple of notions because I want to get feedback from folks about the schedule.

We're obviously running real late. Our agenda for today shows us ending at 6:00. We've covered a lot of material and I'm worried about burnout setting in so I think that I'd like to hold to that 6 o'clock time.

One of the questions that I have is that on our agenda for tomorrow we also have to cover Chapter 2 sections for Comanche Peak and I'd like all of us -- our agenda shows us ending at noon tomorrow. I don't think we'll be able to get through all of the material by noon tomorrow.

But if we can work out internally some plan to see if we can finish by sometime between 2:00 and 3:00 tomorrow afternoon it might help everybody. I know Luminant has people coming in and I hate to have them come in and not get to Chapter 2.

So what I'm asking is Members on the Subcommittee and NRC staff, you know, if we can adjust presentations. If there are some things that are repetitive, if you can skip over in the staffing presentations just so we can try to get everything in, in particular the Chapter 2 material tomorrow afternoon.

So I'll just float that a little bit. We will plan to end at 6 o'clock today just because I'm too worried about people sitting here too many hours without --

MEMBER BLEY: You're going to have some burnout of course.

CHAIR STETKAR: Yes.

MEMBER BLEY: Before we get started with staff here, may I add to your last comment?

CHAIR STETKAR: You may.

MEMBER BLEY: John's last comment about appreciating the level of design detail we had here to review and staff had to review and I guess it re-raises those issues, not for this design but for others, ones we've left with DAC, and we have an agreement to do some getting ourselves involved in the DAC for those plants later.

But the number of RAIs at the detailed level that staff had and the number of questions that we have when you get to the detailed level are significant, I think, indicators of why we're going to need some continuing interaction for those other plants. I just wanted to get that out here. Thank you.

CHAIR STETKAR: And with that, we will let the staff start. I don't know who. Tom?

MR. BERGMAN: Yes. Good afternoon. My name's Tom Bergman. I'm the Director of the Division of Engineering in the Office of New Reactors and I'm not really going to be part of the actual briefing for MHI.

But the Committee recently issued a letter on the mPower Chapter 7 Design-Specific Review Standard and they've raised this issue on other designs, including I think MHI in the past.

The letter related to data communications from a common network bus, passing plant data from safety systems to the main control room, technical support center, emergency support center and plant control signals back to the safety systems, that the staff's position to date has been that those type of access issues were not addressed in the design review, that that was a cyber security issue addressed through the cyber security program.

Our response to you, which its issuance is imminent, says that we are reconsidering that position. We do think we understand your concern. We do recognize the general nature of the question.

The letter says, you know, we'll keep you informed through upcoming meetings of our progress on it with a final staff decision no later than the issuance of the mPower DSRS, which means January 2014.

But in terms of interim sort of schedule, the four branch chiefs involved, the three I&C branch chiefs across NRR and NRO and the cyber security branch chief from NSIR, are developing a set of options for management.

We expect that to be completed in about three weeks and then the division managers will see if we can come to a consensus on a recommendation in the following couple weeks.

And we look to have a meeting at the office-director level very late in May or early in June, so sometime this summer we should at least have a draft position as to where we look to be headed so we'll keep you informed as we make progress.

MEMBER BLEY: We'd appreciate that. Thank you very much.

CHAIR STETKAR: Thanks a lot.

MEMBER BROWN: Can I make one observation?

CHAIR STETKAR: You may.

MEMBER BROWN: I'm just referring to your initial lead in. The concern is not necessarily communication between the protection systems and their main control room.

It's the fact that the data's on a bus which has access to some firewall to a corporate, or, like, through a management computer or a firewall to corporate systems and whatever they are. It's that interface, and just to make sure I had that statement.

MR. BERGMAN: Yes, we understand.

MEMBER BROWN: I guess the other observation, based on I didn't say it in the meeting the other day, the informal meeting, but we'd like not to wait for the DSRS thing. We'd like to have some interaction when you come to a decision.

MR. BERGMAN: We will. We just wanted to put a backstop in because this will be tracked by the EDO for completion so we need to give them a date.

MEMBER BROWN: Oh, that's fine. That's fine for commitment purposes but, I mean, if you come to a decision in June or July, we ought to --

MR. BERGMAN: We will.

MEMBER BROWN: We ought to interact on this.

CHAIR STETKAR: Charlie, we'll set up Subcommittee meetings. Don't worry. The important thing was to hear from the staff that --

MEMBER BROWN: I appreciate that.

CHAIR STETKAR: -- indeed, they're moving in response to some of our concerns.

MEMBER BROWN: I understand that.

CHAIR STETKAR: And that's important.

MEMBER BLEY: And our letters have laid out on those.

CHAIR STETKAR: That's right. So we'll --

MR. BERGMAN: Yes, we're trying to move quickly because depending where we go, which option we would take, right, it can affect other activities already ongoing in the agency, whether it's ongoing design reviews, that. So we need to make a decision relatively quickly. We're not trying to drag it out. We just needed the facts out.

MEMBER BROWN: I wasn't trying to imply that. It was just decision interaction before a final paper's done. That's all. I mean, the informal paper.

CHAIR STETKAR: Thanks, Charlie.

MEMBER BROWN: That's it. Thank you, John. Can I interrupt again? No.

CHAIR STETKAR: No.

(Crosstalk)

CHAIR STETKAR: We've had enough. Let's get Jeff.

MR. CIOCCO: Yes, Jeff Ciocco, NRC staff. No, I just wanted to say that we have the PRA people here --

CHAIR STETKAR: Yes, good.

MR. CIOCCO: -- if you want to address that issue now before we get started with the status presentation.

CHAIR STETKAR: Yes, I think that's good timing. That's sort of what I was looking for here. One of the things, I'd asked the staff to bring their PRA people down and in the earlier discussion I said I would try to keep my mouth shut about PRA issues until now.

As I read through the DCD, there were several references to the use of the PRA to demonstrate reliability of the design. There were also references to the use of the PRA to demonstrate the fact that the design would work with one channel completely out of service.

And as I was trying to follow up those references, I found places in the technical bases for the tech specs that refer to the PRA for justification, for example, for the 72-hour completion time that's listed in the tech specs.

Now, I have not reviewed the PRA in detail. I did look at some of the specific parts of the models that relate to the digital I&C system. I looked at them earlier kind of very briefly when we were reviewing the PRA Chapter 19.

I went back and did a little more digging, in particular to see if I could follow up some of the words, anyway, that are in the DCD and quite honestly the PRA logic models, at least as they are presented in Revision 3 of the PRA report, are not structured to support the types of analyses that are referenced in the DCD, I mean, particular.

For example, it is not logically possible to bypass both reactor trip breakers in the same train in the PRA model, despite the fact the DCD asserts the fact that that was examined. It is not possible to bypass an entire channel train of input sensors.

And by that I mean, for example, each steam generator has four level sensors, one from Train A, one from Train B, one from Train C, one from Train D.

Train A level sensors, there's one in each steam generator. In the PRA model you cannot logically take out Train A simultaneously from all four steam generators. You cannot do it. It's logically precluded.

The technical specifications allow you to remove one train of sensors indefinitely. The tech specs require that three trains must be operable and if a second train becomes inoperable you have a 72-hour time. The PRA models explicitly preclude you from having any more than one train of sensors out, in fact, any more than an individual sensor.

So it's not clear to me how the PRA model can be used to examine the sensitivity to a 72-hour allowed outage time that applies only when you have two coincident sensors out of service when the PRA model does not logically allow that. In fact, it logically precludes it.

So I read the SER and the staff is really careful about saying in terms of reliability we don't rely on numerical values. We rely on qualitative arguments about reliability.

My concern is that there is still a number of statements in the design certification document and I think little bit bigger concern in the technical specifications, which are part of the licensing basis for this plant, that refer to the PRA for justification in cases where I can't see where the PRA can provide that information.

You would need to change the logic models to do the type of analysis that is inferred in those statements.

So, you know, as I said, I haven't reviewed the PRA and if people can show me how they use the PRA to draw those conclusions I'd be really happy, so that's sort of one request.

If you can't show me how you use the PRA, then I'm really curious about how the staff has reviewed the PRA to that level of detail so that, indeed, the staff can draw a reasonable assurance conclusion that the technical specifications are appropriately justified and that the statements in the design certification document regarding the liability of the digital I&C system are appropriately justified and that statements saying that the PRA has been used to conclude that the reliability is maintained with, for example, one channel completely out of service.

I don't know whether MHI, I know you don't have your PRA people here so I wanted to kind of get it into the record. If you can hear that, you can take it back, Ryan, to your PRA folks.

I did look at the comparisons that were alluded to in your presentation about the difference between a 72-hour time and the time in the standard technical specifications, but those are simply comparisons on unavailability numbers of individual sensors.

For the 72-hour time, I might have an unavailability of x. With a different allowed outage time I might have an unavailability of y. It's not the same as taking an entire train out of service in a correlated fashion, so.

MR. SPRENGEL: Yes, we've heard the message. I know there's some ongoing discussion within MHI on this topic and, you know, it's come up previously in our discussions.

CHAIR STETKAR: Okay, yes.

MR. SPRENGEL: And we had mentioned about some of additional informational briefings in the report.

CHAIR STETKAR: Yes, and that's fine. I only wanted to bring it out because I'd mentioned it earlier in the PRA reviews but it kind of really came home to roost when I started digging in to some of the digital

I&C model.

MR. SPRENGEL: Right, and I think some of the things we're working on is removing that kind of specific connection between the implied analysis that's done and the conclusion so that is being worked on.

But I think your question goes a little deeper than that and it's some of the specifics on kind of what is actually potential in the model and what has been used to kind of get this basis for these values.

CHAIR STETKAR: I mean, I hear statements that are made that -- we had the little discussion about MGL models. Okay, that's one thing, but if I look in some of the PRA models, I mentioned earlier I couldn't find SLS modules modeled consistently through all of the systems. They seem to be in some places and not in others.

So when you say that the PRA model has accounted for common cause failure of the SLS modules, it can't consistently because it doesn't have the wherewithal to be able to do that, so there are some of those details.

How you resolve those, you know, in terms of the design certification and the supporting information to provide reasonable assurance conclusions for the design certification is one issue. That's our concern right at the moment.

We've already discussed in the other venue the ability to use the PRA for risk-informed applications post-COL issuance.

But for the moment, in terms of supporting the reasonable assurance conclusions for the certified design and the licensee basis for the plant, the tech specs, I think we need to really be careful about understanding what the PRA can and cannot, has and has not been used to justify.

And if, indeed, it is used to justify some of those conclusions, that has different implications in terms of the level of detail of the staff's review of those underlying models than perhaps might have been done just to simply examine the models in the context of the DCD Chapter 19 conclusions so I don't know, Lynn, if you want to say anything or --

MS. MROWCA: This Lynn Mrowca. We understand your concerns due to the previous ACRS meetings that we held earlier this month. I just talked to Ian Jung and we're going to get together and talk about this and the specifics of how they reference the PRA and its uses and review concerns.

CHAIR STETKAR: Okay, thanks. You know, if we need to set up another, you know, Subcommittee briefing or something else we can work through that but I --

(Off microphone discussion)

MR. SPRENGEL: That's fine. We've heard the concerns and, you know, the staff will be discussing and we'll interact with the staff and then we'll have future opportunities to address this.

CHAIR STETKAR: I'm confident there's a path forward. I just wanted to make sure that you heard our concerns and that the staff at least had their folks here to hear that.

So with that, we'll let the I&C folks step onto the hot plate.

MR. TANEJA: Thank you. Finally. Well, thanks for giving us the opportunity to present our safety evaluation of the US-APWR I&C design. We have a few open items. I will go over that as we go through the presentation.

And I am Dinesh Taneja. I am the senior I&C engineer in our ICE Branch, Instrumentation, Control and Electronics Engineering Branch, 2. And Ian Jung is our Branch Chief. And along with me are the other staff members that were part of the review of this US-APWR I&C design.

Joe Ashcraft, you know, he was the primary reviewer of Section 7.2 and 7.3, the RP, you know, reactor system and the SFAS and he would be presenting, you know, on the redundancy part of the presentation.

Khoi Nguyen, he reviewed 7.6 and 7.9 so data communication was primarily his review area and he'll be talking about independence and simplicity.

And Erick Martinez, he is the primary reviewer of the DAS system so he'll cover DAS.

And I have Jung. You know, he's sitting over there on the side. He's my software guy that looked at the SPM manual at the SDOE so we'll have him go through, you know, his review process.

You know, we're going to focus our presentation on the key technical areas rather than going through the complete, you know, 350-some pages of our safety evaluation.

So we'll, you know, focus on the redundancy, independence, determinism, you know, the key I&C areas that have been of interest to the Committee in our other design center, so we're trying to focus our review on that also.

And, next slide, so the other, you know, technical topics I will want to cover today's presentation is the Software Program Manual since we have an open item in the PAM instrumentation area so we want to go over some of that.

And then another open item we have on the impact on safety due to failure in the PCMS system. So we'll briefly brief the, you know, the Committee on a non-concurrence that we had on the safety evaluation that we put together.

So as a little introduction and background, you know, the MHI submitted their application on December 31st and I realize that's been over five years that we've been looking at that.

You know, there was a, slow getting started. You know, didn't get to the acceptance review till about six months later and then initially we had Oak Ridge, you know, that was contracted to, you know, support us in this technical evaluation.

So in April 2010, you know, I&C technical review was on critical path and there were some technical issues and challenges at that time that were really, you know, challenging us from making progress in this area.

And MELTAC platform, you know, initially the applicant wanted the MELTAC platform to review on its own merits as a topical report so they can use it in operating reactors in other places. And that become a factor in us completing our US-APWR review.

The MELCO, you know, who is the supplier and the, you know, subcontractor to MHI for MELTAC did not have an Appendix B program and that also impacted the review that we were doing at that time.

And then there were significant number of outstanding unresolved RAIs at that time that needed to be controlled, and then we had significant issues with data communication independence and that was also very challenging.

So in August 2010, you know, put together a closure plan to kind of, you know, get control of all the situations here. We identified and, you know, worked on a resolution plan of all outstanding RAIs.

The topical reports that were submitted for MELTAC, you know, and safety I&C system, they turn into technical reports and now they got reviewed as part of the US-APWR design certification rather than a separate review.

The Software Program Manual was revised to address, you know, the software QA issues including MELTAC Basic and Application softwares.

And the emphasis was placed on the key digital I&C design principles and that's, you know, primarily from our experience with the other design centers and the feedback that we got from the Subcommittee on, you know, the focus on the critical and the principal design principles for digital I&C, so that became the focus.

Simultaneously I think MELCO established an Appendix B program, you know, for building the multi-platform for the US-APWR. So these were some of the things that were done to kind of get the project back on track. Next slide.

To support our evaluation we also did two significant audits. One was in Kobe, Japan, and one was in Arlington, Virginia. You know, the topics of our audits are listed here. And some of the things that I'm going to add to that is that we also had the opportunity to visit Oi nuclear power plant while we were there.

That plant uses MELTAC for RPS safety system and non-safety reactor control, turbine control, in-core instrumentation, control hard drive, rod positioning indication and radiation monitoring system.

So we were not only able to see the equipment in the plant but we were able to also talk to the plant staff members and their experience with the MELTAC equipment over there, so that was some of the supplemental things.

And in addition to that, MELCO gave us demonstration on MELTAC platform, demonstrating some of our key technical areas that we wanted to confirm that are in the DCD.

So we have six open items right now that we are dealing with. Two of the open items are located in Section 7.1 of our SCR. One deals with the QA of the vendors' safety software and the other is MELTAC platform and the commercial-grade dedication issues.

And then we have another one in 7.5 which is dealing with the basis for the PAMs variable and I'll go over that when we get to, you know, what is going on with that thing.

In 7.7 we have this new RAI that we just issued recently and we haven't really gotten a response back. It's the impact of PCMS failures, multiple, single, whatever, on the safety systems.

And there's a number of questions that either we are reviewing or waiting for response on D3 coping analysis that are in 7.8.

And then there is one open item in 7.9 which is dealing with the operational VDU interface to control safety components.

CHAIR STETKAR: Dinesh, when I read through the SER, there was one section that might not have been updated and it's 7.1.4.9.3. Just go back and check that because there are statements in there that says the staff has identified several open items identified in the previous section, which is part of 7.1, and that has to do with channel checks and all of that kind of stuff.

I don't think that there are open items but I wasn't sure whether something had been left out or not. This body count kind of confirms that there aren't. Might want to go back and --

MR. TANEJA: Yes, we'll go back and look at it. There were but I think those responses were acceptable and they should have been -

CHAIR STETKAR: Yes, I mean there was nothing saying that, you know, we reached acceptance. It just says several open items, a lot about standing RAIs and that stuff. Okay.

MR. TANEJA: Well, that was the case one time --

CHAIR STETKAR: No, no. I'm sure it was. As I said, I think it's just an editorial thing but I just wanted -- that table helps.

MR. TANEJA: Yes, all right. Well, we'll, you know, go back and take a look at that.

You already, I think, heard about these documents earlier today. In addition to the DCD, you know, these technical reports and one topical report, you know, these are the primary measure documents that we use in our evaluation.

MEMBER BLEY: Well, this would be a good time for me to ask the question that was linked to before, is they told us these all started out as topical reports and have moved over. They decided not to be technical reports. If they were topicals, you would have read them and given an SER on them.

Now specific areas are referenced in the DCD. I suppose your review of the DCD, anything that's referenced out there, you're essentially reviewing that part of the technical report as if it's part of the DCD, is that right?

MR. TANEJA: That is correct.

MEMBER BLEY: So we get the same kind of review we would have had only it's on the parts that are of significance to the DCD?

MR. TANEJA: If it was a topical review report, then it would have been a separate topical and then you don't have a plant design to associate it with that. So all you're looking at is the, you know, the quality abilities of the MELTAC. Now, you don't have an application so you really can't address those.

So when you look at the 603 criteria, some of them apply some of them later, pending. So those become like an action item in a topical report review.

MEMBER BLEY: But now as you're reviewing it you're --

MR. TANEJA: We have the complete picture.

MEMBER BLEY: You have the whole thing so you're looking at the quality of the documents analysis --

MR. TANEJA: Exactly.

MEMBER BLEY: -- as well as its applicability to this --

MR. TANEJA: We're looking at the complete picture. So what we did is not only the DCD. We also looked at the technical reports. We also looked at the Tier 1 ITAACs. So really we, you know, we looked at all these things in its entirety.

And one of the things that I want to point out here is that we coordinated our review with other technical branches. You know, our review included coordination with Reactor Systems, coordination with Human Factors, coordination with Containment Systems, you know, Tech Specs Branch, ITAAC Branch.

So it's like, you know, this review and the PRA Branch. We did coordinate to a certain extent with PRA Branch. John is looking at me with a grin on it but that was part of our review, Dennis. Thank you.

CHAIR STETKAR: Now, before you leave it, I'll ask you now that you're up here. Now, I think we heard a long time ago today. I understand all of that except you do have an SER on the one topical report on this list on 07006.

The DCD, at least Rev. 3 of the DCD, and I believe the current SER refer to that topical report pretty extensively. The design, as I understand it, has changed and it is now different from the design that's documented in that approved topical report.

What happens going forward? I mean, how do we make sure that the information in the DCD and any other associated technical reports reflect the real DAS design going forward?

In other words, how do we know that the right bits and pieces from MUAP-07006 that are still valid but might not have been documented anywhere else are picked up and documented elsewhere so that they become a valid part of the licensing basis for the plant and the new information is reflected somewhere, unless there's a plan to reissue MUAP-006, whatever it is, 7006?

MR. TANEJA: I believe that's one of the options that's been discussed but let me have Erick answer these questions because he's been dealing with them extensively.

MR. MARTINEZ: Yes, hi. This is Erick Martinez for the I&C branch. When we were reviewing the DCD and the coping analysis, which is still an open item, the applicant references that topical report in several sections.

But when you actually look at the details from that topical report, it describes their process in a very general way so when they reference that it's still relevant to the DCD. Any information updated as part of the DCD review supercedes the information from the topical report.

So even if the topical report, for example, states that there are only two DACs, the diverse actuation cabinets, and the DCD has been revised and added four cabinets, that information is the current design for the US-APWR.

Any information referenced from the coping analysis is just the general D3 approach for the US-APWR but we don't take any sort of those details from the coping analysis as far as the DCD.

CHAIR STETKAR: When you say coping, you have to be careful because you keep saying coping analysis.

MR. MARTINEZ: Oh, I said coping, yes.

CHAIR STETKAR: Well, actually in the SER you refer to 7014 for details of the design and they aren't in there. They're actually in 7006. So even here in this presentation, we have an example of my concern.

MR. MARTINEZ: Okay.

CHAIR STETKAR: The details of the design, a design, are in 7006. 7004 does not contain any details of the design.

MR. MARTINEZ: Not as many details. In general --

CHAIR STETKAR: It's a philosophy, if you will.

MR. MARTINEZ: Yes.

CHAIR STETKAR: My concern is making sure that going forward when the design is certified we have a complete set of information for DAS in particular because it's the only thing that is affected by that topical report that has been reviewed by the staff and we have traceability to documents that actually have --

MR. MARTINEZ: I agree with your concern. I guess what we can do is --

CHAIR STETKAR: I'm just laying it out on the table. There are different ways to approach it but --

MR. MARTINEZ: Yes, we can verify that and let's go back and just make sure that everything that is referenced from that topical report, it is actually --

CHAIR STETKAR: It either needs to be documented to that level of detail in the DCD itself or it needs to be migrated into some other technical --

MR. MARTINEZ: Area, yes.

CHAIR STETKAR: -- report so we have that.

MR. MARTINEZ: I understand your concern, all right, and I appreciate the comment. Thank you.

MR. TANEJA: You know, the staff identified significant technical issues in the original design, the complex architecture, bidirectional data communication issues, the continuous connection between the safety system and the maintenance network, capabilities to make online software changes.

The DAS was two-out-of-two logic with two cabinets and then use of time-critical manual actions from DAS. Some of those are highlights of some of the, you know, design issues that we found. Next slide.

And applicant, you know, MHI, MELCO, MAPI, you know, they've been, very, very responsive to these issues that we've identified and I think you've seen some of the design details earlier today.

The data communication, you know, has been reduced, the interface between the safety and non-safety. Now it's only limited to the manual control of safety components from operational VDU.

And there were automatic signals the original design had coming from the unit bus into the safety system. They have been removed. Now they come via hardware interface and are using isolator scheme, so the non-safety automatic actuation signals are no longer coming on the unit bus.

The interface between the PSMS and the maintenance network is now temporary. I think we saw the details of that earlier today.

Software changes, they cannot be made online. You know, they explain the process, how they are done offline now.

And the enable/disable switch is added to provide the capability to disconnect any input coming from the operational VDU into the PSMS.

And the DAS got upgraded to four cabinets and now it uses one-out-of-two taken twice logic instead of two-out-of-two, you know. Next slide.

The time critical DAS manual actuation, they got converted to automatic actions rather than the manual actions.

Now, you know, priority logic is employed throughout the safety system design. Before it was limited use of priority logic, you know.

And the additional design details on data communication, they got added to the DCD and technical reports so we got a lot more technical information to be able to, you know, base our review on.

CHAIR STETKAR: Dinesh, I haven't looked

through your slides. Are you going to talk more later about those time critical operator actions or is this the only time to ask about those?

MR. TANEJA: We are having a discussion on DAS later on. I think Erick can explain a couple of the time critical manual operator actions that were being performed from DAS that got converted to --

CHAIR STETKAR: Were you planning to do that later or now?

MR. MARTINEZ: We can do it now or later, whichever. There's a slide specifically that will also mention this so --

CHAIR STETKAR: Okay, that's fine. Let's do it later when we're thinking about DAS then. Thanks.

MR. ASHCRAFT: My name is Joe Ashcraft and I guess I drew the long straw so I got redundancy. This will be the first of many slides addressing our principles.

I guess based on this morning there really didn't appear to be any issues so I just wanted to comment that we have no issues at this time in our SER.

I have noted several places in our evaluation where we talk about redundancy and some of it is redundancy of dual controllers, et cetera, that was used more in reliability.

But our finding in this aspect is from single failure we have no issues and there is an ITAAC to verify that later on. So unless there's questions I think there's a lot more pending issues.

MEMBER BROWN: The only question I would have is we talked about the utilization of the priority logic for both the DAS final output stages and, you know, I kind of left that. We finished that discussion. I mean, that's part of the safety systems for the DAS part of it.

I presume you all got yourself comfortable with that one point of common usage of logic, that it's simple enough that in the testing of the 3 months and the other 24 months was satisfactory to convince you that that would maintain the sanctity of that particular use.

MR. TANEJA: The PIF module right, the power interface module?

MEMBER BROWN: Right, yes.

MR. TANEJA: Actually that was one of the item that we actually got our hands on when we were in Kobe and ran some, do some testing on it, you know, so we saw the hardware-based, non-software-based portion of the board which is like separated from it and the input's coming in and we saw a complete 100 percent test of a very simple logic, you know.

So it was so many input, so many outputs and, you know, it was thoroughly tested and I believe every board is going to be tested, you know, for each application.

MEMBER BROWN: Well, that's on a design basis. But, I mean, the operational they explained their ability to operationally test it, like, every 90 days or something and then every two years you had a complete test where you actually saw that it -- I just wanted to make sure you were satisfied with the lack of complexity and the simplicity of it, the fact that that's a single point now for both the DAS and the normal automatic systems and it's just a question. You're shaking your head up and down. I'm going to take you at your word.

MR. TANEJA: Yes, it's a single point. I understand that, right? But, you know, if you look at ESFAS, each component has its own unique PIF module, right? So you have redundancy between Train A/Train B so, you know, you have independence in that respect so they're redundant.

So if you do fail, let's say, a random failure of the PIF module you lose one component, one pump. You still have the other train available to you so we were okay with that.

MEMBER BROWN: Okay.

MR. TANEJA: Yes.

MEMBER BROWN: That was it for my question on that.

MR. ASHCRAFT: And following up with John's wanting us to hurry up, these are just kind of follow-up slides. We did talk about redundancy as they did at PCMS but really this has nothing to do with our safety finding. So unless there's questions, I'm done. Next slide.

MALE PARTICIPANT: Khoi.

MR. NGUYEN: Hi. My name is Khoi, Instrumentation and Control Branch 2. The review of independence cover four areas, physical, electrical, functional and communication independence.

The staff found that with reasonable assurance that the US-APWR design on physical, electrical and functional independence met the regulation and guidelines.

There are some issue and concern associated with communication independence. Most of the concern and issue would result either by the proposed design change that you had heard this morning or the --

MEMBER BROWN: External communication or are you talking about the watchdog timer?

MR. NGUYEN: No, some of these agenda we'll cover later if you --

MEMBER BROWN: Oh, okay.

MR. NGUYEN: -- if you are interested and either by the design change or the addition of the significant amount of detail design, design details that help the staff understand more about the design.

However, there's one issue that remain as an open item that I will cover later. For the purpose of this presentation I only focus on the communication independence unless you have a question on other areas.

MEMBER BROWN: No, that's fine, fine. You can go ahead.

MR. NGUYEN: Our staff review of communication independence cover independence among the safety trains and between safety and non-safety system.

This symbol plot diagram show the interface between safety and non-safety system. Unless you have question, I will skip this slide. And here are the regulation and guidance that reveal independence.

Among the safety train, the communication limited to voting logic, bypass status and status of the signal and the communication performed by one-way, point-to-point data link protocol with no communication handshaking.

Failure or communication fail of a single train will not affect the other train. All safety functions are performed without interruption by any other signals. You heard a lot about the priority logic this morning so I wouldn't address more about that.

CHAIR STETKAR: Khoi.

MR. NGUYEN: Yes.

CHAIR STETKAR: You heard a lot about it and you heard a little bit of concern on my part about how do we know that the safe state is really the safe state for all events. Did you look at that, and particularly SLS priority logic?

MR. NGUYEN: Well, I heard this morning from MHI that they haven't come up with a final determination which one is the safe state or not. But during the audit in Kobe, we was able to witness the demonstration, the priority logic if the safety signal or the signal including the safety state signal had the priority over the non-safe signal. But why safety signal to be on the list, I don't know.

CHAIR STETKAR: So you haven't looked at that?

MR. NGUYEN: At least I looked at some of them but not the complete list.

CHAIR STETKAR: Why not?

MR. NGUYEN: We want to ensure that the safe state signal had the priority over the non-safe state signals and that's a --

CHAIR STETKAR: I understand that but, for example, the example that I used for emergency feedwater, there are two safe state signals. One is closed. One is open.

Now, we heard a rationale about why they selected the closed signal as the one that would have priority. There might be a different rationale that said the open signal might be the one that should have the priority.

And there are a number of components, I'm not sure how many because I certainly didn't do the review, where there might be that type of disparity and I was just curious whether you tried to identify those and give yourself assurance that, indeed, the selected safe state made sense.

MR. TANEJA: No, we did not go that far.

MR. NGUYEN: In order to answer your question I need the coordination review with the reactor system.

CHAIR STETKAR: Yes.

MR. NGUYEN: Because with the I&C review perspective we don't look to that depth what signal should be safety state or which one is not. We will ensure that the safe state signal have the priority over the non-safe state signal.

MR. TANEJA: Because I believe what we are, you know, hearing is that safe state really depends on the mode of operation.

CHAIR STETKAR: Yes.

MR. TANEJA: Right? Now, we are getting into the details of modes of operation and I think we had similar -- when we were dealing with the development of the post-action monitoring parameters, similar kind of concerns because it's a performance-based list.

So we're really looking at, you know, how do you manage certain events and whether you use what's available, right? So here I think I'm hearing is the same thing, that I need the level of detail where I know exactly, you know, what is a safe state for what given mode of operation?

The I&C Chapter 7 did not go into that depth. It's just basically looking at priority scheme, you know, how do they handle priority scheme?

CHAIR STETKAR: Given a safe state, does the system invoke that safe state?

MR. TANEJA: Right.

CHAIR STETKAR: The problem is that if you look at Chapter 15 analyses, the Chapter 15 analysis for a steam line break inside containment, we'll want to close certain valves. A separate Chapter 15 analysis for another type of trans-interaction, might want to open those same valves.

So Chapter 15 doesn't look at the integration. Chapter 7 doesn't look at the integration. Nobody looks at the integration?

MEMBER BLEY: Could Chapter 18 look at the integration? Is there anybody here who's --

CHAIR STETKAR: Chapter 18 is human factors.

MEMBER BLEY: Al was here all day but he's disappeared. Well, it is but it's the interface too and they are looking at accident scenarios and all of that. So I don't know where it gets looked at but with this design because --

MR. TANEJA: But it's a very good question I think.

MEMBER BLEY: -- because you cannot override that unless you get in and manually manipulate things operators don't usually manually manipulate. It ought to get looked at. It could be very significant.

CHAIR STETKAR: There may not be all that many places where you have this potential conflict. I mean, I'll give you the fact that starting a high-pressure injection pump or starting an emergency feedwater pump on -- I'm not quite sure when you might want to shut them off unless you can overfill --

MEMBER BLEY: In a cold --

CHAIR STETKAR: Right.

MEMBER BLEY: -- cold fracture thing but maybe they're immune from that. I would hope so. I didn't look at that yet.

CHAIR STETKAR: They have other protections against that particular one but the whole notion is going through that. There is a rationale somewhere. MHI said it's an internal document so it's not anything that we've seen.

MEMBER BLEY: I meant to ask but I didn't. I don't know if one day there will be a table of all the safe states. It's not there now.

MR. TANEJA: We'll follow up on this. I think it's a valid question.

CHAIR STETKAR: Okay, thanks.

MR. TANEJA: You know, so we'll follow up on it, you know, because I think what we hear is that, you know, you really can't override some of these functions, I mean, meaning like --

MEMBER BLEY: The system wins, yes. You can't --

MR. TANEJA: Yes, if the system says that a safe state is open, it'll open it, you know, and if you want to --

MEMBER BLEY: It will stay open unless you go into the, you know, disable the logic.

MR. TANEJA: Okay. I'll follow up on this.

MEMBER BLEY: That's not a terribly hard thing to do but it's not what we like people to do with power plants.

CHAIR STETKAR: Yes.

MEMBER BLEY: We used to go in and use popsicle sticks to jimmy relays and things and jumpers and we don't do that anymore.

CHAIR STETKAR: We don't do that anymore.

MEMBER BLEY: Because it leads to --

CHAIR STETKAR: People leaving popsicle sticks and jumpers in places where they ought not to be.

MEMBER BLEY: That was a few years ago but it was real.

MR. TANEJA: Beyond design basis.

(Laughter)

MR. NGUYEN: Okay, this design feature you saw earlier today so I don't repeat it.

On this diagram I would like to point out the communication between safety and non-safety system. You can see the arrow of the data flow. The non-safety signal can only go into the safety system through the COM-2 at the sub-communication system and I will cover that later on.

Communication from non-safety to safety system through COM-2 are limited to manual control commands of the safety component from operational VDU and manual operating maintenance, bypass, lock, reset command from operational VDUs.

CHAIR STETKAR: Khoi, let me ask you before you get to this one and you can tell me maybe you'll address it later.

As part of the non-safety to safety communications in the SER, there's a statement that says, "The applicant responded," and it's to RAI 7785866, Question 07.09-24 -- I only mention that because in case you need to look it up tonight -- "on November 28th, 2012, and stated that the applicant has decided to employ the hardwired interface design for non-safety automatic control signals from the PCMS to the PSMS to make the data communication design simpler."

What does that mean? Because I didn't hear anything about any hardwired anything or other this morning.

MR. NGUYEN: I think we already cover but maybe in different language. Originally the non-safety automatic signal was connected to the safety signal through the unit bus and we said that's very hard for us to review. It's very complicated.

So after, you know, several RAI trials and public meetings, MHI had agreed that, okay, we don't connect those signal through the unit bus. We will hardwire and those signal no longer, you know, connected to the safety system via unit bus, so --

CHAIR STETKAR: Do you have an example of a non-safety automatic signal that is processed this way? I mean, I understand the manual stuff so --

MR. TANEJA: Yes, the typical automatic signals are like existing PWRs. They have some balance of plant signals that are preempted that may come into the safety system.

CHAIR STETKAR: I'm asking for some -- I want to understand what we're talking about here.

MR. TANEJA: Well, I think a handful of signals that come in -- pressurizer level you said?

Pressurizer heaters? You know, I guess I can elaborate on the signals. So what happens is the unit bus is connected to the entire plant, right? So these data is available on unit bus. Now, one way to do it is just bring it down into COM-2 and just come in and do the action.

CHAIR STETKAR: Yes, right.

MR. TANEJA: Now, here what we felt is the manual action we know when they're being taken by the operator using the operational VDU. So if there is a malfunction because of whatever reason, at least you know that, you know, you just took an action so you're more aware of it.

But if an automatic signal is floating around on the unit bus and can come in any time, we didn't feel comfortable with that one. We were trying to ask more questions.

So one alternate was they said, all right, what we'll do is we'll bring it in hardwired to isolators into an I/O module that eliminate use of the unit bus and that interface where it would be coming in.

And if there was a fault on that signal, now it's a non-digital signal so it can be treated as a traditional interface. That's really what the issue is.

CHAIR STETKAR: So essentially in the context of this diagram, you'd have a non-safety automated controller someplace floating around up there at the top with a wire that comes down to the safety bus that finally gets processed.

MR. TANEJA: Right.

CHAIR STETKAR: Is that the way to think about it?

MR. TANEJA: See, the way it is is on each controller, right, ESFAS controller, let's say, or RPS controller, you have the I/O modules, right? So the inputs come in, outputs go out.

So the input that's coming in from non-safety site, you know, you bring it in, you put in an isolator, the traditional isolator like we saw for the DAS. And then you bring the signal in from that way.

CHAIR STETKAR: And when you say ESFAS controller, you really mean down at the SLS level or do you mean up at the --

MR. TANEJA: Any one of the controller, right? I mean, we are really treating that signal as a traditional interface and that isolator, which is a Class 1E isolator, becomes our boundary of safety.

So what we are saying is we take credit for that so any failure of the signal on the other side would not have an adverse impact to safety.

CHAIR STETKAR: Got you, got you. Thank you.

MR. TANEJA: Thank you.

MR. NGUYEN: For the data communication between the safety and non-safety system, the staff used digital I&C interim staff guide in ISG-04 as the key guidance. And the following support the staff finding. All safety function, whether manual or automatic, are performed without interrupt by the non-safety signal regardless of whether the known safety signal are valid or erroneous.

And, again, the priority logic provide that prioritization for safety function over non-safety signal. And these are design feature we cover earlier so unless you have question I will cover those design features.

MEMBER BROWN: Let me ask. You don't have to go back to anything but relative to John's question, the question of the, you know, input from the non-safety place, the operational VDU.

I went back and I looked at the figure that MHI, you know, the overall figure for the ESFAS and SLS.

And I don't see any lines that give the impression of going directly to the safety bus other than coming down through the safety VDU from the remote console or from the operator console, the operational VDU. Everything else seems to come down through the unit bus and the COM, COM-1 or COM-2.

(Crosstalk)

MR. NGUYEN: Yes, because there is no data below --

MEMBER BROWN: It's Figure 7.3-1 that you have the general picture. I mean, it's kind of a very high-level picture.

MR. NGUYEN: Right, it is a high level. It doesn't get into the --

MEMBER BROWN: But I would have expected, based on what you were talking about, it's something manual or automatic. I didn't see --

MR. TANEJA: Well, the manual controls are still coming from operational VDU, right? That's an open item that we are still --

MEMBER BROWN: Yes, well, right now those come through that COM-2 --

MR. TANEJA: They come through the COM-2. COM-2 --

MEMBER BROWN: -- and down to the safety bus before they get to the SLS.

MR. TANEJA: Right. Now, there were also previous design had automatic signals from non-safety side that were coming in as well.

MEMBER BROWN: And John's looking for some examples of that. I mean, I understand pressurizer heater control is an obvious --

MR. TANEJA: Well, there's a handful of signals that do come in, you know. I don't know where, you know, those come in through and since they have the entire plant on the unit bus, so you have that data available in that data packet on the unit bus so you can use it anywhere you would need to use it. So it's a convenient way of getting to it, you know.

MEMBER BROWN: Well, that data comes from the RPS system, right, the plant parameter evaluate. That's where the parameters are actually, the sensors come into the --

MR. TANEJA: The non-safety signals are coming from your non-safety side of the plant. Those are the signals that are used to maybe take some protective action preemptively which they don't take credit for, maybe like the turbine trip, for example. That signal does not come in over the unit bus. You know, it comes in through the hardwired interfaces. That's what you're talking about. Some of those --

MEMBER BROWN: All right, go on. I'm just trying to get a handle on it. Go ahead.

CHAIR STETKAR: I got it. You know, there was just that one paragraph in the SER. I understand what's being done.

MR. TANEJA: I don't think the cartoon shows that.

CHAIR STETKAR: No.

MEMBER BROWN: No, it doesn't. It's not on here.

CHAIR STETKAR: Well, probably because it's not a general function. You know, like you said, there's probably a handful of specific applications, if you will, that would have that feature.

MR. NGUYEN: Again, on this slide the design features have been covered by MHI earlier. Maybe slightly different but basically the design features are the same so if you have any questions --

MEMBER BROWN: This question is open right now relative to, I mean, we discussed this with MHI relative to how does the watchdog timer actually execute a partial reactor trip in a train if it locks up, if the timer times out.

So this says what it's supposed to do but they agree to do something relative to providing a figure --

MR. NGUYEN: Detail design on how to escape it.

MEMBER BROWN: -- how the watchdog timer operates and how it actually executes that. I'm not working on the four times gross, whatever it is. That's not unusual, okay, and that's in the transcript.

There's a series of two or three questions that they said they would do something with relative to providing it, hopefully in the DCD or someplace where it's documented, whether they revise the technical report or whether they do a DCD revision to show that.

So I'm just saying just the words themselves as long as, that's an open issue as far as I'm concerned until we see how that gets done.

MR. NGUYEN: Okay.

MEMBER BROWN: Okay?

MR. NGUYEN: The staff state earlier that they perform audits. The purpose of the audits was to reveal the documents and to confirm the key design feature as described and listed in the technical and topical reports. The staff had witnessed the demonstration on the actual MELTAC controllers to address the staff concern.

There's one open item associated with the independence review. The staff request the applicant to justify the use of the non-safety component to operate safety equipment. In this case it's operational VDU.

The justification for the use of operational VDU is based on HFE. That's enhanced performance of safety function. That's including reduce the task burden and reduce the potential of human error.

So the staff had been coordinate with the human factor experts and also we request the applicant to provide more testing or quantitative analysis to demonstrate that the use of operational VDU actually enhance the performance of safety function.

Also staff request the ITAAC to test all the transmission conditions, either normal or abnormal of the safety and non-safety signal interface.

MR. TANEJA: We have not received the RAI response yet.

MR. NGUYEN: These are ongoing items.

MEMBER BROWN: This seems kind of subjective. I mean, how do you gauge enhancement?

MR. NGUYEN: That's why we need the --

MEMBER BROWN: Is there a metric of --

MR. NGUYEN: -- in-depth review and more detail.

MR. TANEJA: Well, there are two issues here. Okay, when we look at the ISG-04 guidance, you still have to assure that interface from non-safety to safety does not adversely impact any of my safety function.

That is independence question that, you know, has to be answered, that we have reasonable assurance that there is no adverse impact with that connection to the safety functions. That's one issue.

And I think we have criteria in our ISG-04 which says don't make that connection unless you have some enhancement to safety. I mean, there has to be a good reason for you for making that connection.

So that's a separate way of answering that question but regardless of what the answer is independence has to assure that there is no adverse impact to safety.

CHAIR STETKAR: I understand that. But there's a difference between no adverse impact and enhancement.

MR. TANEJA: Right.

CHAIR STETKAR: If it's no adverse impact and neutral to safety, that's not enhancement but it's no adverse impact.

MR. TANEJA: Right.

CHAIR STETKAR: And I think my concern personally from having operated a plant where you had to have two people control feedwater because the controls were widely separated and a single person couldn't do it and you lost feedwater a lot because of that, having a control for a non-safety charging pump located in one place and a control for the safety-related charging valve because it's safety related because it gets a containment isolation signal, for example, in another place, strikes me as not necessarily being the best way to run a nuclear power plant exactly.

And so, you know, this subjective HFE thing is not really subjective when you get in the real world and try to operate things, like controlling feedwater or charging or letdown or, you know, anything that the operators really get involved in, so.

MR. TANEJA: And that's where we are interfacing with the Human Factors Branch to, you know, get that assessment from them to see, you know, is there any objectivity to it or is it all subjective that there is enhancement?

CHAIR STETKAR: Well, I think what I'm trying to understand here is I personally absolutely agree with this notion that no non-safety to safety interface should adversely affect the safety function. I agree with that.

On the other hand, if the burden of proof is for MHI to prove to you that that enhances the safety function, I got a really problem with that personally because that's a much different burden of proof. So if you're asking MHI to prove that that connection must enhance the safety function, I have a real question about that.

MR. TANEJA: Well, see, this is still, you know, we don't have any acceptance criteria on any qualitative number. What does that really mean, enhancement, right?

CHAIR STETKAR: Well, I'm asking. You said this is still an area of open discussion.

MR. TANEJA: It is.

CHAIR STETKAR: You haven't gotten response but I'm trying to get a sense back from you who've written the RAI and will have to review the response to that RAI, are you as a staff essentially asking MHI to prove that that connection enhances safety?

MR. TANEJA: Yes, that's our question.

CHAIR STETKAR: That is the question?

MR. NGUYEN: To make it clear, to ask MHI to prove that the connection enhances safety is very subjective and very big and is almost impossible to do it.

But we actually asked the MHI to justify how the connection enhance the performance of safety function. That's a different thing. That's something to do with HFE. The safety concern is safety function.

MEMBER BLEY: I kind of agree with Mr. Stetkar here on this one.

MR. SPRENGEL: Well, unfortunately some of the staff are not here to discuss this but the communication we've received from the entire staff is looking at the global perspective as you're pointing out and mainly from an HFE perspective the staff agree with you and they do see the safety benefit.

CHAIR STETKAR: Okay, thanks. And sort of hearing your feedback I'm a little bit less concerned about this notion of proof of enhancement versus sort of a global assessment of, you know, one ought not to hurt it but --

MR. SPRENGEL: And I think whenever we discuss collectively with the different areas the same perspective comes out.

CHAIR STETKAR: Yes, okay. Thank you. Thanks.

MR. TANEJA: And I guess the status of the RAI response, this morning's presentation, it was mentioned that MHI would do a quantitative analysis on this one. It was on their Slide 82. I think that's what they're proposing to send so we'll see what that looks, you know.

It says, "MHI can provide RAI response demonstrating safety merits on operational VDU including quantitative analysis for reduced task burden."

CHAIR STETKAR: Okay. Thank you.

MR. NGUYEN: That's all I have for independence. Do you have any question regarding the independence?

CHAIR STETKAR: Anything else? No. Good.

MR. TANEJA: So next topic we want to talk about is determinism and these were the regulation and guidance that are applicable to our review for determinism.

And our findings verified that, you know, software failures of system malfunction, you know, are the system malfunction that accommodated by the internal diagnostics that are built in and the watchdog timers, you know.

You, I guess, saw that they showed you each function is executed, cyclical similar task processing. Cycle times are predetermined and fixed for all of the processors and the message size and communication rates are constant and that's what we found. Next slide.

One other thing that we did ask the question that we found out was that it was on processor loading. Now, what we were told, that based on their design that the processor can run 100 percent loading in a very deterministic fashion. However, their design practice limits it to 80 percent loading to allow for margins and everything else.

MEMBER BROWN: Well, all you're talking about is they leave enough time in the cycle time that they're not pushing it right out to the edge every time.

MR. TANEJA: Right.

MEMBER BROWN: And that should be the case. With a fixed cycle processing, that should not be a problem at all.

The only time it is is when you have interrupt-driven execution, you know, executive program which decides to do all kinds of miscellaneous things at variable times where you can jam the thing up with what I call background tasks instead of doing your main cycle programming.

MR. TANEJA: Right.

MEMBER BROWN: The fixed cycle just works, makes everything kind of easy.

MR. TANEJA: Yes, so they have that, you know, the spare time diagnostics that they run and whatever the time allowed is, you know, but it's a fixed cycle time.

You had a question about the external interrupts versus internal interrupts. You know, what's in there, what we saw, was that there are two internal interrupts. One is a CPU interrupt and one is a peripheral interrupt.

MEMBER BROWN: Yes, I read those.

MR. TANEJA: Right. CPU interrupt is the one that halts the processing and generates a fail-safe output and then --

MEMBER BROWN: Logical thing to use. That's called --

MR. TANEJA: And then the peripheral

interrupt is kind of alarmed but the process continues, you know, so that's a distinction between the two of them, you know. And the rest of the information is pretty much what we saw this morning. Next slide.

And we also reviewed the response time analysis that is part of the technical report on response time for I&C systems. So the way that whole report is put together is that there is an analytical limit which is based on Chapter 15 so that becomes the timing that they assign. It's the allocated time for that function, safety function, okay?

So the calculated time has to be for the entire, from the sensor to the operating component needs to be bounded by this allocated response time that's in Chapter 15.

So that's really what the report is based on, is this gives us a list of all the allocated time that came from Chapter 15. Then it adds up every single timing factor including all the transmission rates for each of the loop.

And then there's an ITAAC in place which will actually test, calculate the minimum and maximum time and verify that the functions are performed within the allocated times that --

MEMBER BROWN: That's from input to output, input to output?

MR. TANEJA: From the sensor operation to the actual component -- the biggest delays usually are, you know, you got valves that have 15-second operating time maybe on a motor-operated valve.

Your transmitter or your level sensor probably have a bigger time delay than the digital system may. You know, I mean, we heard 50 millisecond. We heard, you know, 100 millisecond, 300 millisecond.

But when you look at some of these times, it's like 2 seconds, 3 seconds in Chapter 15 analysis. So, you know, so those, you have to account for the other components, you know, so. Next slide.

Any questions on determinism? Okay. Erick, you want to start with D3?

MR. MARTINEZ: Yes. Well, this slide pretty much is a quick overview of just the DAS design features. That was discussed earlier this morning so unless you want me to go over them in the interest of time I'll keep going. Does anybody want me to discuss just the basics for the DAS? Okay. This is the policy and guidance that the staff used. Next slide.

CHAIR STETKAR: Yes, actually, I did want to ask a couple of things. In the DCD there's a discussion about a couple of different switches and I didn't ask MHI this morning for a variety of reasons.

There's one switch that's called a permissive switch for DAS HSI and in the old design where you only had two DACs that switch enabled power to DAC 1 such that if that switch was open because it was a two-out-of-two logic you couldn't get DAS actuation.

MR. MARTINEZ: Yes.

CHAIR STETKAR: There's another, I'll call it a switch because I don't know what else to call it. There's a diverse actuation signal defeat switch which basically defeats all of DAS.

MR. MARTINEZ: Which is actuated in the --

CHAIR STETKAR: Both trains.

MR. MARTINEZ: I think it's in the VDU. It's shown in there, yes. Yes, there is a switch.

CHAIR STETKAR: Because all I have is, you know, cartoon schematics. First of all, those are two separate switches. There's one that defeats all of DAS and a second one that -- does the power switch still exist in the new design?

MR. MARTINEZ: Yes.

CHAIR STETKAR: It does. What does it do? It shuts off power to two of the cabinets now, because it's one-out-of-two taken twice.

MR. MARTINEZ: What power switch

specifically? You're talking about in the --

CHAIR STETKAR: Well, all I have is names of things.

MR. MARTINEZ: Do you know the specific section that you're going through? Maybe I can --

CHAIR STETKAR: Of the SER or DCD?

MR. MARTINEZ: SER, yes.

CHAIR STETKAR: Well, it's the DCD.

MR. MARTINEZ: Or DCD, yes. Either one.

CHAIR STETKAR: E is Section 78111, and this might be a take-away if you want to come back tomorrow, that talks about the permissive switch for DAS HSI. And that's simply a power on/off switch.

MR. MARTINEZ: That's the second sentence in the last paragraph in DCD?

CHAIR STETKAR: I don't know. I excerpt these things from -- don't hold me to lines or --

MR. MARTINEZ: Okay, okay. I think from the draft Rev. 4 version that we have, that name is being taken out for the sake of confusion but --

CHAIR STETKAR: Yes, hence, my confusion.

MR. MARTINEZ: Yes.

CHAIR STETKAR: But let me ask either you or maybe MHI can help me on this. I didn't ask this morning because I have a different question for the staff.

But just to avoid my confusion, in the new design where you now have four DAAC cabinets, is there still a switch that cuts power to two of those cabinets? I'm assuming it has to be two because otherwise it wouldn't be different.

MR. MARTINEZ: Yes, but for the sake of --

CHAIR STETKAR: If we don't have a quick answer, let me just get it out on the table. I want to understand whether there are one or two switches first of all.

I know that there is some sort of DAS defeat switch because we've already established that that exists and in the design document that DAS defeat switch defeats all of DAS. I don't care where they're at, you know, two trains or two cabinets or four cabinets. DAS is out of there.

I'm trying to find out whether there is also an additional power supply switch that cuts off power to half of DAS such that regardless of the DAS defeat switch, you know, DAS won't work.

MALE PARTICIPANT: And now.

MR. SCAROLA: Okay. First let me talk about the DAS defeat switch.

CHAIR STETKAR: Yes.

MR. SCAROLA: That's actually defeating all the automated functions in DAS so that you can shut down the plant.

For example, one of the automatic inputs in DAS is low pressurizer pressure. Well, I have to defeat that otherwise I can't depressurize, right? So that's what the defeat switch does, blocks all the automated functions.

Now, there are two manual switches. There's an actuation switch for each individual function on the diverse HSI panel so, for example, there's an actuation switch for safety injection, a system-level actuation. There's an actuation switch for main steam isolation valves.

However, we don't want a single switch failure to give us these spurious actuations so we have this second switch that is probably misnamed but it's called, I think, DAS power disconnect switch.

So when you activate the power disconnect switch, you get one half of the two-out-of-two logic for all the manual functions. You get one out of the two, the second one-out-of-two, to give you two-out-of-two is the individual switch. So the power disconnect gives you one leg for every function or it eliminates one leg normally. In normal operation you don't have that leg.

CHAIR STETKAR: Okay. So, now, if I'm the operator sitting in the control room and some alarm goes off that says DAS, DAS, DAS, I must actuate that switch --

MR. SCAROLA: The power disconnect switch.

CHAIR STETKAR: The power, and then I must go to the DAS panel and push the appropriate button for manual.

MR. SCAROLA: They're both at the DAS panel. The power disconnect is like a master manual enable switch at the DAS panel.

CHAIR STETKAR: Okay, it is on the DAS panel?

MR. SCAROLA: On the DAS panel.

CHAIR STETKAR: All right. Now, to MHI in this, I needed to find out if there were two switches or one switch.

Now that I know that there are two switches, this power disconnect switch, in the DCD this, I'll call it the power switch for lack of confusion, is located in the main control room but physically separated from the DHP. Physically separated from the DHP to minimize the effect of fire propagation. You just told me it's on the DHP.

MR. SCAROLA: I'm wrong.

CHAIR STETKAR: So now if I have a -- oh, you're wrong.

MR. SCAROLA: I got confused. It's on the DHP at the US-Basic HSI simulator in Pittsburgh. However, we recognized in the design that we could have a fire inside the DHP itself.

CHAIR STETKAR: Hence my question about where is it.

MR. SCAROLA: Therefore we decided that we needed to have some physical separation.

CHAIR STETKAR: Yes.

MR. SCAROLA: So one is actually on the DHP and another one is physically separated. We have not identified a specific location.

CHAIR STETKAR: You don't know where it is? My question was going to be where is it and did the staff look at where it is such that if I have a fire, wherever it is, I can both disable a bunch of stuff in my normal plant in that location and disable DAS? Because if that switch is open, DAS doesn't work.

So is there then a fire location in the control room that will both affect normal safety systems and DAS because of the location of that switch? Because it's not on the DAS panel and it's not clear whether -- I'm not sure I want it on the DAS panel.

But I want to make sure it's in a place in the control room where if I get a fire in that location

I don't somehow simultaneously affect things that, you know, both of those functions. And you've told me that you don't know where it's going to be located yet.

MR. SCAROLA: It's a detailed design aspect. All we know is that we have to maintain a fire barrier between the two switches and we have not identified a specific location for that switch.

CHAIR STETKAR: Yes, I'm more concerned about what else is around the -- if this is a separate switch like a light switch on a post in the wall, I'm probably okay with that.

If it's a switch on one of the panels in the control room, I'd be pretty interested on what else is in that panel or in proximity to that panel. So that's something that hasn't been looked at obviously because you don't know where the switch is.

MR. MARTINEZ: We'll look into it. Thank you, yes, and they don't specify the specific location --

CHAIR STETKAR: No, all it says is it's separated and I can understand why it should be because I wouldn't want a fire in the DAS panel to inadvertently cause DAS actuation, which it could if the switch was there.

On the other hand, if it's located somewhere else, the other place of its location can be important because a fire there could affect now two functions. Sorry, for the long, involved thing. It took me a while to --

MR. MARTINEZ: No. Thank you.

CHAIR STETKAR: -- get to the point where I could even ask an incoherent question.

MR. MARTINEZ: Okay, I guess I will continue. The next slide, part of the staff's review, and I guess we already discussed the involvement on the topical report SE and the staff will look into that.

As part of the SE for this topical report, there were a couple of application-specific action items that were developed as part of the SE for the topical report. The staff addresses those in the SER.

Additional information here is pretty much that the applicant references that topical report and the D3 coping analysis technical report MUAP-07014. Basic information that the DAS functions are design based on a best estimate D3 coping analysis and that their review of the D3 coping analysis is coordinated with the experts from Human Factors and Reactor Systems.

Here is a slide about pretty much the basic DAS design changes that occurred during our review. I'm going to go over them real briefly here. The ECCS actuation from manual actuation was converted into automatic.

And I guess this would be a good point to -- you had a question earlier about the automatic actions or the manual actions from DAS that you wanted to ask earlier. I guess this would be a good slide if you had anything there.

MEMBER SHACK: Yes, you had an earlier slide and you said you --

(Crosstalk)

CHAIR STETKAR: Yes. Let me, I've got a few questions on DAS and the review.

MALE PARTICIPANT: Time critical operator.

CHAIR STETKAR: Yes, I understand. You've got two slides. Get to the end and then --

MR. MARTINEZ: The last one? All right.

CHAIR STETKAR: Then I'll raise the questions I had.

MR. MARTINEZ: Okay, perfect, okay.

CHAIR STETKAR: It's easier.

MR. MARTINEZ: Quick changes in the DAS. DAS upgraded to seismic classification to Category 1. The DAS cabinets were changed from two to four using one-out-of-two taken twice logic and there were a couple of other upgrades based on the internal and external hazards done to DAS.

And this is my final slide on this so I'll take questions after this. For the staff's open item, the staff has a couple of outstanding RAIs related to the current review of the D3 coping analysis and their reactor systems folks are working on evaluating and they are awaiting additional responses to these RAIs. And I guess I'll take any questions you have on these areas at this point.

CHAIR STETKAR: Before I get into human factors, there were a couple of things in the SER that I had questions about.

In SER Section 7.8.4.4, where you talk about ATWS, it's noted that an instrument power supply independent of the power supplies for the existing RPS provides the power for the logic and actuation device for the ATWS mitigation system, in the context of DAS now.

Well, that was true under the old DAS design where it had non-1E power supplies. As I understand it now, each of the four DAC cabinets are supplied from the Class 1E power. I believe I read that.

MR. MARTINEZ: Yes.

CHAIR STETKAR: Which seems to be the same power supply for the reactor trip system. So I was curious whether that conclusion in the SER about the diversity of power supplies for the ATWS function still is valid under the new design with its Class 1E power supplies. I don't know how you make that --

MR. MARTINEZ: The way we looked at the Class 1E UPS change for the DAS is that even if you lose power you still have that UPS which is a, pretty much a battery, correct? So you still have DAS capabilities even if you lose power.

But you are correct. It is still Class 1E and that is something that the last couple days we noticed and that is something that we want to clarify in terms of the independence from the Class 1E for the DAS to the Class 1E for the RPS. So you are correct and we are aware of that and we're looking into it. That is a small but, yes, thanks for mentioning it and yes.

CHAIR STETKAR: Okay. Hang on a second. Let me write a note. You'll find as you get older you don't remember anything more than about five minutes and if you don't write it down it's gone.

This does not affect new design. This is rather convoluted. There apparently was some question from the staff about the particular parameter indications, I think, on the DAS panel. And in particular there, I guess, was a question about containment pressure indications.

And I won't read the whole response here. I'll try to paraphrase it. In the response to the RAI MHI apparently said, well -- oh, I know. It was the status indication of containment isolation valves.

MALE PARTICIPANT: Right. Yes.

CHAIR STETKAR: That's it. I'm trying to read quickly through my notes. And MHI said, well, we have containment pressure indication and we can use that as a surrogate for the information that the containment is isolated.

And in the SER it says even though monitoring containment pressure is more comprehensive than monitoring the position of the containment isolation valves because it encompasses any breaches in the containment, not just penetrations related to automatic isolation valves, the containment isolation function can be indirectly monitored by the containment pressure instrumentation on the DAS panel. The staff found this approach acceptable.

Well, I understand how that sort of applies for a large penetration that's directly open to the containment atmosphere like the containment purge valves, for example.

It's not at all clear to me how I understand whether fluid systems are isolated by looking at containment pressure. For example, the normal letdown line is connected to the reactor coolant system. It gets an isolation signal on containment isolation.

Since the reactor coolant system is, until we get a really big LOCA or core damage, not connected to the containment air space, I'm not sure how I can use containment pressure to understand that the letdown line is isolated or a lot of other fluid systems.

MR. MARTINEZ: We did raise that concern as you saw from the RAI. The staff did communicate that concern with the Containment Branch folks.

And after their conversations, they came to the conclusion that because the DAS uses a best estimate analysis, the containment pressure would be -- we found the RAI responses here. The containment pressure would be a sort of offbeat indicator for containment isolation.

When you actuate containment isolation on the DAS, we assume that that function has occurred as needed, right? So --

CHAIR STETKAR: Well, that's actually the answer, is you have assumed that when you push the containment isolation button on DAS --

MR. MARTINEZ: Correct.

CHAIR STETKAR: The lawyers tell me that I assume that all of the valves go closed, and that's fine.

If the lawyers tell me that that's what happens, then I don't care what containment pressure is because the lawyers have told me that all the valves are closed.

I don't need a technical justification from that point because the technical justification doesn't make sense. I don't care whether you say best estimate or design. I'm sorry, I don't understand how you can use containment pressure to understand whether or not the letdown line is isolated.

Or if containment pressure is increasing slowly but increasing, do I know -- I'm an operator now. I don't know lawyers. Do I know that it's increasing slowly because there's a certain energy release rate into the containment or that there's a larger energy release rate but I have a small line open somewhere? And if I have a small line open, which line is it? I mean, I don't know. You know, I don't have that perfect knowledge as an operator.

So my concern is the staff's acceptance of an argument as if it's a technical argument and this notion of a best estimate analysis to say, well, containment pressure is an adequate surrogate for understanding that the valves are closed. I just don't understand that.

I can understand a legal argument in the same way as we accept design basis accident analyses that no more than one piece of equipment can fail or in this case since DAS is designed for beyond design basis accidents that we can presume that all equipment works. I understand those types of legal arguments.

But it bothers me that the staff acceptance of a particular condition is somehow justified from some pseudo-technical argument that I don't understand. Maybe I don't understand the technical argument but I'm not hearing a lot of convincing response in that area.

MR. MARTINEZ: Well, maybe I can't express it very well because I'm not an expert in the containment area. If there's a foul, you would use containment pressure in this aspect to have an adequate indication of containment isolation.

MR. JUNG: John, we'll take it back and --

(Crosstalk)

MR. MARTINEZ: I guess what we can do is take it back.

CHAIR STETKAR: I mean, there are a lot of lines, you know, main feedwater lines and there are a lot of lines that don't connect to the --

MALE PARTICIPANT: Understand. We'll take it back and --

MR. MARTINEZ: I apologize for not being able to give you a straight answer. We'll take it back and --

CHAIR STETKAR: Okay, thanks. Thanks. Now, hang on a second because as I said -- on the human factors engineering, I need to read my notes here and I'm also a slow reader.

In the sense of time, I'll just ask one of the questions. There are statements in here about you mentioned that there's this notion of any actions that had a time window of nominally less than ten minutes are now automated so that's why we have some of the automated DAS functions.

MR. MARTINEZ: Yes.

CHAIR STETKAR: I understand that many, if not all, I hope that the word all is closer to many, of the DAS manual actions will be included in the human factors engineering verification and validation process so that, indeed, there are nominal times in there.

You get times like 31-1/2 minutes because it's assumed that the operators will take 30 seconds to energize the DAS panel from this switch that we don't know where it is and 30 seconds to pull out the right procedure and 30 seconds to push the right button.

Now, that minute and a half presumes that the operators immediately and perfectly know that they must use DAS for any conceivable event. There's reference made to, you know, a unique alarm.

MR. MARTINEZ: Prompting alarm, yes.

CHAIR STETKAR: Prompting alarm, that that prompting alarm immediately and perfectly comes in at Time 0 and the operators immediately and perfectly always know at Time 0 such that the time window doesn't have any delays in it.

For example, the operators don't have any delays to say, hey, what's going on here? Maybe I ought to try to use the thing that I live with day in and day out every day of my life and then go to use DAS.

But that's fine. I have some confidence that, indeed, the human factors engineering verification and validation will sort out those times and still give you confidence that you have margin the same way as the local actions in the plant that right now have a nominal 30 minutes.

However, for the 30-minute one, in the SER it says the applicant explained that since actions after 30 minutes are not considered time critical the HFE evaluation is conducted to confirm HSI suitability and availability with reasonable consideration of time constraints. That's my minute and a half thing.

The applicant indicated that it does not plan to document a detailed assessment of the time margin between time available and time required based on the steps in special event EOPs.

That means that for any action with greater than 30-minute time available, they're not going to look at the amount of margin to that available time limit.

In other words, if for some reason they feel it can be completed in 29 minutes and 58 seconds, that's okay and that kind of bothers me. We've had some discussions about this before, is why --

MEMBER BLEY: Actually the guidance was revised to account for those concerns.

CHAIR STETKAR: Well, yes. On the other hand, the guidance was but in the SER for this particular it says --

MEMBER BLEY: Yes. No, I'm saying this is not in accordance with my understanding of the latest guidance.

CHAIR STETKAR: The staff finds this to be a satisfactory plan. Manual actions performed within 30 minutes of event initiation are validated and the results documented in accordance with regulatory guidance. True.

Manual actions performed after 30 minutes are also validated but detailed documentation of the margin between time required and time available is not planned and there is no regulatory guidance that suggests to do so.

MEMBER BLEY: I think that's not true.

CHAIR STETKAR: It's not clear.

MEMBER BROWN: No, we actually -- yes.

MEMBER BLEY: Yes.

MEMBER BROWN: We actually put stuff out --

(Crosstalk)

MALE PARTICIPANT: That guidance has changed --

MR. JUNG: John, we'll take it back. As you know, 7-19 we worked with you, issued --

CHAIR STETKAR: Yes, yes.

MR. JUNG: -- late last year or so, right?

CHAIR STETKAR: I'm just a little concerned because you said going in that you've had a lot of interactions with your human factors engineering folks so if you have and they signed off on this it means somebody hasn't gotten the message.

MR. JUNG: So given that new guidance that came, we'll take a look at it.

MEMBER BROWN: Well, there was an ISG for it and then it was put in the BTP --

(Multiple agreement)

MEMBER BROWN: -- 14 or 19, whichever one

--

CHAIR STETKAR: Okay. Anyway, Ian's got the right answer. Thank you. I just wanted to get it into the record.

MR. MARTINEZ: You have additional questions? Anything you want --

CHAIR STETKAR: Let's plan for timing. Let's get through the slides on simplicity if there aren't any more questions on DAS because there's only a couple more questions, then we've kind of hit all of the basic technical issues.

MR. NGUYEN: Hi, this is Khoi Nguyen again. The staff we approach on review of the simplicity is that the guidance discuss simple mean to address the hazard for specific design aspect like data communication and obviously that more complex design alternatives require a more in-depth and detailed review by the staff.

There are several design changes that make the system more simple and one of the examples that we covered several times this morning is the change in the connection of the non-safety automatic signal to unit bus, to the hardwire.

Also additional of the enable and disable switch to disconnect the non-safety signal to the safety system.

CHAIR STETKAR: When you say enable/disable, that's the -- I think it's called a permissive switch on the safety VDU or is this a separate switch?

MR. NGUYEN: That's a separate switch.

CHAIR STETKAR: It's a separate switch, okay.

MR. NGUYEN: Yes, based on a separate VDU we call enable/disable switch.

CHAIR STETKAR: Oh, okay.

MR. NGUYEN: Whenever you need to disconnect the non-safety signal from safety system, you, that's a soft switch not the hardwire switch.

CHAIR STETKAR: Is it one for each of the four divisions?

MR. NGUYEN: Yes.

CHAIR STETKAR: Okay.

MR. NGUYEN: On each except the VDU.

CHAIR STETKAR: If I go to the VDU, Train A VDU, and I hit this switch, does that just disable the non-safety into Train A or does it disable it for all four of them? So to completely cut off, I've got to hit it on all four of the safety VDUs?

MR. NGUYEN: That's correct.

MEMBER BROWN: To disconnect the

operational, the non-safety VDU?

CHAIR STETKAR: Yes.

MEMBER BROWN: Okay.

CHAIR STETKAR: Yes.

MR. NGUYEN: For simplicity, actually we don't have any regulation or guidance so for -- a good engineering practice we would like to review simplicity throughout all the design of the US-APWR and the following is data support the staff finding to support the simplicity. Suggest a single platform, the MELTAC controllers, be used for the entire branch, both safety and non-safety side.

Last is the hardwired analog system, not complex. It's not digital so it's not complex. All functions are executed with cyclical single task processing and no external interruption.

All the software module are executed during the fixed cycle time in a predefined order. Application software is written in a graphical symbolized manner so that function can be easily understood, verified and validated. And no dynamic allocation of memory. That will be fixed. Is not dynamic.

CHAIR STETKAR: I think for a variety of reasons what I'd like to do is to stop the presentation here if that's okay with the staff, unless you have conflicts with coming back tomorrow morning. Is it --

MR. JUNG: John, we're okay. We can come back tomorrow morning.

CHAIR STETKAR: You can come back tomorrow morning? Okay. The reason is when we get into the Software Program Manual and some of the nonconcurrence, they're linked and there's no way that we're going to get through all of the slides this evening.

So I think what I'd like to do is ask the Members if you have any more questions on the topics that we've just covered and, if not, we'll pick up tomorrow morning with your presentation, finish that out and if MHI has any follow-up items you want to bring back from questions that were raised, that's fine. We'll do that.

I'd like to thank the staff a lot for streamlining your presentation. I know that you all wanted to say a lot of things but I really appreciate. We're back much closer to being on time and we have, I think, pretty good hope of actually finishing tomorrow. Maybe not by noon but I really appreciated that.

And with that, we are recessed until tomorrow morning.

(Whereupon, the meeting in the above-entitled matter was concluded at 5:50 p.m.)

Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
US-APWR Subcommittee Meeting

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Friday, April 26, 2013

Work Order No.: NRC-4166 Pages 1-155

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-APWR SUBCOMMITTEE

+ + + + +

FRIDAY

APRIL 26, 2013

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

COMMITTEE MEMBERS:

JOHN W. STETKAR, Chairman

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR., Member

JOY REMPE, Member

STEPHEN P. SCHULTZ, Member

WILLIAM J. SHACK, Member

NRC STAFF PRESENT:

GIRIJA SHUKLA, Designated Federal Official

JEFF CIOCCO,

BRAD HARVEY,

IAN JUNG,

ERICK MARTINEZ,

STEPHEN MONARQUE,

KHOI NGUYEN,

TARUN ROY,

SESHAGIRI RAO TAMMARA

DINESH TANEJA

TUNG TRUONG

ALSO PRESENT:

TIM CLOUSER

KEVIN LYNN

MARVIN MORRIS

ROB REIBLE

HITOMI SASKI

KEN SAROLLA

RYAN SPRENGEL

DON WOODLAN

TABLE OF CONTENTS

P R O C E E D I N G S

8:30 a.m.

CHAIR STETKAR: The meeting will now come to order. We'll resume where we were yesterday. All of the logistics remain in effect.

I will remind people to silence your cell phones, please, and if you have anything to say from the audience, please come up to the microphone and make sure you identify yourself.

Jeff, I don't know if you want to say something for introduction or --

MR. CIOCCO: No. I think we are ready to go, John. Thank you.

CHAIR STETKAR: Okay. And the bridgeline is open.

Folks on the bridgeline, if you can hear us. We keep the bridgeline on mute. I will open up the bridgeline for comments after we finish the discussion of Chapter 7.

For logistics, I don't know if MHI has any responses to any items that we discussed yesterday.

Ryan, do you have anything?

MR. SPRENGEL: We do. There was --

CHAIR STETKAR: You do. Okay. What I'd like to do is finish the staff's presentation, get your input and then transition to the COL Chapter 7, so we just sort of keep the DCD and COL organized that way.

And, with all of that, Dinesh, it's your turn.

MR. TANEJA: Good morning.

So I hope everybody got a little bit of rest and now they are fresh to -- we appreciate yesterday's very constructive feedbacks, and I think it will only make the design better, you know, what we get from you guys.

So, what we'll do is, we'll start off with the software program and we'll wrap up the presentation. Then we have some feedback that we can give you from yesterday, and then just kind of go over some of the, you know, items that we took down from yesterday's meeting and, you know, I'm just going to run through them.

With that, I'm going to turn it over to Tom.

MR. TRUONG: Okay. Good morning. My name is Tung Truong. I work in the Office of New Reactors, and today we are discussing the software program manual, MUAP-07017 Rev. 4 and also the Appendix C, the SDOE, the software development operational environment.

The US-APWR SPM describes the software life cycle, process he used to develop the protection system/monitoring system, and this description has provided twelve separate plans in the SPM.

And some of those plans are the software development plan, software quality assurance plan, software verification/validation plan, software configuration master plan and so on.

And the majority of the software plans in the SPM are also applicable to the EPSMS augment quality.

These are the regulations and guidance the staff used. GDC-1, for example, states, in part, "The safety systems must be designed, fabricated, installed and tested to the quality standards commensurate with the importance of safety functions to be performed."

And the staff used mainly BTP 7-14 technical position 714 to do these evaluation. The staff has used twelve separate plans against 714 and the associated regulatory guides and endorsed IEEE standards.

For the security development operational environment -- that is Appendix C of the US-APWR software program. That was reviewed against Reg Guide -- Regulatory Guide 1.152, Rev 3.

MEMBER BROWN: That is the one we just went through? That's the most recent revision that we discussed a year or two ago?

MR. TRUONG: Yes.

MEMBER BROWN: Something like that?

MR. TRUONG: Yes, sir. And I think, Member Brown, you had a question yesterday concerning SDOE.

MEMBER BROWN: Well, yes. A question to them.

MR. TRUONG: Yes.

MEMBER BROWN: Hadn't gotten to you.

MR. TRUONG: Okay.

MEMBER BROWN: Other than yesterday after the meeting.

MR. TRUONG: I'm sorry. So, the staff went back to look at the -- based on the slides, that image I presented yesterday, that the -- the cartoon or the -- the diagram for -- I'm thinking of one, if you're looking at it, MHI.

The corporate electronic archive system and development environment system, so the staff found -- found that diagram -- not in the SPM, but in the -- in the UAP-07005.

And it is consistent, Member Brown, with what is in the last evaluation there. However, during the discussion yesterday, Member Brown and MHI was learned that, besides nuclear, perhaps other projects, not -- like nonnuclear. So that would be a concern. So, that's something the staff needs to discuss and then we try after the fact.

MEMBER BROWN: Okay.

MR. TRUONG: Is there any other question that you had?

MEMBER BROWN: No, no. It was on that.

MR. TRUONG: There is one open item, like Dinesh alluded to yesterday, and that is the staff requested the applicant MHR to explain or describe the process it plans to use to ensure that it's going to -- the safety software development process and the resulting software conform to NRC regulation and guidance.

And, in addition, the staff requested the applicant to include ITAAC to provide a fabrication of such a process.

Are there any other questions for the SPM or SDOE?

MR. TANEJA: I'll see if I can -- I think we just received a draft response. We haven't had a chance to --

MR. TRUONG: Yes. We have received a draft response from MHI earlier this week.

MR. TANEJA: Yes. But we haven't had the opportunity to review it.

MR. TRUONG: Okay.

CHAIR STETKAR: All right. We'll wait and see how that works out.

MR. TRUONG: Next is PAM's.

MR. TANEJA: Yes. The postaction monitoring parameters, MHI made a decision to include in the DCD the list of PAM variables, and the existing plans list, based on our Regulatory Guide 197, Rev 2 and Rev 3.

In that list, we have tables that proscribe for BWR type plans and PWR type plans what parameters we consider required for postaction monitoring.

All the new designs, you know, their list needs to be performed on the basis of Reg Guide 197, Rev 4, which is a performance-based. Okay. There is no list, so you have to use -- it endorses IEEE 497, which requires you to have EOP's and AOP's, and based on your management of these events, you know, what you -- what the instruments you need to use becomes your basis for developing this list.

EOP's and AOP's do not exist, and I guess they will exist after we license. So, one of the options was to have this thing as a COL action item, but they chose to proceed with a list at this stage.

So, we've been working with MHR. We've made a lot of progress. You know, we are almost there.

So, we had to use alternate methods, you know. I guess what they gave us to look at is -- the emergency response guidelines are in draft.

They have prepared them, so we audited the Emergency Response Guidelines to see how those events are describe. And I guess, since it is a PWR 4-loop unit, a lot of the PWR PAM variables are directly applicable.

So we had asked MHI to do a comparison between the Rev 3 list versus their list to look at the delta. I guess there are some design differences.

MEMBER BROWN: Rev 3 of the DCD was --

MR. TANEJA: Rev 3 of the Regulatory Guideline 1.97.

MEMBER BROWN: 1.97.

MR. TANEJA: Okay.

MEMBER BROWN: Yes.

MR. TANEJA: Which provides a proscribed list of parameters.

MEMBER BROWN: That's before --

CHAIR STETKAR: As if every plant in the world is precisely the same.

MEMBER BROWN: No, I understand that.

When I asked that question I just -- I wanted to understand. At one point you're talking about 1.97.

MR. TANEJA: 1.97. Right.

MEMBER BROWN: Now, when was changed to a performance-based? Is that Rev 4?

MR. TANEJA: Rev 4. Rev 4.

MEMBER BROWN: You know, when --

MR. TANEJA: Right.

MEMBER BROWN: -- was that done?

MR. TANEJA: Oh, that was done back in 2007, I think.

MEMBER BROWN: Okay. I just -- it was before --

MR. TANEJA: Yes.

MEMBER BROWN: -- before I got here. That's all I wanted to know.

MR. TANEJA: Well, it was -- right. It was changed and the intent was that all new licensees coming in --

MEMBER BROWN: Yes, I got that --

MR. TANEJA: -- they, you know --

MEMBER BROWN: Let me get on with this.

MR. TANEJA: Okay. All right.

MEMBER BROWN: So, what I'm trying to figure out is why do we need the mouse-milk? What parameters are monitored -- I mean, PWR. You put a bunch of parameters in that are consistently knowing, now we're going to evaluate whether we only need half of those --

MR. TANEJA: Well, this is --

MEMBER BROWN: -- because of --

MR. TANEJA: This -- this regulation --

MEMBER BROWN: I'm not going to argue against a --

MR. TANEJA: Right.

MEMBER BROWN: This seems like a mindless application of performance --

MR. TANEJA: Well, this regulation, is it a result of the TMI accident. Okay. After the --

MEMBER BROWN: I understand why that came.

MR. TANEJA: Right. Post-TMI, there was a requirement to have a dedicated set of parameters based on what events you are going to manage, whether they need to be Class 1E, whether they need to be redundant.

So, they were categorized. You know, Categories A, B, C, and A being full category. Make two sets. If one doesn't work, I have another on available.

So, you know, we -- yes. We all know we have all these key parameters that we do need, you know. But, EOP's will dictate, you know, hey, for me to manage this event, I must have this information available to me.

And that's really -- you know, it's a limited set. It's not an unlimited set, you know. So, what set -- so we are really working with them and they've been very, you know, forthcoming with a lot of the information.

And I have reactor systems. I have tech specs people. I have human factors people. They are working with me, because I need systems people. I mean, I really -- we don't have the EOP, so I need the operations, so --

MEMBER BROWN: This is my problem, and it's just -- you've got a list. I mean, it's -- I'm asking a different question. I mean, I just --

MR. TANEJA: Okay.

MEMBER BROWN: You're worried about because they don't have EOP's, and yet they've provided a minimum list and it's based on past PWR operations, so at least you've got a decent start, and it's something to work from instead of, you know, well, gee, you only need half of these or something like that.

CHAIR STETKAR: That was my question, honestly. I mean, if I -- I read the open item and I read the SER. It sounds like you're trying to extend this out into the COL space when -- when MHI is doing something that very few of the other vendors have chosen to do.

They've actually taken the initiative to try to specify this at the design phase so that we -- we have a little bit better handle on what, indeed, will be displayed, you know, either over on the safety panels or -- or only on the nonsafety panels.

And now they seem to be being penalized because they don't have EOP's written. So, my question to you, since -- since this is an integrated review effect, and we have thousands of people here now with a lot of experience in the nuclear power industry.

What particular indications that are not on this list does the staff want on the list, and why?

MR. TANEJA: Well, because --

CHAIR STETKAR: Because, you know, that's part of the review responsibility.

MR. TANEJA: Right.

CHAIR STETKAR: You can't just say bring me the world and I'll tell you I don't have enough information, and you need to bring me more information.

What concerns do you have specifically with the list that they have?

MR. TANEJA: Well, the --

CHAIR STETKAR: And unless -- and I'm

asking the staff to tell us that.

MR. TANEJA: Yes.

CHAIR STETKAR: I want that information.

MR. TANEJA: Right.

CHAIR STETKAR: As a subcommittee. So --

MR. TANEJA: So a couple of --

CHAIR STETKAR: -- that's a take-away item that I want the staff to answer.

MR. TANEJA: Yes. A couple of areas that we are remaining to work on, I'm in -- like I said, the exercise has been, you know, looking at -- like, for example, Category 8, based on Rev Guide 1.97, Rev 4 are the parameters that are credited manual actions that are in Chapter 15.

CHAIR STETKAR: Sure.

MR. TANEJA: So we have Chapter 15. We know what the required manual actions are. Now, those manual actions, the parameters that you use to take those actions, they need to be categorized as Category 8, highest category.

They've had agreed, read them, and all that. In that area, the way Chapter 15 has already accepted is the use of alarms to take manual actions. And we worked diligently on -- listen, alarms are not safety-related.

CHAIR STETKAR: That's true.

MR. TANEJA: So, how can we put those on this list?

CHAIR STETKAR: That's right.

MR. TANEJA: While these are -- Chapter 15 has already accepted it. What's your problem? So, I went to Chapter 15. I said, "Did you guys accept it?"

"Yes." Alarm initiates my action and I have this much time to take my action, and I can do it.

CHAIR STETKAR: And that's -- and that's fair.

MR. TANEJA: Right.

CHAIR STETKAR: That's a fair --

MR. TANEJA: So, now, what is the source of that alarm.

CHAIR STETKAR: Right.

MR. TANEJA: So, you know, we rectify that problem to -- went back to which parameters.

CHAIR STETKAR: Okay.

MR. TANEJA: Now, one of the open area right now is, I guess it's the steam generator tube rupture event, where we have, I guess -- M16 is the direct way to really see which -- which is your affected steam generator.

M16's are nonsafety-related in the existing plans and -- but, you know, the interesting dilemma is that EPR made them safety-related, and they are using them as a primary means of detecting.

So -- so that's the area we are still working with reactor systems, to see, you know, what they are okay with. You know, the alternate options that you have in front of you, I mean, Jeff Schmidt that I'm working with, he's a former operator and he said, "You know, I always looked at M16's, whether they were there or not, and I really didn't have any regulatory basis to really judge whether I need to make them safety-related. But, now you're saying Reg Guide 1.97, Rev 4. So maybe I need to relook that idea." So, these are the areas we are --

CHAIR STETKAR: Has the RAI's, because we -- we have access to the RAI's --

MR. TANEJA: Yes.

CHAIR STETKAR: -- but don't, in practice, read all of them. Have the RAI's been to that level of specificity because what I read in the -- in the SER --

MR. TANEJA: Yes.

CHAIR STETKAR: -- is pretty broad.

It seems to be saying, you know, we can't make these decisions until we have the procedures and that just sends to kick it --

MR. TANEJA: Right. RAI is about -- I think it's about a 60-page RAI response right now.

CHAIR STETKAR: Okay.

MR. TANEJA: So we are like that second or third revision to that RAI response and --

CHAIR STETKAR: And it does get to the specificity --

MR. TANEJA: Oh, yes.

CHAIR STETKAR: -- of signal? Okay. Good.

MEMBER REMPE: What is the number of RAI?

CHAIR STETKAR: Yes. What is that?

MR. TANEJA: Seven -- question number 7.18-15. 7.5-18 --

CHAIR STETKAR: If it's --

MR. TANEJA: -- is the question number, but it's on the last page --

MR. CIOCCO: It is RAI 568-4588.

MEMBER REMPE: 568 --

MR. CIOCCO: 4588.

MR. TANEJA: 4588.

MR. CIOCCO: 4588, and then Dinesh said it's 7.05-18?

CHAIR STETKAR: Yes. I suspect -- I

suspect we have it. It's --

MR. TANEJA: Yes, it's --

MR. CIOCCO: What you don't have is some of the draft responses that are being worked on that aren't -- aren't complete yet.

CHAIR STETKAR: Yes.

MR. TANEJA: Yes. We just received a, you know, the last draft, you know, like beginning of April.

CHAIR STETKAR: Okay.

MR. TANEJA: And I had Paul, you know, looking at that and yesterday Paul was here and today he could not be here.

But, basically, Paul said that we are almost there.

CHAIR STETKAR: Okay.

MR. TANEJA: You know, so we are almost there.

CHAIR STETKAR: That is encouraging.

MR. TANEJA: Yes.

CHAIR STETKAR: I'll take a look at that.

MR. TANEJA: You know, so we've -- we've done a lot of work in that area. And, because we are trying to establish a list, in the absence of actually EOP's/AOP's, so we are really having to understand --

CHAIR STETKAR: Well, but in the absence

of EOP's in the sense of what precisely is written in Step, you know, 1.2.3.7, in terms of accident management, I don't think you need that level of specificity.

MR. TANEJA: Right.

CHAIR STETKAR: Chapter 15 and the general knowledge of people for -- as you said, this is a PWR. There are design differences.

MR. TANEJA: Right. Right.

CHAIR STETKAR: You know, you don't need a level --

MR. TANEJA: Yes.

CHAIR STETKAR: -- in the RWSP for switchover, for example --

MR. TANEJA: Yes.

CHAIR STETKAR: -- because there isn't any switchover.

MR. TANEJA: Exactly.

CHAIR STETKAR: So, you know, the availability of that level instrument --

MR. TANEJA: Yes.

MR. JUNG: John --

CHAIR STETKAR: -- is the question.

MR. JUNG: I know you have -- the initial reaction was very strong --

CHAIR STETKAR: If -- if the -- if the RAI's have some of that specificity -- and I'll go back and look at them -- some of that initial reaction will be --

MR. JUNG: You know, overall --

CHAIR STETKAR: -- satisfied. But -- but I -- as I read the SER, the impression that I got was here is one of the few people coming in in the design certification stage who has actually taken the initiative to provide the list, where other people have just said, "Oh, no, no. We're not going to do it. We don't have to do it according to the regulations. The heck with you. We're going to leave it to the post-COL issuance.

MR. JUNG: Right. The staff -- the staff believes this is the better way to do it.

CHAIR STETKAR: It's absolutely the better the way, and I don't -- I'm hoping that we don't penalize someone for actually taking the better path.

MR. JUNG: I don't think that there's any intention of that. I think we started with actually the focusing on the delta, understanding the delta better, so that we can establish the list --

CHAIR STETKAR: Okay.

MR. JUNG: -- with a good confidence that it will remain the same, rather than later revisions to the DCD --

CHAIR STETKAR: Right.

MR. JUNG: -- type of things. So, that was our intent.

CHAIR STETKAR: Yes.

MR. TANEJA: Yes. So, you know, what the RAI response does, it actually attaches changes to the DCD, which explains all these variables and the basis, you know, why they selected it.

And then, I think one of the technical report either gets it, the comparison between the Rev 3 of the -- the list of the Rev 3, and -- and the US-APWR list.

CHAIR STETKAR: Yes. I looked -- well, I looked at that.

MR. TANEJA: Right. And then that comparison is there and then I believe the other thing that -- well, the list, actually, that's in DCD of the actual PAM variables.

I know we have had like some, then, from Category B to A. Some got added. So, there's been an ongoing -- in a revision to that, and maybe a couple of parameters got added.

And, you know, containment isolation I

think, valve position indications got added. You know, we were trying to use the containment pressure. The, I guess, you know, the -- when we worked on it, said, you know, come on. Those are safety-related. What's the big deal? Why don't we add them to that, you know?

So, all the -- you know, all the containment isolation valve positions were -- you know, so it's -- it's a work-in-progress. We've mad a lot of -- a lot of progress on that.

So, we're almost there, and I think we should be done with it next month or so.

CHAIR STETKAR: Good. That's -- that's encouraging --

MR. TANEJA: Yes.

CHAIR STETKAR: -- because that's a different impression, certainly, that I got from reading the SER and the old item. It sounded like --

MR. TANEJA: Well, we didn't have much to go on in Rev 3, you know, to write the case, you know.

CHAIR STETKAR: Okay.

MR. TANEJA: So -- all right. So, the next slide is regulation, and I think I've already discussed the open item.

CHAIR STETKAR: Yes.

MR. TANEJA: On page 49. Any other

questions on postaction monitoring?

(No response.)

MR. TANEJA: Okay. Go to the PCMS strike.

MR. MARTINEZ Good morning. This is Erick again. Can you hear me all right?

CHAIR STETKAR: Yes.

MR. MARTINEZ I can't tell. Better.

CHAIR STETKAR: Just be careful not to hit the microphone.

MR. MARTINEZ Thank you. And so this slide is to pretty much give you a quick overview on an RAI that the staff recently sent out to MHI. You might have seen that already in MHI's presentation where the last RAI that they talked about in their slides.

The staff pretty much issued this RAI to get a better understanding on how the PCMS failures are -- are addressed and they don't affect the safety function of the -- of the PCMS.

So, pretty much, we're asking for additional clarification and details on just how specifically the PCMS does not affect the safety function. And, unless you have anything to add to that there is just no --

CHAIR STETKAR: Erick, is --

MR. MARTINEZ -- way that we --

CHAIR STETKAR: And I have to -- in the interest of time, I'm not going to try to shuffle through all of my notes, so I'll just ask you here.

As it's -- as it's presented on the slide here, it just says the affects of control system failures on the safety function.

Does -- does that include both -- I understand the manual signals that come in through the unit bus and COM-2 and all of that stuff. I don't really understand it, but I can say those words today, and they're probably wrong.

Does it also include the effects of those automatic control signals that I asked about yesterday that I was confused that are now hard-wired from the automatic controls into PSMS?

Because, those are -- I'm trying to find out what the scope of that open item applies to --

MR. TANEJA: The genesis of this question is, in DCD 7.7, I guess there is statements in there that claim that any failures in the PCMS is bounded by Chapter 15 analyses for AOO's and PA's. Okay.

Now, the PCMS being software-based, okay, we wanted to make sure -- you know, traditional plants feed pretty much analyze failures of feedwater system and its consequences and, you know, some of the turbine trip and its consequences.

But, these are taken one at a time.

CHAIR STETKAR: Yes.

MR. TANEJA: Now, could there be a concurrent failure of multiple things and has that been analyzed?

CHAIR STETKAR: Okay.

MR. TANEJA: Right?

CHAIR STETKAR: Yes.

MR. TANEJA: Now, I guess the -- and, you know, and yesterday's presentation, what we saw and which I say that they will demonstrate how the analyses in Chapter 15 bound these multiple -- potential multiple failures of the PCMS.

So, I think that's the gist of the whole question.

CHAIR STETKAR: So, at that level, we don't --

MR. TANEJA: Yes.

CHAIR STETKAR: -- it doesn't distinguish between manual or automatic or any --

MR. TANEJA: It's just simply --

CHAIR STETKAR: -- it's just PCMS --

MR. TANEJA: Right. Globally.

CHAIR STETKAR: Globally. Okay. Okay.

I just wanted to make sure I understood, in my own head --

MR. TANEJA: Right.

CHAIR STETKAR: -- what that scope was. Thanks.

MR. TANEJA: You know, back -- I guess it was August when we had the SE with Open Items ready to go. One of the NRC employees submitted a nonconcurrence on the SE, and raised three issues, namely, commercial-grade dedication of MELTAC system, and basic question on the lifecycle development process for the basis software and, you know, issues with the US-APWR data communication, specifically interface of operational VDU with the DSMS. Next slide.

So, for the benefit of people that may not be familiar with a nonconcurrence, I'm going to read a statement that comes out of our procedure here.

"The NRC strives to establish and maintain an environment that encourages all employees to properly raise concerns and differing views without fear of reprisal and to promote methods for raising concerns that will ensure its strong safety culture and support agency's mission.

"Individuals are expected to discuss their views and concerns with their immediate supervisors on a regular basis and ongoing basis. If informal discussions do not resolve concerns, individuals have various mechanism for expressing and having their concerns and differing views heard and considered by management.

"The nonconcurrence process allows employees to document their differing views and concerns early in the decisionmaking process, have them responded to and attach them to proposed documents moving through the management approval chain."

And that's exactly what took place. And it's Management Directive MD-10.1.5.8 that allows this nonconcurrence process to take place.

CHAIR STETKAR: And just -- just for the record and to make sure that I understand the process correctly, a nonconcurrence is raised during the staff's reviewed by a member of the staff who was involved in that review.

MR. TANEJA: That is correct.

CHAIR STETKAR: And that -- and that nonconcurrence must reach some level -- must be resolved, anyway, by the time the Safety Evaluation Report is listed. Is that correct?

MR. TANEJA: The normal process is the already contributing individuals. And, in this case, our product is the Safety Evaluation Report on Chapter 7 concur.

CHAIR STETKAR: Yes.

MR. TANEJA: Right?

CHAIR STETKAR: Right.

MR. TANEJA: And we actually -- you know, every individual concurs when we are done with the product and we are sending.

So, at that time, if you have issues with that, I guess the first step is informal discussions with your supervisor and, you know -- and even the management at that level to raise your concerns and issues.

And I guess that went through -- we went through that process and it went beyond that and then it got documented, and these three issues were documented as being issues of concern.

CHAIR STETKAR: Where I was going is, I wanted to make sure I understood the process.

MR. TANEJA: Right.

CHAIR STETKAR: At the point when the Safety Evaluation Report -- the final SER is issued, there's still another opportunity called a Differing Professional Opinion, which --

MR. TANEJA: That is correct.

CHAIR STETKAR: -- which can actually be raised, it's my understanding, by anyone.

MR. TANEJA: Yes.

CHAIR STETKAR: It's not only restricted -- the nonconcurrence is restricted to people who have been actively involved --

MR. TANEJA: Right.

CHAIR STETKAR: -- in the review activity.

MR. TANEJA: Yes.

CHAIR STETKAR: The DPO could be those people if they don't feel their concerns have been adequately resolved, or any other individual, but that's after the final SER is issued.

MR. TANEJA: That is correct.

CHAIR STETKAR: Okay. I just --

MR. TANEJA: That is correct.

CHAIR STETKAR: -- wanted to make sure for the record that -- that I understood the differences between the nonconcurrence and the DPO process. Thanks.

MR. TANEJA: So in this process, the nonconcurring individual wrote his concerns. The concerns were given to, you know, the branch chief, and branch chief proceeded to summarize those concerns and then the staff provided a written response to each of the, you know, three issues that were summarized.

And then, the -- our management looked at the nonconcurring views and looked at the staff's response, and they discussed it with us and they discussed it with nonconcurring individuals, and then they provided us with the actions that need to be taken to resolve the nonconcurrence.

So, the actions that are listed here on these slides, actually were followed up and turned into RAI's and they are right now in our SER captured as open items.

CHAIR STETKAR: Okay.

MR. TANEJA: So I'll just quickly go through these items. The first item was related to the MELTAC. Originally, like I think we were mentioning that MELTAC was being commercially-dedicated because MELCO did not have a QA program.

So, you know, that is the genesis of that concern and now there has been a shift.

MEMBER BROWN: That wasn't a QA. They got a QA. It's just not a -- an Appendix B.

CHAIR STETKAR: It's not an Appendix B QA.

MEMBER BROWN: B QA program.

CHAIR STETKAR: Right.

MR. TANEJA: It's a Japanese QA program on that. Right.

MEMBER BROWN: I'm just saying, because they have a QA program.

MR. TANEJA: Exactly.

MEMBER BROWN: It's just not an Appendix B program.

MR. TANEJA: Right.

MEMBER BROWN: That's all.

MR. TANEJA: So now they have established an Appendix B program and the way that DCD states right now is that they are procuring the system as a Class 1E from an Appendix B vendor. Right?

So the question it's asking is to, you know, verify that all the critical characteristics of the MELTAC are documented in the DCD, and then the ITAAC is there that verifies these critical characteristics on the as-built machine.

They are there but, you know, the idea is, now we want to close the loop to ensure that, you know, because the way you do commercial grade dedication is you identify all the critical characteristics and you verify that they are all verified. And that's a method of doing commercial grade dedication.

CHAIR STETKAR: Okay. But they are not going to do that?

MR. TANEJA: They are not going to do that, but we do have the like MELTAC technical report. All the details are there. So, you know, we want to make sure that all the critical characteristics are defined in the -- in the docketed DCD material for MELTAC, and then the ITAAC's are there to verify that those are all properly working and functioning. So that was the action that was endorsed.

CHAIR STETKAR: Let me ask you, because I'm not a QA person at all. Let's say you didn't have this history of MHI, MELCO, MELTAC, whatever, and somebody came into you clean and said, "I'm a Vendor X. I'm building -- I'm designing this particular power plant and I have a subcontractor who is supplying, you know, a widget."

MR. TANEJA: Yes.

CHAIR STETKAR: "And my subcontractor -- I, the Vendor X have an Appendix B quality" -- this is -- the widget has to be a safety-related widget.

"I have an Appendix B QA program and my subcontractor has asserted that they have an Appendix B QA program."

In terms of the staff's review of -- of that situation, would you be requiring Vendor X to be listing critical characteristics of the widget in their DCD?

MR. TANEJA: Well, I'll take a simple example. Right. Now, let's say a reactor vessel component. Same QA issue, right. I mean, we have our design and the DCD will tell us all the critical features, the materials --

CHAIR STETKAR: Okay. Right.

MR. TANEJA: -- size, valves, all that stuff. Right?

And they are -- you know, our QA program that we have in the NRC on vendor inspection and ratification. So, the ultimate responsibility for quality lies with the licensee. Correct?

CHAIR STETKAR: Yes.

MR. TANEJA: The licensee has to ensure that their vendors are supplying good stuff.

CHAIR STETKAR: Right.

MR. TANEJA: And they have the oversight process -- at least that's what I understood when I interacted with our QA people.

So, in the MELTAC case -- you know, when we initially had gotten the documentation on commercial grade dedication, they prepared a number of pages, we actually went to our QA for their assistance.

So, basically what they said there is, approving that we have in the NRC where our vendor inspection branch periodically inspects the people that have a QA program, and we'll make sure that this is a good stuff, because we do that inspection part.

CHAIR STETKAR: But they inspect against those -- those attributes that are listed in the DCD?

MR. TANEJA: They inspect their QA process.

CHAIR STETKAR: Okay. Right.

MR. TANEJA: Okay. And what they told me is this way, is that MELCO -- they will look at their purchase order.

CHAIR STETKAR: Right.

MR. TANEJA: Right. So the purchase order, let's say, comes from MHI to MELCO and what we expect that purchase order to say, "Give me this widget that does this thing."

CHAIR STETKAR: Right.

MR. TANEJA: "What's in the DCD." Right?

CHAIR STETKAR: Yes.

MR. TANEJA: And so, when my vendor branch goes and looks at MELCO then, hey, where's your purchase order? Let's see what you are supposed to build. Are you doing what you're supposed to be doing?"

CHAIR STETKAR: Okay. Right.

MR. TANEJA: Are you doing what you're supposed to be doing.

CHAIR STETKAR: Okay.

MR. TANEJA: Right. I think that's my understanding.

CHAIR STETKAR: Okay. Okay. Yes.

MR. TANEJA: Yes.

CHAIR STETKAR: I think that helps a little bit. I'm still a little vague, but go on.

MR. TANEJA: I wish I could get the QA people here. They are all caught up another meeting this week. So --

CHAIR STETKAR: Sorry.

MR. TANEJA: You know. So that was the one item. And then the second item.

MEMBER BROWN: Let me ask one other question.

MR. TANEJA: Yes.

MEMBER BROWN: I just went back and looked at the version of the MELTAC platform we have here and Section 6.3 talks about the establishment of the 10 CFR Part 50, Appendix B QA program and the MELTAC Reevaluation Program.

MR. TANEJA: Yes.

MEMBER BROWN: Why, if that's in the technical report, does that mean they've already completed that or does that mean they are going to do it or why does this -- why is this hanging fruit still hanging there if there's that level of documentation -- or at least that statements --

MR. TANEJA: Well --

MEMBER BROWN: -- in the technical report, Rev 8?

MR. TANEJA: When we receive the MRP, I'll give you a little bit of background. The MRP document was, I think, 500-plus pages. Right?

MEMBER BROWN: MRP.

MR. TANEJA: Reevaluation.

MEMBER BROWN: Reevaluation. Okay.

MR. TANEJA: Reevaluation Program. I'm sorry.

MEMBER BROWN: That's okay.

MR. TANEJA: Okay. MELTAC Reevaluation Program. Now, what that document gave us is, here are the critical characteristics.

Method of verification, they wrote down a specification number, or a drawing number. Right? There were -- I don't know, maybe -- I would say close to hundreds of documents that were listed there, and then some test report number.

Now, what does that document tell me? Nothing. Right. So, when I took it to vendor, he was like, "Come on, guys. You don't need" --

MEMBER BROWN: When you took it to who? When you took it to who? Your --

MR. TANEJA: Our vendor inspection people here.

MEMBER BROWN: Oh.

MR. TANEJA: Right. I said, "You know, how do you look at these things?" They said, "We're going to have to go and, you know, either you audit every single one of them or we'll do it under the vendor inspection program where we go and we do checks on that."

So there was an inspection done and, you know, they invited us to come along with that. So, we were able to inspect most of those documents.

And I think our finding that we came up with was a one finding because they did not adequately document the burn-in period. I think the guideline that they were using was a pre-Guideline which says, "If you're going to use a commercial PLC in a safety application" -- that's really what it says.

If you are going to take this commercial PLC and put it in a safety application, burn it for 28, 48 hours or something like that and make sure that there aren't latent failures before you put it in here.

And this eval, we do burn in, you know, but there was no proper documentation of that. So, that was the only finding that we came up with.

It's like, you know, when you say -- so what the decision was made at that time --

MEMBER BROWN: Let me interrupt for just a --

MR. TANEJA: Yes.

MEMBER BROWN: I just want to understand your -- what you're saying is you effectively -- when the platform was designed --

MR. TANEJA: Right.

MEMBER BROWN: -- and built and used in other applications, there was a level of QA system processes that applied.

MR. TANEJA: Right.

MEMBER BROWN: Now, you're going backwards and looking at what was done to see if those items contained the metrics, the judgment metrics for meeting the Appendix B requirements --

MR. TANEJA: Right.

MEMBER BROWN: -- in terms of the details, how long was it burned in, you know, what were the temperatures they get it to, what were the current levels, what were the data rates, whatever applies to the particular component.

MR. TANEJA: Right.

MEMBER BROWN: And what you're saying is, if you go back and look at that documentation, the one you found is that it didn't have the documentation.

And I faced this, looking at what people have done in the world I've worked in in the last 13 years and qualifying stuff.

You go say, "Well, hold it." You got -- you say it tested okay. You go back and look at the test -- well, hold it. There's no temperatures here. There's no humidities. There's no voltage variations. There's no -- you didn't write down what you tested it to.

So, is that the -- that's the type of stuff you're -- you didn't document it as part of the overall -- in those days.

MR. TANEJA: Right.

MEMBER BROWN: Whereas, if you were -- so, you have to make a judgment, is that okay --

MR. TANEJA: Yes.

MEMBER BROWN: -- or does it have to be redone. Is that -- am I correct?

MR. TANEJA: Well, so their corrective action was, when we build machine for the US-APWR --

CHAIR STETKAR: Yes. That's what I was

going to say. What they did in the past is a bit of a moot point as far as --

MEMBER BROWN: Well, no, it's not if they actually --

CHAIR STETKAR: But they're taking a different approach now.

MEMBER BROWN: Yes. I'm just saying, it's not a -- it's not a moot point if they, in fact, tested it.

MR. TANEJA: Correct.

MEMBER BROWN: They need the values and documented in the manner that something has to be done to get you through that hoop if they didn't.

And so now you're telling me, when they build the units for APWR, the lead unit, whatever it is, they're going to do something.

MR. TANEJA: Right.

MEMBER BROWN: And that something is --

MR. TANEJA: They are going to burn it in for X number of hours --

CHAIR STETKAR: Well, they don't talk to the Appendix B program --

MEMBER BROWN: Yes. They'll do it for the Appendix B program.

CHAIR STETKAR: Right.

MEMBER BROWN: So that what -- does that mean they will run the unit -- unit, okay, because you don't do it to every unit, I guess, through a complete Appendix B qualification program.

MR. TANEJA: Right.

MEMBER BROWN: So there will be no shortcuts, there will be no loss of data --

MR. TANEJA: Right.

MEMBER BROWN: -- or anything like that. So you will have that.

MR. TANEJA: Right.

MEMBER BROWN: And that's what's committed to where? In the test report --

MR. TANEJA: In the DCD.

MEMBER BROWN: -- or in the DCD?

MR. TANEJA: DCD.

MEMBER BROWN: Yes, I'm looking at the report right now, so I didn't see it.

MR. TANEJA: Yes. DCD says that the MELTAC is a Class 1E Appendix B program.

CHAIR STETKAR: Built under Appendix B.

MEMBER BROWN: Okay.

CHAIR STETKAR: That's what I got from the DCD.

MR. TANEJA: Right. So it's built under

Appendix B program and now, as a result of this question that we raised I believe MHI has committed to clean up the documentation to kind of clarify that we are not mostly dedicating any year, we are basically building it under the Appendix B program.

You know, so let's see how the documents get clean --

MEMBER BROWN: Okay. I just wanted to understand --

MR. TANEJA: Right.

MEMBER BROWN: -- the flow of what you were -- and put that in relation to the nonconcurrence. How it is going to be resolved --

MR. TANEJA: Right.

MEMBER BROWN: -- as opposed to with hand-waving.

MR. TANEJA: So, you know, the follow-up to our inspection was, you know, like on that finding, MELCOR committed to adding to their procedures a, you know, actual documentation of the burning and of all the cabinets.

The way they explained it to us is that the existing cabinets, they actually, when they build it and when they are testing it, it says it's continuously-powered. It's getting burned-in all the time, you know. So, that's what they take credit for, versus actual, you know, --

CHAIR STETKAR: But Dinesh, I'm still sitting here saying, "I don't care what they did in the past."

MR. TANEJA: Right. That's right.

CHAIR STETKAR: I only care what they are going to do for this --

MR. TANEJA: For the licensee.

CHAIR STETKAR: For the equipment that they construct and install in our licensed US-APWR.

MR. TANEJA: Correct.

CHAIR STETKAR: I don't care what they did in the past. And I don't care how they did it.

MEMBER BROWN: Well, but see, the problem, John, is if you look at the table --

CHAIR STETKAR: I don't care --

MEMBER BROWN: No. Hold it.

CHAIR STETKAR: Okay.

MEMBER BROWN: Just let me finish. You'll know that I'm talking about.

CHAIR STETKAR: Yes.

MEMBER BROWN: They have a column of Appendix B based QAP requirements, and then there's another column that says "Previous QAP," and there's sporadic listings. Not covers everything, but a sporadic listing, and I guess my concern is, is do they view that as already saying they're okay, or is it, as Dinesh is stating, they're going to redo those when they build the next unit?

CHAIR STETKAR: I think in the technical report you're seeing a snapshot in time with remnants of an attempt to still try to justify commercial grade dedication.

MEMBER BROWN: Well, I don't see them rushing -- they're shaking their head up and down.

MR. SPRENGEL: No. I agree, and I think the kind of adjustment that Dinesh is referring to is in alignment with what -- what you are saying.

MEMBER BROWN: Yes.

MR. SPRENGEL: We are looking forward and trying to clean up some of the language to kind of clarify that -- that these are really future commitments and a commitment for the ultimate kind of procured and purchased, I guess, design to meet requirements that are in the DC.

MEMBER BROWN: So, is part of that they found they had to change something, you'd make a change if it didn't pass?

MR. SPRENGEL: Correct. And it would be

done under the existing community programs.

MEMBER BROWN: Yes. Okay.

MR. SPRENGEL: Right. And it's not to say that the information that is in that technical report won't be credited, but it will be part of the -- part of the entire process.

MEMBER BROWN: Thank you.

MR. SCAROLLA: Excuse me, John. Can I make --

CHAIR STETKAR: You may, Ken.

MR. SCAROLLA: Ken Scarolla. Well, Charlie, I want to make sure there's no misunderstanding here.

There was no issue --

MEMBER BROWN: You might make this worse.

MR. SCAROLLA: -- with regard to the type testing the design.

MEMBER BROWN: There was no what? Say that again.

MR. SCAROLLA: There was no issue in the finding with regard to the type testing of the design, qualification. This was a recurring burn-in for production systems where there's a requirement for the system to sit on the factory floor for some number of weeks before you ship it.

This has nothing to do with a design test.

MEMBER BROWN: I understand that point.

MR. SCAROLLA: Okay.

MEMBER BROWN: Okay. I understand that point, and the fact is, I like burn-in, okay, based on personal experience.

MR. SCAROLLA: Okay.

MEMBER BROWN: So, I'm not going to -- I've saved a lot of equipment by watching it explode on the factory floor before we shipped it, so -- not "explode," but kind of melt down. So, burn-in does work.

I even turned TV's back into a Macey's at one time because I took it home, started turning it on and off and all of a sudden the solid state channel changer broke. I just took it back to them. Thirty days, but every day I operated it, cycled up and down, took it back, got a new TV. It's amazing how it works.

They don't do that when they build TV's. They just put them together and ship them.

MR. TANEJA: So you did the burn-in.

MEMBER BROWN: I did the burn-in. If you do it in time, then you can get a new one.

CHAIR STETKAR: All right. That's --

MEMBER BROWN: Well, that one works. I'm not kidding you. It's happened twice. I got two new

TV's out of that. Solid state TV's. So, that's why I'm a fan of burn-in.

MR. TANEJA: All right. Well, you know, we agree with you on that one.

CHAIR STETKAR: Well, that was the first one. What's the second one?

MR. TANEJA: Second one has to do with the basic software for the MELTAC. You know, so we -- the issue is that, you know, I guess we are not evaluating or -- you know, the -- you know, so our -- the basic software program.

The basic software program is predeveloped for MELTAC, so it's not something that needs to be developed by US-APWR MHI. It's something.

So, I guess the concern was that, you know, NRC should review and evaluate the software program manual for the basic software, whereas -- I think maybe, you know, Jung, you can elaborate on, you know, that one -- you know, the concern the way you understood it and what we need to do to wrap it up.

MR. TRUONG: I think the staff's concern was the basic -- the basic SPM which was originally docketed and later withdrawn.

CHAIR STETKAR: Can you just speak up a little bit so that we --

MEMBER BROWN: Put the mic a little closer.

CHAIR STETKAR: Put the mic closer to you or scream a little bit louder. Thank you.

MR. TRUONG: I think the staff will raise the nonconcurrence had concern that the basic SPM which was originally docketed, but then later was withdrawn, you know, and the staff that wrote a nonconcurrence, had concern that because it -- basically it's not been reviewed, that the staff may not be able to assess the software quality for the basic software which MHIS had went over briefly, which is the systems, the system of software.

CHAIR STETKAR: Okay. I think I understand at least the concern, what's the -- what's the resolution?

MR. TRUONG: So there's -- so staff wrote a RAI, you know, and MHIB responded this week and we will be evaluating the RAI.

CHAIR STETKAR: Okay. Is -- well, we'll let the -- we'll let that process work itself out.

MR. TANEJA: Right. The question of the RAI is how -- what we see on the slide, you know. And the third issue was, you know, I guess controlling safety components from, you know, nonsafety control Operational VDU in this case.

And the concern is, you know, multiple-fold, I guess, you cannot use nonsafety-related or controlled safety-related components and, you know, so --

CHAIR STETKAR: We had some discussion of this yesterday.

MR. TANEJA: Right. So the -- you know, I guess -- so the ITAAC, we -- you know, the action that we were asked to take was to have the applicant provide additional clarification on this connection that we have between Operational VDU and the ESMS.

And one was the, you know, that results in enhancement of safety function performance, you know, a demonstration of that. You know, so that really is words coming out of the ISG-4.

We use the ISG-4 as a guidance to evaluate this connection, and I believe that's the only one that remains to be, you know, verified. Others, we found them to be --

MEMBER BROWN: And, of course, the adverse effects you're -- it doesn't have any adverse -- that's -- there's two pieces to that if I remember the discussion.

MR. TANEJA: Right. There are two pieces to that. Right.

MEMBER BROWN: One that doesn't provide any adverse effect --

MR. TANEJA: Right.

MEMBER BROWN: -- to the PSMS. The other is that, even if it has no adverse effect, it should provide whatever this -- and we had this discussion yesterday. And what do we mean by "enhancement"?

MR. TANEJA: Right.

MEMBER BROWN: And there was -- you know, if it's neutral, does it mean that you can't do it or does it have to have some significant benefit, like reducing complexity of operations or something.

MR. TANEJA: Right.

MEMBER BROWN: And that's the part that's open yet for your evaluation?

MR. TANEJA: Correct.

MEMBER BROWN: And that's an active open item at the present time?

MR. TANEJA: That is an active open item, right.

CHAIR STETKAR: Does that -- okay. Does that -- but that somehow relates also to the concern about no failures in PCMS resulting in anything that has been not analyzed in Chapter 15, doesn't it?

MR. TANEJA: Sort of, because --

CHAIR STETKAR: Aren't they related somehow?

MR. TANEJA: -- you know, PCMS is also connected on the unit bus.

CHAIR STETKAR: Yes. I mean --

MR. TANEJA: Right.

CHAIR STETKAR: -- last I checked, an O-VDU is part of the PCMA.

MR. TANEJA: Right. So, the way we evaluated the connection from operational VDU to PSMS is that the PSMS has the protective features built into it which protects itself against anything bad coming in. Right?

So, that's really our focus of review here, was to look at the -- the shield that's built around the PSMS that protects itself from something penetrating that.

Okay. I only want what I want. I don't want anything undesirable. So, that's what I asked you for guidance, provided us the tools to evaluate that interface.

The PCMS failure is more of a system-level discussion, and if systems fail --

CHAIR STETKAR: Yes. Okay. Yes. Okay.

MR. TANEJA: -- right, how do they affect.

So, here we are talking about data communication. There we are talking about systems.

MEMBER BROWN: Well, but the operational VDU also connects through the COM system down to the safety bus which --

MR. TANEJA: That's really what we are talking about here.

MEMBER BROWN: That's what he's talking about here --

MR. TANEJA: Yes. Right.

MEMBER BROWN: -- in this specific --

CHAIR STETKAR: Well, from the PCS, but that's -- the safety bus is part of the PSMS.

MR. TANEJA: True.

MEMBER BROWN: So it does have a direct connection to that and --

MR. TANEJA: It does.

MEMBER BROWN: -- so that's -- that's where you needed to look at that from a shield standpoint.

MR. TANEJA: Right. Exactly.

MEMBER BROWN: I want to make sure that's what we're talking about.

MR. TANEJA: Got it.

MEMBER BROWN: So you're satisfied that it does not provide -- it does not adversely affect the

PSMS by being a direction action. There's no mode, no failure mode of the O-VDU that -- that could impact or impair the performance of the safety bus in performing demands made from -- onto it from the PSMS?

MR. TANEJA: I believe you've done a lot of looking in that area. You know, we -- actually, the audits and the inspections we did, we spent a lot of time on that part of it, that special led interface issues.

MEMBER BROWN: And you think it's okay?

MR. TANEJA: And, you know, like I said, you know, we use the ISG-4 -- I mean, reason -- you know, reasonable assurances there. I mean, I can never say a hundred percent sure.

MEMBER BROWN: Did you come --

MR. TANEJA: Yes.

MEMBER BROWN: -- to your conclusion, yes, it's a reasonable assurance --

MR. TANEJA: It's a reasonable assurance.

MEMBER BROWN: -- you quit working on that now?

MR. TANEJA: Yes. It's reasonable assurance and that's it.

MEMBER BROWN: That should be a yes or a no.

MR. TANEJA: Yes. Right.

MEMBER BROWN: Okay. The only one open is the enhancement part?

MR. TANEJA: Right.

MEMBER BROWN: Okay. I just wanted to make sure where you all stood right now.

MR. TANEJA: Right.

MEMBER BROWN: Sorry. I just needed to make sure I --

CHAIR STETKAR: No, no. That's --

MEMBER BROWN: -- understood that point.

CHAIR STETKAR: That is important.

MR. TANEJA: Right. So that's really the three issues. And so we have those as an open item and we are going to work through this process that our management -- and let the -- you know, let the NRC's Management Directive, you know, handle, you know, how we handle this nonconcurrence.

And this step concludes our presentation and we really thank you for your feedback and I'm open for any discussion or comments at this time.

CHAIR STETKAR: Thank you. Do any of the members.

MEMBER BROWN: Yes. Just one -- just, when you say "finish it," I presume that at some point management, then, has to agree with your conclusions that this other stuff, when you finish -- when you resolve the nonconcurrence within the management structure in accordance with the nonconcurrence process.

MR. TANEJA: Right. So what we have on the nonconcurrence process is an actions that we need to take.

MEMBER BROWN: Okay.

MR. TANEJA: So I need to provide feedback to my management the result of the action that we have taken.

MEMBER BROWN: And they have to agree?

MR. TANEJA: And they have to agree with, you know, what we come up with.

CHAIR STETKAR: Oh, they have to -- right now it's in the context of open items.

MEMBER BROWN: Yes. I understand --

CHAIR STETKAR: Under the SER --

MEMBER BROWN: I just --

CHAIR STETKAR: -- and those open items will be resolved through the normal process of --

MEMBER BROWN: The final, the final process.

CHAIR STETKAR: -- of, you know, closing

out open items. The nonconcurrence, itself, is my understanding, is -- has been disposed of. Let me just put it that way.

MR. TANEJA: Yes.

CHAIR STETKAR: So there's no feedback to the nonconcurrence. It's now in the context of these open items. Right, Ian?

MR. JUNG: That is correct, John. The only thing to add is the final SER, the Phase 4 stage. The resolution of these open items would be documented.

CHAIR STETKAR: Right.

MR. JUNG: The nonconcurring individual has an opportunity --

MEMBER BROWN: Sure. That's --

MR. JUNG: -- to agree and disagree and gets another opportunity --

MEMBER BROWN: Right. Right.

MR. JUNG: -- to express their views.

CHAIR STETKAR: Because that individual is still part of the status --

MR. TANEJA: Correct. After that decision is made with FSER, the individual and anybody else could raise through the EPO process --

CHAIR STETKAR: Right.

MR. TANEJA: -- if they have any --

MEMBER BROWN: Okay. I just wanted to make sure whoever that, somehow that non -- management decision still got fed back and still was subject to additional discussion --

MR. TANEJA: Yes. Oh, yes.

MEMBER BROWN: -- within that process with the nonconcurring individual.

CHAIR STETKAR: Or anybody else involved.

MEMBER BROWN: Or anybody else.

CHAIR STETKAR: You know, someone --

MEMBER BROWN: Exactly. Got it.

CHAIR STETKAR: -- else involved in the review might disagree --

MEMBER BROWN: Okay.

CHAIR STETKAR: -- with -- with the close-out of one of these particular open items.

MEMBER BROWN: That's all I have.

CHAIR STETKAR: Anything else for the staff?

If not --

MR. TANEJA: I have one thing that --

CHAIR STETKAR: -- some folks that we had some feedback, so let's hear that.

MR. TANEJA: Khoi has the list that you asked us which safety functions -- or which nonsafety functions are coming wire-hardwired.

CHAIR STETKAR: Oh.

MR. TANEJA: Okay?

CHAIR STETKAR: Good.

MR. TANEJA: So, you know, that is a -- you know, RAI -- I mean, response to the RAI which is an update to the Chapter 7.

CHAIR STETKAR: This real is full. Thank you.

MR. TANEJA: These are not all, but these are the significant ones.

CHAIR STETKAR: Significant ones.

MR. TANEJA: Significant one, I guess I should say.

CHAIR STETKAR: I've learned not to use words like "all" and "none."

MEMBER BROWN: So these will be -- this will be part of Rev 4 of the DCD?

MR. TANEJA: Yes.

MEMBER BROWN: Okay.

MR. TANEJA: Yes. They are part of the Rev 4. And in the -- can we go over this list now or --

CHAIR STETKAR: I don't think -- in the interest of time. We're trying to get through Chapter 7 and COL Chapter 2 Sections, and get people out for airplanes.

So, as long as the subcommittee members agree, I think we can look at this list, and if we have questions about it, we can -- we can get back to you.

MR. JUNG: Yes, John. We'll -- we are -- we developed a list of action items. We will work with Girija and the committee to make sure we are capturing all your action items.

CHAIR STETKAR: Great. I think that's -- that's the most time-effective way to treat it.

MR. TANEJA: Okay. All right.

CHAIR STETKAR: And I really appreciate getting us the list this quickly.

MEMBER BROWN: Now, to read this paper, just -- this is a summary of the items here, the first page?

MR. TANEJA: The first page --

MEMBER BROWN: And the other part is --

MR. TANEJA: In the DCD.

MEMBER BROWN: -- in the DCD.

MR. TANEJA: Yes.

MEMBER BROWN: That's the Rev -- Rev stuff. Okay.

CHAIR STETKAR: Anything else?

(No response.)

CHAIR STETKAR: Nothing? If not, thank you very much. You covered a lot of material. I really appreciate the -- the shortcuts that you took to get through the slides and get us in some reasonable sense of schedule, and I think we had a good discussion.

So, I really appreciate that. Thank you very much.

MR. TANEJA: Thank you. Thank you.

CHAIR STETKAR: What we'll do now is, MHI, I believe, had some number of items that you wanted to respond to.

MEMBER BROWN: Somebody is standing at the mic. Do you want him up front, or do you --

CHAIR STETKAR: No. He can stand.

MEMBER BROWN: He can stand back there. That's fine.

CHAIR STETKAR: So the longer he stands and the less comfortable he is, the happier I am.

MR. LYNN A portion of the people can't see me back here, so I'm okay.

CHAIR STETKAR: Just identify yourself and speak with sufficient clarity and volume.

MR. LYNN This is Kevin Lynn from MNES. I wanted to clarify one of the questions you asked yesterday in regard to reactor vessel water level.

You'd identified in one section of the DCD, and then there was a table in the DCD, and it seemed like there was an inconsistency between the two.

The DCD section referred to the water level of the reactor vessel from the top of the fuel alignment plate to the reactor vessel head, whereas the DC table said the bottom of the hot leg to the top of the vessel.

In MHI's phraseology, the top of the fuel alignment plate is the same as the upper core plate which is at the bottom of the hot leg.

CHAIR STETKAR: Oh. Okay.

MR. LYNN: So the two descriptions are --

CHAIR STETKAR: Okay.

MR. LYNN -- identical in application, although different terms are used.

CHAIR STETKAR: Okay. So that level indication just tells me I'm below the bottom of the hot leg?

MR. LYNN Yes.

CHAIR STETKAR: Okay.

MR. LYNN: If it was zero, then you would know that it was --

CHAIR STETKAR: If it was zero. Okay.

MR. LYNN: -- below that --

CHAIR STETKAR: Thank you.

Anything else?

MS. SASAKI: I am Hitomi Sasaki, Mitsubishi Electric Corporation. I'll explain about this DOE. Would you have a look at yesterday's presentation material, Sheet No. 81. Sheet No. 81.

CHAIR STETKAR: Okay.

MS. SASAKI: I will explain what --

CHAIR STETKAR: Give us a chance. We are old. At least I am. Okay. I have the slide now. Thanks.

MS. SASAKI: It's DOE's --

CHAIR STETKAR: Yes.

MS. SASAKI: -- presentation material.

CHAIR STETKAR: Yes.

MS. SASAKI: First, I'd like to say these DC -- these two system incorporate electric card COM system CAS, and development environment, nuclear dedicated system.

CHAIR STETKAR: Okay.

MS. SASAKI: Next, CAS points in development environment points extreme. I will explain.

CAS points these one, two, three, four, five -- five points. One point, stores basic software and the application software. Two point, access control by password. Three point, physical security. Four point, system does not arrow, prior delete or change only.

Part one, POD backup. And additional one point, I'd like to use -- CAS is isolated from the corporate network.

Next, development environment, three points. One point, access control to development machine by password. Two point, entry/exit control of the development area. Three point, isolated it from the corporate network.

CHAIR STETKAR: Okay.

MS. SASAKI: My explanation is all.

CHAIR STETKAR: Okay. Thank you. And I think we heard from the staff this morning that -- that they are going to actually look into this a little bit more and make sure that they have --

MEMBER BROWN: Yes.

CHAIR STETKAR: -- satisfaction that it, indeed, is a plausible control --

MEMBER BROWN: Yes. This is the same thing we talked about yesterday, but --

CHAIR STETKAR: -- environment, so. Unless the staff has anything to add --

MR. TRUONG: I just want to ask -- so,

yesterday's conversation it was brought up, perhaps, that other projects besides nuclear, but now you are confirming that it's only nuclear. It is only US -- US-APWR projects?

CHAIR STETKAR: I think she's -- I think she said only nuclear. She -- I didn't hear only US-APWR.

MR. SPRENGEL: That's correct.

CHAIR STETKAR: I think -- I think we've heard --

MR. SPRENGEL: That's a point of clarification --

CHAIR STETKAR: -- both things and it's my -- in the interest of time here --

MEMBER BROWN: They ought to resolve that separate --

CHAIR STETKAR: -- I think the staff can --

MR. SPRENGEL: Are there any other, I guess --

MEMBER BROWN: No. My fundamental issue is --

MR. SPRENGEL: Had a good control --

MEMBER BROWN: -- archiving -- who has access to the archiving area. Not arguing with all the other, you know, points that are made. They were here yesterday about passwords.

I mean, we can argue about how good is password security all day.

MR. SPRENGEL: Sure.

MEMBER BROWN: That can be hacked by almost anybody that's halfway smart if you're computer-literate.

So -- not me, per se, because I couldn't do it but they -- the issue is how many people have access via their passwords to get into this database, and what is the accessibility of multiple databases within this archive, because it's electronic. So, you know --

MR. JUNG: John, the staff will take this as an action and they will work with MHI, too.

MEMBER BROWN: Yes. Yes.

CHAIR STETKAR: Yes. I mean, that sounds like --

MEMBER BROWN: Okay.

CHAIR STETKAR: I think that it -- there's some assurance from what we heard this morning that it isn't quite as open as -- as we may have thought yesterday, but I think it still merits a little bit of discussion.

MR. SPRENGEL: Okay. And then the last

topic, I think it's more for clarification. It's on the -- it's the load rejection for -- is it turbine bypass? -- for turbine bypass control.

I wanted to understand better what -- I have some more details on it, but I'm not sure what the real concern is.

CHAIR STETKAR: That -- that actually -- in sense -- Ryan, that was more my curiosity. It is not -- in the purview of the ACRS, it is not a safety issue.

MR. SPRENGEL: Okay.

CHAIR STETKAR: I was just curious because I understand that your plant is designed to automatically run back to island mode operation.

Whether it successfully does that or not, quite honestly, in my mind, is not a safety concern because, if it doesn't, the reactor is going to trip. It's not an unanalyzed type of event.

I just couldn't figure out from the information that I saw in the drawings how -- how it would actually accomplish that run-back and, you know, maintain generation.

But that's -- that's not, in my mind, anyway, a safety concern.

MR. SPRENGEL: Okay.

CHAIR STETKAR: So, I -- I personally, since I raised the question, I don't personally feel it's necessary to -- to follow-up on that. It's more a curiosity --

MR. SPRENGEL: Okay.

CHAIR STETKAR: -- as I was trying to understand that --

MR. SPRENGEL: Okay. Well, what I'd like to do, then, and it might be along the way, but we have additional detail that's actually in Chapter 10, but it's not showing up until Rev 4.

CHAIR STETKAR: Okay.

MR. SPRENGEL: Of the DC --

CHAIR STETKAR: Great. Thank you. That -- that will help.

MR. SPRENGEL: So, we'll track that and --

CHAIR STETKAR: Sure.

MR. SPRENGEL: -- keep it as an item for our -- the next time we interact for Chapter 10 as a discussion point you will have --

CHAIR STETKAR: Great.

MR. SPRENGEL: -- just to -- it adds more detail on that. And if you want to know, the Section is 10.2.2.3.1.5.

CHAIR STETKAR: 10.2.2.3.1.5.

MR. SPRENGEL: Yes. And again, that will be coming in in August.

CHAIR STETKAR: Yes. Thank you.

Anything else?

MR. SPRENGEL: Nothing else on our side.

CHAIR STETKAR: Okay. What I'd like to do is -- because we've -- we've been at Chapter 7 for the DCD now for an awfully long time -- is ask if we have any members of the public or anyone in the room who would like to make any comments, in particular related to Chapter 7 of the DCD.

We have the bridgeline open. Is there anyone out there? If we can open the bridgeline so I can ask for comments. It just -- it just helps, rather than waiting till the end to get through the COL and Chapter 2 if we close out any comments on this particular subject.

It's a low-budget operation. We -- we don't have any indications when it's open. I -- someone has to come in and say they think it's open. With Sequestration, we're going to install Campbell soup cans in individual strings throughout the United States. We'll know it better then.

Okay. Thank you.

PARTICIPANT: -- show the line is open.

CHAIR STETKAR: No, great. Thanks a lot. I appreciate that because, as I said, we don't have any other indications.

So, is there anyone out there? We now know the line is open. Is there anyone out there who does have a comment or a question?

(No response.)

CHAIR STETKAR: Okay. Hearing none, we will re -- we will reclose the bridgeline and put it on mute -- Thanks Girija. -- and call Luminant up to hear about the COL Chapter 7, which I trust will be somewhat less complex.

And, Don and Bob, I'll just remind you, just be careful of those microphones when you're shuffling things up there. It's really difficult for our recorder.

Don, it's yours.

MR. WOODLAN: Well, I was going to say good afternoon, but I'll probably say good morning.

I'm Don Woodland. I'm the licensing manager for Luminant and we are here to present Chapter 7 from the -- our COL application for Comanche Peak Units 3 and 4.

As Bob is going to address, Chapter 7 is primarily a chapter where we've incorporated, adopted the design information from the standard plant design for the US-APWR.

There are a few locations where there is site-specific information that needs to be provided to supplement the standard plan information, and that's what Bob Reible is going to present.

Bob.

MR. REIBLE: Thank you.

My name is Bob Reible. I'm the lead for Chapter 7. Today we're going to discuss three specific areas and introduction, site-specific aspects and then a short summary.

The COL uses incorporated-by-reference methodology, and for FSAR, Chapter 7, there are no departures from the US-APWR DCD.

The current version of the CPNPP COLA is Revision 2 which was June of 2011, and the next revision is Revision 3, which is due in June of 2013.

MR. WOODLAN: No. Rev 3 was filed in June of 2012. Right?

MR. REIBLE: No. Is our slide incorrect?

MR. WOODLAN: No. The slide is correct.

CHAIR STETKAR: The slide is correct. We have Rev 3.

MR. WOODLAN: They have Rev 3.

MR. REIBLE: Okay.

MR. WOODLAN: Rev 4 is coming out in November.

CHAIR STETKAR: November of this year?

MR. WOODLAN: Of this year. Correct.

MR. REIBLE: Right. Excuse me.

MR. WOODLAN: That's all right.

MR. REIBLE: And there no contentions pending before the ASLB.

The following sections of the Chapter 7 are a hundred percent IBR. That's Section 7.0, 7.1, 7.2, 7.3, 7.6, 7.7, 7.8 and 7.9 with no departures for supplements.

Section 7.4, Systems Required for Safe Shutdown is IBR with the following site-specific editions. The editions are related to the normal components and indication that would be necessary for safe shutdown. These editions would be related to the ultimate heat sink. The NRC SER summary has no outstanding issues.

For Section 7.5, Information Systems Important to Safety is IBR with the following site-specific editions. Section 7.5 editions are the D PAM variables, performance of safety systems and the E PAM variable meteorology monitoring and radiation protection or core radiation protection associated with site-specific components and monitoring.

These postaccident sampling variables are associated with the site-specific normal components associated with the ultimate heat sink and the EOF, emergency operations facility.

In addition, there is a short section discussion of the space in the displays that are found in the emergency operations facility and in the technical support center.

The NRC SER summary has no outstanding issues.

CHAIR STETKAR: Well, that was short. The bad news is, I have a couple of questions.

On the EOF description it says, "Displays associated with CPNPP Units 3 and 4 are common to both units with a multidisplay selection -- with a unit display selection capability."

That gives me the impression is you have one set of displays and if I want to see what's going on in Unit 3, I have a switch in one position and if I want to see what's going on in Unit 4, I switch over to see what's going on in Unit 4. Is that correct?

MR. REIBLE: It's my understanding that that's going to be modified because the requirements of the EP rule now are that you have the ability to display both units at the same time or all four units at the same time.

CHAIR STETKAR: Okay. So you're actually --

MR. REIBLE: Yes. Our anticipation is that --

CHAIR STETKAR: Okay.

MR. REIBLE: -- we will have displays for all four units.

CHAIR STETKAR: I was going to raise the question in the context of post-Fukushima, but it -- it comes up in several different venues.

So, you are expecting to change that. Thank you.

MEMBER BROWN: When do you expect to do that? I mean, you say "expecting to do that." Does that mean you're going to do it or you're just thinking about it?

MR. REIBLE: No. We are going to do it. We are in the process of doing it on our operating units right now.

MEMBER BROWN: Okay. That's fine. I just -- I was confused between the word "expecting" --

MR. REIBLE: Sorry.

MEMBER BROWN: -- as opposed to "doing."

MR. REIBLE: Thank you.

MR. SHUKLA: The EP rule has a deadline.

MEMBER BROWN: Yes. That's fine. We don't need to -- we're done.

CHAIR STETKAR: I just wanted to make sure that, if --

MEMBER BROWN: I got it.

CHAIR STETKAR: -- they were doing it, when. Then, I understand the expectation versus commitment in a public meeting. So, that's fine.

The other question that I had, because I do take notes, and MHI, yesterday, had their Slide 8, which shows their -- their current design for protecting essentially communications between the unit and the station bus and communications between the station bus and the outside world, separated.

And their -- their slides, just for reference, shows that the station bus communicates to the EOF and the ERDS system but, in particular, I was thinking about the EOF because, obviously, the EOF is shared among all four units now.

And the question I raised yesterday, and they said, "Well, it's a COL issue," so I'll raise it to Luminant, is -- what protections are available on

-- is there a single station bus, and is there a protection provided that prevents information coming in from the outside world, let's say, on the Unit 2 part of that station bus propagating back through?

Now, supposedly, the protections that they show between the Unit 3/4 unit bus and the station bus would prevent that from coming back to Units 3 and 4. But I was just curious what -- whether there are protections over on the Unit 1 side that are similar -- functionally similar to what's shown now on the Unit 3/4 side, in particular on the station bus.

MR. REIBLE: Yes. And the answer to that is, yes, there are. The protections are very similar to what is being proposed by Mitsubishi.

There is a deterministic isolation device between the control aspects and then for -- between the EOF and the outside, there is a deterministic --

CHAIR STETKAR: Okay.

MR. REIBLE: -- isolation valve.

CHAIR STETKAR: Okay.

MEMBER BROWN: When you say "deterministic" you mean hardware, one-way?

MR. REIBLE: Yes.

MEMBER BROWN: Similar to what is shown that --

MR. REIBLE: Exactly.

MEMBER BROWN: -- connect any external networks --

MR. REIBLE: Right.

MEMBER BROWN: -- it's just separate from the one that would be around for the Units 3 and 4?

MR. REIBLE: That's correct.

MEMBER BROWN: Okay. So it's there today.

CHAIR STETKAR: Yes. That was the only question in terms of --

MEMBER BROWN: Yes. Yes, this is a hangover --

CHAIR STETKAR: So that's --

MEMBER BROWN: -- from yesterday.

CHAIR STETKAR: -- that's good. Thank you.

Any of the members have any questions for MHI? I'm sorry. Whoever you are. Luminant. I've spent a week here in the last two days.

(No response.)

CHAIR STETKAR: If not, thank you very much. And you actually got to answer some questions, so that was exciting.

And we'll have the staff come up on the COL Chapter 7.

MR. MONARQUE Okay. Good morning, my name is Stephen Monarque. I'm the lead project manager for Comanche Peak safety review application, and today I'm going to do the staff's presentation on the safety evaluation report for Chapter 7, Instrumentation and Controls.

I'm the lead project manager for this combined license application review, and Bill Ward was a project manager, and Eugene Eagle was a technical reviewer for the Instrumentation Controls Branch.

There were no open items, as Luminant described earlier. Most of the sections were IBR with the exception of 7.4, 7.5, which is systems required for safe shutdown and information systems important to safety.

And with that, that concludes our presentation. We're now ready for any questions.

CHAIR STETKAR: This may be a record.

MR. MONARQUE I'm glad they --

CHAIR STETKAR: No. In terms of number of slides. Usually we get some -- some more introduction -- thank you very much.

Seriously, any -- any questions for the staff?

(No response.)

CHAIR STETKAR: If not, Stephen, thank you.

MR. MONARQUE Thank you.

CHAIR STETKAR: And I believe that closes out the discussion of Chapter 7 for both the DCD and the COL.

MR. MONARQUE I need to get the reviewers for Chapter 2, if you wish to commence on that.

CHAIR STETKAR: Yes. We'll -- we'll take a break. Is 15 minutes long enough for you to do that?

MR. MONARQUE Yes.

CHAIR STETKAR: Okay. Before we do -- do that, I mean, start summoning them.

As we usually do, I'll go around the table and see, at least for the Chapter 7 part of the proceedings.

Do members have any final questions or comments? Joy?

MEMBER REMPE: No.

CHAIR STETKAR: Charlie?

MEMBER BROWN: Just one relative to -- there's going to be a final SER, obviously --

CHAIR STETKAR: Yes.

MEMBER BROWN: -- and since there's open items. And the -- at least a couple of items that I discussed yesterday on the watchdogs and the -- now, I've forgotten what the other one was. Whatever it was, it was written down. It's on my sheet.

Oh, the control of access, which they said they would have upgraded. I'm presuming that we will get to see the final setup, how those are finally resolved.

CHAIR STETKAR: Yes. No, we -- we will -- the ACRS must write a letter --

MEMBER BROWN: Yes.

CHAIR STETKAR: -- based on the final SER.

MEMBER BROWN: I was just trying to make sure I knew where we were relative to that. I know we're not going to do one right now, and I just -- because I did want to see the final results in the DCD as to how these were shown for execution purposes on the watchdog as well as seeing it finally cranked in on the control of access thing.

CHAIR STETKAR: The whole purpose of having these exchanges on the Draft SER with Open Items is for subcommittee members and the ACRS, through our interim letters, to provide some -- some early feedback to the staff in terms of areas of concern.

And the staff and MHI will work toward closing out the existing open items if they feel they need to issue additional RAI's as a result of these discussions. They'll -- they'll issue them.

In some cases, you know, we get feedback directly from the staff or from MHI to answer questions where -- where they feel sufficient information is available.

But, in answer to your concern, we certainly do get another opportunity to review the entire final SER.

MEMBER BROWN: Good.

CHAIR STETKAR: And I can raise -- you know, if we don't feel our current concerns are resolved by that point we can --

MEMBER BROWN: Have another try.

CHAIR STETKAR: -- keep them open and -- and we have the opportunity to raise additional concerns at that time. So, we're not done with this by a long shot.

MEMBER BROWN: Okay. Other than that, I -- you know, the only other comment is I wanted to thank MHI and the presenters. They really did put together a good presentation which clarified and made very clear what was going on, made sure we understood -- I understood it, and that was good. That's a real plus on this review.

MEMBER SHACK: I will just echo Charlie's.

I mean, yesterday's discussions were very helpful for a nonexpert.

CHAIR STETKAR: And I will say the same thing. I -- I -- you know, I'm sorry we ran over in time, but I think it was well worth the time spent. I -- especially MHI. I really appreciate the effort you put into all of the presentations, your ability to answer our questions here. I think we -- we really appreciate that.

I think it -- it helped our confidence, both in the understanding of the design and I hope it helped you to -- to hear a few of our concerns, and I think it was a really useful process.

With that, I will take a break and hopefully the staff can get your Chapter 2 reviewers here in a timely manner, and we will recess until 10:10.

(Whereupon, a short recess was taken from 9:54 a.m. until 10:12 a.m.)

CHAIR STETKAR: We are back in session. We are going to hear about the Comanche Peak Combined License Application, in particular FSAR Sections 2.0, 2.1, 2.2, 2.3.

I understand that the remaining sections of Section 2 will come in at some later date. We're not quite sure when that will be yet. We don't have it on the -- on our agenda, anyway.

With that, Don, welcome back.

MR. WOODLAN: Thank you.

CHAIR STETKAR: It's been a long time.

MR. WOODLAN: Thanks, John.

We are ready to go. As you pointed out, we are presenting a portion of Chapter 2, primarily regarding the site characteristics.

As the title implies, this is not as IBR, as many of our other sections. We do have quite a bit of site-specific information in there.

The general agenda we are going to follow is our standard agenda. We will start with an introduction. We do have one SER open item that we'll discuss and then we will get into a summary or a high level overview of the site-specific information provided.

In our introduction, again, we do follow the IBR methodology, and there is material that is incorporated from the standard plant design. We are taking no departures from the standard plant design in these sections.

All COL items that were included in this -- in the standard plant are -- have been addressed in the FSAR.

As I mentioned, we have one open item, SER open item. We have no confirmatory items that remain, and we have no contentions pending before the ASLB.

I'll address the open item first. The open item really was initiated by us from the standard plant. There was a -- some changes made to the layout of the standard plant, and those were made to address seismic concerns.

Those changes, however, do affect some of our dispersion calculations in that those are very location-dependent so if a discharge point moves a couple feet, that changes the calculation. We need to adjust the calculation to address that.

We have done all those adjustments. We have updated the tables in the FSAR, and that information has been provided to the staff. All the differences were very minor. Second decimal point kind of thing.

CHAIR STETKAR: Did you have to move the buildings around very much?

MR. WOODLAN: We -- well, we personally didn't move them, but the standard plant did. They -- you may remember the power block was a multiple set of buildings and they moved it into a single power reactor building complex now.

CHAIR STETKAR: Oh, hum.

MR. WOODLAN: And so that, as a result, some of the buildings moved two or three feet, maybe. Some of the discharge points elevations may have changed a couple feet.

MEMBER BLEY This is for the regular, the --

CHAIR STETKAR: That's -- that's for -- and it's in the certified design now?

MR. WOODLAN: Yes.

CHAIR STETKAR: So it's not a site-specific.

MR. WOODLAN: That's correct. It's part of what we are IBR'ing.

CHAIR STETKAR: Okay.

MR. WOODLAN: And I assume that will all be presented once we get to the site --

CHAIR STETKAR: That will be --

MR. WOODLAN: -- presentations.

CHAIR STETKAR: Yes. Well, we haven't heard that part of the DCD yet, either --

MR. WOODLAN: Right.

CHAIR STETKAR: -- in terms of seismic. So, thank you.

MR. WOODLAN: With that, I'm going to cover 2.0. We had a choice. I had the first choice, so I picked 2.0.

And the primary, I think, points of interest there are the key parameters in the DCD. There are a set of parameters which were used to complete the standard plant design, and the site-specific applications are supposed to confirm that we're within those bounds, therefore, justifying that the standard plant analyses are applicable to us and do apply.

And we have done that, and the table shows that. I will state that some of the material in there is still ongoing. Some numbers, I expect, are going to change, and we're -- we're following that.

We update the -- the DCD -- as the DCD gets updated, we do update the FSAR to correspond to that. And I know of nothing, no changes at this point in time in which we do not remain bounded by the standard plant parameters.

With that, we'll move to 2.1 and I'm going to turn it over to Tim Clouser.

Tim.

MR. CLOUSER: Good morning. As Don said, I'm Tim Clouser. I'm going to talk just briefly about Section 2.1 and then I'll turn it over to Bob Reible for Section 2.2 and then I'll come back for 2.3 and wrap it up.

So, a proposed site for --

MR. WOODLAN: And then go catch an airplane.

MR. CLOUSER: Hopefully, because it may actually be delayed again.

Our proposed site for Units 3 and 4 is co-located with our Unit 1 and 2 site. We are located in North Central Texas on a site that's just under 8,000 acres. We are about 40 miles southwest of downtown Fort Worth, Texas.

The nearest population center which is defined as a city of greater than 25,000 people Cleburne, Texas, and that's 24 miles east of the plant. And that is our basic geography and demography.

Any questions?

CHAIR STETKAR: Yes. The demography numbers in the FSAR are based on the 2000 Census data, extrapolated through some modeling process to, first 2007, and then taken out to, I think, 2056.

That assumes a construction completion date of 2016, which you're -- I'm just going to guess. You're probably not going to make that.

MR. CLOUSER: Probably no.

CHAIR STETKAR: My question was, Texas, in the 2000's, certain areas of Texas experience pretty dramatic population growth. I ran out some 2010 Census figures and compared them to 2000 in areas -- like Granbury, in particular, increased about 40 percent population over that decade.

Fort Worth is also about 40 percent. Glenrose, not so much, about 15 percent. Cleburn, about 15 percent.

Since your construction date -- I'm guessing -- most likely will be later than 2016, have you thought about updating your demographics to account for the 2010 Census, rather than something that's now 13 years old, projected out over, you know, the next 50 years or 60 years of 70 years or something?

MR. CLOUSER: That's a fair question.

MR. REIBLE: I can answer part of that.

MR. CLOUSER: Okay.

MR. REIBLE: Part of that is that, for our operating units, because of the EP rule change, we had to revisit our demographics and reassess our ETD's for evacuation, and incorporate the new population statistics.

Those will be incorporated into our COLA so, with that process, we will do a revision to the 2010 population.

CHAIR STETKAR: And we see new statistics

-- the 2010 Census?

MR. REIBLE: Yes.

CHAIR STETKAR: Okay. Good. Thank you.

MR. CLOUSER: All right. If there's no other questions, then Bob is going to talk to you about nearby industrial, transportation and military facilities.

MR. REIBLE: The nearby industrial, transportation and military facilities, CPNPP Units 3 and 4 design is bounded by the DCD, Section 2.2.

Evaluated the design basis events for hazardous materials and activities in the vicinity of the site, and no additional mitigation was required.

CHAIR STETKAR: Now, you didn't bring your maps, so I'm going to have to walk through this orally.

There are some airways that are looked at. I looked at the airports and I looked at the airways, and this may be a better question for the staff, but I'll ask you first.

The Standard Review Plan has some guidance in it that's kind of stylized, but the guidance says that, for example, you can presume that the probability of an aircraft crash is -- it says the probability is considered to be less than an order of magnitude of ten to the minus seven per year by inspection -- whatever that means.

If the distances from the plant meet all of the criteria listed below, a couple of the criteria are a number -- it's Item B, "The plant is at least five statute miles from the nearest edge of military training routes."

Item C, "The plan is at least two statute miles beyond the nearest edge of a Federal airway."

I did some calculations looking at the military and civilian airways and there's a military airway, VR-158 that, if I take the standard widths of airways, its closest edge seems to be less than five miles from the center of the plant.

The center line is more than five miles, but not the closest edge, because they're -- they're about, I think, 10 or 11 nautical miles wide.

And the nearest edge of civilian airway V-17-18-568, depending on the resolution that I can get, seems to be just about two miles from the center point of the plant.

So, I was curious why, by inspection for those two particular airways, I could presume that the frequency of crashes is less than ten to the minus seven, in other words, how those two airways satisfy those criteria.

I'll ask the staff more about this because they, indeed, have no open items and they look at the standard review plan.

But I just wanted to note that. You probably don't have answers unless you have a lot of maps with you and really close distances. But when I ran out the distances and I checked them a couple of different ways, at least the military aircraft -- airway, I don't see any way that you can say that -- that the nearest edge of that airway is more than five miles from the center -- the center point of the two units.

The civilian airway, I could get it -- it's -- I got it to be 2.0 miles, but that's -- that pretty coarse, given the maps I was using, so --

MR. REIBLE: I think the current -- the FSAR list, the VR-158, within 10 miles and, you know, based on your comment, I think we need to --

CHAIR STETKAR: That's the center --

MR. REIBLE: -- revisit that.

CHAIR STETKAR: That's the center line distance, though. It's actually -- my mapping stuff put it at 7.8 miles, which is in -- which is within 10 miles but if you then take the -- the normal width of those airways, you know, you get within much less than five miles from the nearest edge.

So, you may want to -- you may want to think about that. I -- I realize we are not going to get a resolution on that today, and I am more interested in how the staff reached their conclusion, given this information. So, I just wanted to raise that point about the airways.

You are far enough away from the airports. Just -- just barely from DFW, but that's okay.

MR. CLOUSER: Are you all done, Bob?

MR. REIBLE: Yes.

MR. CLOUSER: Any other questions for Section 2.2?

(No response.)

MR. CLOUSER: All right. I'll cover meteorology, then. As I mentioned earlier, we're in North Central Texas, which is about 280 miles from the coast, so we don't see a lot of hurricane activity.

However, in reviewing the hurricanes since 1900 in the State of Texas, we did have one Category 1 hurricane that approached within 50 miles.

CHAIR STETKAR: Let me interrupt you.

MR. CLOUSER: Okay.

CHAIR STETKAR: I'm sorry about that. I

know people have flights to make, but we have things to do also.

So, -- and I didn't realize this. Bob, the pipeline -- as I read through the FSAR, there were a couple of assumptions -- and, in particular, I'm talking about the Sunoco Oil pipeline, the close one there.

MR. CLOUSER: Right.

CHAIR STETKAR: There were a couple of numbers in the FSAR regarding assumed durations of leaks from that pipeline. And, in particular, it says that, for a large break of the pipeline in Section 2.2.3.1.2.3, it says the flow rate, which is 47 cubic feet per second, is assumed for a one-minute duration, the time to detect and isolate the large break.

It's also noted in the FSAR that there are no valves within five miles of CPNPP and the nearest station associated with the pipeline is over 30 miles away.

So, I was curious about how people effectively detect and isolate a break in that pipeline within one minute. That's -- sounds darned good to me.

So, I'm interested to find out -- since that's in the FSAR, I'm interested to learn what the basis for that -- did you -- you know, did you get information from the pipeline company, what sort of detectors do they have, what sort of assurance that, within a one-minute time after this -- it has to be a large rupture, but those things actually happen as we're well-aware, in pipelines, how you can get assurance that it would be isolated within a minute.

And then, there's a small-break case that says the largest -- for the small break, the flow rate is .62 cf -- cubic feet per second or about 275 gallons per minute.

It says that leak rate was assumed for a period of 32 hours, and that's -- it says the rate is based on the largest undetectable leak and the longest period of time the spillage would go on observed.

So, I was curious what the basis for that, 32 hours and the detection within that time period. I'm, quite honestly, less concerned about the small leak, obviously, than the large leak, but -- but there didn't seem to be any bases in there for those times.

I'm a -- I'm a, as I said, a little more questioning about that one minute.

MR. REIBLE: Okay.

CHAIR STETKAR: Okay.

MR. REIBLE: Yes, I can see the specific references that you are making, and we'll take that as an action --

CHAIR STETKAR: Yes. They are both in 2.2.3.1.2.3.

MR. REIBLE: Right.

CHAIR STETKAR: There's a large-break case and a small-break case.

MR. REIBLE: Right.

CHAIR STETKAR: Thank you. And I'm sorry.

MR. REIBLE: That's all right.

CHAIR STETKAR: I don't read all that quickly here.

MR. REIBLE: Okay. Back to Section 3?

CHAIR STETKAR: Yes.

MR. REIBLE: We were talking about the hurricanes and the one that was recorded in the last 160 years was in 1900, and it was -- exited the 50-mile radius around the plant at about 65 miles an hour.

So, although our maximum hurricane site characteristics are bounded by the US-APWR Reg Guide 1.221. So, a likely candidate for concern are tornados and, in the 56-year period from 1950 to 2006 there were three tornados sighted in Summervell County, which is the location of the plant site, and maximum tornado site characteristics are bounded by the US-APWR Reg Guide 1.76.

Any questions?

CHAIR STETKAR: Yes. Several. Since you mentioned hurricane first let me look at my hurricane notes here.

There's a statement in the FSAR that says, "Assuming a" -- there's a model in there. It says, "Assuming a maximum landfall wind speed of 208 knots, a translational velocity of 16 knots, and a distance of 400 miles from the CPNPP site to Galveston, gives a maximum possible wind speed of 61 miles per hour at the CPNPP site. This could -- should be considered as the upper bound of possible hurricane wind speed at the CPNPP site."

That's in the FSAR.

MR. CLOUSER: Yes.

CHAIR STETKAR: You mentioned 65 miles per hour. I looked up the hurricane data, and within 50 miles of the site there was an unnamed hurricane on September 9th, 1900 that had a wind speed of 74.8 miles per hour, and Hurricane Carla, on September 12th, 1961 that had a wind speed of 69 miles per hour. That's within the 50-mile radius of the site.

So, I'm curious, given that evidence, why the upper bound of possible hurricane wind speeds at the site is 61 miles per hour.

MR. CLOUSER: Do we have any assistance on that question?

CHAIR STETKAR: I understand how the model calculated that wind speed. I sort of like to look at data.

MR. CLOUSER: Right. Understand.

CHAIR STETKAR: Okay. If you don't, let me --

MR. MORRIS: This is Marvin Morris. The discussion -- can you hear me okay?

CHAIR STETKAR: I think so.

MEMBER BROWN: Try to get closer so the recorder can pick you up.

MR. WOODLAN: Try to get closer to the mic.

MR. MORRIS: Okay. Thank you. Marvin Morris. The discussion in the FSAR is just an example of the decay of hurricane wind speeds as they go inland due to friction and also due to loss of the driving force, water temperature that -- that goes away as it crosses inland.

And that's just an example of the decay, you know, an exponential type decay as it goes inland, you know, and the assumption was 240 mile per hour hurricane hitting the coast and decaying exponentially and they come up with 61 mile per hour as a -- as what that translates to.

CHAIR STETKAR: Right. Yes. And I understand that's from someone's model of hurricane wind speed decay, and I wouldn't have any problems if it's presented in the FSAR as here's an example of some way that people have calculated possible wind speeds, and here is our data -- here are our data.

But, that was -- what I quoted was from the FSAR and it uses words of "a maximum possible wind speed of 61 miles per hour. This should be considered as the upper bound of possible hurricane wind speed at the CPNPP site."

MR. MORRIS: Right. Based on -- based on that assumed 240 mile an hour wind speed at the coast.

However, what we're using for the design basis is from Reg Guide 1.221, which is 160 miles per hour at the site. So, it just -- it shows a degree of a conservatism.

CHAIR STETKAR: That's -- I'm sorry. That's the design basis. We're trying to compare what margin you have between actual experience and the design basis.

MR. MORRIS: Yes.

CHAIR STETKAR: I understand what the -- and I'll grant if, for hurricanes, I think you have substantial margin available.

However, I'm also interested in not mischaracterizing numbers as maximum possible upper bound of the highest wind speed we could ever expect at the site when there is actual evidence from data that -- that leads me to suspect that number.

So, that's my biggest concern about that. It's -- I'm not -- I'm going to -- in this particular case, I'm not actually questioning do you have adequate margin.

MR. MORRIS: Right.

CHAIR STETKAR: It's just the way that -- that --

MR. MORRIS: It's been phrased.

CHAIR STETKAR: -- the hurricane wind speed model is characterized, given -- given data.

Now, in particular, let me raise a different question here before I get to tornados and a couple of other things.

In the meteorological section you've used basically 30 years of meteorological data from Fort Worth and there are a few -- there are a few met stations they use, Fort Worth -- they make a lot of reference to DFW.

MR. MORRIS: Right.

CHAIR STETKAR: And there's a couple of

others. I've forgotten the names. I've got them listed here somewhere.

But, the point is that the -- the database that you've used for essentially looking at fairly rare events spans 30 years.

Now, I went back into Weather Service records and for DF -- I'm sorry. Let me get the -- so I'm correct on the record here. DFW is limited because DFW didn't exist for very long back in history.

But if I look at weather records for Fort Worth Meacham Field, KFTW, they go back to 1945. Dallas Love, KDAL are back to 1946. Mineral Wells, KMWL are back to 1948. DFW is only back to '74 in terms of daily records because, you know, it didn't exist.

So, my question is: Because we're trying to project very rare extreme events and, indeed, I have data available back for, I don't know, 60, 65 years, why haven't I used all of that data? Why have I restricted myself to only 30 years from 1971 through 2000, whatever the -- whatever the database period was?

MR. CLOUSER: And that is a very good question. I don't have an answer for that, but we can get back to you --

CHAIR STETKAR: Okay.

MR. CLOUSER: -- with that data and see if we need to expand that.

CHAIR STETKAR: Where it comes up in some of my concerns is you're close to the margin on a couple of meteorological parameters. One is the maximum -- however it's characterized -- zero percent exceedance frequency dry bulb temperatures, 115 degrees. That's the design value.

And, indeed, August 19th, 1984 there was a recorded high daily temperature of 115 degrees at Glen Rose. Not DFW. Not Fort Worth. Not -- at Glen Rose.

And that's -- that's right at it. That doesn't give me a lot of margin. I don't know what the temperatures were if I go back another 30 years back into the historical record.

It doesn't give me a lot of confidence about margin to that maximum temperature in the certified design. So that's one case where having more meteorological data might discover data points that, indeed, exceed it, or it might give you greater confidence that -- that whatever -- however you characterize the zero percent exceedance, and I know there's a stylized notion of what that means, you can have greater confidence that you are not actually going to exceed that over the next 60 years of the plant.

MR. CLOUSER: Sure. So what I understand

that you're saying is you're concerned that some parameters don't have as much margin as we might like to see and we have more data available than we have used to do some analysis, and we might want to take a look at that and see if we need to --

CHAIR STETKAR: Yes. Exactly.

MR. CLOUSER: -- make an adjustment.

CHAIR STETKAR: Exactly. Exactly.

MR. WOODLAN: Marvin, do you have anything to add?

MR. MORRIS: Yes. I was going to -- I was going to add that, you know, the criteria definition that we use for determining zero percent exceedance, which is not what you might think is zero percent exceedance which would be you would never exceed.

CHAIR STETKAR: Right.

MR. MORRIS: Zero percent exceedance, the definition that we've used and the same definition that was used in AP-1000 plants is the temperature that's only exceeded two hours in a 30-year period of record.

And so that's -- that's one we've used and, you know, that -- that implies enough -- you know, it says you should use a 30-period of the record, which is what -- what we did.

CHAIR STETKAR: And, quite honestly, if you had much larger margins in that 30-year period perhaps I wouldn't be as concerned, but since, in the period -- even in that 30-year period of record, you've hit -- apparently hit that value.

And I'm not sure about two hours and all of that --

MR. MORRIS: Yes.

CHAIR STETKAR: -- stuff, but --

MR. MORRIS: But I think if you look at it in terms of plant operation, if you hit it -- hit it for one hour, it has no effect on plant operations.

CHAIR STETKAR: I'm trying to understand where -- we're now transitioning from the certified design to the Glen Rose site. And I'm trying to understand what margins are available under the regulatory basis at the site to the design, because that gives us a measure of confidence in terms of -- of where you -- how much margin you have on those external effects.

What -- what the impact of exceeding 115 degrees for ten minutes or two hours or whatever, is a different issue. But the certified design says 115 degrees is what it's --

MR. MORRIS: Right.

CHAIR STETKAR: -- is what it's built to.

MR. WOODLAN: I think we understand the question. We don't have an answer today --

CHAIR STETKAR: So, in terms of the two things to try to keep the discussion going, the two things that I found, the one where -- I think that the entire story about meteorology would benefit from looking at longer than the 30-year period.

In particular, I'm not quite sure about the margin on temperature. Rainfall, you got a pretty good margin. Wind speeds you can't do much with, three-second wind gust speeds, because they weren't recorded in that way back before the -- I don't remember, Marvin, 1980's or even later than that sometimes.

So, you can't really go ferret out, you know, wind -- straight-line wind speed data. Rainfall, you can lead up pretty good margins there. Temperature, you certainly can. Everybody has recorded temperature.

Okay. And we talked about the hurricane. Tornados. You know, I'm going to ask the staff about tornados. I know what you did. I'm going to ask the staff. It's better to ask them. So, I'll let you off the hook on that.

MR. CLOUSER: Okay. Any other questions on Chapter 2?

CHAIR STETKAR: Oh. Yes. You have to

excuse me. I -- I take a lot of notes and then, now, out of order, so I have numbers that I have to look at.

Somebody's rubbing things on a microphone. Please stop. You get two warnings and then it's not pretty after that.

In Section 2.3.1.2.8 on precipitation, there's a statement that says "Probable Maximum Precipitation, PMP." Sometimes called "Maximum Possible Precipitation," which, depending on whose reference you look at, there is -- there is a notion that PMP is a meteorological limit for the absolute upper bounds of the amount of precipitation that can occur.

There are other interpretations of that term. It says, "Probably Maximum Precipitation, sometimes called Maximum Possible Precipitation for a given area and duration is the depth which can be reached, but not exceeded under known meteorological conditions." So, in this sense it's -- it's the worst it could possibly get.

For the site area, using a 100-year return period, the PMP for 6, 12, 24 and 48 hours is 6.9, 8.3, 9.5 and 11.0 inches, respectively. And there's a table that lists those values.

Now, if the PMP is the maximum possible that could ever occur, why do we have a PMP with a 100-year return period?

MR. CLOUSER: I don't have the answer to that question.

CHAIR STETKAR: That's an exceedance frequency. It's not a maximum upper bound. In principle, if this is the hundred-year, if I ask you what the thousand-year is, you'd probably get larger values. For the million-year, you'd get even larger values.

And, in some place, if you actually interpret the PMP as the absolute maximum, it couldn't get any bigger than that.

But, this notion -- the way it's presented in the FSAR, the notion of PMP has a recurrence frequency attached to it which -- I've never seen that.

Have you, Bill? You're a PMP guy?

THE WITNESS: No, that's a -- that's a new one.

CHAIR STETKAR: Okay. So I'll raise that issue.

MR. CLOUSER: Okay. I understand the question to be why do we have a recurrence factor on a maximum value --

CHAIR STETKAR: Right.

MR. CLOUSER: Basically.

CHAIR STETKAR: And -- and have you -- I mean, one of the questions I asked you earlier on demographics, you said that you've revaluated the demographics for Units 1 and 2 for emergency planning.

Have you developed PMP estimates for Units 1 and 2, and are they the same as these?

MR. CLOUSER: How do I say that, Bob?

CHAIR STETKAR: I'm suspecting that, as post-Fukushima things you will be doing that, but --

MR. CLOUSER: Right. Right. Right.

CHAIR STETKAR: But, I was just curious. I mean, it --

MR. CLOUSER: Well, I can't give you a full answer, but I can give you an answer based on what I read. First of all, there's several PMP values, depending on the -- the situation you are trying to evaluate, and PMP will vary based on various zones within the watershed.

CHAIR STETKAR: Sure.

MR. CLOUSER: And so, yes, Unit 1 and 2 has values, but they are a quarter of a mile away. Their values are actually different. Their zoning is different.

CHAIR STETKAR: Okay.

MR. CLOUSER: And so they have a different number than we use, and we actually use several PMP values, one for flooding in Squaw Creek Reservoir, one for actual water development on the site and local water levels on the site.

CHAIR STETKAR: Right.

MR. CLOUSER: Because they are --

CHAIR STETKAR: So that has to do with drainage --

MR. CLOUSER: And whether or not you're looking at a short term, because it's a higher number per minute if you're looking for a very short-term event. But if you're looking for a 24-hour event, it's a different number.

CHAIR STETKAR: Sure.

MR. CLOUSER: So, yes, we do have differing numbers. I'm not saying they're inconsistent.

CHAIR STETKAR: Yes. Those are -- those are intensity values.

MR. CLOUSER: Yes.

CHAIR STETKAR: You know, but they're still -- they're still -- in everything that I've seen, they are still going back to this hundred-year recurrence frequency. They are all -- they are always considered. That's whether or not you believe that the maximum -- the probably more realistic thing to look at them is a hundred years.

MR. CLOUSER: Oh. Oh, yes.

CHAIR STETKAR: But that's a different question. That's a different question.

MR. CLOUSER: Yes. And, as we said, we -- we will take an action --

CHAIR STETKAR: Okay.

MR. CLOUSER: -- to try and clarify that wording.

CHAIR STETKAR: And, with that, I don't think I have anything more on 2.3.

MR. CLOUSER: Okay.

CHAIR STETKAR: But I had a lot of details, but a lot of the details essentially -- oh. Yes. I was going to ask the staff about a lot of these because a lot of the details go back to better confidence using a broader meteorological database than the 30 years.

MR. CLOUSER: Right.

CHAIR STETKAR: So, with that, do any of the members have any questions for Luminant?

(No response.)

CHAIR STETKAR: You don't?

MR. CLOUSER: All right. Then this concludes our presentation.

CHAIR STETKAR: That was not too bad.

Thank you.

And we'll ask the staff to come up and hear from them.

Stephen, do you want to say anything?

MR. MONARQUE: No, thanks. We'll just go ahead and start our presentation and I'll turn it over now to Tarun Roy, who is a project manager for Chapter 2.

MR. ROY: Yes.

CHAIR STETKAR: And, again, make sure you are really careful about your paper not hitting those microphones. Thank you.

MR. ROY: My name is Tarun Roy. I am an NRO project manager responsible for coordinating staff review for Chapter 2, site characteristics, COLA application.

The NRC technical review involved with the review of the Comanche Peak Unit 1 and -- 3 and 4. Mr. Seshagiri Rao Tammara, physical scientist here in and Kevin Quinlan, physical scientist, hydrology and metrology branch, and the staff reviewer.

During this meeting, the staff plans to make a presentation of the Chapter 2, only Section 2.0, 2.1, 2.2 and 2.3, security relation report with open item.

In summary, staff issued a ten questions on 2.1, 2.2 to the applicant, requesting additional information. There is no open item in that review.

The second item, the staff issued a total of 49 questions in 2.3 to the applicant, requesting additional information. There is one open item in the review.

If you have any question regarding this chapter, I would turn over to presentation -- over to the technical reviewer, Seshagiri Rao Tammara or the Section 2.1 and 2.2.

MR. TAMMARA: My name is Seshagiri Rao Tammara. I'm a technical reviewer for the Chapter 2, Section 2.1 and 2.2.

2.1 covers the geography and demography. 2.2 covers the nearby industrial transportation and military facilities.

CHAIR STETKAR: Again, please be really careful not to hit that microphone. It's really, really sensitive. Both Tarun -- thanks.

If you had the things plugged in your ears that our recorder has -- we have amplifiers on these microphones -- you'd appreciate why we say that.

MR. TAMMARA: 2.1, geography and demography covers the site-specific information pertaining to site location, exclusion area boundary, population distribution projections, population center and population density.

The applicant addressed all this site-specific information. Based on the staff's review of this information and information obtained from the publicly-available sources and also independent confirmatory calculations.

The staff concludes that the applicant addressed the information is appropriate, adequate and acceptable, as it conforms, the requirements meets the acceptance criteria and also satisfies the NRC guidance, and there are no open items.

The Section 2.2, nearby facilities pertains to the first, Section 2.2.1-2.2.2, describes the locations and also descriptions of the products and the facilities in the nearby plant within particularly five miles, or up to the 10 miles in the airports and airways.

Most of the information is -- what are applicable is incorporated by reference, but this is mostly site-specific information, therefore, the site-specific information covered nearby industrial, transportation and military facilities, pipelines, gas wells and also the existing units are also considered as nearby facility, Units 1 and 2, and also on-site chemical storage facilities.

The applicant addressed all these specific -- site-specific information. Based on the staff's review of this information and also information obtained for the locations and the products from the public-available sources.

The staff concludes the applicant has addressed the information appropriately and it conforms the requirements, meets the acceptance criteria, and there are no open items.

CHAIR STETKAR: Let me ask you about the airways now. Why is the nearest edge of military airway V-158 more than five miles from the center of the plant?

MR. TAMMARA: Well, the edge of the plant is around 7.8 miles, so we looked at the map, but in any event, what we have considered is we have not -- I mean, it has been considered to calculate the probability in the Chapter 3.

Even though -- you know, even though the airway is designated as at one but in the evaluation of aircraft impacts in 3.6 -- 3.5.1.6, we have evaluated what is the potential probability of the military aircraft, and addressing that impact section.

This -- this Chapter 2.2.1 uses only the description, but the evaluation is performed and the impacts are evaluated in that section, aircrafts impact section.

CHAIR STETKAR: Well, we haven't had the benefit of --

MR. TAMMARA: Right. I think it is --

CHAIR STETKAR: -- yet?

MR. TAMMARA: Yes. That's correct. But if you -- I mean, I have also completed that section. Now, --

CHAIR STETKAR: Now --

MR. TAMMARA: -- it might be too early to --

CHAIR STETKAR: Yes. No, I -- I don't to open up that discussion at the moment because it's not fair to -- to anyone to do that. But, I guess, you know, I'm a bit frustrated because now I'm not quite sure why we do the Chapter 2 review at all.

The Chapter 2 review is supposed to look at -- at acceptability of the site, compared to guidance in the regulations.

MR. TAMMARA: Right.

CHAIR STETKAR: And the site is deemed to be acceptable if the frequency of aircraft crashes is deemed to be less than ten to the minus seven, and there are some presumed crash frequencies based on distances.

And, if you meet those distances, it's

presumed that the crash frequency is less than ten to the minus seven.

MR. TAMMARA: That's true.

CHAIR STETKAR: Now, that's not actually true. If you do a real aircraft crash analysis -- I did a little back-of-the-envelope calculation for one of the civilian airways that is nominally acceptable and, if you look at flight densities -- and it depends on the type of carrier and the type of model that you use, I can get crash frequencies greater than ten to the minus seven.

So, it's all stylized, but for screening there are criteria that says it's okay if I'm more than five miles from the nearest edge of a military airway.

Your safety evaluation report says it's okay. It doesn't say they have to do a site-specific calculation. It says it's okay.

MR. TAMMARA: No, that is --

CHAIR STETKAR: They meet the regulations. Then, I don't understand how they meet the regulations.

MR. TAMMARA: That is okay -- the five-mile is okay for the civilian, but there is one more clause, I think, in the SRP, if it is a military, they have to look at it should not be more than 1000 flights and which would give a -

CHAIR STETKAR: The quote -- the quote from the SRP, just to get it on the record, is SRP 3.1.5. -- 3.5.1.6, Item B. "The plant is at least five statute miles from the nearest edge of military training routes, including low-level training routes, except for those associated with usage greater than 1000 flights per year or where activities, such as practice bombing may create unusual stress situations."

That says to me that you need to do a site-specific analysis if you have more than a thousand flights per year regardless of the distance or, if you are less than five miles from the nearest edge.

This plant is less than five miles from the nearest edge. In your safety evaluation report I saw no mention of the fact that this plant must do, according to this standard review plan, a site-specific analysis for that particular airway.

Now, the same question for a civilian airway where, depending on how you read the word "at least two statute miles" when you come up to something that calculates to be 2.0.

Why the SER for Chapter 2 didn't say that site-specific analyses are required -- why it just says, "This site is acceptable."

MR. TAMMARA: No. That is -- that is being done as a part of 3.5.1.6.

CHAIR STETKAR: Okay.

MR. TAMMARA: It is only in 2.2.1 is identification of the facilities and descriptions. Nothing --

CHAIR STETKAR: I hear what -- I hear what you are saying.

MR. TAMMARA: So that --

CHAIR STETKAR: Then, we'll revisit it in --

MR. TAMMARA: Yes.

CHAIR STETKAR: -- in Section 3.

MR. TAMMARA: So, in the -- if you go the 3.5.1.6, we have evaluated and we have concluded, based upon the real FAA data, we looked at it and then we confirmed it is -- it meets the -- you know, the conclusion was made in that section.

But it -- it did not regard the SER presentation.

CHAIR STETKAR: Yes. No, we'll -- we'll look at that when we get to Chapter 3. But it's -- it's still -- okay. I understand the philosophy. I don't have to agree with it. I don't --

MR. TAMMARA: But some of the applicants, what they do is, they will put a point of saying that the impact analysis is done or what -- what the reader, so that they will go and take a look at the analysis in 3. -- Chapter 3.

CHAIR STETKAR: Right.

MR. TAMMARA: So, maybe it might be advisable to add a sentence saying that the impacts are evaluated in Chapter 3 so that the reader will have a pointer to go there. Maybe that -- that can be probably the resolution.

CHAIR STETKAR: I mean, I would have thought that at least in Chapter 2, as a reviewer, you would have made note of the fact that this particular site doesn't satisfy those criteria in the SRP.

MR. TAMMARA: Since that section deals with the description we stopped it there. Of course, we can -- we can put that pointer, saying that the evaluation is performed and concluded in Chapter 3.5.1.6.

CHAIR STETKAR: Okay. Well, we'll certainly revisit this Section 3.5, whenever that comes to us.

MR. MONARQUE: Now, Chairman Stetkar.

CHAIR STETKAR: Yes.

MR. MONARQUE: Was there another issue where you found a discrepancy between the distances and FSAR and your own examination?

CHAIR STETKAR: No. No. No. No, I -- I did a couple of double-checks on that. The distances, the center line distances all seem to gibe.

It was just when I -- when I then expanded the edges of those air routes, there were -- this military air route that's -- the nearest edge is well-within that five-mile limit.

The estimates in the FSAR say three to four hundred flights per year so you don't trip over the -- the thousand flights per year. But -- but the nearest edge is well-within the five miles.

The other one is right -- seems to be right -- it's a civilian airway and it seems to be right at two miles, and you're comparing --

MR. MONARQUE: Yes. Just the --

CHAIR STETKAR: You're comparing the edge of the airway with the center point of the two units, so there's -- there's a -- you know, a few hundred yards one way or the other. It's pretty close.

MR. MONARQUE: Yes. Pretty close.

CHAIR STETKAR: Okay. Okay.

MR. TAMMARA: So, the Section 2.2.3 is the evaluation for potential accidents. The evaluation of potential accidents to the new units, due to the potential -- I mean, include explosions, gas due to sources gas pipelines, fires, aircraft hazards which are addressed in 3.5.1.6, toxic chemicals from the control room habitability and liquid spills and the collision with intake structures.

The applicant analyzed and addressed the potential hazards from these identified nearby sources, and the new -- for the new units from the potential accidents.

Based on the review of the applicant's information provided in the FSAR, attending to the potential accidents, and also a review of the information provided by the applicant as responses to the staff's requested for additional information, and also staff's independent confirmatory analysis.

The evaluation of all the applicant's -- staff concludes that the applicant has addressed the information appropriately, adequately and acceptably and, as the information is meeting the acceptance criteria, and satisfies the guidance, and there are no open items.

CHAIR STETKAR: I had a question about the toxic chemical conclusion. And this is another issue where we have regulations and then we have people. The applicant noted that they could not conclude that the frequency of tanker truck accidents on Farm-to-Market

Road 56 was -- well, their -- their conclusion was results show the total frequency for road-based hazardous material release is higher than the ten to the minus six screening frequency of Regulatory Guide 1.7.8.

They then did a release analysis, assuming that they had a dual tanker truck full of chlorine.

MR. TAMMARA: Right.

CHAIR STETKAR: And -- and looked at concentrations in the man control room and concluded that, indeed, the concentrations remained below the immediately dangerous to life and health limit of 10 ppm for chlorine.

Their analysis goes on to say that human detection threshold for chlorine is about 0.08 ppm, eight one hundredths -- 0.08 ppm, and that would occur at approximately a quarter of a minute, .25 minutes, and the concentration reaches the maximum concentration 8.0 ppm in about 16 minutes.

That's from their stylized analysis. So, maximum concentration of eight is less than the ten, so you're not going to kill anybody.

And I looked at a couple of different scenarios that they -- they evaluated, and those scenarios are 5.7 to 8 ppm maximum concentration in the control room.

Now, there are no toxic gas sensors in this plant, so it's presumed that the operators -- there's a quote that says, "Regulatory Guide 1.78 states that it is expected that a control room operator will don a respirator and protective clothing or take other mitigating action with two minutes after detection.

"Also, during a toxic gas emergency, the control room operators have the option of manually actuating emergency isolation mode of the main control room HVAC system."

Do we have any problems with having main control room operators operating in respirators or with concentrations in the main control room that might not kill me, but chlorine is a really nasty substance, and I pretty much don't want to stay in there in those kind of concentrations.

In other words, has there been any consideration by the staff to examine toxic gas monitors at this plant, given -- given this site-specific situation?

MR. TAMMARA: Okay. This is a -- this aspect of control room habitability is an interface between the Chapter 2 and Chapter 6. I mean, I want to picturize what -- what we evaluated and what they do, whatever.

As far as the -- as far as the Chapter 2 is concerned, what we are doing here is -- is there any problem with the -- any of the hazardous or chemicals that have the potential to exceed the limit in concentrations in the control room?

If -- because there are hundreds of chemicals --

CHAIR STETKAR: Right.

MR. TAMMARA: -- being addressed from the various sources and also on-site storage.

So, it is very difficult for all the chemicals to really analyze in Chapter 6.

CHAIR STETKAR: Yes.

MR. TAMMARA: Therefore, Chapter 2 is looking at all the chemicals which can be screened out --

CHAIR STETKAR: Yes.

MR. TAMMARA: And identify those chemicals which have the potential, but my have a control room habitability issue.

CHAIR STETKAR: Okay.

MR. TAMMARA: So, from that respect to what Chapter 2 does is we gather all the information from various sources, various products and identify the chemicals --

CHAIR STETKAR: Okay.

MR. TAMMARA: -- and go through our screening methodology and see what would be the concentration from a source to the control room intake.

If that control room intake concentration is higher than the limiting concentration for that chemical, then we conclude, A, this chemical has a potential. It might have an impact in the control room.

CHAIR STETKAR: Yes.

MR. TAMMARA: So we will pass on to control room habitability. Say, "Hey, take a look at this chemical from the perspective of your control room scenario, the dilution, the flow, the release -- I mean, the intake --

CHAIR STETKAR: Yes.

MR. TAMMARA: -- and whatever the mechanisms you have in the control room and see whether that -- that concentration is lower than the limiting concentration.

If not, what are the mitigating to emergency want to institute whether, you know, you want to bring in a bottle of fresh water -- air, or whatever.

So, that is all done in 6.4.2.

CHAIR STETKAR: Okay.

MR. TAMMARA: But what I'm saying, because that is the purview of their -- your question and answer should be more -- that conclusion should be in 6.4.2.

CHAIR STETKAR: But let me see if I can make sure I understand this, though. In this particular case, their analysis shows that the concentration is lower than the IDLH.

MR. TAMMARA: Correct.

CHAIR STETKAR: So does that mean that, in Chapter 6, they don't need to look at chlorine because it's --

MR. TAMMARA: No, they --

CHAIR STETKAR: -- effectively --

MR. TAMMARA: -- look at -- they independently -- because it is outside the concentration it is higher than what it is -- it is exceeding.

So, therefore, they will take a look at what -- how -- you know, they will take a look at how rapidly the concentration is going down and what it is and then they will conclude, even though intake concentration is higher than the limiting concentration.

But the control room habitability is -- is okay or not okay.

CHAIR STETKAR: Okay.

MR. TAMMARA: If not okay, what are the,

you know, remedies. I do not know, but I -- I haven't --

CHAIR STETKAR: I got it. I made the note. We'll look at -- Chapter 6 is another one we haven't gotten to yet.

MR. TAMMARA: Right. These are the interviews that I want to explain because --

CHAIR STETKAR: It's on the list.

MR. TAMMARA: -- that is not my area of expertise --

CHAIR STETKAR: Okay.

MR. TAMMARA: -- to answer you fully.

CHAIR STETKAR: Okay. Thank you.

MR. TAMMARA: Are there any questions for me from my presentation?

CHAIR STETKAR: Anything else on this section?

(No response.)

CHAIR STETKAR: Good.

MR. TAMMARA: Thank you, Chairman.

MR. QUINLAN Good morning. Can you hear me okay?

My name is Kevin Quinlan. I'm a meteorologist in the Hydrology and Meteorology Branch within the Division of Site Safety and Environmental

Analysis. I'll be discussing Section 2.3 of the SER for meteorology.

This incorporates Comanche Peak FSAR's Section 2.3 of the US-APWR DCD. There are five subsections in SER Section 2.3 related to regional climatology, local meteorology, the on-site meteorological measurements program, short-term atmosphere dispersion estimates for accidental releases and long-term atmospheric dispersion estimates for routine releases.

Comanche Peak Supplemental Item 2.0, Part 1 includes Table 2.0-1R, which is a comparison table for the US-APWR DCD site parameters and the Comanche Peak site characteristics.

SER Section 2.3.1 describes the review of the meteorological -- the regional climatological information and addresses 1 US-APWR COL information item and one supplementary information item.

The information item states, in part, that the Applicant should provide site-specific information related to regional climatology. The Comanche Peak Supplemental Information Item 2.3, Part 1 states that the applicant provides a description of the meteorology for its site and its surrounding areas.

This resulted in the comparison between the site meteorological characteristics and the DCE site parameters.

This section also addresses the 50- and 100-year return period of three-second gust wind speeds. The wind speeds were confirmed by the staff through the use of figure 6-1A of the ASCE 705 document and by examination of the NOAA Coastal Services Center Hurricane Database.

The maximum tornado wind speed of 230 miles an hour was determined through the use of Regulatory Guide 1.76, Revision 1. Because the applicant identified the most conservative tornado site characteristic by following the NRC guidance, the staff found it acceptable.

The staff compared the extreme wind speed against the guidance provided in Reg Guide 1.221, Design Basis Hurricane and Hurricane Missiles for Nuclear Power Plants and found the hurricane wind speeds and the missiles were bounded by the tornado wind speed characteristics.

To determine the maximum winter precipitation roofload, the applicant followed the guidance provided in Interim Staff Guidance Document 7, Interim Staff Guidance on Assessment of Normal and Extreme Winter Precipitation Roofloads on the Roofs of

Seismic Category 1 Structures. Because the applicant followed this guidance, the staff found the analysis to be correct and acceptable.

Ambient temperature and humidity site characteristics were confirmed through the use of 30 years of National Climatic Data Center Records for the Dallas/Fort Worth National Weather Service Reporting Station.

The calculation of 100-year return period temperatures, used a method endorsed by the ASHRAE Fundamentals Handbook, and because the applicant followed the NRC guidance and a conservative method, the staff found their analysis to be acceptable.

The applicant presented this information, FSAR Section 2.3.1, and the staff found that all the Comanche Peak site characteristics were bounded by the US-APWR DCD site parameters and, therefore, found it acceptable.

The US-APWR COL information Item 2.3, Part 1, also states that the applicant should provide site-specific information related to local meteorology. This section of the FSAR addresses the potential cooling tower-induced effects on ambient temperature, moisture and salt deposition.

This section of the FSAR also provides

detailed information showing that the Comanche Peak meteorological data are representative of the site area.

The applicant presented the information in Section 2.3.2 of the FSAR and the staff found it correct and adequate.

Next slide.

CHAIR STETKAR: No, not next slide.

MR. QUINLAN Oh. Sure.

CHAIR STETKAR: Why -- what we are trying to do here is to understand -- we understand what the design is, as in specified values, and we're trying to understand the margins between this particular site and the design values.

And, in may cases, although we don't like to use probablistic risk assessment in these areas, there are many inferred probabilities and frequencies and stylized methods that are designed to give us some measure of confidence about what margins we have to that design.

Words like "conservate" get thrown around. Words like "probably maximum" get thrown around. Words like "hundred-year exceedance " get thrown around.

My question is: Why is it okay to use only 30-years worth of data when we are trying to look at very rare events and gain confidence that the particular conditions at this site either will not exceed the design conditions or give us some confidence about how close to those design conditions we come.

You heard the discussion before but, in particular, if the design conditions say the maximum temperature -- and I don't want to get into the stylized analyses of should it be greater or less than 2.0 hours under somebody's inference of what might be good enough.

If the design says I shouldn't have a temperature, exterior, higher than 115 degrees and I have a data point that says, "In Glen Rose, Texas, in 1984 it got up to 115 degrees," that doesn't give me a lot confidence in the margin for this particular site to the design.

And why is it okay just to take a snapshot, especially if I've got 60 to 70 years worth of data from only 30 years to support that confidence from the staff's perspective.

MR. QUINLAN Well, you asked about the reason we used 30 years.

CHAIR STETKAR: Yes.

MR. QUINLAN At some point, NOAA determined that 30 years was a climatological period.

Now, often we use -- we use more than that, and I think in this case I pulled data from some other sources and found that Dallas/Fort Worth, their hourly data set was the most representative of the site area, and provided the -- the more conservative estimates.

CHAIR STETKAR: DFW in particular?

MR. QUINLAN Correct. Yes, that's why I used Dallas/Fort Worth --

CHAIR STETKAR: DFW only goes back to the Seventies. It didn't exist.

MR. QUINLAN Yes.

CHAIR STETKAR: That's why -- that's why I pulled up values for Fort Worth and -- because -- because Meacham Air Field has existed for a long time. Love Field existed for a long time, and I was surprised Mineral Wells I can go back and get data from the Forties.

I didn't mine the data, but I know it exists.

MR. QUINLAN As far as the analysis goes, you know, I employed the hourly data and run some -- some programs on the hourly data to find the maximum two-hour period which I don't -- didn't want to get into, but --

CHAIR STETKAR: I've done that, too. That's the most convenient data set that you could download to run those programs.

MR. QUINLAN Yes.

CHAIR STETKAR: Fine. I'm asking about confidence not only based on historical data, but projecting out over the next 70 years or so how close we're going to come to the margins on this plant.

MR. QUINLAN Well --

CHAIR STETKAR: And if we're well-away from the margins I can understand using convenience.

MR. QUINLAN Yes.

CHAIR STETKAR: If we're not so far away from the -- from the design, it seems that it would require a little bit more effort.

MR. QUINLAN Well, I think -- I didn't, you know, write the guidance or the DCD. But I think, as far as a hundred-year return period goes, it represents a --

CHAIR STETKAR: Hundred years being three times longer than 30.

MR. QUINLAN Yes, but it --

CHAIR STETKAR: Okay.

MR. QUINLAN Well, it represents a one percent chance of this being exceeded in any given year.

CHAIR STETKAR: Yes.

MR. QUINLAN So, over the life, you know, say, even a 40-year life of the plant you could expect --

CHAIR STETKAR: Let's say a 60-year.

MR. QUINLAN Okay. Then you could reasonably expect --

CHAIR STETKAR: Sixty percent probability that this will --

MR. QUINLAN That there will be better exceeded over the --

CHAIR STETKAR: Better than even?

MR. QUINLAN Yes. So, I don't think the -- at least in this case, the hundred-year return period is meant to bound something that has almost no chance of happening, something like a tenth to the seventh probability of happening.

CHAIR STETKAR: What would you do if you went back -- and I'm not saying that it existed. When you went back and mined those data sets and you found two events in the last 70 years where the temperature was 120 degrees, what would you do?

MR. QUINLAN Well, it's happened in some of the other applications that we received.

CHAIR STETKAR: Two events in 70 years is one in 35 years, which is a lot more than a hundred-year event. So, it's not even a hundred-year event. You'd expect it to occur once in a 30-year plant life.

MR. QUINLAN Well, in that case, I would

expect that our analysis would show a greater than -- well, I mean, at least 120-degree temperature for the hundred-year return period which, at that point I would have sent an RAI to the applicant, asking them to --

CHAIR STETKAR: Well, you didn't go back and look for that, did you?

MR. QUINLAN I -- I don't want to say hundred percent certainty. I know I downloaded other data sets.

CHAIR STETKAR: Okay.

MR. QUINLAN And I found Dallas/Fort Worth to be -- to provide the -- not only the ones that are most likely to recur at the site or the most representative, but I think it also provided the -- the most conservative estimates.

CHAIR STETKAR: When I looked at the local meteorology data, the site, FSAR seems to say Mineral Wells seems to track it a lot better than DFW.

MR. QUINLAN I don't know that I downloaded --

CHAIR STETKAR: It seems to be a little further away. I don't know why that is, but they seem to focus on Mineral Wells rather than these DFW for a few things.

MR. QUINLAN Yes.

CHAIR STETKAR: Anyway, I've raised the point enough. I'm just troubled by some of these things, especially when the data exists. I understand if you're limited for -- you know, you're out in the middle of nowhere and there hasn't been a station anywhere within 50 miles for any time.

I understand that. But -- but in cases where you have the data, I just don't understand why you don't use it, and I've belabored that point too long, so I'll just stop that there.

Let me ask you about tornados. The applicant provided a table of tornado experience. It's in Table 2.3-209 where they actually list tornados in a -- I think it was a five-county -- I could be wrong about that.

MR. QUINLAN No, area --

CHAIR STETKAR: Area. 3,414 square miles. And they -- they presumed a .21 square mile average tornado footprint which, you know, you can do that.

And they just estimated an overall tornado strike frequency of 1.7 times ten to the minus four.

MR. QUINLAN Yes.

CHAIR STETKAR: That's for any intensity tornado. It's just, you know, that gives you a sense of -- of the tornado frequency.

They then went back and, as I gather, in response to an RAI, did the analysis -- redid the analyses according to the methodology in NUREG/CR-4461, and determined that the site characteristics for tornados are acceptable because, according to that analysis the frequency of tornados with wind speeds that exceed 95th percentile confidence level of 217 miles per hour is less than ten to the minus seven per year.

Okay. That's -- that's one way to do things. I did it a little different way. Now, we're going to get into enhanced Fujita versus Fujita intensities and uncertainties about wind speeds, and that -- we could take up a lot of time talking about that.

But again, in the sense of my confidence to design margins, I don't want to get into the fine structure, that fine structure detail.

In -- in the applicant's table, they also give Fujita intensities for each of the tornados, and I'm assuming that's on the old Fujita scale because the data were compiled from 1950 to 2006.

And there was one F-4 tornado in that area. And, if I take their methodology of just saying an F-4 tornado has .21 square mile footprint which is -- which is actually optimistic because the big tornados have big footprints. So, that's probably optimistic.

But if I just move that tornado around in their 3414 square miles and look at the exposure period, I get about a ten to the minus six strike frequency, about an order of magnitude higher.

MR. QUINLAN Okay.

CHAIR STETKAR: And in old Fujita, you know, terminology an F-4 was 207 to 260 miles per hour, with an average of 233, which is -- let's just say close to their design value of 230.

So, my question is, now, from that sort of perspective, how do I have confidence that this particular site meets the design tornado wind speed?

MR. QUINLAN Well, I think it's important to keep in mind that the enhanced Fujita scale, which is what our newest regulatory guidance is based off of, dramatically reduced tornado wind speeds.

The old Fujita scale overestimated the maximum -- maximum wind speeds in a tornado, so I went with the new revision to Reg Guide -- to the Reg Guide came out, then, you know, it brought all of the wind speeds down.

So, I don't know that the -- relying on wind speeds for tornados that occurred a long time ago, you know, with the old Fujita scale really applies anymore.

CHAIR STETKAR: Well, I guess I don't know why it doesn't. So, what -- my concern here is we're talking about really small numbers of really severe events.

We've learned that we need to be careful about really small numbers for really severe events. Mother Nature has taught us that sometimes we don't understand those really small numbers.

And, from my perspective, given this evidence, why aren't we at least performing a more sophisticated analysis tornado strikes for this site than kind of the stylized analysis in the NUREG, or even the simplistic analysis that I just did, which was just moving a -- you know, moving a footprint around in an area.

MR. QUINLAN Sure. Well, I don't --

CHAIR STETKAR: You know, why do -- why do we have confidence that the frequency of a tornado that challenges that nominal 230 miles per hour is -- is less than ten to the minus seven per year. That's a really tiny number.

Now, I'm not saying anything about damage to the plant, even if we do get a tornado, that it exceeds 230 miles per hour. That's a different story.

But we're just saying, nominally, tornados are not an issue here, and I -- I don't understand that confidence.

MR. QUINLAN Well, they used the -- Region I in Reg Guide 1.76 is the area for the most extreme -- extreme -- where you would expect the most extreme tornados to occur, and so that's what they based their --

CHAIR STETKAR: That's good, because they --

MR. QUINLAN -- characteristics on. Yes, exactly.

So, with that, the 230-mile-an-hour maximum wind speed, you know, was used and that's why I was saying that's based off of the -- the enhanced Fujita scale now.

So, I may not -- I may not be able to explain --

CHAIR STETKAR: There's some -- as I understand it -- you know, I'm not a meteorologist. As I understand it, there's -- there was when -- when folks transitioned to the enhanced Fujita scale a -- and you may correct me because you -- you do have the background -- kind of a negotiated scaling that was done.

So there seems to be some uncertainty about how enhanced Fujita relates to old Fujita, if you will.

MR. QUINLAN Sure. Well, the --

CHAIR STETKAR: Recognizing that, even given that, there are -- pretty uncertainty abounds in those -- in those wind speed ranges.

MR. QUINLAN Sure. Well, the enhanced Fujita scale uses a -- well, I was going to say, the enhanced Fujita scale is based off of the amount of damage that -- that they observed.

So, if there was a building that they didn't think was built to withstand 150-mile-per-hour winds and it was completely destroyed, then they can say that, necessarily the tornado was more than 150 miles an hour.

The old Fujita scale was based off of, from what I understand, an upper bound physical limit that they understood at the time, you know, because you -- it's almost impossible to get direct measurements inside of a tornado.

So I think, just as the, you know, modeling got better, maybe some observations were taken using some advanced radars now, yes, they worked with the enhanced Fujita scale and, like you said, it is a bit of a -- an estimation.

CHAIR STETKAR: It's an estimation and there's -- there must be uncertainty. I'll let you speak in a second here.

Uncertainty involved, and my problem is, because there is uncertainty and because we are talking about really small frequencies.

MEMBER SHACK But this is a stylized design basis world. I mean, you know, we -- we set up limits. You know, we think those limits are big enough to accommodate uncertainties but, you know, once you're there, you're there.

And, you know, it's like saying, you know, okay, I've set the limit here to account for uncertainties, but now that I'm close to that limit, do I really want some more, and that's just not the way we do design basis world.

I mean, you know, if we -- if we're in a different world, I'd understand your concern, but --

CHAIR STETKAR: Well, but some --

MEMBER SHACK -- in the design basis world, you know, the ten to the minus seven is a fictional number, too.

CHAIR STETKAR: That's -- but that's what I was going to say. This is -- this is --

MEMBER SHACK But, you know, it's an agreed-upon number in the Reg Guide that, you know, we -- you know, we can go back and argue over that again, but I think, you know, it's -- it's within the Reg Guide limits. It's a design basis world. It's acceptable.

MR. HARVEY: This is Brad Harvey with the Office of New Reactors. That was one in compliance that I was going to make. The Reg Guide is one acceptable method that the applicant can use, and if they meet that criteria in the Reg Guide then, legalistically, it becomes difficult for us to challenge them to go further than what we've already pointed out as -- as an acceptable approach the staff has used.

The other point I want to make, in terms of the analysis, Mr. Chairman, that you did -- and I applaud you for going to a level of detail, but you talked about a 2.1 square mile footprint.

CHAIR STETKAR: No. 4.21.

MR. HARVEY: 4.21.

CHAIR STETKAR: That's what they used. They -- they actually had some path linked information and you know how the data are. You don't get that path linked information --

MR. HARVEY: No.

CHAIR STETKAR: -- very well --

MR. HARVEY: But the point I was trying to make is that you've got the -- in a four tornado, that is theoretically the highest intensity in that tornado, but the entire footprint is not in that four. It's going to be other -- and the assumptions are, when the Reg Guide -- was it 4461, made the assumption that it wasn't all a hundred percent F-4 footprint.

CHAIR STETKAR: Yes. No.

MR. HARVEY: So, I think that would bring your strike probabilities up a little bit.

CHAIR STETKAR: Well, as I said, I was -- I was just trying to get ballpark numbers out of this, and they used a .21 based on the information they had from the -- however many tornados there were in the -- in their database. I've lost it already.

Some -- some number of tornados. A hundred -- 158 tornados, but they didn't have path links for nearly all of those. They just took a limited -- they just added them up and divided by n and said, well, it's .21, and applied that to -- whether it was an F-1 or an F-4 or anything.

So, it's -- there's a lot of uncertainty in that, obviously, also, not even getting into the distribution of the -- of the peak wind speed over the -- you know, the cross-section of the tornado.

My point here is not to try to get into details of the calculation. My point is trying to probe and see how much analysis should be done to develop a

-- a level of confidence in margins.

For example, I looked at the probable maximum precipitation. I don't understand what a hundred-year probable maximum precipitation is, but I looked at all of those estimates, and the margins are so large -- you didn't hear me asking about those absolute values.

I was asking about temperature because there's a data point. I was asking about tornados because it's not clear to me.

I didn't ask about hurricanes even because, although the stylized 61 miles per hour, there's still a lot of margin there. But in areas where --

MR. HARVEY: Well, would you -- a hurricane and a tornado, there's no question which winds at this site.

CHAIR STETKAR: No, that's right. There's absolutely no question, but even in the sense of hurricanes -- but my point is, in places where we do a simple stylized -- we can call it a design basis analysis or a stylized analysis, and it indicates that we -- we might not have a very large margin, there doesn't seem to be any emphasis of going beyond that and saying can we -- do we need to fine-tune it a little bit. It's just a -- a pass/fail.

And I understand one of the philosophies of it's a design basis is the design basis is the design basis, but --

MR. HARVEY: Well, you know, I mean, we could do a best estimate with uncertainties and, you know, you get very different answers when you do that and it's a different approach.

We've decided that both are acceptable and, you know, but to somehow ask to do the design basis plus the uncertainty analysis is -- you know, that's -- it's sort of a mix and match kind of thing and --

Now, you might have a better argument for arguing if the ten to the minus six wind speed is 191 miles an hour, did we suddenly see the hundred -- the ten to the minus six tornado.

CHAIR STETKAR: Well, that's another way of looking at it.

MEMBER SHACK That's another way of looking at it.

CHAIR STETKAR: But there is some chance that we have.

MR. HARVEY: Yes, there is. There is.

CHAIR STETKAR: I mean, there is --

MR. HARVEY: I mean, you know, there's some chance that we have -- you know, I'd be more sympathetic if you argued that there was something wrong with the way we came up with the design basis than I am, you know, once we make the argument that, you know, we've got the design basis, and now we -- now we did a let, but --

CHAIR STETKAR: I -- I just sort of raised the issue. I -- I -- in those two particular areas, temperature, where you might gain more confidence looking at a broader set of meteorological data, and -- and tornados where, depending on different ways of doing the analysis, you might have different conclusions about a ten to the minus seven exceedance frequency for a 230-mile-per-hour design basis wind speed.

I'll just raise it and leave it there. I -- I personally feel uncomfortable. Bill doesn't, obviously, you know, and in the subcommittee meetings all you're hearing is feedback from individual members of the subcommittee which, you know is not an ACRS opinion. So I'll just leave it there.

Anything else on meteorology from anyone else who likes rainfall and wind speeds and all that stuff?

(No response.)

CHAIR STETKAR: Okay.

MR. QUINLAN I only have a little bit more.

CHAIR STETKAR: Good.

MR. QUINLAN Yes, so we're on 2.3.3. US-APWR COL Information Item 2.3.1 states the applicant should describe site-specific on-site meteorological measurements program. Section 2.3.3 describes a review of this program. That addresses this information item.

The staff determined the applicant adequately provided all the relevant information in FSAR Section 2.3.3. The staff verified the location of the meteorology towers representative of the site area and meets the guidance provided in Regulatory Guide 1.2.3 in Revision 1.

Next slide, please. SER Section 2.3.4 describes the review of the short-term atmospheric dispersion estimates or chi/Q values that are used to evaluate design basis accidental releases to the exclusion area boundary, the outer boundary of the low-population zone and the control room.

US-APWR COL Information Item 2.3, Part 2, states that the applicant should provide site-specific short-term atmospheric dispersion estimates.

Using NRC-approved computer models, the applicant provided this information and staff has accepted it as correct and adequate.

US-APWR COL Information Item 2.3, Part 3, states that the applicant shall provide site-specific atmospheric dispersion estimates for routine releases of radioactive materials to the atmosphere.

SER Section 2.3.5 describes a review of long-term atmospheric dispersion estimates that are used to evaluate releases of radiological effluence to the atmosphere during normal plant operation.

Again, using NRC-approved computer models, the applicant provided the information and the staff accepted it as correct and adequate.

Next slide. In conclusion, all the Comanche Peak site characteristics presented in FSAR Section 2.3 have been found to be acceptable and bounding -- or bounded by the corresponding US-APWR site parameters.

Section 2.3 of the Comanche Peak COL FSAR has been reviewed by the staff and been found to adhere to all regulatory requirements.

Section 2.3 of the SER has been submitted with no open items -- sorry -- one open item. No exemptions and no departures. The one open item is related to updated control room chi/Q values as part of the integrated seismic closure plan. Thank you.

CHAIR STETKAR: Great. Anything else for the staff?

(No response.)

CHAIR STETKAR: If not, thank you. It's probably more than you expected.

What I'd like to do, get the bridgeline open. We need to ask for comments.

I'll ask for any comments or questions from anyone in the room if we have any. We'll get the bridgeline open and see if anyone out there wants to add anything. It sounds like a crackle pop.

Well, if someone is out there, just please make some utterance so that we can confirm the bridgeline is open. Just say something. Is someone trying to speak?

Honestly, if someone said something I -- we -- it sounded like something was coming through, but it was really garbled. So, if someone's out there, could you actually try to say something again, please.

I guess not. I thought I heard something.

MEMBER SHACK Well, I think we heard a random noise.

CHAIR STETKAR: Okay.

MEMBER SHACK But, if we can't repeat it, we'll assume it was random, rather than purposeful.

CHAIR STETKAR: So, hearing no comments, I would like to thank the staff and Luminant for a good presentation. I think we have some things to follow up in other chapters of -- of the FSAR 3 and 6, in particular.

And let me do what we always do. Joy, any final comments?

MEMBER REMPE: No.

CHAIR STETKAR: Charlie?

MEMBER BROWN: Negative.

CHAIR STETKAR: Bill?

MEMBER SHACK No.

CHAIR STETKAR: I don't have anything, and occasionally miracles do happen. We are adjourned. Oh. On time.

(Whereupon, the meeting was concluded at 11:44 a.m.)

US-APWR Chapter 7

Presentation for ACRS

April 25-26, 2013

Mitsubishi Heavy Industries, Ltd.

Contents

1. Introduction

Topics

- ✓ Topical/Technical Reports
- ✓ I&C Systems
- ✓ Main Control Room Layout
- ✓ System Architecture
- ✓ Data Flow to External Networks

1. Introduction

Topical / Technical Reports

<table>
<tr><th rowspan="2">DCD</th><th colspan="4">Design Bases, Requirement & Description</th><th rowspan="2">Analysis, Evaluation & Methodology, etc.</th></tr>
<tr><th>I&C System</th><th>HSI System</th><th>Hardware Basic Software</th><th>Application Software</th></tr>
<tr><td>7.1</td><td rowspan="7">MUAP-07004</td><td>MUAP-07007</td><td rowspan="3">MUAP-07005</td><td>MUAP-07017</td><td>MUAP-07030 & 08015</td></tr>
<tr><td>7.2</td><td>-</td><td>-</td><td>MUAP-09022 & 11014</td></tr>
<tr><td>7.3</td><td>-</td><td>-</td><td>MUAP-09020 & 09022</td></tr>
<tr><td>7.4</td><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>7.5</td><td>MUAP-07007</td><td>-</td><td>-</td><td>MUAP-07014 08015 & 09022</td></tr>
<tr><td>7.6</td><td>MUAP-07007</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>7.7</td><td>-</td><td>MUAP-07005</td><td>-</td><td>-</td></tr>
<tr><td>7.8</td><td colspan="3">MUAP-07006</td><td>-</td><td>MUAP-07014 & 09022</td></tr>
<tr><td>7.9</td><td>MUAP-07004</td><td>-</td><td>MUAP-07005</td><td>MUAP-07017</td><td>MUAP-07014 & 09021</td></tr>
</table>

- MUAP-07004: Safety I&C System Description and Design Process
- MUAP-07005: Safety System Digital Platform -MELTAC-
- MUAP-07006: Defense-in-Depth and Diversity
- MUAP-07007: HSI System Description and HFE Process
- MUAP-07014: Defense in Depth and Diversity Coping Analysis
- MUAP-07017: Software Program Manual
- MUAP-07030: US-APWR Probabilistic Risk Assessment
- MUAP-08015: US-APWR Equipment Qualification Program
- MUAP-09020: Function Assignment Analysis for Safety Logic System
- MUAP-09021: Response Time of Safety I&C System
- MUAP-09022: Instrument Setpoint Methodology
- MUAP-11014: Mitsubishi Design Bases for Over Temperature ΔT and Over Power ΔT Reactor Trip Functions

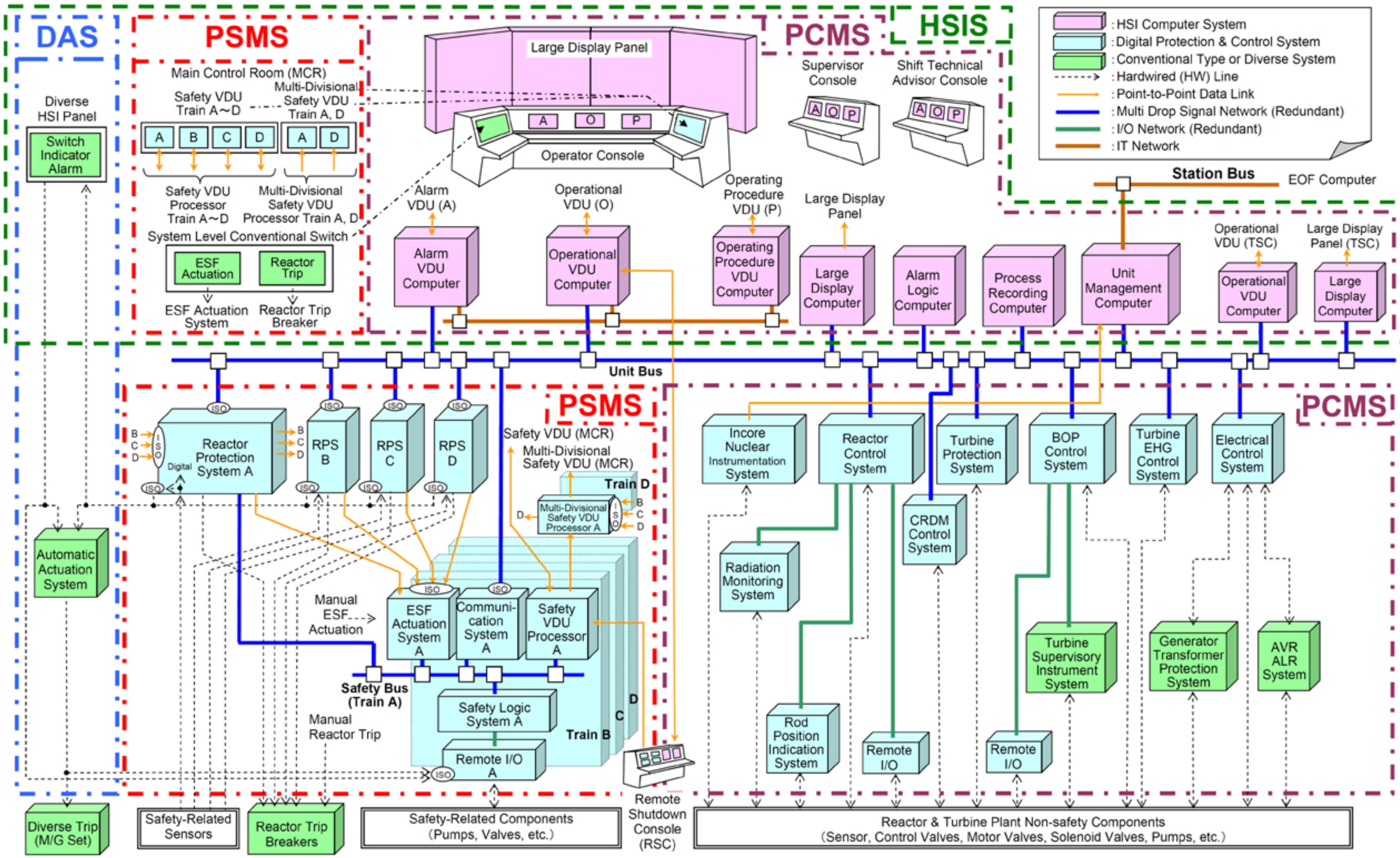
1. Introduction

I&C Systems

- **Protection and Safety Monitoring System (PSMS)**
  - ✓ Four train redundant, fully digital system for safety-related I&C
- **Plant Control and Monitoring System (PCMS)**
  - ✓ Duplex redundant, fully digital system for non-safety I&C
- **Diverse Actuation System (DAS)**
  - ✓ Analog system that is hardwired for diverse and independent control
- **Main Control Board (MCB)**
  - ✓ Consists of the large display panel (LDP), safety VDUs (S-VDUs), non-safety VDUs, and conventional switches
- **Data Communication System (DCS)**
  - ✓ Consists of multi-drop networks and point to point data links, fully redundant, self-testing

Main Control Room Layout

System Architecture



DAS : Diverse Actuation System PSMS : Protection and Safety Monitoring System HSIS : Human System Interface System PCMS : Plant Control and Monitoring System

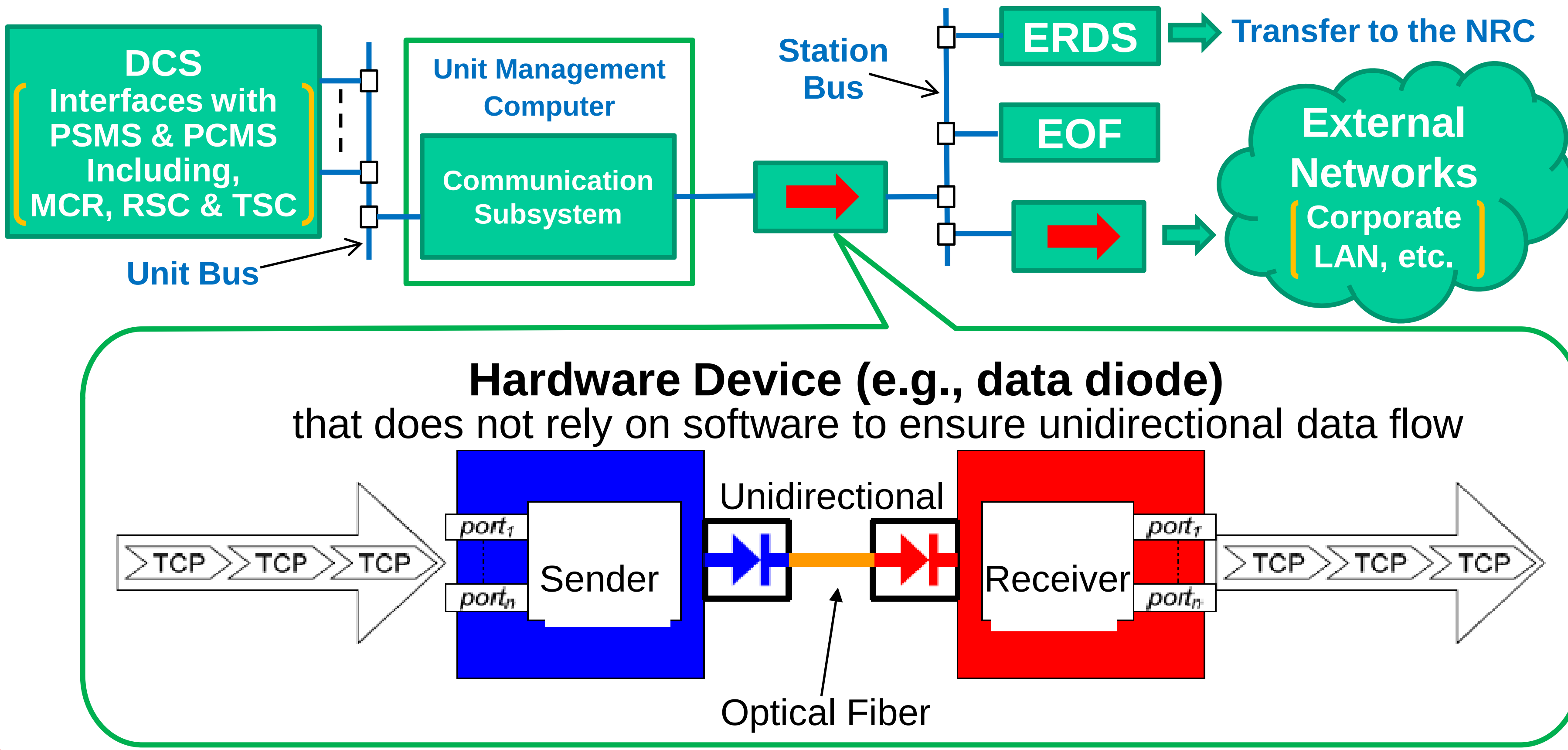
DCD Figure 7.1-1

Data Flow To External Networks (1/2)

- **DCD Section 7.9 describes:**
- **Data flow to the station bus**
  - ✓ The station bus provides information to plant and corporate personnel and to EOF and ERDS
  - ✓ The station bus receives information from DCS via the unit management computer
  - ✓ The unit management computer provides a firewalled interface, which allows only outbound communication
  - ✓ There are no other connections from external sources to DCS
- **Data flow to the external networks**
  - ✓ The only interface from the PCMS and PSMS to external networks is via the firewall within the unit management computer
  - ✓ The unit management computer provides an outbound only interface to the plant station bus to allow communication to EOF computers, the NRC (via ERDS), corporate information systems and plant personnel computers

Data Flow To External Networks (2/2)

- MHI feels it is necessary to add a hardware device (e.g., data diode) to ensure unidirectional data flow from PSMS and PCMS to the station bus and the external networks in DCD Chapter 7.9



2. Safety Related Systems

Protection and Safety Monitoring System Topics

- ✓ PSMS Scope
- ✓ Configuration of Reactor Protection System (RPS)
- ✓ Configuration of Engineered Safety Features Actuation System (ESFAS) and Safety Logic System (SLS)
- ✓ PSMS Interfaces
- ✓ PSMS Data Communication Systems
- ✓ Systems Required for Safe Shutdown
- ✓ Safety-Visual Display Unit (S-VDU)
- ✓ Interlock Systems Important to Safety
- ✓ Information Systems Important to Safety
- ✓ Reactor Trip on Turbine Trip
- ✓ Turbine Trip on Reactor Trip

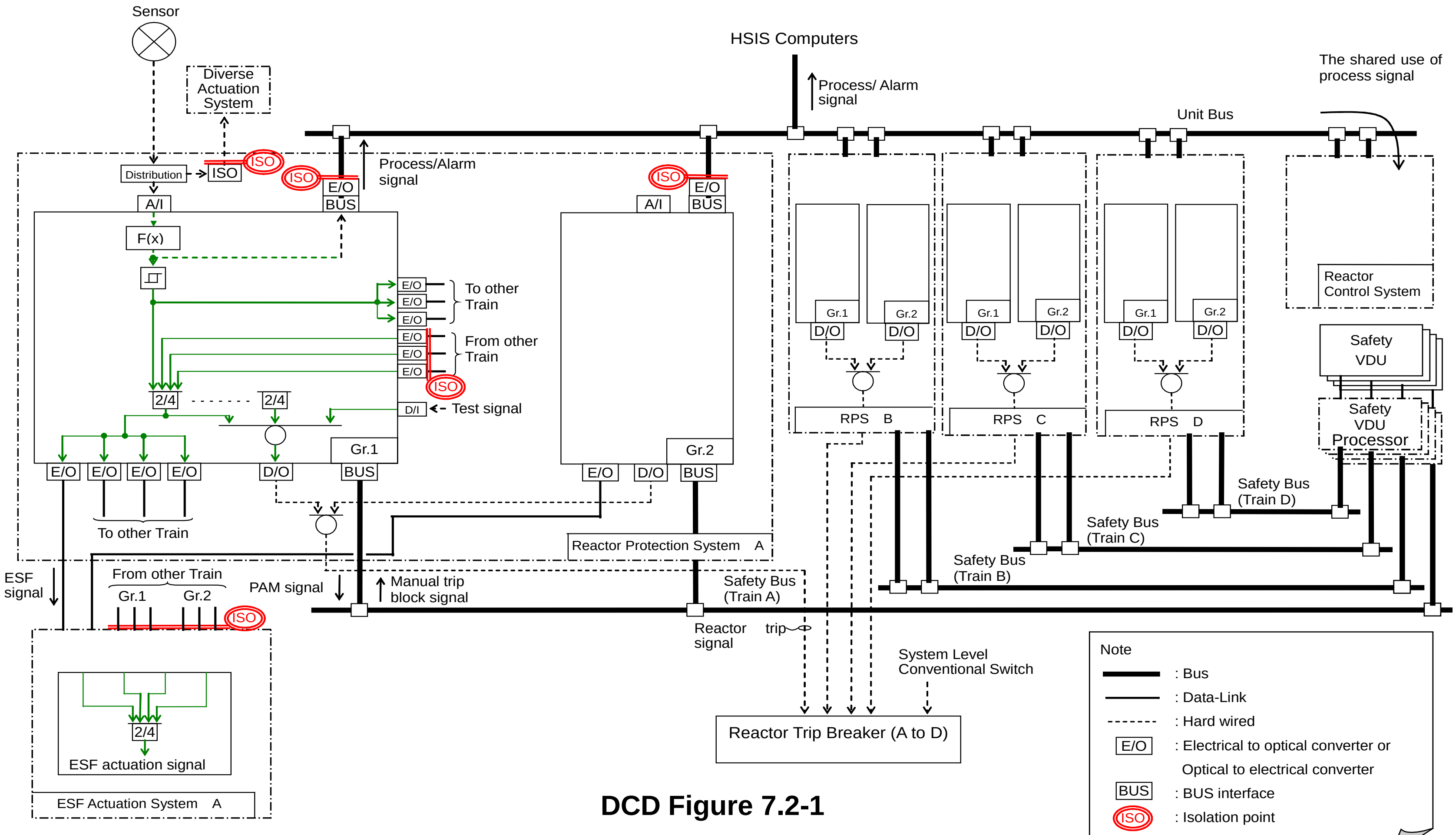
2. Safety Related Systems

PSMS Scope

- **PSMS consists of five digital subsystems:**
  1) Reactor Protection System (RPS)
  2) Engineered Safety Features Actuation System (ESFAS)
  3) Safety Logic System (SLS)
  4) Communication Subsystem (COM)
  5) Safety-related human system interface system (HSIS)
- **I&C safety functions of US-APWR are implemented using one or more of these subsystems**

Configuration of RPS

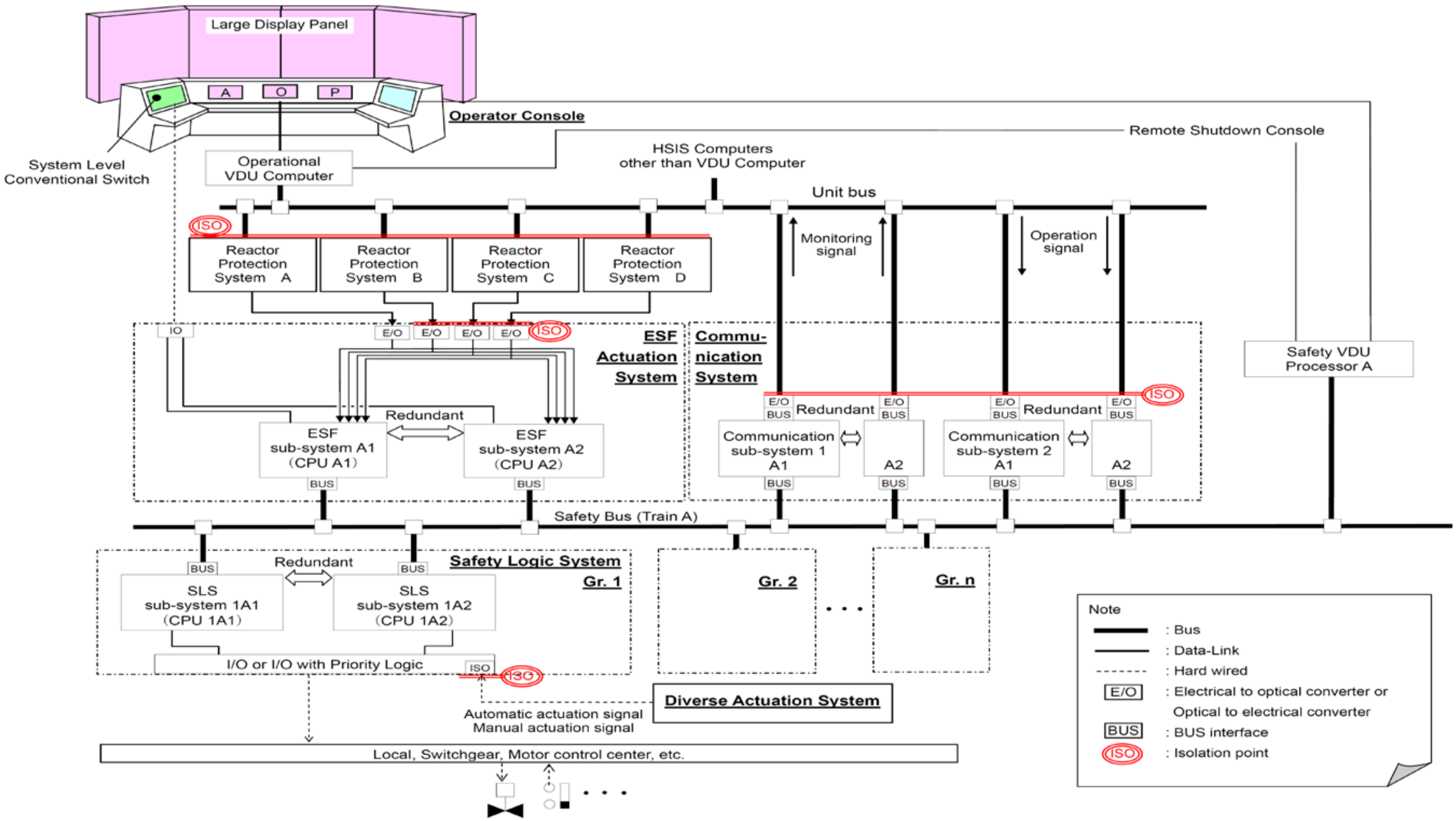
- Trip functions are distributed to 2 controllers per train to achieve functional diversity



DCD Figure 7.2-1

Configuration of ESFAS and SLS

- Redundant controllers within each train increases reliability



DCD Figure 7.3-1

2. Safety Related System

PSMS Interfaces

- **PSMS interfaces with safety sensors and actuators**
- **PSMS interfaces with the following non-safety I&C systems:**
  - ✓ Non-safety Human System Interface System (HSIS)
  - ✓ Reactor Control System
  - ✓ Turbine Protection System
  - ✓ BOP Control System
  - ✓ Diverse Actuation System
- **Interfaces with other systems do not negatively impact functions of PSMS due to PSMS independence**

PSMS Data Communication Systems (DCS)

- **There are only two types of inter-divisional data communication interface methods applied in the PSMS**
  - ✓ Point-to-point Data Link
    - Between RPS trains for partial trip
    - Between RPS and ESFAS for partial ESF actuation
    - Between multi-divisional S-VDU trains for monitoring information
  - ✓ Multi-drop Network
    - Between PSMS and non-safety systems via Unit Bus for monitoring and control information to non-safety systems,
      and manual control commands from O-VDUs
- **PSMS safety function is ensured by functional and communication independence**
  - ✓ Failure of one PSMS division does not negatively impact functions of other PSMS divisions
  - ✓ Failure of non-safety system does not negatively impact functions of any PSMS division

Systems Required for Safe Shutdown

- Normal shutdown can be achieved and maintained using Operational VDUs (O-VDUs) from MCR or RSR
- Safe Shutdown (hot and cold) can be achieved and maintained using only PSMS from MCR or RSR
- S-VDUs or O-VDUs can be used with PSMS to achieve safe shutdown from MCR or RSR
- MCR-RSR Master Transfer switches are provided for each PSMS train and PCMS
- Master Transfer switches are located on the pathway between MCR and RSR, and within RSR (2/2 actuation)

2. Safety Related Systems

Safety VDU (S-VDU)

- **S-VDU consists of S-VDU processor and S-VDU panel**
- **There are two type of S-VDUs:**
  - ✓ Single divisional S-VDU
    - Four train redundant
    - Control and monitor all safety related functions of each safety train
  - ✓ Multidivisional S-VDU
    - Two train redundant
    - S-VDU display parameters from all four trains for accident mitigation and safe shutdown
    - This S-VDU has no control capability
- **S-VDU consists of the same digital platform as PSMS and satisfies all safety criteria and requirements**

Interlock Systems Important to Safety

- **Interlocks implemented in PSMS are credited in DCD Chapter 15 to prevent accidents and to help ensure availability of safety systems**

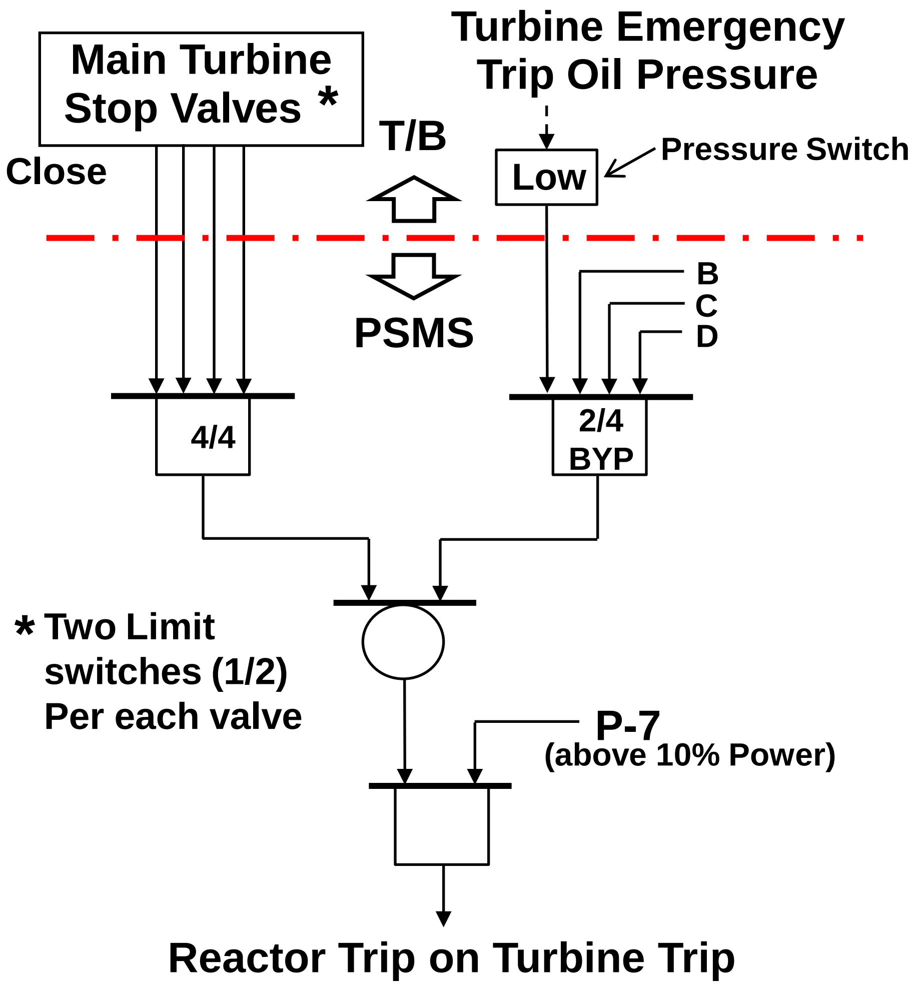
- **Interlocks important to safety are:**
  - ✓ CS/RHR Hot Leg Isolation Valve Open Permissive Interlock
  - ✓ CS/RHR Valve Open Block Interlock
  - ✓ Primary Makeup Water Line Isolation Interlock
  - ✓ Accumulator Discharge Valve Open Interlock
  - ✓ CCW Supply Line Isolation Interlock
  - ✓ RCP Thermal Barrier HX CCW Return Line Isolation Interlock
  - ✓ Low-pressure Letdown Line Isolation Interlock

2. Safety Related Systems

Information Systems Important to Safety

- **Post Accident Monitoring (PAM)**
- **There are five types of PAM parameters:**
  - ✓ Type A – credited manual actions
  - ✓ Type B – critical safety functions
  - ✓ Type C – potential breach of fission product barriers
  - ✓ Type D – performance of safety systems
  - ✓ Type E – radioactive release
- **Type A and B parameters have spatially dedicated continuously visible displays on S-VDUs and LDP**
- **Type A, B and C parameters have Class 1E power, are processed by PSMS, and are displayed on S-VDUs**
- **The performance of PAM variables, such as range, accuracy, response time, required instrumentation duration, and reliability, have been selected in accordance with Clause 5 of IEEE 497-2002**
- **The selection basis for PAM variables to demonstrate complete accident coverage is an Open Item**

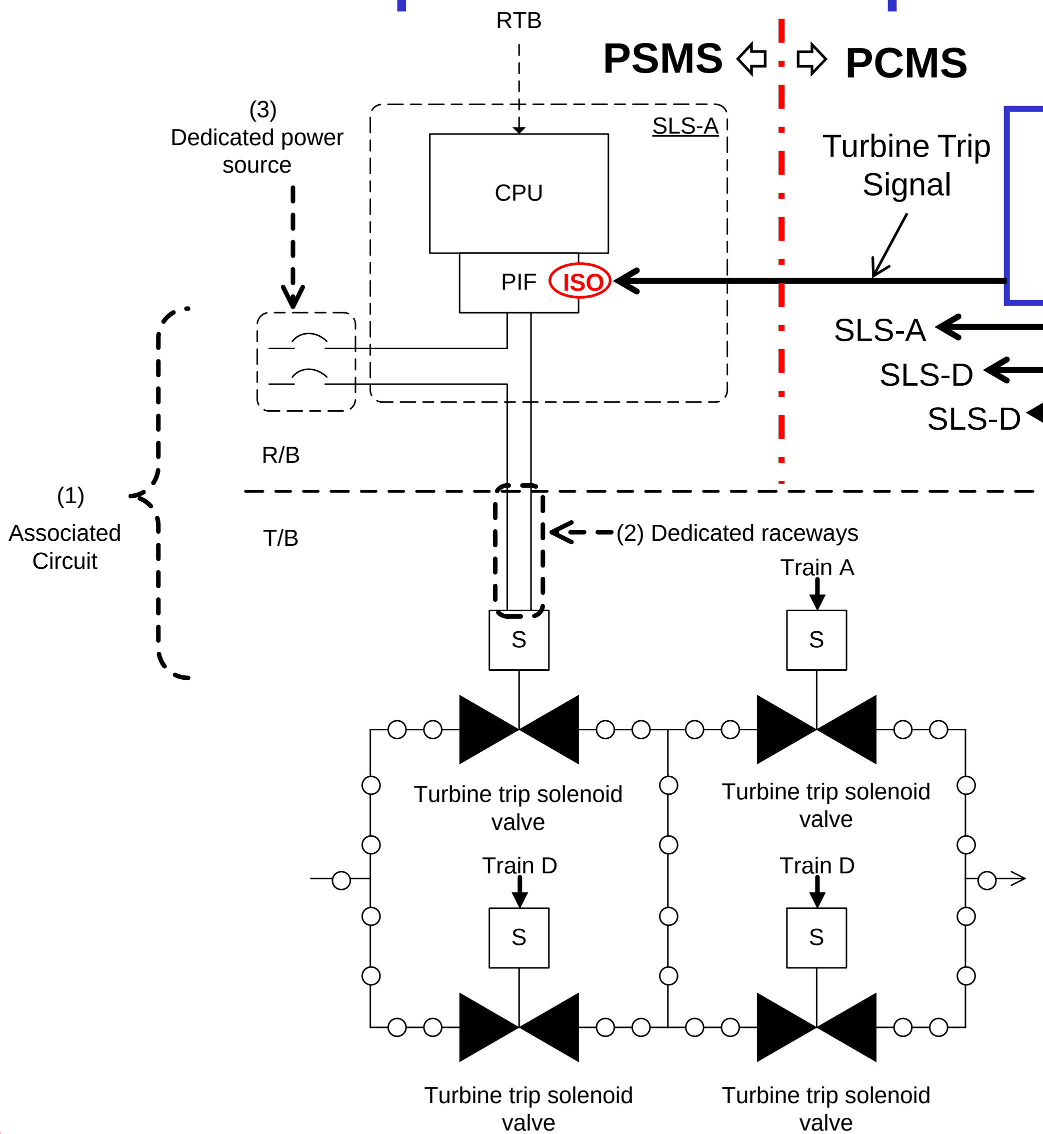
Reactor Trip on Turbine Trip



- Anticipatory trip functions, and not credited in DCD Chapter 15 analysis
- Cannot be Class 1E due to non-safety turbine and non-seismic turbine building location, but designed to be highly reliable:
  - ✓ Seismically and environmentally qualified sensors
  - ✓ Powered from Class 1E sources
  - ✓ Diverse and redundant sensors
  - ✓ Separation of sensors and cables
  - ✓ Both RT functions are maintained by Tech Spec., including periodic surveillance tests

2. Safety Related Systems

Turbine Trip on Reactor Trip



- Turbine Trip Signal from PSMS and Turbine Protection System are combined (1-out-of-2 logic) in hardwired portions of PIF module
- Turbine Protections System is a dedicated system, consists of four redundant digital sub-systems
- Turbine Control System is a dedicated system, consists of duplex redundant digital sub-systems
- Independent sensors, including speed sensors, are used for Turbine Protections System and Turbine Control System

3. Non Safety Systems

Plant Control and Monitoring System Topics

- ✓ Plant Control System
- ✓ Shared Sensors
- ✓ Alarms for Credited Manual Actions
- ✓ Non-Safety Data Communication Systems (DCS)
- ✓ Information Systems
- ✓ Operational Visual Display Unit (O-VDU)
- ✓ Turbine Bypass Valves Interlock

3. Non Safety Systems

Plant Control Systems

- Non-safety systems are controlled by PCMS
- Control functions are distributed to multiple PCMS controller groups to ensure transients due to spurious signals from one control group are bounded in DCD Chapter 15 AOOs analysis
- Controller redundancy and distributed functions to multiple control groups minimize the potential for single or complete control function failure
- Input and Output (I/O) redundancy applied to components (e.g., I/O for feedwater regulation valves) that could cause plant trip
- Spurious actuations cause by PCMS failures, including software design defects, are being examined for plant affects as an Open Item

3. Non Safety Systems

Shared Sensors

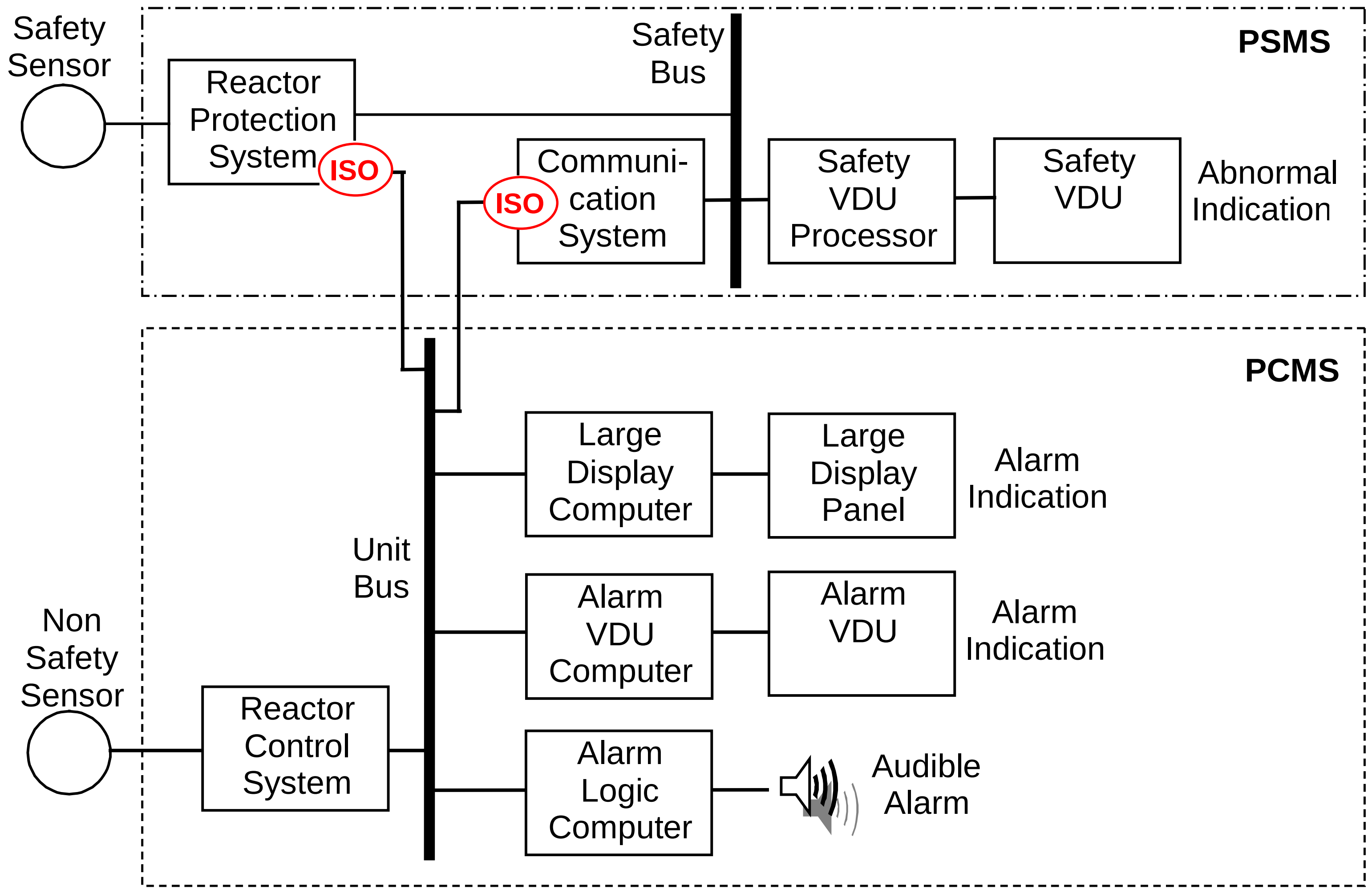
- PCMS shares sensors with RPS for many control functions
  - ✓ Sensor sharing reduces pressure boundary penetrations and local maintenance work in accordance with ALARA
- PCMS avoids adverse control/protection interaction by using multiple redundant sensors and the Signal Selection Algorithm (SSA)
  - ✓ SSA selects 2nd highest of 3 or 4 sensors
- Sensor failure does not cause adverse control system actions while PSMS is in a degraded state from that same sensor failure (IEEE-603)
- Augmented quality has been applied to SSA

3. Non Safety Systems

Alarms for Credited Manual Actions (1/2)

- **In accordance with SECY-93-087, the reliability of alarms to prompt manual actions credited in the safety analysis is assured by the following design features:**
  - ✓ Redundancy is provided for all HSI alarm components
  - ✓ Separation between redundant segments is provided
  - ✓ Testability is provided from self-diagnosis of PSMS, PCMS and HSI computers
  - ✓ Alarm functions have Augmented Quality
  - ✓ In addition to alarms, abnormal indications for credited manual operator actions are provided on safety VDUs

Alarms for Credited Manual Actions (2/2)



Non-safety Data Communication Systems (DCS)

- **DCS is non-safety and consists of the plant-wide Unit Bus and Station Bus**
- **Unit Bus interfaces with all I&C systems of US-APWR including information and controls for MCR, RSR, and TSC**
- **Unit Bus interfaces with Station Bus, which is an information technology network via the unit management computer**
- **Station Bus is the plant's information technology network, provides information to NRC via ERDS, to EOF and to plant personnel, it contains systems such as:**
  - ✓ Work order management
  - ✓ Personnel management
  - ✓ Long term data archiving

3. Non Safety Systems

Information Systems

- **Non safety information systems include safety parameter display system and bypassed and inoperable status indication**
  - ✓ Safety parameter display system (SPDS)
    - Key parameters for critical safety functions and dynamic safety function status trees (per EOPs)
    - Key parameters for performance of normal and emergency systems used to maintain/restore critical safety functions
  - ✓ Bypassed and inoperable status Indication (BISI)
    - Availability status of emergency systems for all critical safety functions
- **Displayed in MCR, RSR, TSC, and EOF**

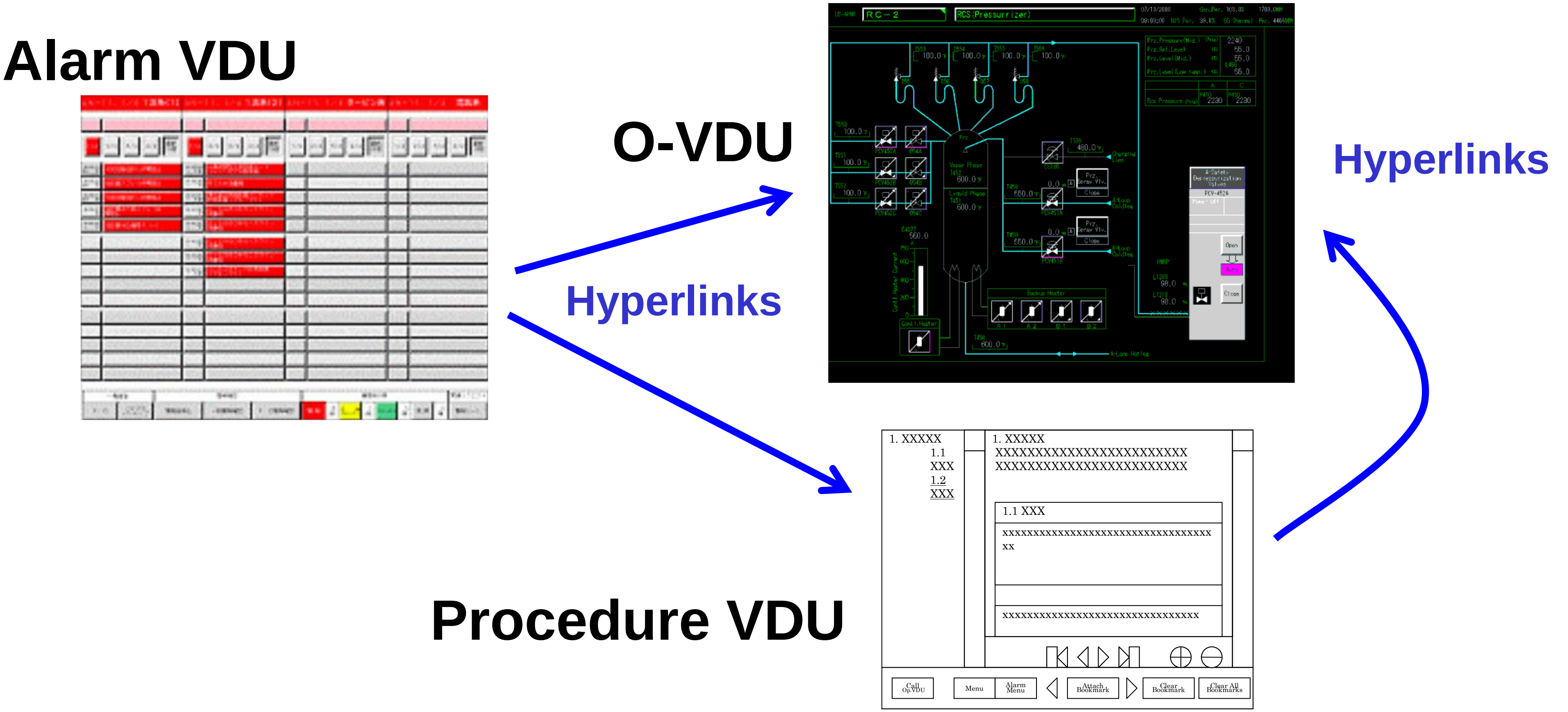
3. Non Safety Systems

Operational VDU (O-VDU) (1/3)

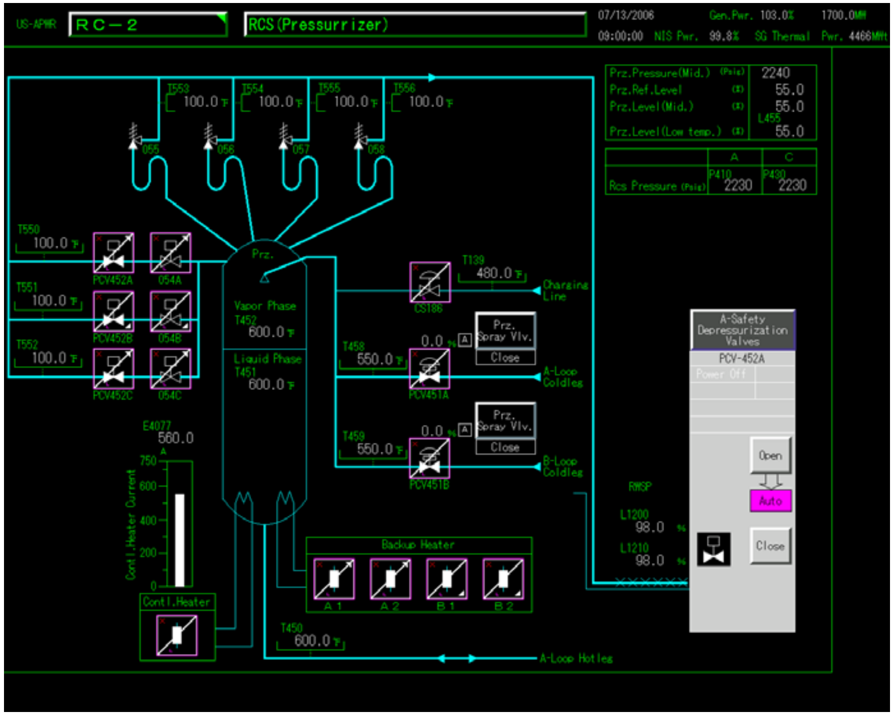
- **Non-safety components and safety components in all divisions, can be operated from non-safety O-VDUs**
- **PSMS protects itself from any adverse interaction from O-VDUs based on compliance with IEEE 603 independence criteria**
  - ✓ Physical and Electrical independence
  - ✓ Communication independence
  - ✓ Functional independence (priority for all safety functions, including S-VDUs)
- **O-VDUs enhance plant safety by**
  - ✓ Reducing operator task burden resulting in:
    - Reduced time for operator actions, improved margin to safety
    - More mental resources available for plant-wide situation awareness
  - ✓ Reducing potential for human performance errors
- **Safety enhancements have been validated through full scope simulator testing using 13 crews of US SROs and ROs**

O-VDU (Hyperlink Design) (2/3)

- Hyperlinks among the non-safety HSIs reduce operator task burden, potential for human errors, and time required for safety action responses



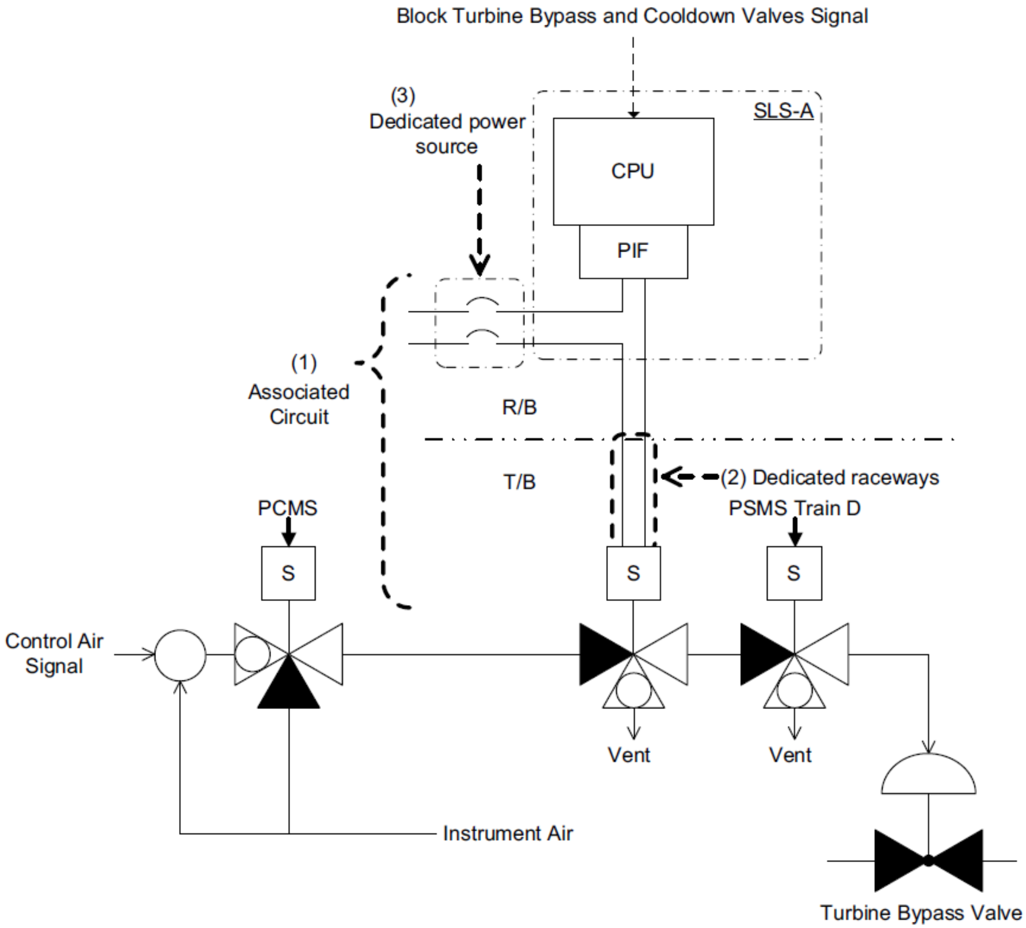
O-VDU (Graphical User Interface GUI） (3/3)



- GUI reduces mental processing time for both monitoring and control actions
- GUI reduce the potential for operator selecting the wrong component
- Using the same screen, allows a single operator to coordinate safety and non-safety success paths more easily than two operators at separate interfaces

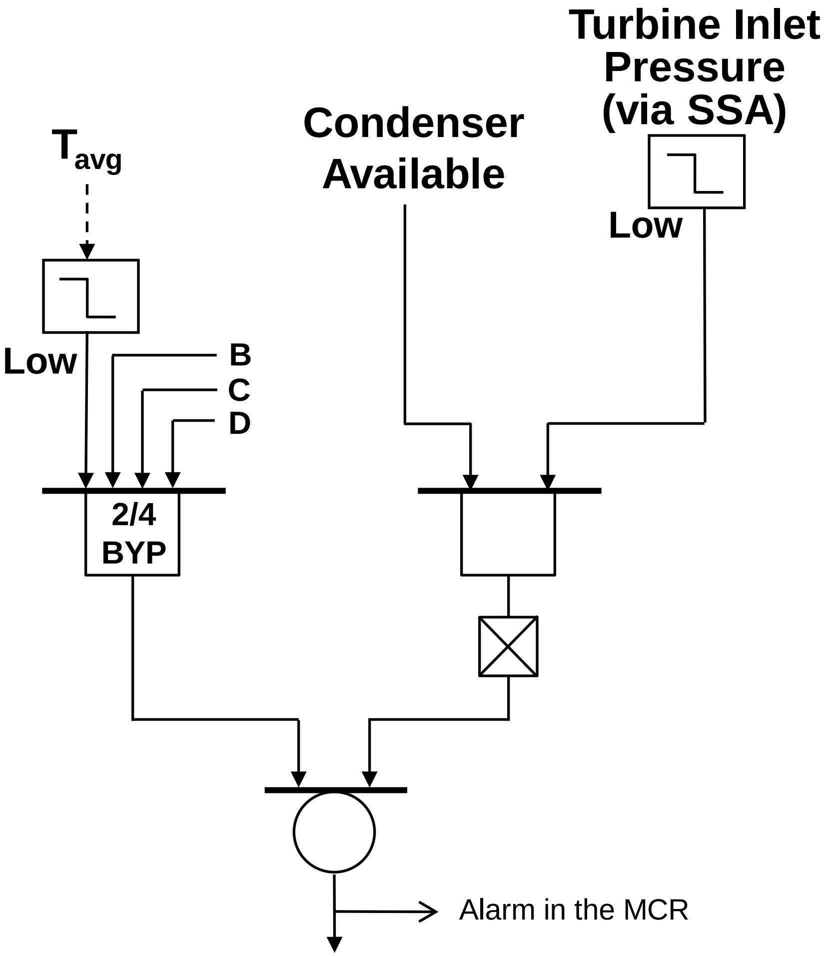
- Safety is enhanced when time for operator action is reduced, potential for errors is reduced, and tasks are simplified
- MHI is in the process of quantitatively evaluating the safety advantages of O-VDU use in response to an Open Item

Turbine Bypass Valves Interlock (1/2)



- Erroneous Turbine Bypass Control signals are prevented by the PSMS which controls redundant non-Class 1E permissive solenoids from SLS trains A and D
- Turbine Bypass Control function output signals are provided by the reactor control system in PCMS to I/P converters and trip open solenoids

Turbine Bypass Valves Interlock (2/2)



Block Turbine Bypass Valve Signal

- **Block Turbine Bypass Valve signal is generated under the following conditions:**
  a. 2-out-of-4 RCS loops indicate low-low T_{avg}
  b. Turbine inlet pressure via SSA does not indicate the rate of decrease in the turbine load
  c. Condenser is not available
- **At hot full power, condition b is established, and Block Turbine Bypass Valve signals are generated in PSMS trains A and D**

4. Diverse I&C Systems

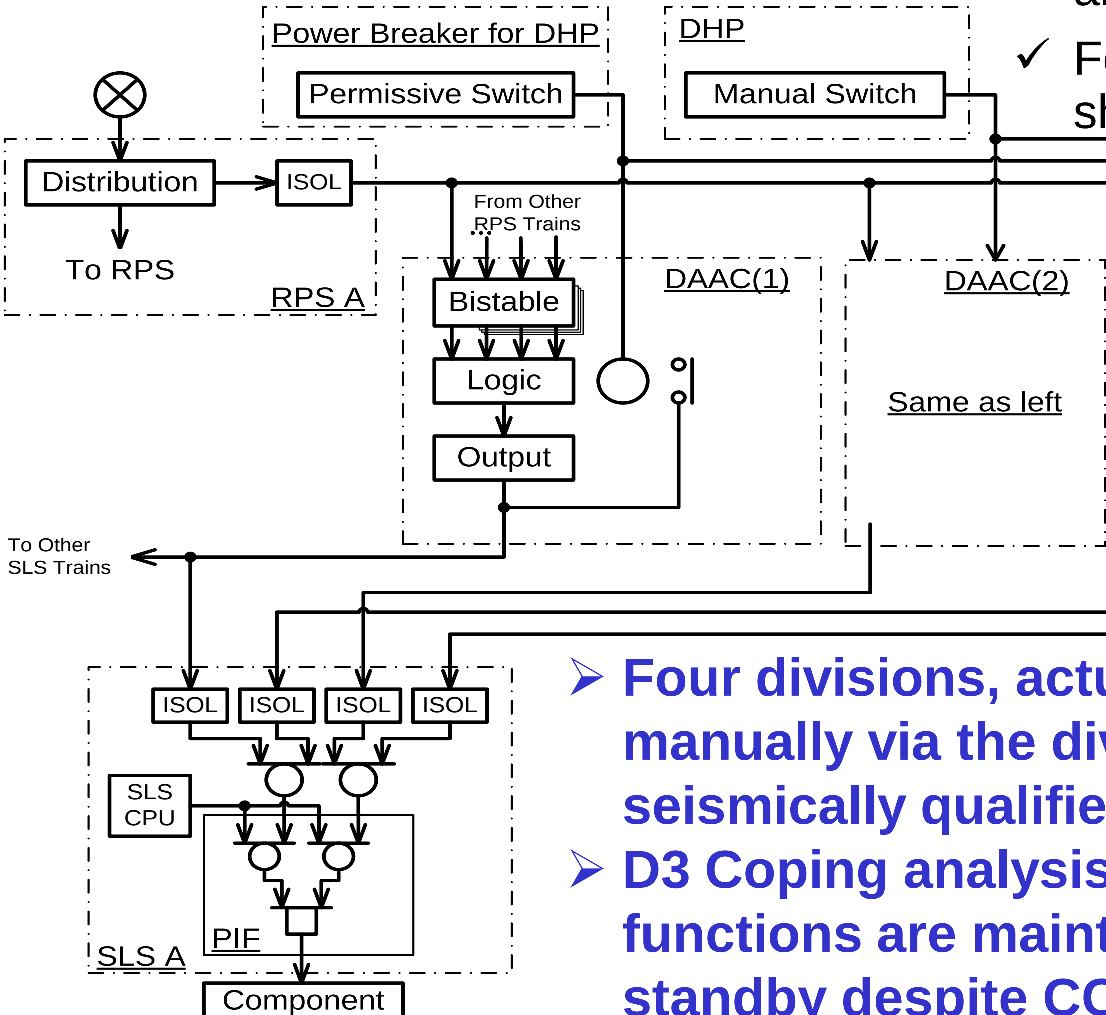
Diverse Actuation Systems Topics

- ✓ Basic Architecture
- ✓ DAS Function
- ✓ Actuated Components
- ✓ Monitored Variables
- ✓ Diverse RT and ESF Actuation Signal Selection
- ✓ D3 Coping Analysis
- ✓ Augmented Quality

4. Diverse I&C Systems

Basic Architecture

- ✓ For RT DAS trips MG-Set and PSMS trips RTB
- ✓ For ESF DAS and PSMS share PIF

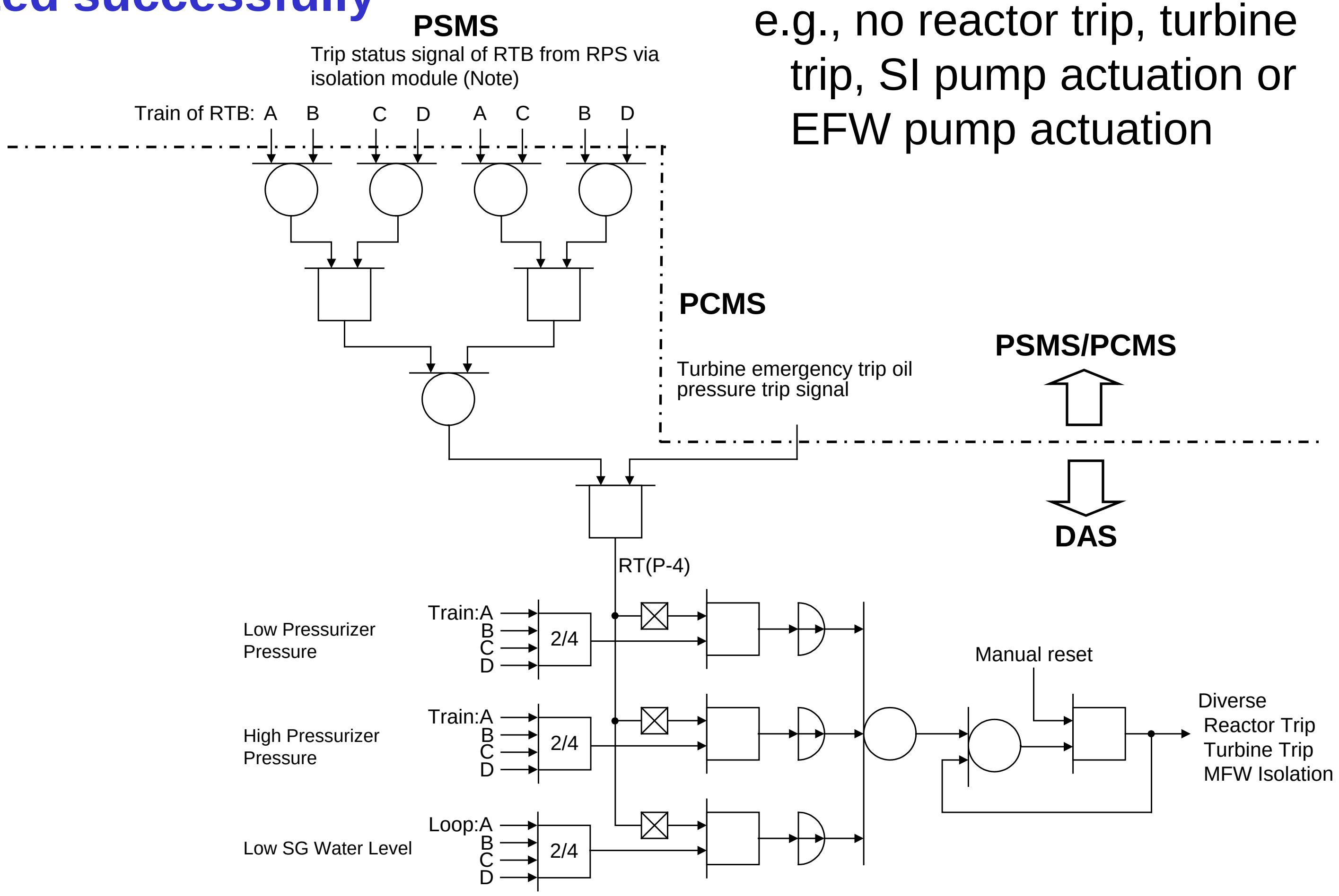


- Four divisions, actuated automatically or manually via the diverse HSI panel, and is seismically qualified
- D3 Coping analysis shows critical safety functions are maintained to achieve hot standby despite CCF, with concurrent accident, fire, flood or seismic events

DAS Function

- Actuated if accident is detected and safety components are not actuated successfully

e.g., no reactor trip, turbine trip, SI pump actuation or EFW pump actuation



Note: Actuation status signal (aux. contact etc.) via hardware of the PSMS

Actuated Components

Safety Function or Associated Components	Actuation Type
Diverse Reactor Trip (Motor-Generator Set Trip)	Automatic/Manual (MCR)
Turbine Trip	Automatic/Manual (MCR)
EFW Pump	Automatic/Manual (MCR)
Safety Injection Pump	Automatic/Manual (MCR)
Safety Depressurization Valve	Manual (MCR)
Main Steam Depressurization Valve	Manual (MCR)
SG Blowdown Isolation Valve	Automatic/Manual (MCR)
MFW Regulation Valve (Close)	Automatic/Manual (MCR)
EFW Control Valve	Manual (MCR)
Containment Isolation Valves	Manual (MCR)
Main Steam Line Isolation Valve	Manual (MCR)

Sourced from DCD Table 7.8-5

Monitored Variables

Critical Safety Function	Variables	Number of Channel
Reactivity Control	Wide Range Neutron Flux	1
RCS Integrity	Pressurizer Pressure *	1
	Reactor Coolant Pressure	1
Core Heat Removal	Reactor Coolant Cold Leg Temperature	1 per Loop
RCS Inventory Control	Pressurizer Water Level	1
Secondary Heat Sink	SG Water Level *	1 per SG
	Main Steam Line Pressure	1 per SG
Containment Integrity	Containment Pressure	1

* These variables are used for automatic actuation functions

DCD Table 7.8-2

Diverse RT and ESF Actuation Signal Selection

- **DAS has three automatic diverse RT and ESF actuation signals:**
  - ✓ High pressurizer pressure
  - ✓ Low pressurizer pressure
  - ✓ Low steam generator water level
- **These signals were selected to be the minimum set required to mitigate occurrence of a Chapter 15 AOO or PA concurrent with a CCF**
- **Adequacy of these three DAS RT and ESF actuation signals is demonstrated by D3 coping analysis**

D3 Coping Analysis

- **Demonstrates pressure boundary integrity, core coolability, and offsite dose limits for Chapter 15 events with concurrent CCF**
- **Analysis considers partial actuation and failure to actuate with false indications**
  - ✓ Partial Actuation
    - AOO and PA analyzed with failure of PSMS and PCMS, failure of only PSMS
    - The only failure of concern is a partial failure that blocks DAS, this could occur due to:
      - Conflicting Commands - Mitigated by PIF state based priority logic
      - Erroneous Blocking Signals – Mitigated by blocking signals hardwired from actuated plant components, not PSMS
      - Erroneous actuation of components not monitored by DAS – Mitigated by normally open valves in series with pumps monitored by DAS, and abnormal valve position alarms
  - ✓ Failure to actuate with false indication that actuation has occurred
    - Analysis demonstrates this would require CCF of multiple software blocks which is beyond the scope of BTP 7-19
- **MHI is justifying the inputs and assumptions of D3 Coping Analysis in response to an Open Item**

4. Diverse I&C Systems

Augmented Quality

- **DAS is an augmented quality, non-safety system, as defined by Generic Letter 85-06 and described in Subsection 7.1.3.20**
- **Attributes of the augmented quality program of DAS are:**
  - ✓ Designed using a nuclear quality program that meets the US-APWR QAP descriptions and the guidance of GL 85-06
  - ✓ Uses components with a history of successful operation
  - ✓ Uses components commonly used in conventional non-digital safety systems
  - ✓ Design process includes an independent review
  - ✓ Seismic testing method is equivalent to that for seismic category I

5. Safety Criteria Conformance

Essential Safety Criteria

- ✓ Overview
- ✓ Redundancy
- ✓ Independence
  - Physical, Electrical, Communication, Functional
- ✓ Determinism
- ✓ Diversity
  - Software, Functional
- ✓ Simplicity
- ✓ Testability
- ✓ Reliability
- ✓ Quality
- ✓ Equipment Qualification
- ✓ Secure Development & Operational Environment (SDOE)

5. Safety Criteria Conformance

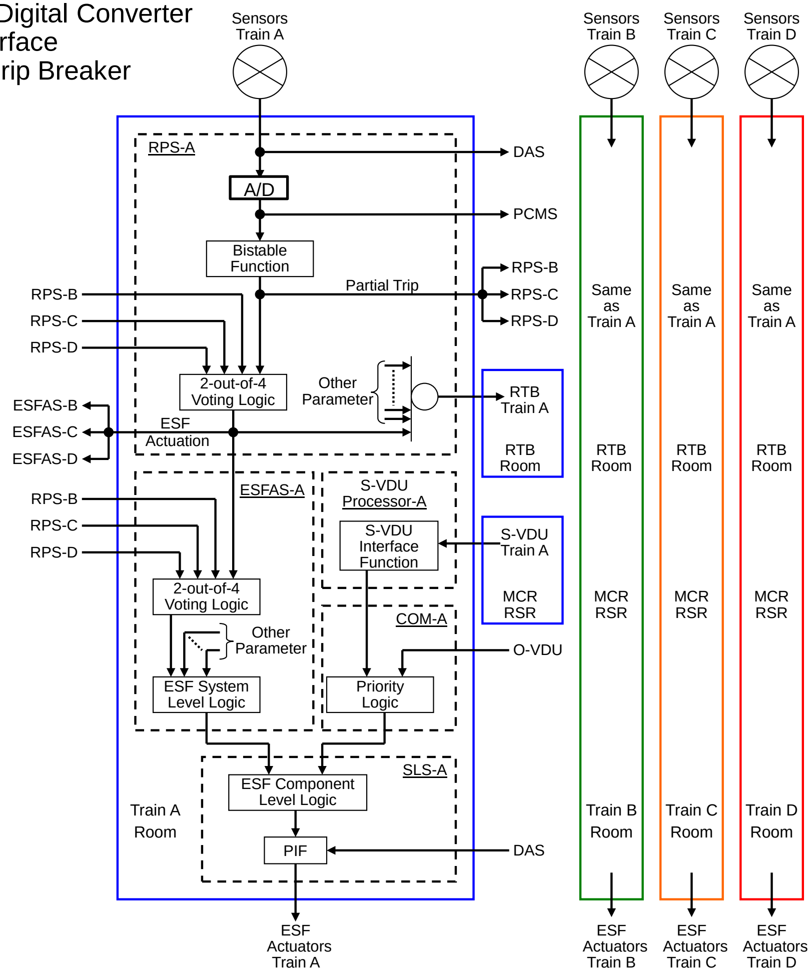
Overview

- DCD and related I&C reports demonstrate PSMS design conformance to essential safety criteria
- Overall conformance to the essential safety criteria is described in DCD Chapter 7 Section 7.1.4
- Detailed conformance is described in “Safety I&C System Description and Design Process,” MUAP-07004
  - ✓ Section 3.0 “Applicable Code, Standards and Regulatory Guidance”
  - ✓ Appendix A “Conformance to IEEE 603”
  - ✓ Appendix B “Conformance to IEEE 7-4.3.2”
  - ✓ Appendix F “Safety-related Digital I&C Design Detail Conformance to Essential Safety Criteria”

5. Safety Criteria Conformance

Redundancy

A/D: Analog to Digital Converter
PIF: Power Interface
RTB: Reactor Trip Breaker



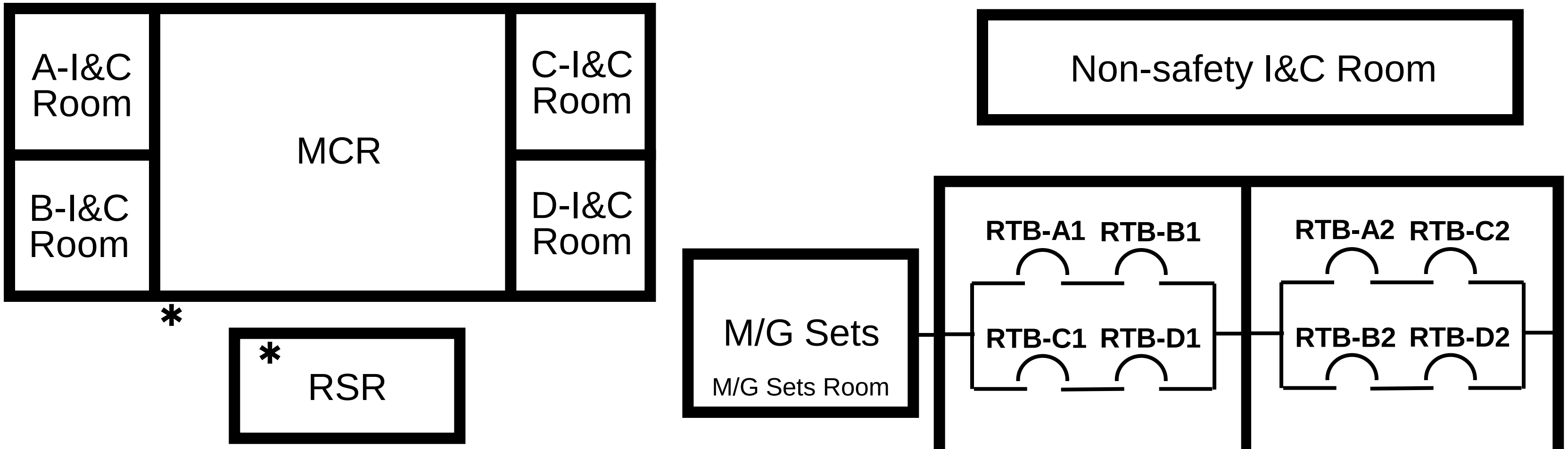
- PSMS consists of 4 redundant and independent trains
- RPS performs its function with any 2-out-of-4 trains tripped
- The ESFAS, SLS, COM and HSIS perform their function by any 2-out-of-4 trains to actuate safety systems with 50% capability, or any 1-out-of-2 trains with 100% capability, depending on the mechanical system design

Independence

- **Independence of the redundant PSMS divisions is achieved through four methods:**
  - ✓ Physical Independence
  - ✓ Electrical Independence
  - ✓ Communication Independence
  - ✓ Functional Independence
- **Methods of ensuring Physical, Electrical and Communication independence are common throughout the entire PSMS**
- **Functional independence is application dependent**

Physical Independence

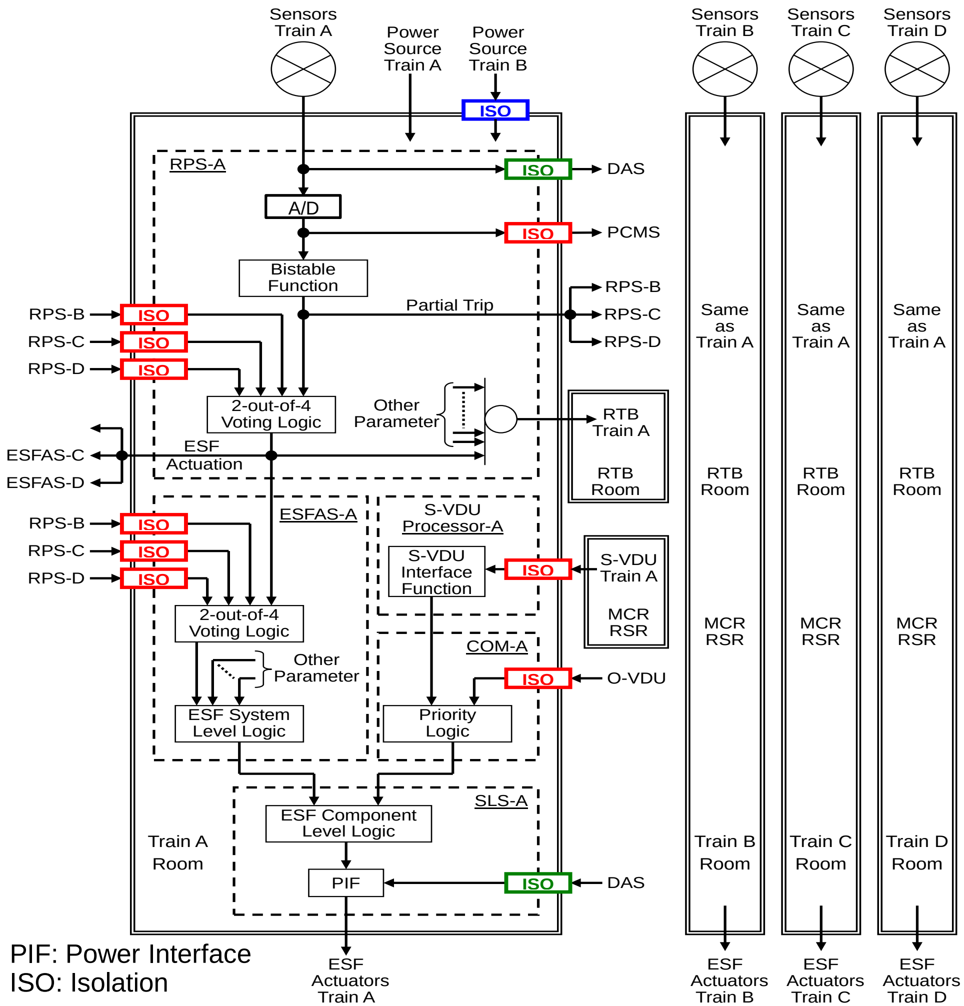
- Four PSMS trains are separated into four I&C equipment rooms
- Four Reactor Trip Breaker (RTB) trains are separated into two equipment rooms, which are separated from the Motor Generator (M/G) set room
- PCMS is located in the Non-Safety I&C equipment room



* Wall mounted MCR/RSR Transfer Switches, one is located outside MCR fire zone, and another in RSR

5. Safety Criteria Conformance

Electrical Independence (1/3)

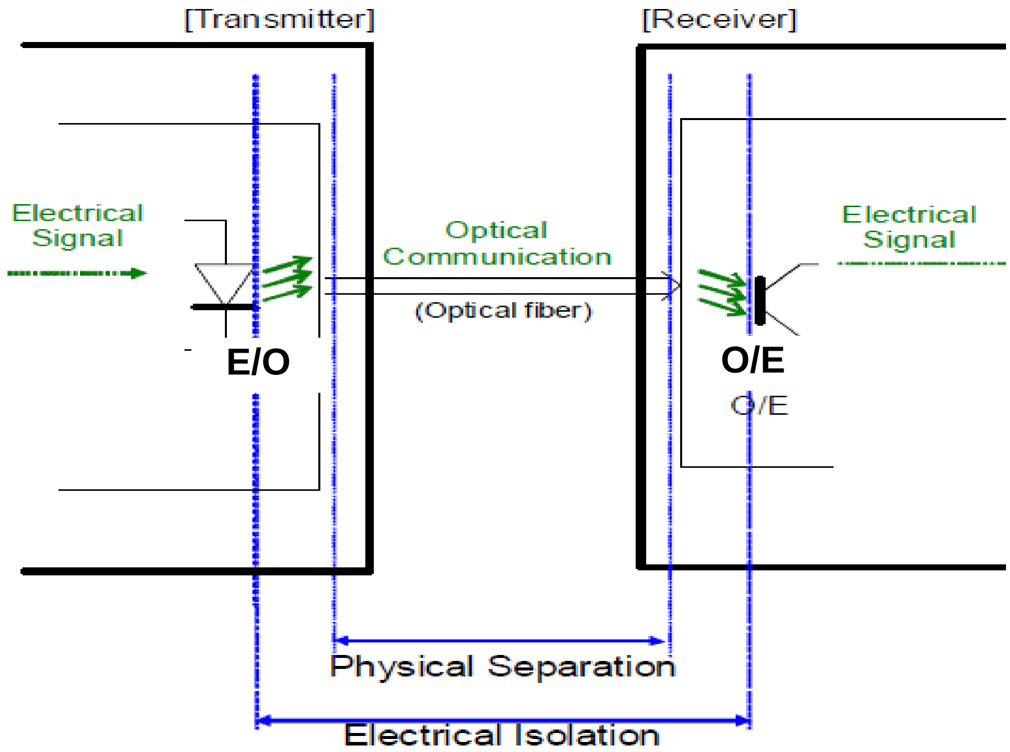


PIF: Power Interface
ISO: Isolation

- Each PSMS train is electrically independent from each other and from the non-safety systems
- Electrical independence between PSMS trains, between PSMS and PCMS, and between MCR, RSR, and I&C equipment rooms is maintained through qualified fiber optic data cables (red lines)
- Electrical independence between PSMS and DAS is maintained through qualified conventional electrical signal isolation devices (green lines)
- Electrical independence between PSMS power sources is maintained through conventional electrical power isolation devices (blue lines)

Electrical Independence (2/3)

Optical Fiber Isolation



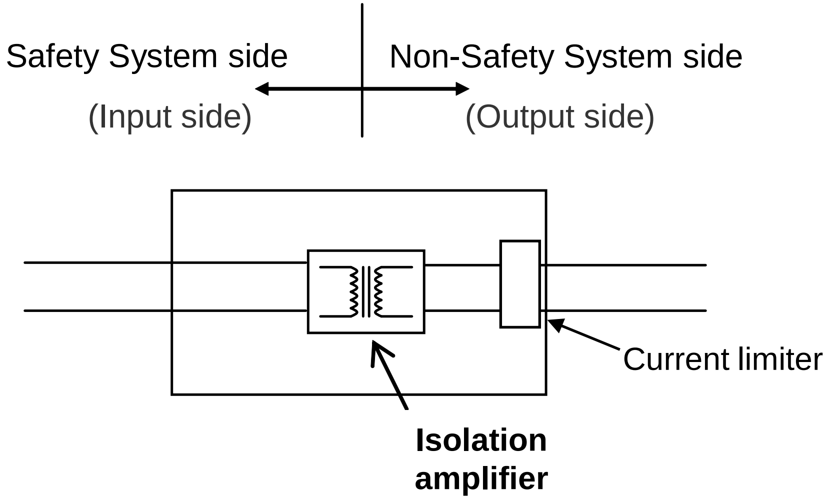
- Optical fiber isolation is used for the digital interfaces in PSMS
- Fiber cables are constructed using only non-conducting materials to ensure inherent blocking of electrical faults

E/O: Electrical/Optical Converter
O/E: Optical/Electrical Converter

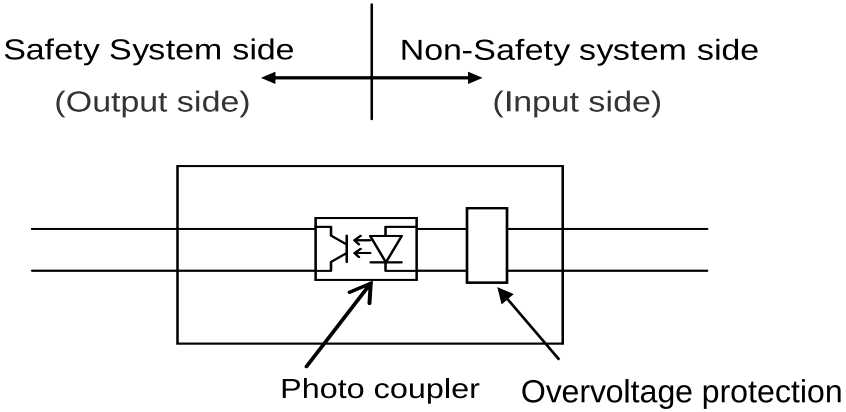
Electrical Independence (3/3)

- Conventional type isolation modules are used for hardwired interfaces, for the DAS, to and from the PSMS, etc.
- Isolation modules are qualified for non-safety side faults of AC480Vrms+10% and ±DC270V in both transverse and common modes by the isolation tests

Analog Isolation Module



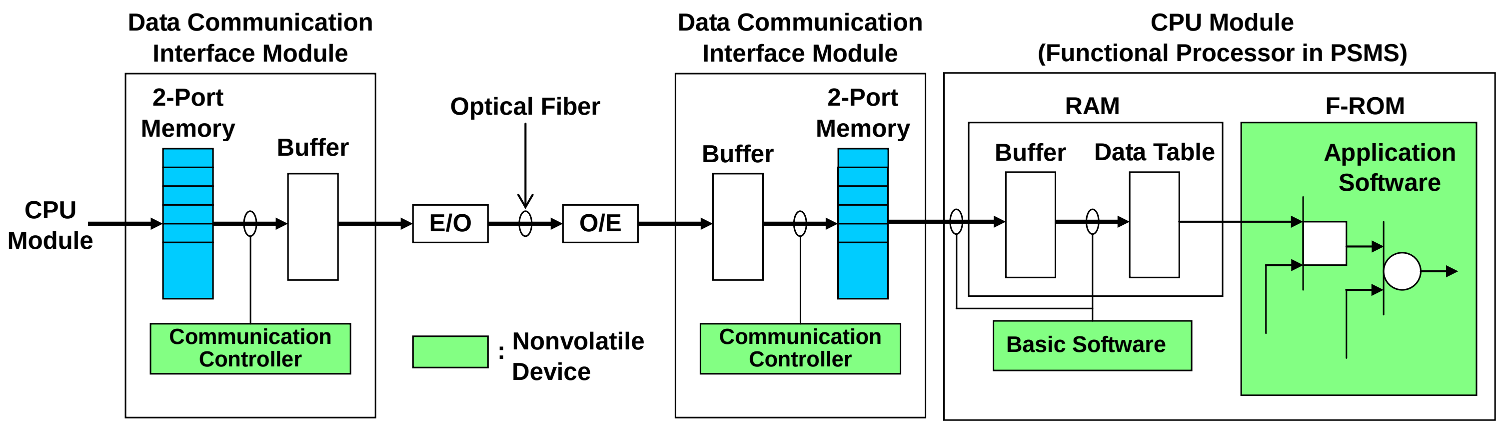
Digital Isolation Module



Communication Independence (1/4)

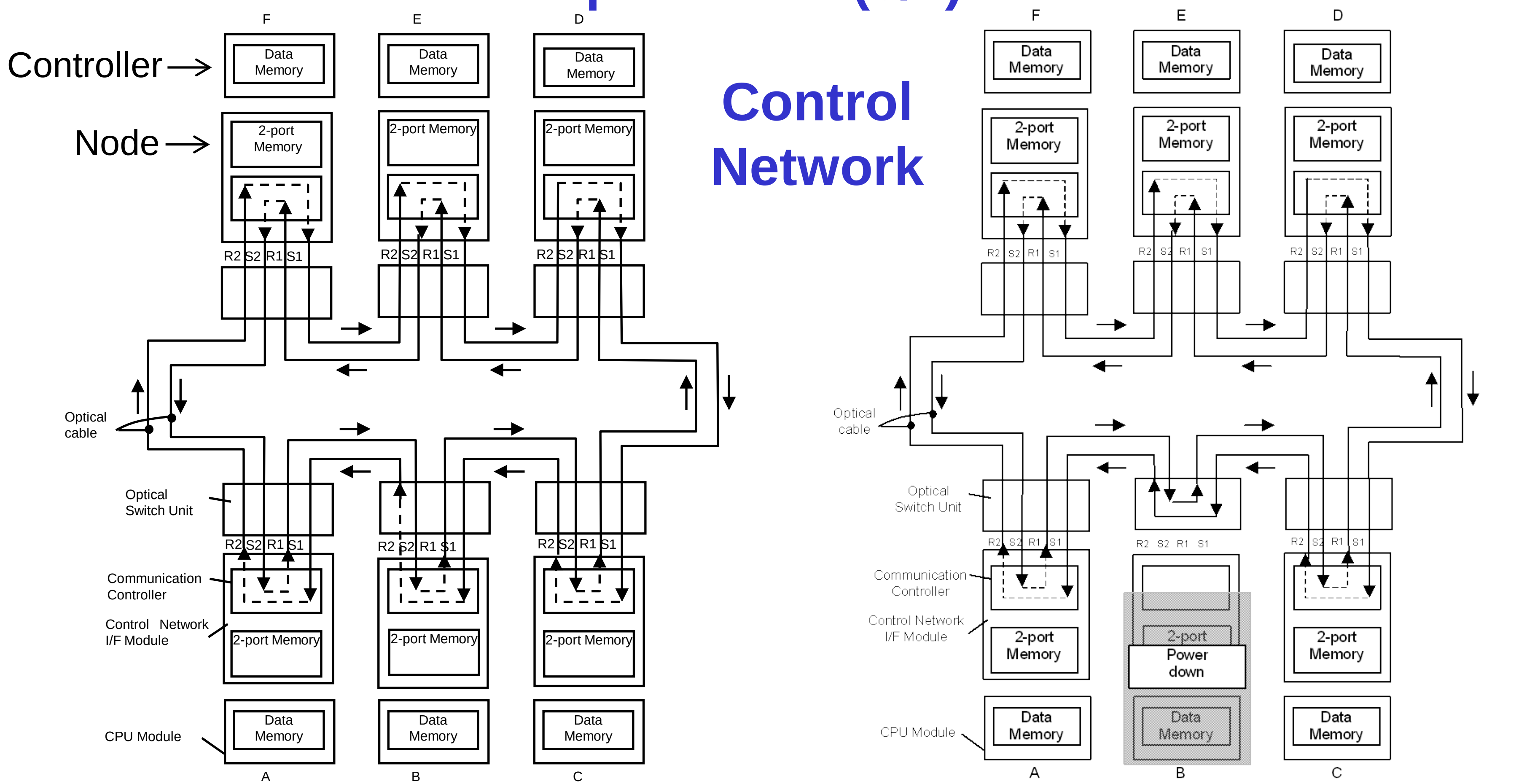
- Data is communicated between PSMS divisions, and between PSMS and PCMS (O-VDU)
- Communication independence allows two digital systems to exchange data while ensuring there is no potential for one digital system to alter the execution of the other digital system in any way
- The PSMS meets all communication independence guidance of DI&C ISG-04
- There are only two types of on-line inter-division communication interface methods applied in the PSMS
  - ✓ Point-to-point Data Link for communication between RPS trains, and between RPS and ESFAS
  - ✓ Multi-drop Network for Unit Bus Interface to the PSMS
- Both types of communication ensure independence by using two port memory, separate communication processors and unalterable memory

Communication Independence (2/4)



- All communication uses 2-Port memory with a separate communication controller and CPU function processor
- Functional processors access 2-port memory asynchronously
- Transmitted signals have pre-defined format, length, and message content

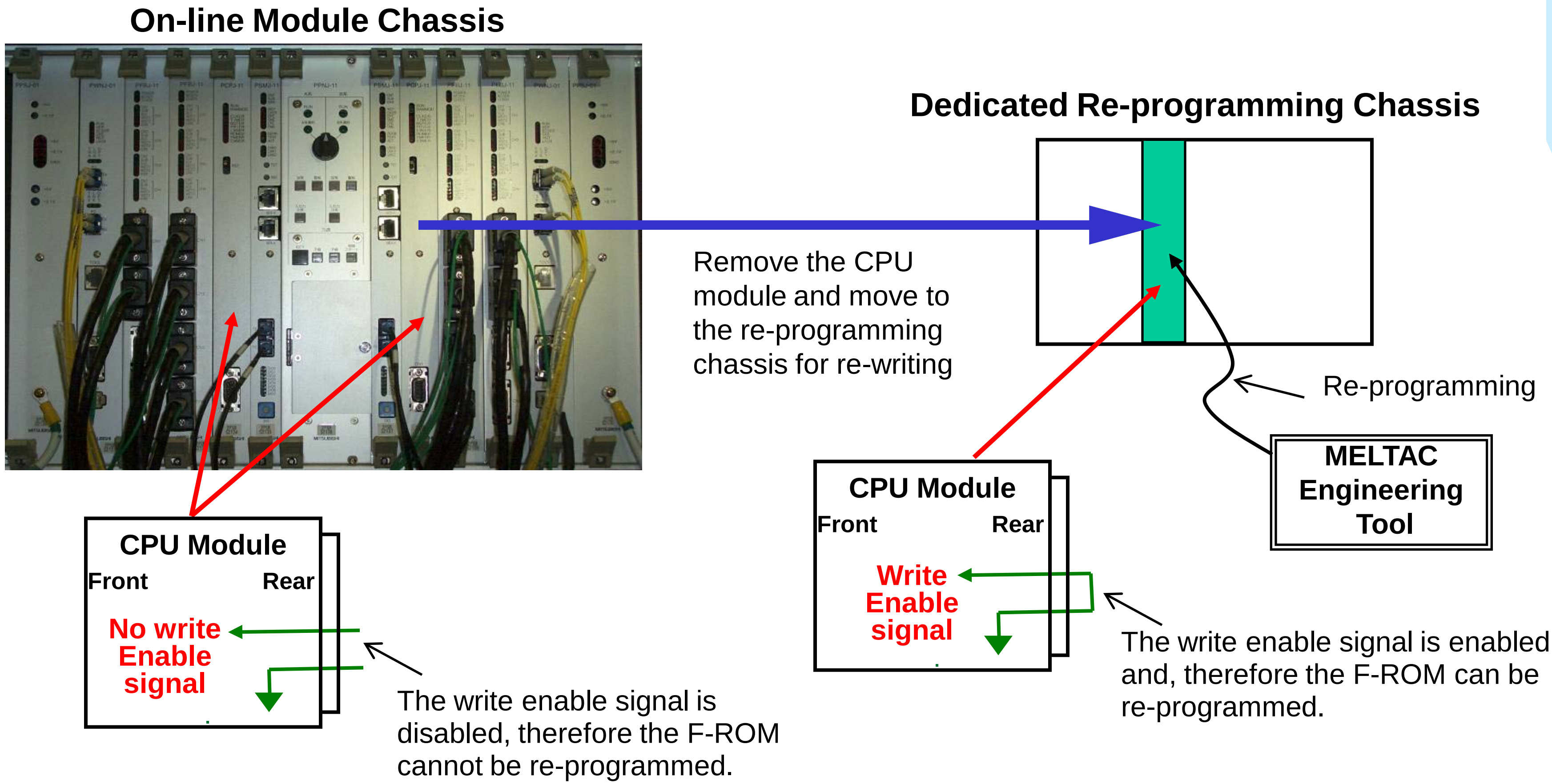
Communication Independence (3/4)



- Controllers are interconnected over redundant optical networks
- Signals are transmitted continuously regardless of data change
- Each node maintains a memory map of the entire network, each controller reads only what it needs for its application programs

Communication Independence (4/4)

- On-line F-ROM Alteration Protection



- ROM/FPGA is only reprogrammable outside of the module chassis and only at the factory (the code and reprogramming tools are not provided to end-users)

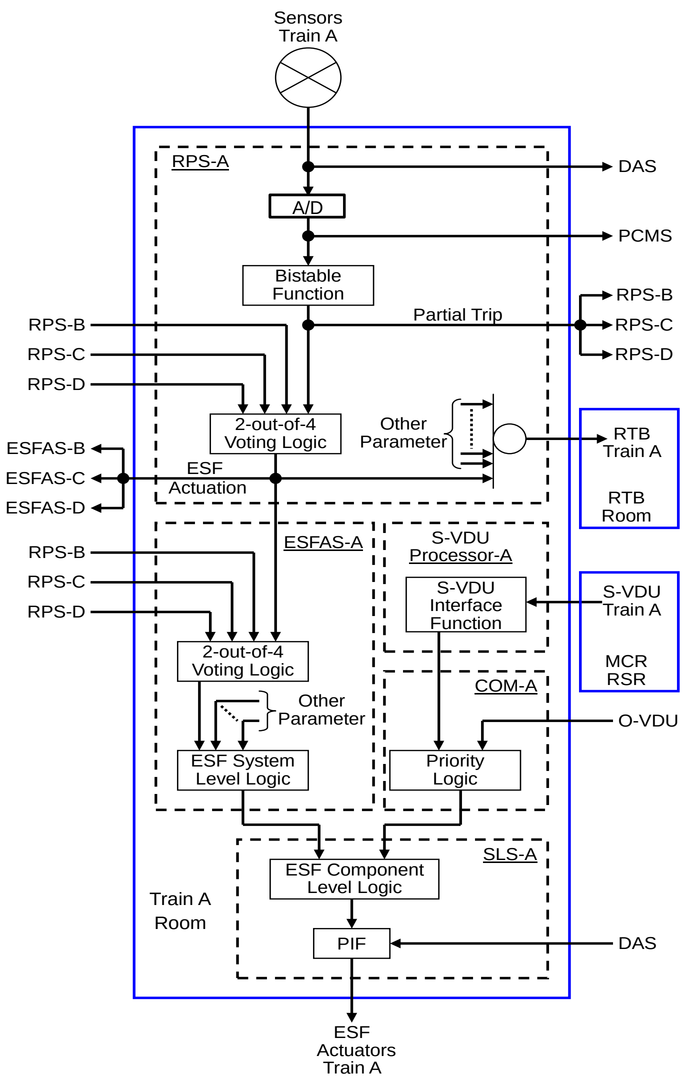
5. Safety Criteria Conformance

Functional Independence (1/5)

- **Each PSMS division receives data from outside its own division:**
  - ✓ From other PSMS divisions
  - ✓ From the PCMS (O-VDU)
  - ✓ From DAS
- **Functional Independence ensures the data received from outside the division cannot adversely affect the safety function being performed within the division**
- **Functional Independence is explained individually for each section of the PSMS – RPS, ESFAS, SLS**
- **The detailed conformance is described in Technical Report "Safety I&C System Description and Design Process," MUAP-07004**
  - ✓ Appendix F "Safety-related Digital I&C Design Detail Conformance to Essential Safety Criteria"

5. Safety Criteria Conformance

Functional Independence (2/5)



- **The following signals are received from across the PSMS train boundaries:**
  - ✓ Reactor and ESFAS partial trip status signal for two-out-of-four trip voting logics
  - ✓ Bypass status signal of each trip parameter for bypass interlocks, bypass allows channel to be tested and allows failed channel to be taken out of service
- **Authenticated messages can have spurious data or frozen data, each train protects itself to ensure the safety function is not affected**
  - ✓ Partial Trip
    - 2-out-of-4 logic prevents a spurious trip and ensures a trip when there are single failures
    - If all inter-division data communication fails, each division will initiate Reactor Trip and ESFAS
  - ✓ Bypass
    First-in blocking logic prevents more than one bypassed channel

5. Safety Criteria Conformance

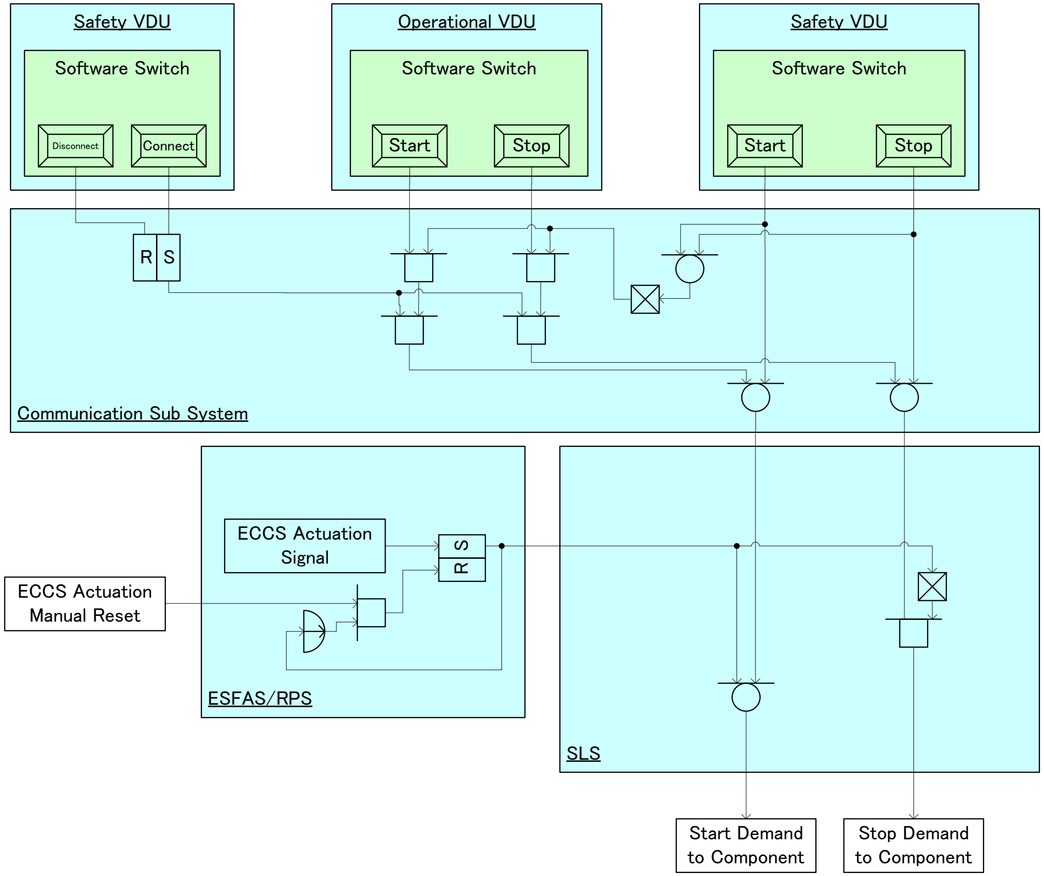
Functional Independence (3/5)

- The following HSI signals are transmitted to the PSMS from the Operational VDUs of the non-safety PCMS:
  - ✓ Component Position commands (on/off, open/close)
  - ✓ Maintenance Bypass commands
  - ✓ Operating Bypass commands
  - ✓ ESFAS Reset commands
  - ✓ Component Lock commands
- For all signals, unalterable priority logic within the PSMS ensures each PSMS division protects itself so that its safety function cannot be adversely affected

5. Safety Criteria Conformance

Functional Independence (4/5)

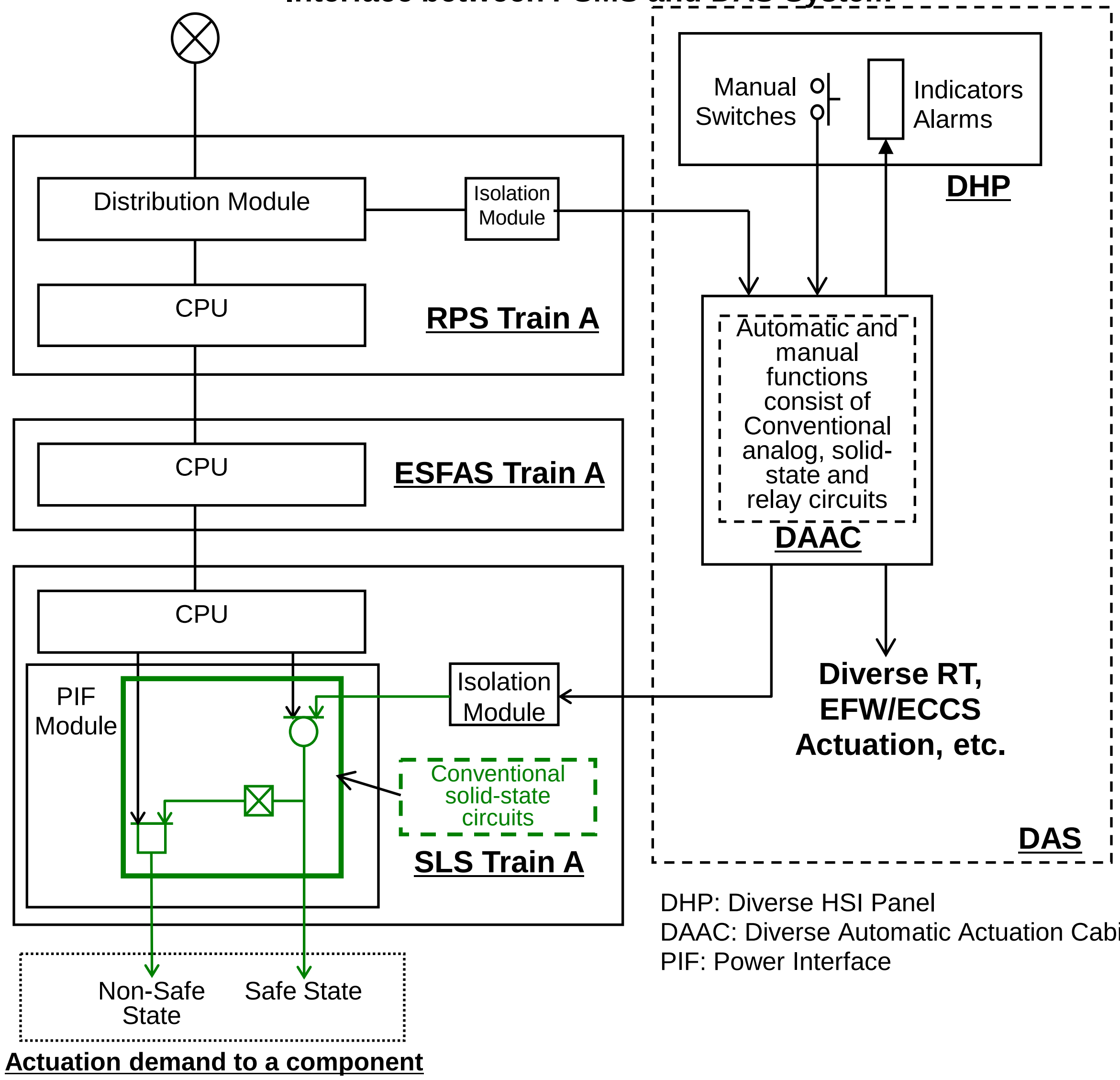
Typical Priority Logic For Manual Operational Signals



- The priority logic within the SLS of each train ensures Class 1E interlocks or ESFAS signals have priority over all manual component position commands, including commands from O-VDU
- All safety components controlled from O-VDUs have ESFAS or Class 1E interlock

5. Safety Criteria Conformance

Interface between PSMS and DAS System

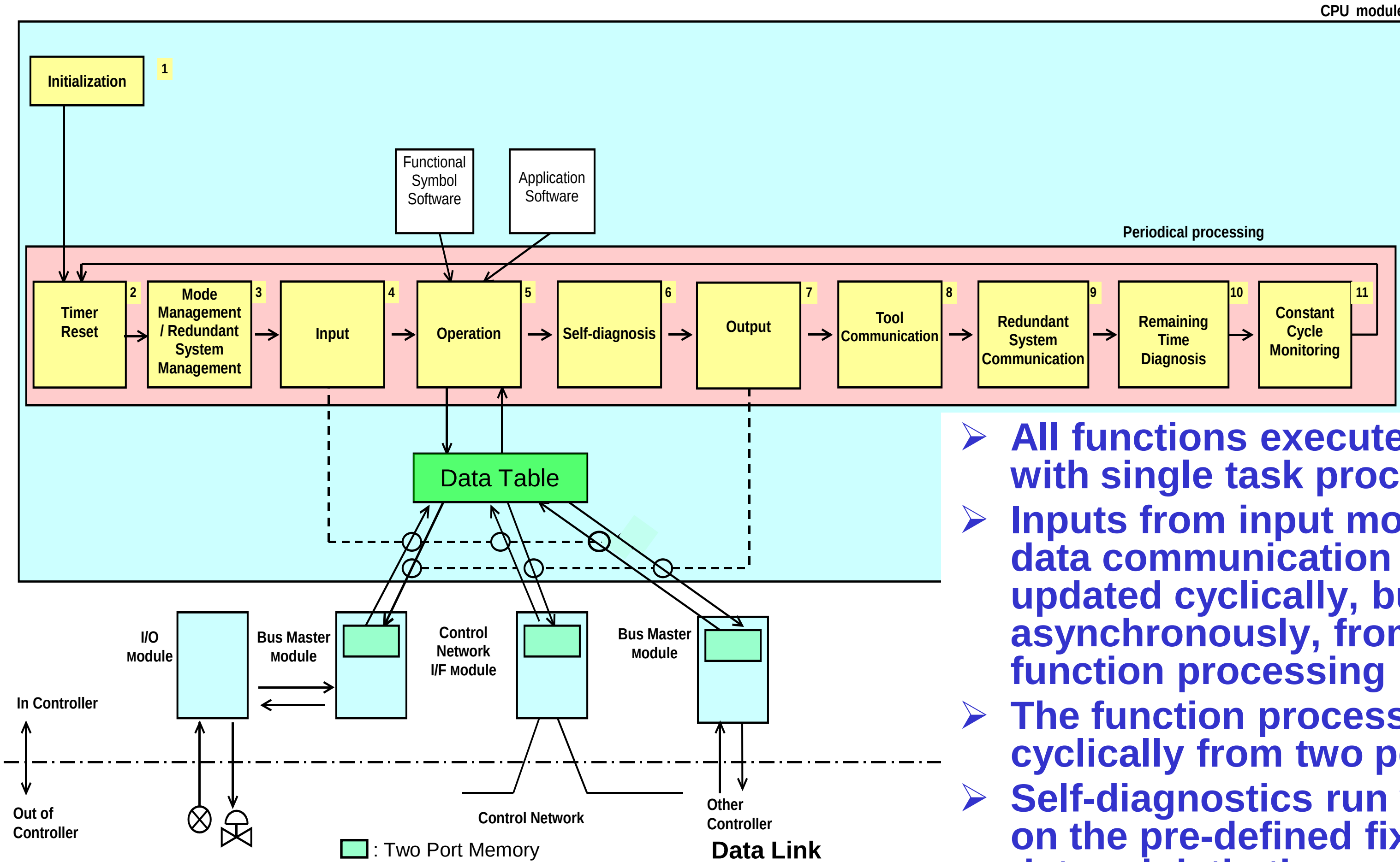


DHP: Diverse HSI Panel
DAAC: Diverse Automatic Actuation Cabinet
PIF: Power Interface

Functional Independence (5/5)

- **The PIF module, PSMS and DAS use common conventional solid state circuits**
  - ✓ There is no potential for software CCF
- **The non-safety DAS interface is hardwired with conventional isolators**
  - ✓ There is no digital communication
- **PIF logic ensures priority is given to the safety function**
  - ✓ It is state based, not system based
  - ✓ It ensures failures of active PSMS or DAS cannot block the safety function

Determinism (1/2)



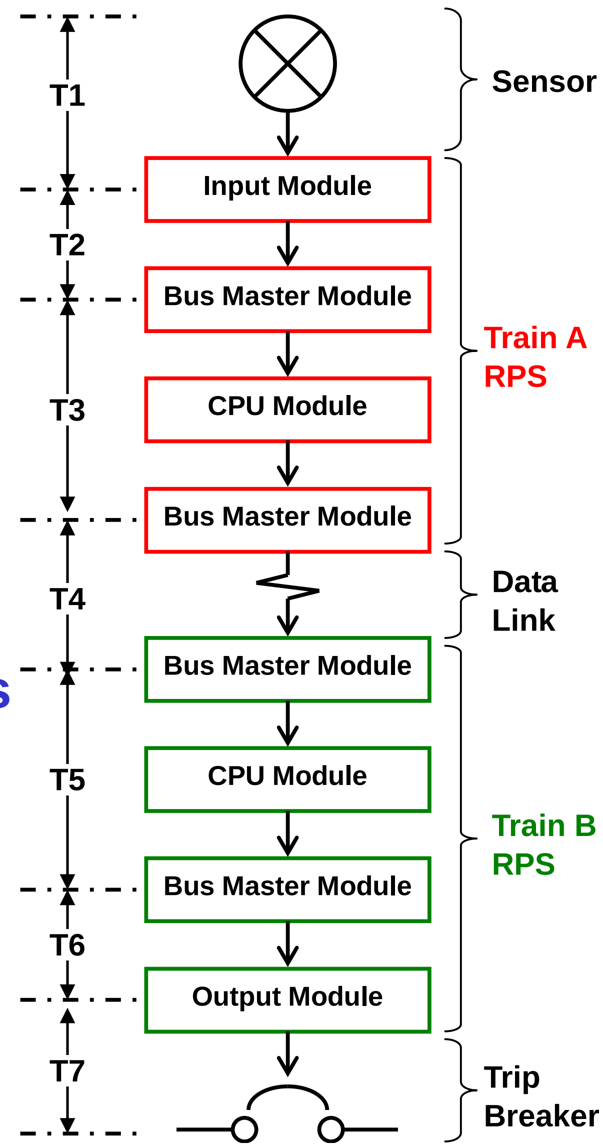
- All functions execute cyclically with single task processing
- Inputs from input modules and data communication modules, are updated cyclically, but asynchronously, from periodic function processing
- The function processor reads data cyclically from two port memory.
- Self-diagnostics run with no affect on the pre-defined fixed deterministic time cycle
- There are no interrupts, except by self-diagnostics
- Time cycle cannot be disrupted by other trains or Unit Bus

5. Safety Criteria Conformance

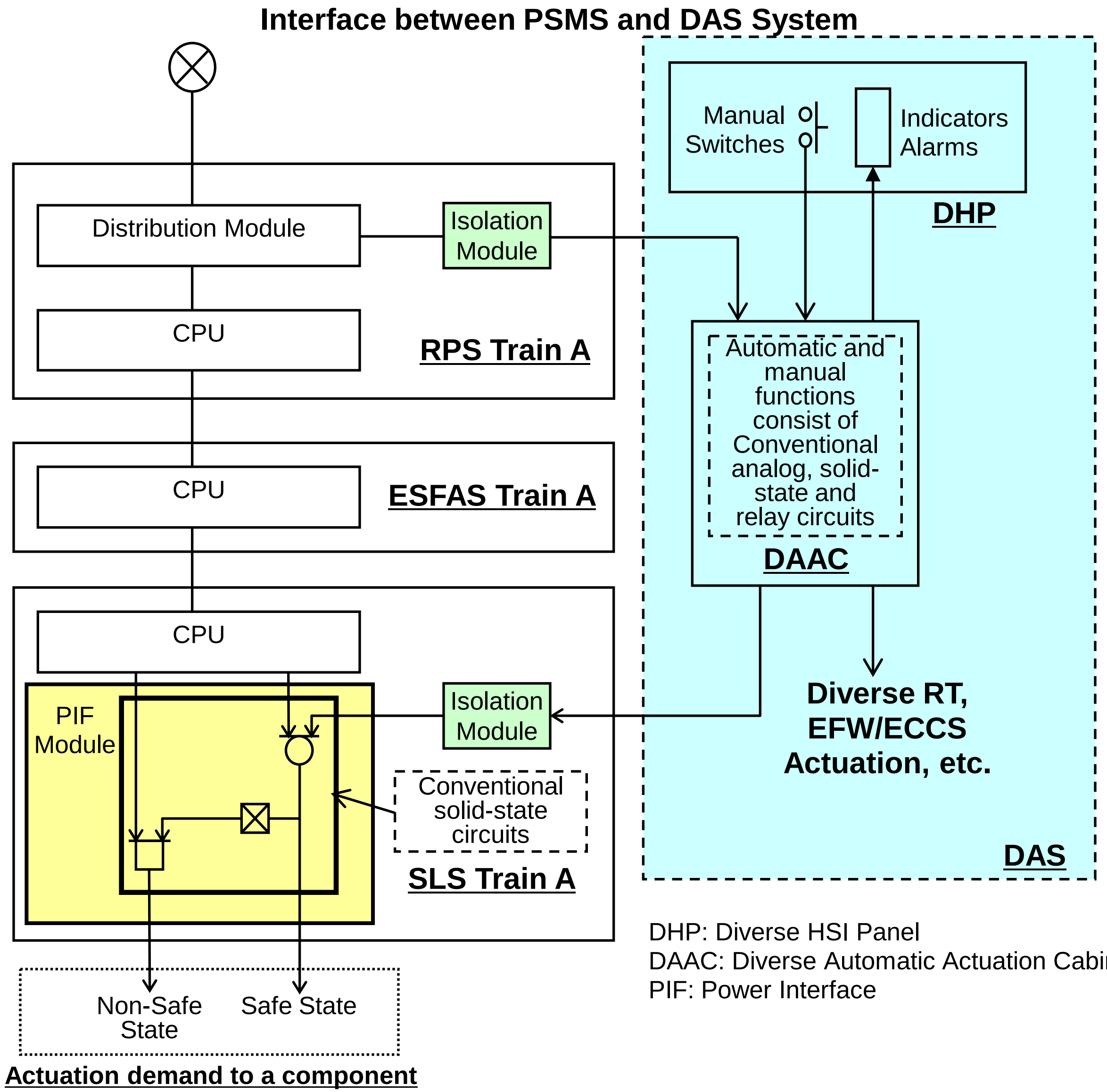
Determinism (2/2)

- **Response Time**
  - ✓ Each module runs in a cyclical deterministic sequence
    - Worst case (basis of safety analysis)
      Input is updated just after input polling (Tmax)
  - ✓ Calculation Result
    - Worst case response time is
      T1max + T2max + T3max + T4max + T5max + T6max + T7max

- **ITAAC confirms the detailed design meets response time requirements as defined in Technical Report "Response Time of Safety I&C System," MUAP-09021**
  - ✓ 300 msec max for digital throughput for reactor trip functions



5. Safety Criteria Conformance



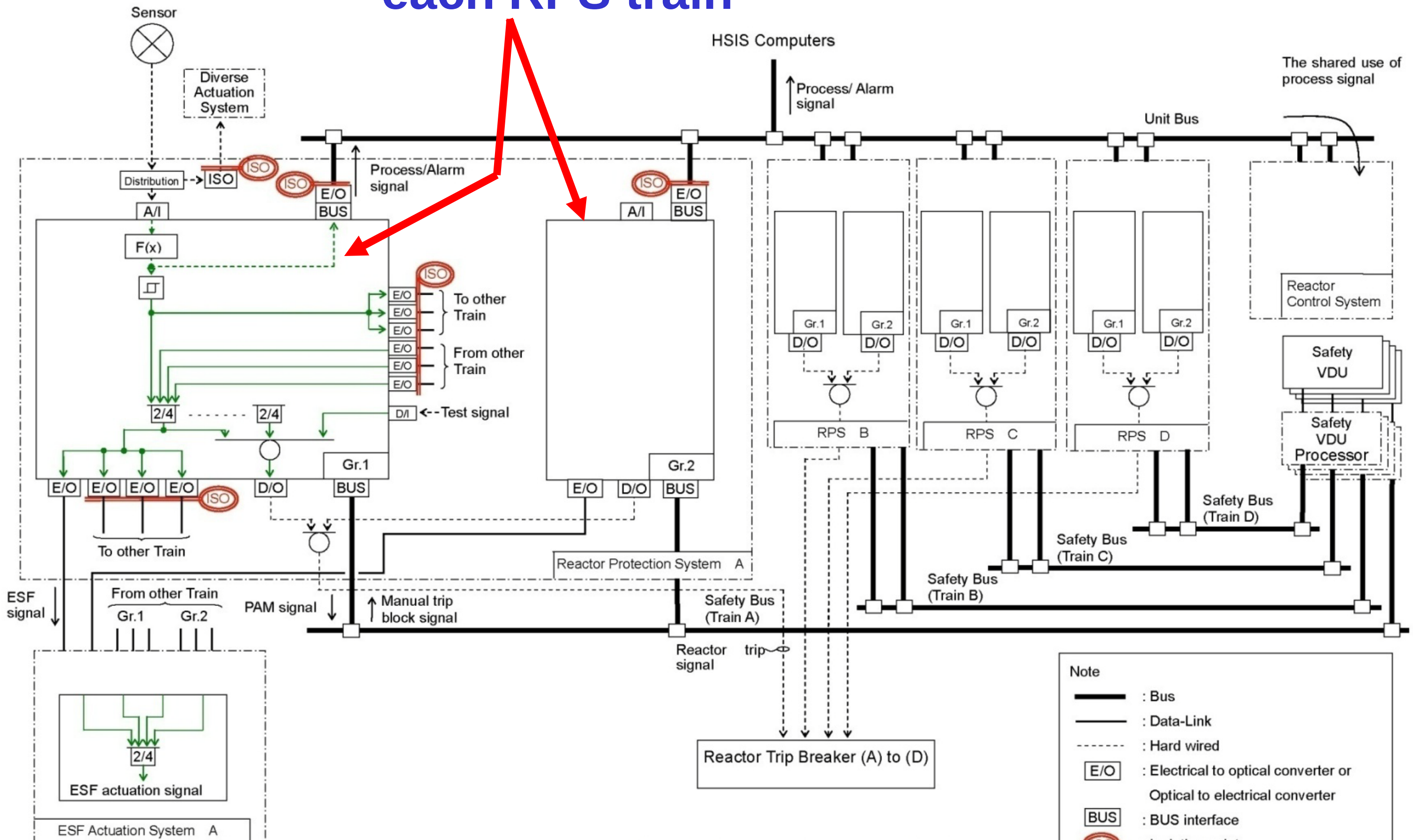
DHP: Diverse HSI Panel
DAAC: Diverse Automatic Actuation Cabinet
PIF: Power Interface

Diversity for Software CCF

- Conventional, analog/binary DAS is provided per BTP 7-19, to accommodate beyond design basis CCFs that could adversely affect PSMS and PCMS, with a concurrent AOO or PA
- DAS provides automated reactor trip, turbine trip, MFW Isolation, EFW actuation and ECCS actuation
- DAS allows operator to monitor the critical safety functions and manually actuate safety system to achieve and maintain safe shutdown

RPS Functional Diversity (1/2)

Two Separate Sub-systems in each RPS train



Configuration of Reactor Protection System

5. Safety Criteria Conformance

RPS Functional Diversity (2/2)

- Two diverse parameters are used to detect an event and initiate protective actions
- Processed in two separate Controller Groups in each train
- The PRA shows significant benefit from functional diversity

Protection	Group-1	Group-2
Over Power	Over Power Delta-T High PR Neutron Flux Rate High	PR Neutron Flux High
Core Heat Removal	RCP Speed Low Over Temp. Delta-T High	RC Flow Low Pressurizer Press. Low
Loss of Heat Sink	SG Water Level Low Pressurizer Water Level High	Pressurizer Press. High
Nuclear Startup	SR Neutron Flux High IR Neutron Flux High	PR Neutron Flux High (Low Setpoint)
Primary Over Pressure	Pressurizer Water Level High	Pressurizer Press. High
Loss of Coolant	C/V Press. High	Pressurizer Press. Low-Low
Steam Line Break	C/V Press. High-High	Main Steam Line Press. Low

5. Safety Criteria Conformance

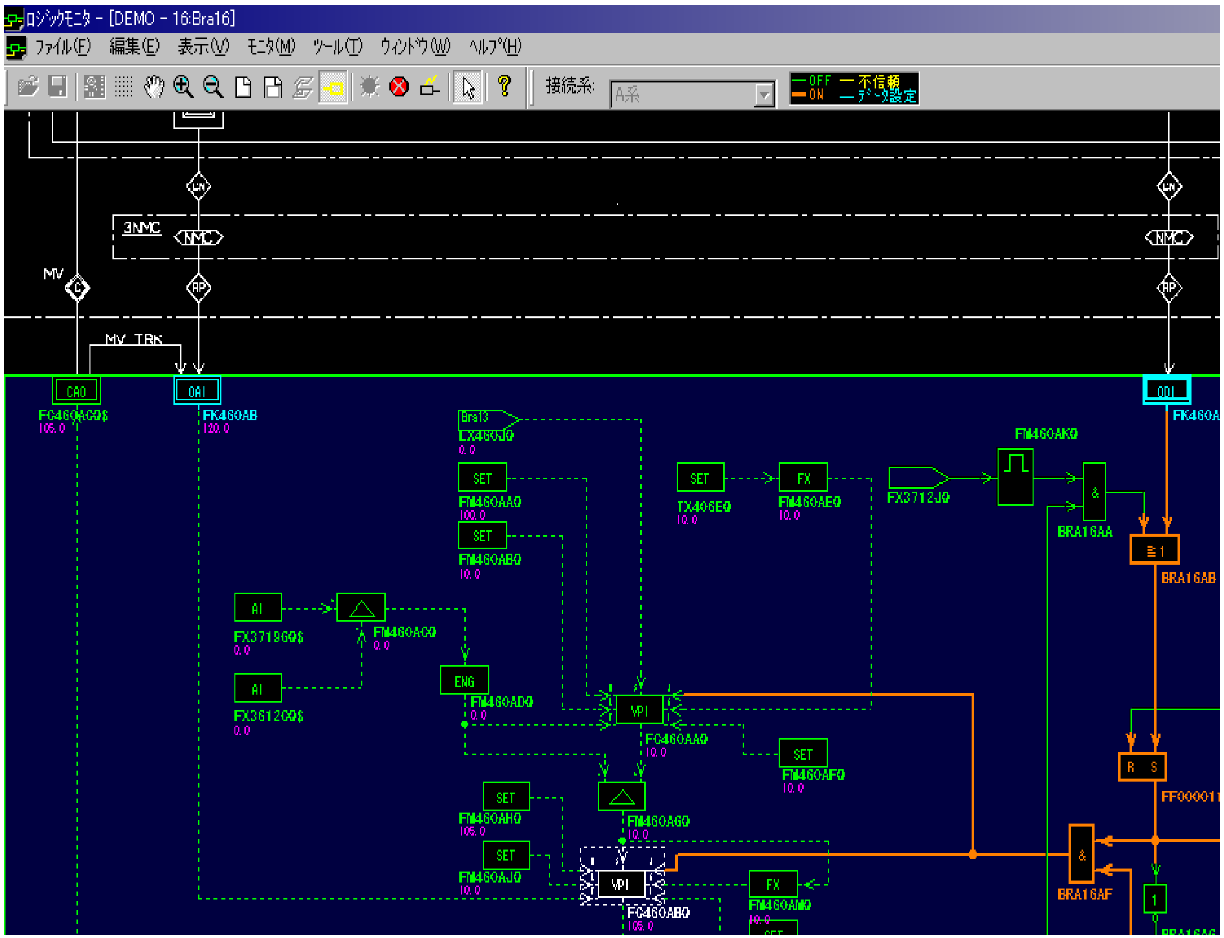
Simplicity (1/2)

- **Overall plant-wide simplicity is achieved through**
  - ✓ One digital platform applied to all safety and non-safety applications
  - ✓ One system, PSMS, provides all safety functions
  - ✓ One system, PCMS, provides all non-safety functions
  - ✓ Standard approach to electrical independence
    - Only 4 common isolators – power, inputs, outputs, fiber optic communications
  - ✓ Standard approach to data communication
    - Only 2 common interfaces – Data Link, Control Network
  - ✓ Standard approach to communication independence
    - Separate communication controllers with two-port memory
  - ✓ Same HSI in MCR and RSR

5. Safety Criteria Conformance

Simplicity (2/2)

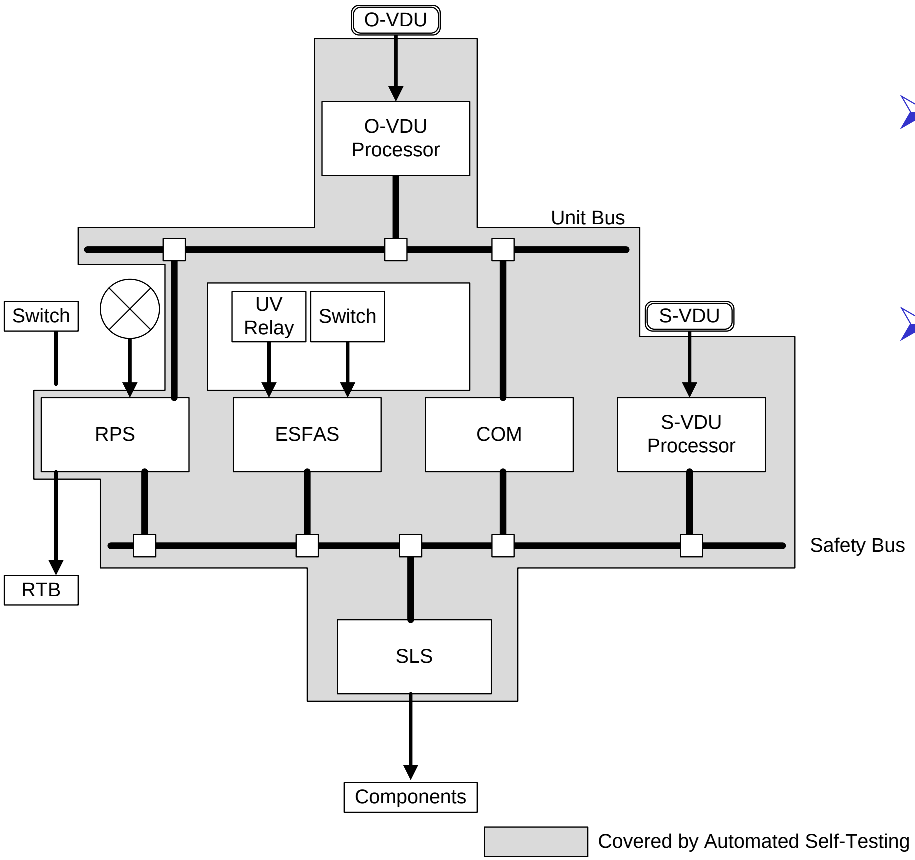
**Example of
Application Software Development Display**



- **Basic software and application software are separated**
- **Basic software block is represented as simple predefined functional blocks, such as, AND, OR, Timer and Latch, etc.**
- **Application software is developed using the off-line Engineering Tool that graphically connects the functional blocks and links those blocks to the I/O**
- **The application software execution data is simply a list of function block connections**

5. Safety Criteria Conformance

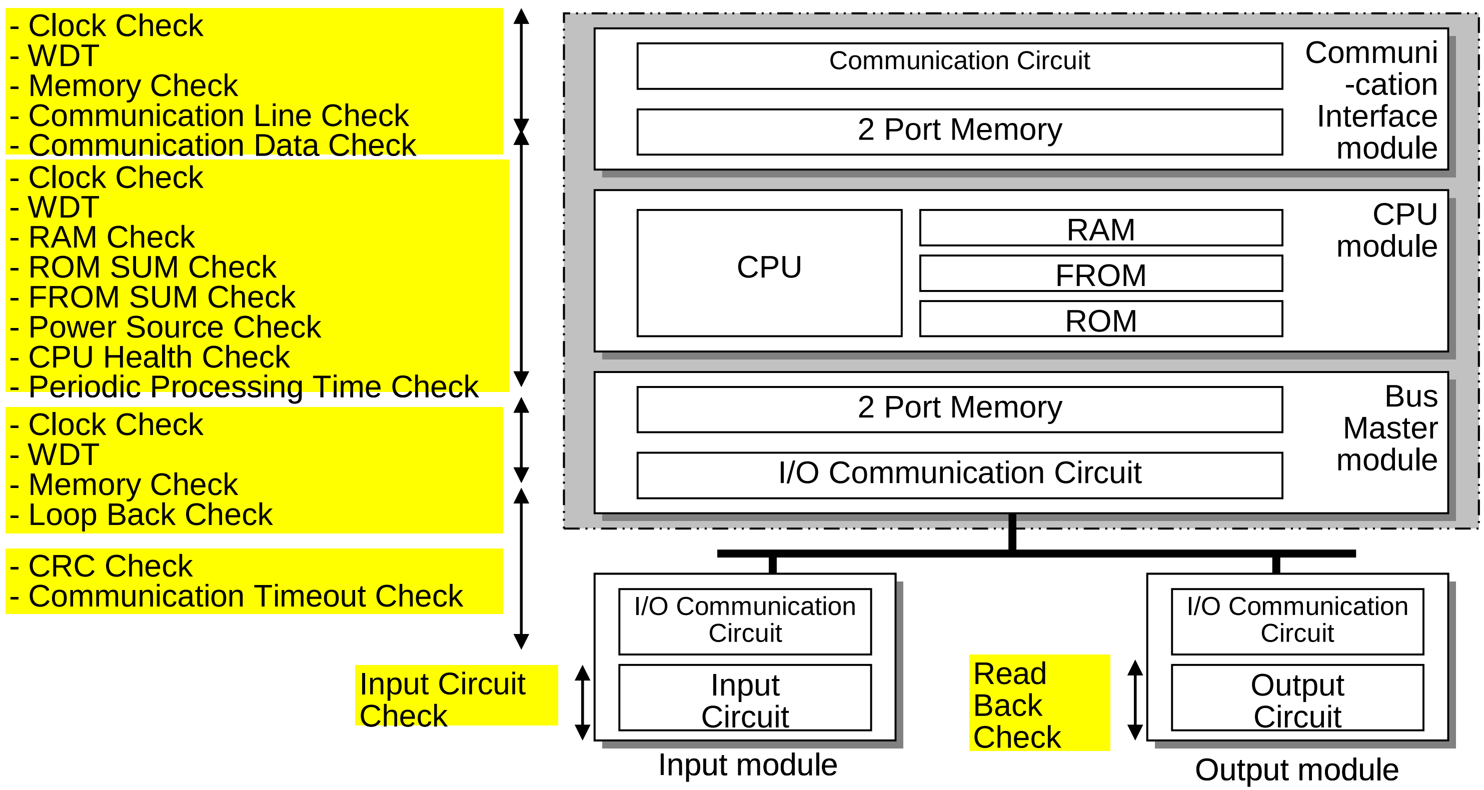
Testability (1/5)



- **Continuous automatic self-testing covers all digital system components, including all controller memory and inter-controller data communication, from input to output**
- **All program memory, including memory that controls the self-testing and setpoints, is confirmed by continuous automatic self-testing**
- **Diverse manual surveillance tests controlled by T-Spec., including the operability of the self-testing functions, confirm the operability of each PSMS controller**
  - ✓ CHANNEL CALIBRATION
    From sensor through controllers and data communication to VDUs
  - ✓ TADOT
    From VDUs through data communication and controllers to plant components, including RTBs
  - ✓ MEMORY INTEGRITY CHECK
    Divers test (from memory self-test) of all Basic and Application Software

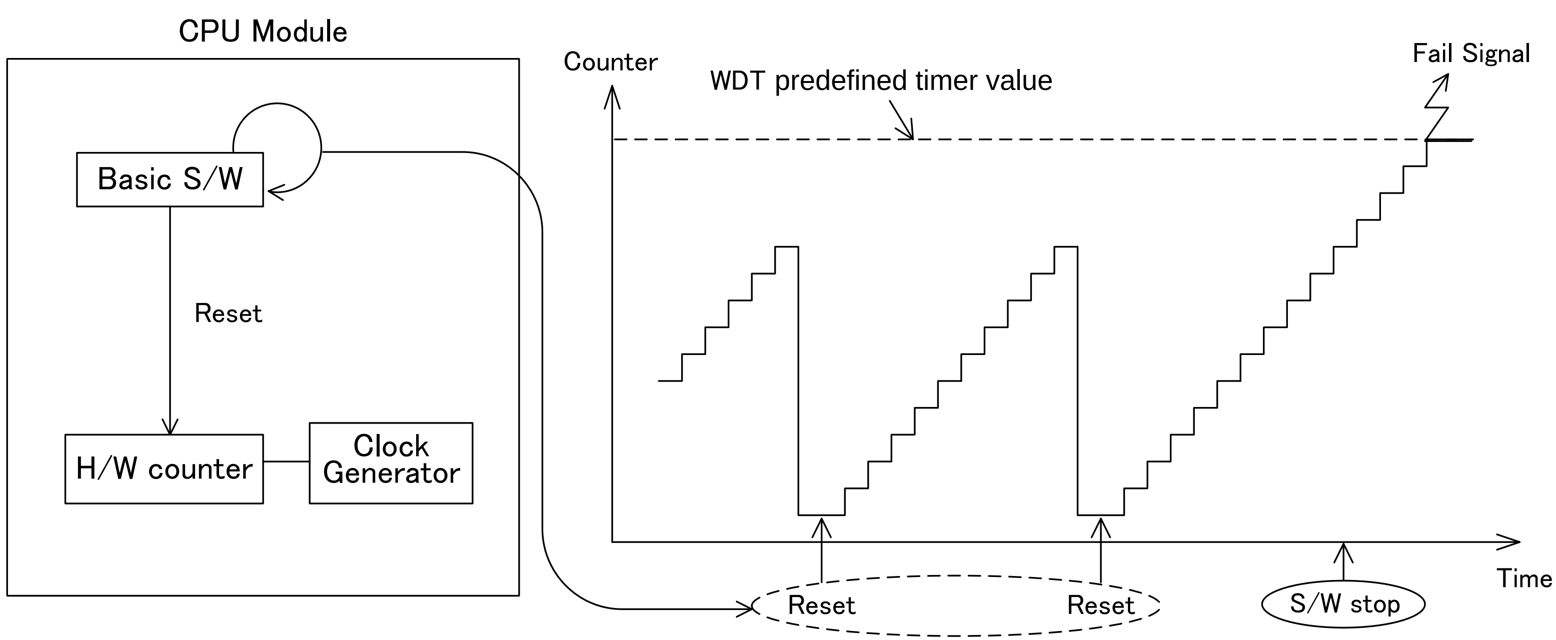
Testability (2/5)

- **The Self Diagnosis function completely tests H/W and S/W**
- **All memory and other H/W that affect safety functions are tested directly**
- **There are two broad tests to detect erroneous function execution:**
  - ✓ Watchdog Timer (WDT) – gross cycle time check by hardware
  - ✓ Periodic Process Time Check – precise cycle time check by software



Testability (3/5)

- **Watchdog Timer**
  - ✓ The WDT consists of a counter with a hardware clock generator, and predefined timer value (for WDT time-out)
  - ✓ The timer counts up, basic software resets the timer at regular intervals (i.e., for each operation cycle) to start recounting from zero
  - ✓ If basic software does not reset the WDT within a predefined timer value then the WDT times out, the controller transitions to a failure state with an alarm, failure state results in partial reactor trip and fail as-is for ESF system signals

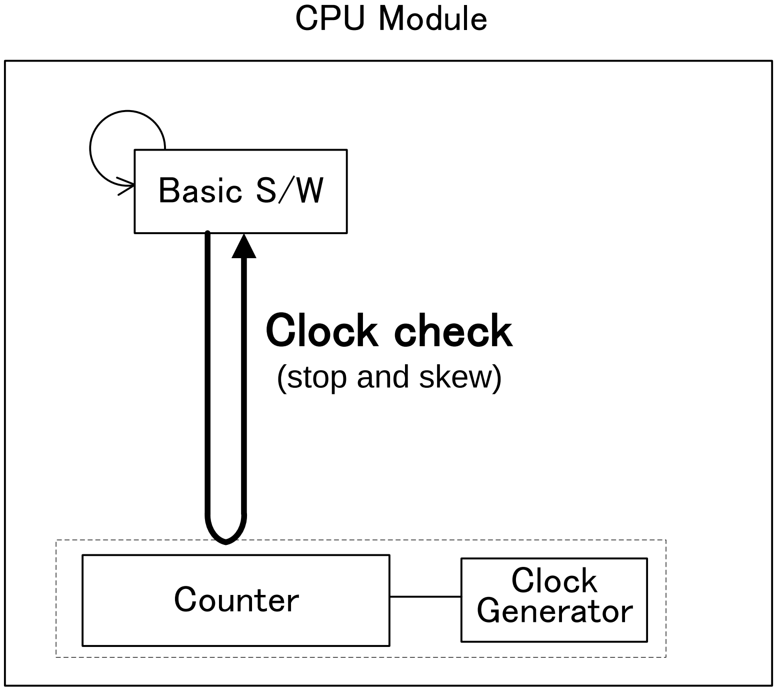


5. Safety Criteria Conformance

Testability (4/5)

➤ Watchdog Timer

- ✓ A failure of the WDT can be detected by monitoring the counter value (WDT clock check)
- ✓ If the counter stops or becomes askew, this indicates abnormality of WDT



- WDT clock check is periodically performed by the Basic software
- If an error is detected by this clock check, the controller transitions to failure state

5. Safety Criteria Conformance

Testability (5/5)

- Self-testing detects hardware or software errors in PSMS
- Logic, algorithms, setpoints, time constant values, and inter-train communication of PSMS are self-tested
- I/O is confirmed by manual periodic tests
- Manual periodic I/O tests also provide diverse confirmation of each controller's ability to execute multiple diverse software functions
- All memory that controls Basic Software (including self-testing) and Application Software (including all logic, setpoints and time constants) is confirmed by the manually initiated software MEMORY INTEGRITY CHECK (MIC) which is diverse from the self-test
- Through the aggregate of these tests, all safety functions of PSMS are confirmed
- Setpoint Methodology Technical Report, MUAP09022, includes the method of allowable value calculation for testing

5. Safety Criteria Conformance

Reliability (1/4)

- **Following key features of PSMS ensure high reliability**
  - ✓ Digital platform (MELTAC) operating history, which demonstrates long component MTBF and no software CCFs
  - ✓ Continuous self-testing with high coverage to detect failures
  - ✓ Periodic surveillance test to ensure 100% test coverage
  - ✓ Redundancy between divisions, and within divisions including safety bus
  - ✓ Diversity within divisions to reduce PSMS CCF potential
  - ✓ Should a PSMS CCF occur, DAS to mitigate accidents
- **Impact of PSMS reliability is analyzed in DCD Chapter 19 PRA**
- **Key elements of PSMS reliability calculation in PRA are:**
  - ✓ Mean Time Between Failures (MTBF) of digital I&C components
  - ✓ Self-test coverage (rate to detect failures) and Periodic test intervals
  - ✓ Common cause failure probabilities
  - ✓ Digital I&C modeling
    - All modules, including modules to perform the safety bus functions, such as network I/F modules and optical switches, are modeled in the PRA
    - Safety bus itself (redundant optical cables) is not modeled because failure rate is negligible

5. Safety Criteria Conformance

Reliability (2/4)

➢ MTBF of digital I&C components

- ✓ The MTBF value of each digital I&C component used in the PSMS is calculated based on MIL standard (MIL-HDBK-217F)
- ✓ The actual MTBF values determined from field operating experiences of the digital platform (MELTAC) are longer than the calculated MTBF values
- ✓ PSMS reliability is assured through the Reliability Assurance Program (design phase and operations phase)
- ✓ PSMS digital platform will be included in D-RAP

5. Safety Criteria Conformance

Reliability (3/4)

- **Periodic test intervals and self-diagnosis rate to detect failures**
  - ✓ The self-diagnosis rate is estimated as 100% based on the FMEA of the platform, conservative value of 90% is used in the PRA to account for uncertainty
  - ✓ The periodic test intervals used in the PRA are provided in the DCD Chapter 16 T-Spec
    - The interval extensions from historical STS values are shown to have negligible effect on CDF, MUAP-07030 “PRA”, Attachment 18A.1
      - \- The summary will be added in DCD Chapter 19 Appendix 19B in DCD Rev.4
    - 24-month sensor calibration interval is the basis of channel uncertainty in the Setpoint Methodology
  - ✓ 0% self-diagnosis rate is used for the hardware devices not covered by self-diagnosis (e.g., sensor, breaker, non-digital part of I/O modules, etc.)

5. Safety Criteria Conformance

Reliability (4/4)

- **Common cause failure (CCF) probabilities.**
  - ✓ Basic Software CCF: 1E-07/demand
    Assuming one CCF through 20-million-hour operating experience, no CCF has occurred in MELTAC platform
    - MELTAC platform has been:
      - In operation since 1987 in Japan
      - Applied to approximately 450 controllers in 30 plants
      - Each controller has 2,000 to 200,000 hours operating history (average 8 years).
    - Platform Operating Experience was approximately 30 million hours (8760 hours/year x 8 years x 450 controllers) as of February 2011
    - “20 million hour” value was used for CCF probability calculation as a conservative estimation at the time of PRA was conducted
  - ✓ Application Software CCF: 1E-05/demand
    Crediting many Class 1E life cycle process management and many defensive measures (e.g., strictly cyclic operation, constant loading of communication and processing buses, static memory allocation and asynchronous operation)
  - ✓ Hardware CCF
    Summing the unavailability of each module multiplying with the generic component parameters of the MGL

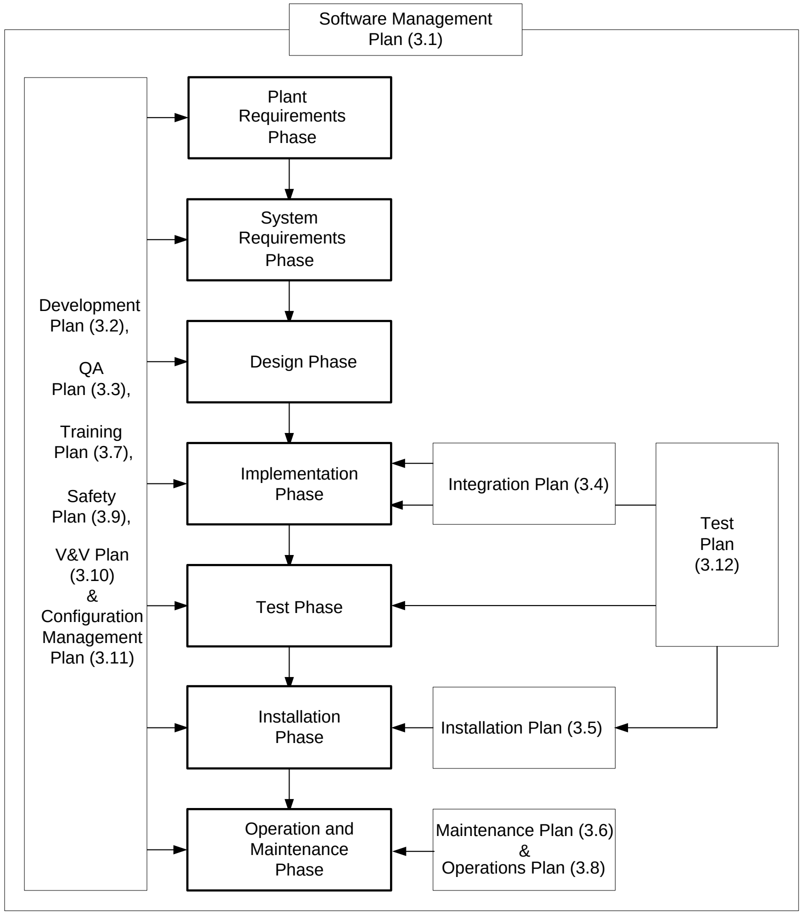
5. Safety Criteria Conformance

Quality (1/3)

- **MELTAC Nplus S Hardware Lifecycle**
  - ✓ Design, manufacture, and test hardware products under the Appendix B QAP
  - ✓ Provide 30 years support proactive obsolescence management and corrective action program
- **MELTAC Nplus S Software Lifecycle (Basic Software)**
  - ✓ Develop and test Basic Software configuration items under the Appendix B QAP
  - ✓ The Appendix B QAP invokes the MELTAC Basic Software Program Manual which satisfies the requirements of BTP 7-14 and complies with RG1.152 and other applicable IEEE standards
- **MHI is to address how to flow down the requirements, and ensure the life cycle process of the MELTAC platform to address Open Items**

Quality (2/3)

- ➢ **Design Process for Application Software is governed by the "Software Program Manual (SPM)", MUAP-07017**
  - ✓ Plant Requirements
  - ✓ System Requirements
  - ✓ Design
  - ✓ Implementation
  - ✓ Test
  - ✓ Installation
  - ✓ Operation and Maintenance
- ➢ **All independent V&V activities are performed by MHI in accordance with the SPM**
- ➢ **Process includes integration of complete system including hardware, basic software, and application software**
- ➢ **ITAAC demonstrates compliance with SPM**



Quality (3/3)

➢ Augmented quality for non safety systems

Items	Specific requirements for non-safety system
Safety Functions Controlled by O-VDUs	DI&C-ISG-04
Safety Parameter Display System (SPDS)	10 CFR 50.34 (f)(2)(iv), “Additional TMI-Related Requirements” regarding the SPDS
	NUREG 0737 Supplement 1, “Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability”, with respect to SPDS
Alarms for Credited Manual Operator Actions	SECY-93-087, Item II. T, “Control Room Annunciator (Alarm) Reliability”
Signal Selection Algorithm (SSA)	RG 1.153, “Criteria for Safety Systems”
	IEEE 603-1991, Clause 6.3 “Interaction between the Sense and Command features and other Systems”
Risk-significant non-safety I&C system	Risk-significant non-safety I&C system identified in DCD Table 17.4-1 (primarily systems that can cause AOO)
Diverse Actuation System	BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems”
	Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related”

5. Safety Criteria Conformance

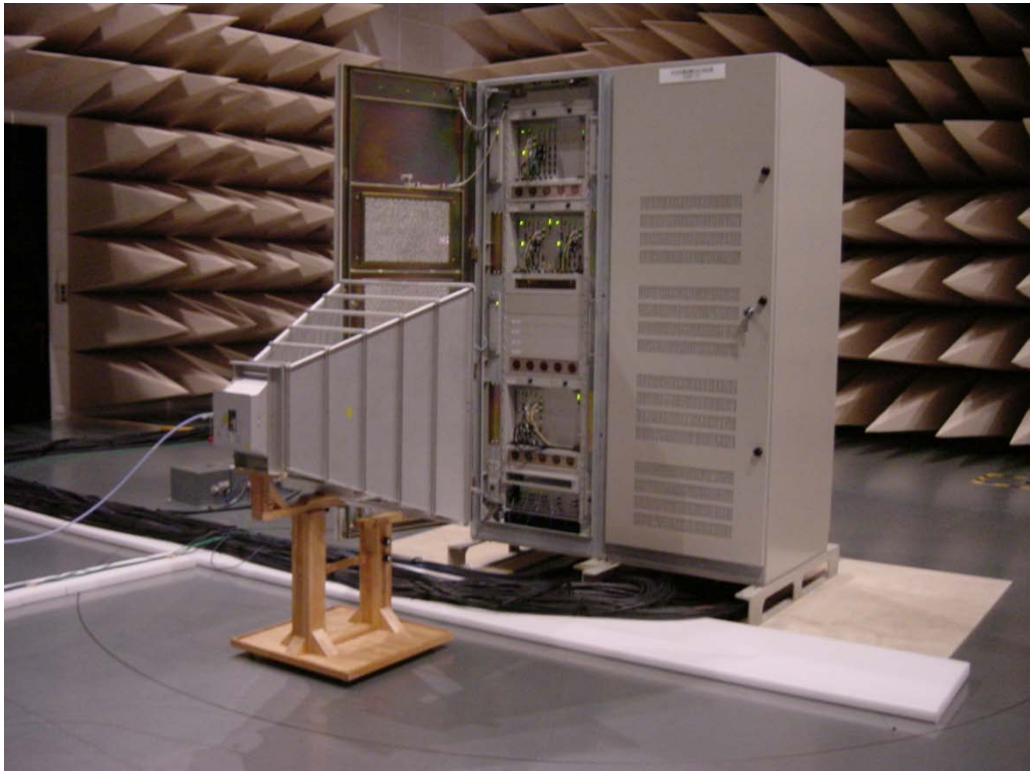
Equipment Qualification (1/2)

- PSMS and other safety-related components are qualified by type tests to generic environmental and seismic conditions that are expected to envelope all potential sites
- Testing is performed in accordance with applicable industry standards (IEEE Std. 323, 344) and regulatory requirements (RG 1.89)
- ITAAC verifies the qualification test results envelope actual site specific conditions
- Instrument sensing lines comply with RG 1.151 which endorses ANSI/ISA S67.02, including freeze protection
- Lines that are connected to ASME Class 1 or 2 process piping or vessels are designed as ASME Class 2 Seismic Category I

5. Safety Criteria Conformance

Equipment Qualification (2/2)

- **Environmental Test**
  - ✓ Mild Environment
  - ✓ Temperature / Humidity
- **Seismic Test**
  - ✓ OBE/SSE requirements are satisfied
  - ✓ Conformance to IEEE Std 344
- **Electromagnetic Compatibility Test**
  - ✓ Conformance to RG 1.180



Secure Development and Operational Environment (SDOE) (1/3)

- **Security of all PSMS software complies with SDOE requirements of RG 1.152**
  - ✓ During development by the independent V&V and configuration control processes defined in the “Software Program Manual”, MUAP-07017, which also encompasses MELTAC Basic Software
  - ✓ During operation by system design features (e.g., locked doors, alarms, module removal restrictions) and Memory Integrity Checks
- **Compliance to the SDOE requirements of RG 1.152 assures:**
  - ✓ Unintended functions have not been introduced at any point in PSMS software development
  - ✓ System contains design features that prevent and detect unintended alterations during its operation

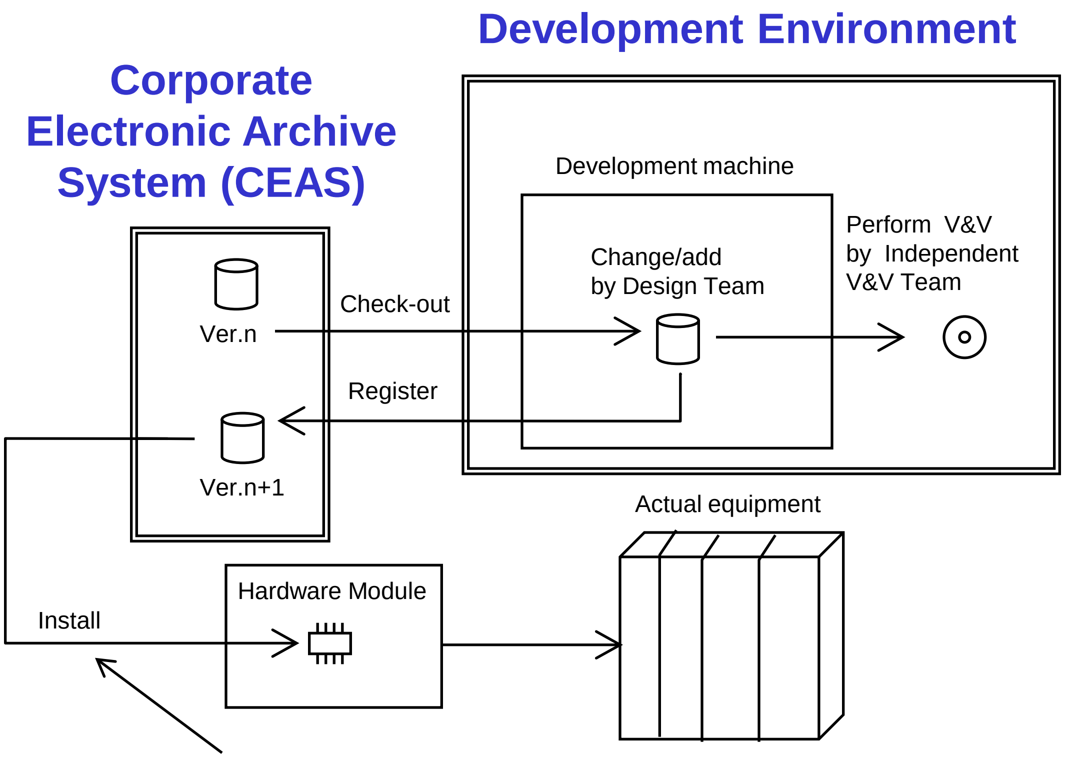
5. Safety Criteria Conformance

SDOE (2/3)

- **All safety functions of PSMS are installed in non-volatile memory that cannot be altered in any manner while operating**
- **PSMS software changes require:**
  - ✓ Equipment room access (locked and alarmed)
  - ✓ Cabinet access (locked and alarmed)
  - ✓ Module removal (alarmed and controlled by Tech Specs)
  - ✓ Module reprogramming in external chassis
  - ✓ Module reinstallation (alarmed)
- **Redundant PSMS divisions are geographically separated in four I&C equipment rooms**
- **Unintended software changes are detectable by the periodic Memory Integrity Check**

US-APWR

SDOE (3/3)



✓Confirmed that data written to the device is same as data stored in CEAS

- **Corporate Electronic Archive System (CEAS)**
  - ✓Stores basic software and application software
  - ✓Access control by password
  - ✓Physically secured
  - ✓System does not allow file delete or change (write only)
  - ✓Periodic backup
- **Development Environment**
  - ✓Access control to development machine by password
  - ✓Entry/exit control of the development area
  - ✓Isolated from the corporate network

6. Open Items

Status of SER Open Items (1/3)

RAI No.	RAI Topic/ NRC Concern	Status
RAI 568-4588	Selection criteria of PAM should be refined	RAI response under NRC review
RAI 753-5742	Basis for the inputs and assumptions used in D3 Coping Analysis	RAI response under NRC review
RAI 992-6999	1.Sufficient evidence to demonstrate that the use of O-VDUs enhance the performance of the safety system 2.ITAAC that adequately verifies testing for normal and abnormal data transmission conditions for all non-safety to safety interfaces	1.MHI will provide RAI response demonstrating safety merit of O-VDU, including quantitative analysis for reduced task burden 2.MHI will add new ITAAC for communication faults

6. Open Items

SER Open Items (2/3)

RAI No.	RAI Topic/ NRC Concern	RAI Response/ DCD Impact
RAI 995-7024	Process to flow down the requirements for MELTAC platform hardware/ software components	RAI response under NRC review
RAI 993-7027	Process to ensure vendor’s safety software development process	RAI response under NRC review
RAI 988-7021	Basis for the inputs and assumptions used in D3 Coping Analysis	RAI response under NRC review

6. Open Items

SER Open Items (3/3)

RAI No.	RAI Topic/ NRC Concern	RAI Response/ DCD Impact
RAI 996-7040	How the plant would be adequately protected from each PCMS failure, including single failures and design defects (i.e., potential software CCFs)	MHI will provide RAI response demonstrating that transients causing PCMS single failures are bounded by AOOs in DCD Ch. 15, and transients caused by potential basic software CCFs are bounded by PAs in DCD Ch. 15

7. Summary

- **Digital I&C Systems provide significant advancements;**
  - ✓ Higher availability
  - ✓ Higher accuracy
  - ✓ Lower potential for human error
  - ✓ Better performance
  - ✓ Improved operator command & control capability
  - ✓ Reduction of maintenance workload & resources
- **The US-APWR employs proven digital designs with many years of demonstrated reliability in Japan**
- **Conventional DAS ensures plant safety is maintained if all digital systems fail**
- **MHI is working closely with NRC to complete US licensing**

List of Acronyms (1/2)

A/I	Analog Input
ALR	Automatic Load Regulator
AOO	Anticipated Operational Occurrence
APWR	Advance Pressurized Water Reactor
ATWS	Anticipated Transient without Scram
AVR	Automatic Voltage Regulator
BISI	Bypass and Inoperable Status Indication
BTP	Branch Technical Position
BOP	Balance of Plant
CCF	Common Cause Failure
CCW	Component Cooling Water
CDF	Core Damage Frequency
CEAS	Corporate Electronic Archive System
CH	Channel
CHP	Charging Pump
COL	Combined License
COM	Communication Subsystem
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRDM	Control Rod Drive Mechanism
CS	Containment Spray
C/V	Containment Vessel
CVCS	Chemical Volume Control System
D-RAP	Design Reliability Assurance Program
D3	Defense in Depth and Diversity
D/A	Digital to Analog Convertor
DAS	Diverse Actuation System
DAAC	Diverse Automatic Actuation Cabinet
DCD	Design Control Document
DHP	Diverse HSI Panel
D/I	Digital Input
DI&C	Digital I&C
D/O	Digital Output
DTM	Design Team Manager
ECCS	Emergency Core Cooling System
EFW	Emergency Feed Water
EHG	Electric Hydraulic Governor
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
E/O	Electrical to Optical or Optical to Electrical
EOF	Emergency Operating Facility
EOP	Emergency Operating Procedure
ERDS	Emergency Response Data System
ESD	Electrostatic Discharge
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FPAG	Field Programmable Gate Array
F-ROM	Flash Electrically Erasable Programmable Read Only Memory
GTG	Gus Turbine Generator
HFE	Human Factors Engineering
HSI	Human System Interface
HSIS	Human System Interface System
HVAC	Heating, Ventilation and Air Conditioning
H/W	Hardware
HX	Heat Exchanger
I&C	Instrumentation and Control
I/F	Interface
I/O	Input/Output
IR	Intermediate Range
ISG	Interim Staff Guidance
ISO	Isolation
IT	Information Technology
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria

List of Acronyms (2/2)

LCO	Limiting Conditions for Operation
LDP	Large Display Panel
LOOP	Loss of Offsite Power
MCC	Motor Control Center
MCCB	Molded Case Circuit Breaker
MCP	Main Control Panel
MCR	Main Control Room
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MFW	Main Feed Water
M/G	Motor Generator
MGL	Multi Greek Letter
MHI	Mitsubishi Heavy Industries, Ltd.
MIC	Memory Integrate Check
MNES	Mitsubishi Nuclear Energy System, Inc.
MRP	MELTAC Re-evaluation Program
MTBF	Mean Time Between Failure
NIS	Nuclear Instrumentation System
NFB	No Fuse Breaker
OBE	Operational Basis Earthquakes
O/E	Optical/Electrical Converter
OLM	On-Line Maintenance
O-VDU	Operational VDU
PA	Postulated Accident
PAM	Post Accident Monitoring
PCMS	Plant Control and Monitoring System
PIF	Power Interface
PR	Power Range
PRA	Probability Risk Assessment
PSMS	Protection and Safety Monitoring System
QA	Quality Assurance
QAP	Quality Assurance Program
RAM	Random Access Memory
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
ROM	Read Only Memory
RPS	Reactor Protection System
RSR	Remote Shutdown Room
RT	Reactor Trip
RTB	Reactor Trip Breaker
SDCV	Spatially Dedicated Continuously Visible
SDOE	Secure Development and Operational Environment
SG	Steam Generator
SIS	Safety Injection System
SLS	Safety Logic System
SPDS	Safety Parameter Display System
SPM	Software Program Manual
SR	Source Range
SSA	Signal Selector Algorithm
SSE	Safe Shutdown Earthquake
STS	Standard Technical Specifications
S-VDU	Safety VDU
S/W	Software
TADOT	Trip Actuation Device Operability Test
TR	Topical Report
T-Spec.	Technical Specification
TSC	Technical Support Center
UPS	Uninterruptible Power Supply
UV	Under Voltage
VCT	Volume Control Tank
VDU	Visual Display Unit
V&V	Verification and Validation
WDT	Watchdog Timer

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Presentation to the ACRS Subcommittee

US-APWR Design Certification Application Review

Safety Evaluation Report with Open Items

Chapter 7: Instrumentation and Controls

April 25-26, 2013

Objective and Expected Outcome

Objective

- Brief the Subcommittee on the staff’s review of the US-APWR instrumentation and control (I&C) system

Expected Outcome

- Common understanding of the background, the staff’s evaluation efforts, and the current status of the US-APWR I&C system review

Staff Review Team

Technical Staff from NRO/DE/ICE2

Dinesh Taneja

Joseph Ashcraft

Khoi Nguyen

Erick Martinez

Tung Truong

Project Managers

William Ward

Jeff Ciocco

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Presentation Outline

- **Introduction**
- **Background**
- **Key Technical Topics of Interest**
  - Redundancy
  - Independence
  - Determinism
  - Defense-in-Depth and Diversity
  - Simplicity

Presentation Outline
(Continued)

- **Other Technical Topics**
  - Software program manual
  - Post accident monitoring (PAM) instruments
  - Non-safety PCMS failures' impact on safety
- **Non-Concurrence**
- **Discussion/Committee Questions**

Introduction

- MHI submitted the US-APWR design certification application on December 31, 2007
- Safety evaluation and related reports represent over five years of effort
- Oak Ridge National Lab was initially contracted for technical support

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Introduction
(Continued)

- **In April 2010, the I&C review was on critical path due to significant technical issues and challenges:**
  - Applicant's original strategy of receiving generic review/approval of MELTAC digital I&C platform was a factor
  - MELCO, MHI's subcontractor and developer of MELTAC platform, did not have an Appendix B program, which impacted the staff review
  - There were a significant number of unresolved RAIs
  - Data communication independence was a significant challenge

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Introduction
(Continued)

- **A closure plan was developed in August 2010 for resolving key issues including:**
  - Identification and resolution of outstanding RAIs
  - Topical Reports MUAP-07004 and MUAP-07005 converted to Technical Reports as part of the US-APWR design certification I&C design
  - SPM revised to address US-APWR software QA issues, including MELTAC Basic and Application software
  - Key digital I&C design principles emphasized
- **MELCO established Appendix B program for building safety-related MELTAC platform**

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Introduction
(Continued)

- **Two Significant Audits**
  - Kobe, Japan and Arlington, Virginia

  - ➢ Data communication independence
  - ➢ Deterministic performance of digital I&C systems including implementation of watchdog timers
  - ➢ US-APWR software development process
  - ➢ Integration of MELTAC basic software into the US-APWR application software for safety I&C systems
  - ➢ MELTAC test reports on products developed for the Japanese nuclear plants
- ➢ Draft US-APWR emergency response guidelines used for determining the required PAM variables

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Status Overview

SRP Section / DCD Section		No. of Open Items	Brief Description of Open Item
7.1	Introduction	2	1. QA of vendors' safety Software 2. MELTAC Platform - CGD
7.2	Reactor Trip System		
7.3	Engineered Safety Features Systems		
7.4	Systems Required for Safe Shutdown		
7.5	Information Systems Important to Safety	1	Bases for PAM Variables
7.6	Interlocks Important to Safety		
7.7	Control Systems Not Required for Safety	1	PCMS failures' impact on safety
7.8	Diverse I&C Systems	1	D3 Coping Analysis
7.9	Data Communication Systems	1	Manual controls of safety components from O-VDU
Total		**6**	

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Background

Major Documents Reviewed

Doc. Number	Title	Revision
Docket 52-021	US-APWR DCD FSAR, Tier 1 Section 2.5; and Tier 2 Chapter 7	3
MUAP-07004P	Safety I&C System Description and Design Process Technical Report	7
MUAP-07005P	Safety System Digital Platform -MELTAC- Technical Report	8
MUAP-07006P	Defense-in-Depth and Diversity Topical Report	2-Acc
MUAP-07014P	Defense-In-Depth and Diversity Coping Analysis Technical Report	5
MUAP-07017P	US-APWR Software Program Manual	4
MUAP-09021P	US-APWR Response Time of Safety I&C Systems	2
MUAP-09022P	US-APWR Instrument Setpoint Methodology	2

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Significant Technical Issues of the Original Design

- Complex architecture
- Bi-directional data communication between safety and non-safety systems
- Continuous connection between safety systems and maintenance network
- Capabilities to make on-line software changes
- Diverse actuation system (DAS) 2-out-of-2 logic
- Use of time-critical manual actions from DAS

Major Design Changes

- Data communication from non-safety to safety systems reduced
  - ➢ Now limited for manual control of safety components (Open Item)
- Automatic signals from non-safety to safety systems hardwired through Class 1E isolators
- Interface between PSMS and maintenance network changed to temporary connection

Major I&C Design Changes
(Continued)

- Software changes made off-line
- Enable/Disable switch added that provides capability to disconnect all non-safety signals going to safety-systems
- DAS upgraded to four cabinets and actuated using 1-out-of-2 taken twice logic

Major Design Changes
(Continued)

- Time-critical DAS manual actuations converted to automatic
- Priority logic employed throughout safety components
- Additional data communication design details added to DCD and technical reports

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Redundancy

- US-APWR I&C Safety Systems
  - PSMS - sustains a single failure and completes its safety function
  - Meet GDC 21 & 24, and Section 5.1 of IEEE Std. 603-1991
  - Have single-failure ITAAC
- Staff's evaluation in Sections 7.1.4.1.1.2, 7.1.4.1.2, 7.1.4.2.2, and additional sections scattered throughout Sections 7.2 through 7.9 of the safety evaluation

Redundancy
(Continued)

- **Regulations and Guidance**
  - GDC 21 & 24
  - 10 CFR 50.55a(h)
  - IEEE Std. 603-1991, Section 5.1
  - RG 1.53 / IEEE Std. 379-2000

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Redundancy
(Continued)

- **PSMS**
  - Redundancy between trains
  - Redundancy within divisions and systems
  - System level failure modes and effects analysis (FMEA)
- **PCMS**
  - Duplex redundant
  - Input and Output (I/O) redundancy

Independence

- Physical Independence
- Electrical Independence
- Functional Independence
- Communication Independence

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

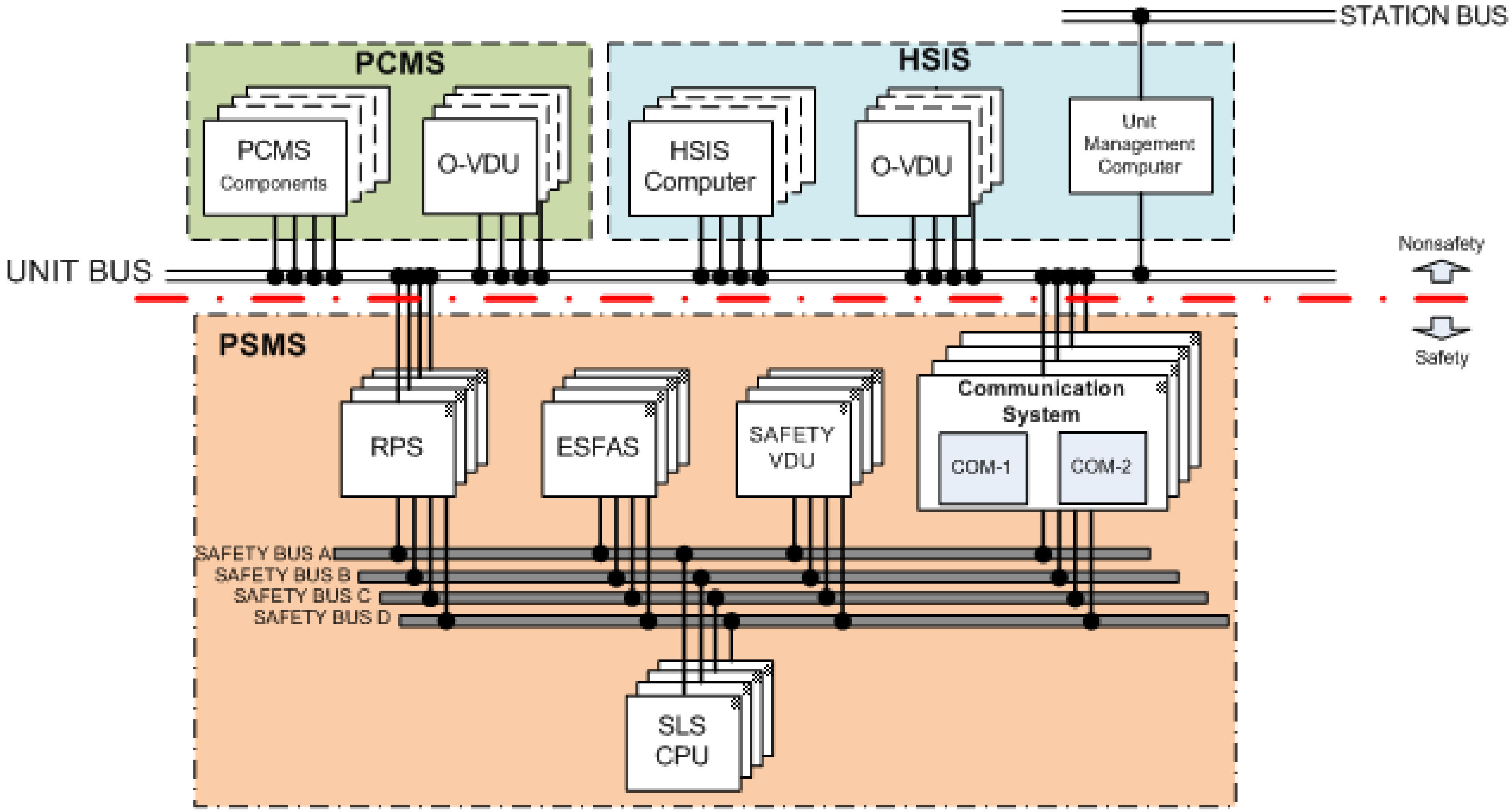
Independence
(Continued)

- **Communication Independence**
  - Among safety trains
  - Between safety and non-safety systems

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Independence
(Continued)

- **Data Communication Interfaces**



DCS Interface Configuration

United States Nuclear Regulatory Commission
Protecting People and the Environment

Independence
(Continued)

- **Regulations and Guidance**
  - 10 CFR 50.55a(h)
  - GDC 22 & 24
  - IEEE Std. 603-1991, Section 5.6
  - SRP 7.9
  - DI&C-ISG-04
  - RG 1.152 / IEEE Std. 7-4.3.2-2003

Independence
(Continued)

- **Independence among Safety Trains**

Design Features Supporting the Staff Findings

- Limited to voting logic, bypass status, and message authentication status
- One-way point-to-point data link protocol with no communication handshaking
- Failure or communication fault of a single train does not affect the other trains

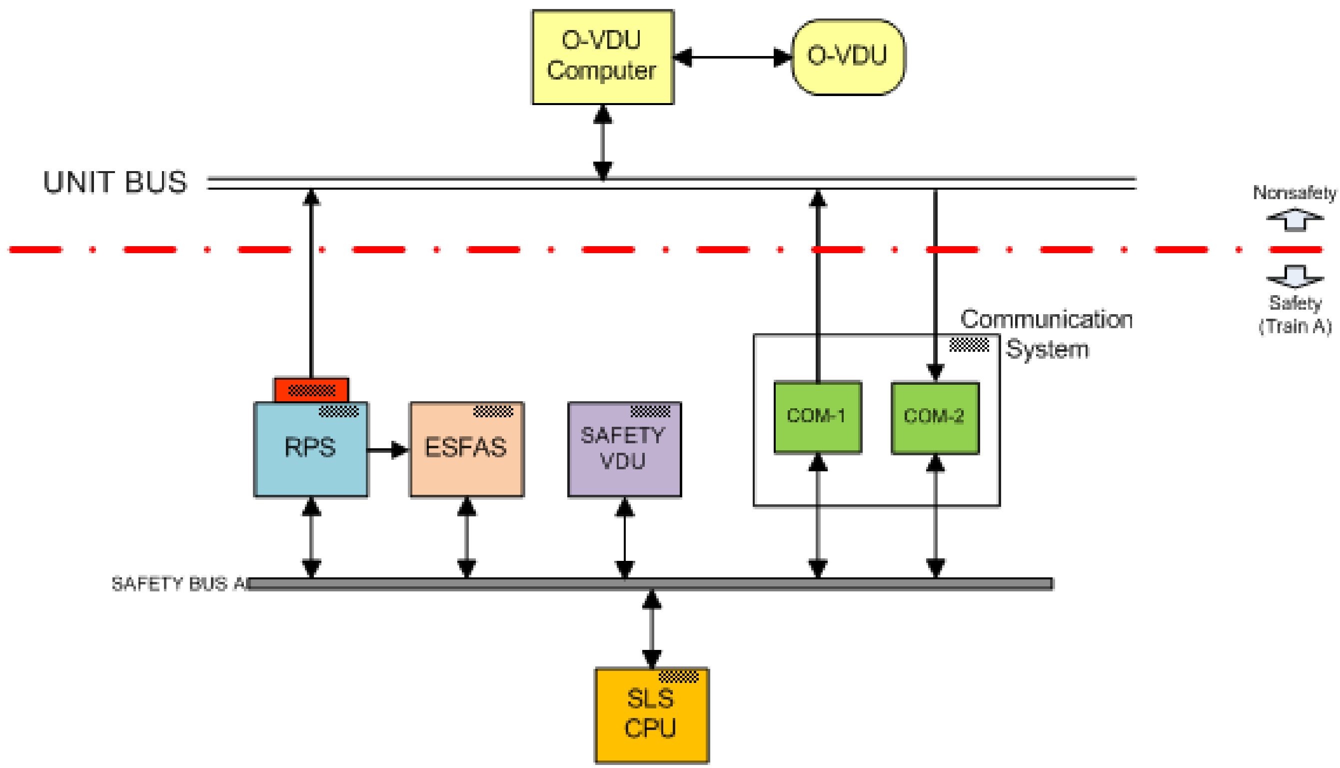
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Independence
(Continued)

- All safety functions are performed without interruption by any other signals. The priority logic provides prioritization of safety signals for safety functions over other signals
- All communications are performed utilizing 2-port memory
- The communication processor is separated from the functional processor

Independence
(Continued)

- **Independence between Safety and Non-safety Systems**



Communication Between Safety and Non-safety Systems

Independence

(Continued)

- **Data Communications through COM-2**
  - Manual control commands of safety components from the O-VDU
  - Manual operating/maintenance bypass, lock, and reset commands from the O-VDU

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Independence
(Continued)

- **Design Features Supporting the Staff Findings**
  - DI&C-ISG-04 is the key guidance used

    Note: Staff evaluation of conformance to ISG-04 can be found in Table 7.9.4-1 of the SE

  - All safety functions, whether manual or automatic, are performed without being interrupted by non-safety signals, regardless of whether these non-safety signals are valid or erroneous. The priority logic provides prioritization of safety signals for safety functions over non-safety signals (ISG-04, Staff Position 1)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Independence
(Continued)

- The communication controller is separate from the functional processor that performs safety functions (ISG-04, Staff Position 4)
- Communications between the control network module and the CPU module are performed via a 2-port memory to ensure no disruption of the CPU's deterministic operation (ISG-04, Staff Position 4)
- Desired data are transmitted in fixed format, fixed length, and predefined message (ISG-04, Staff Position 15)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Independence

(Continued)

- Erroneous data are limited by using data checks (ISG-04, Staff Position 12)

- The execution of all basic software functions is monitored and verified continuously for deterministic cycle time performance by an external hardware watchdog timer, which detects anomalies and forces fail-safe processing termination (ISG-04, Staff Position 5)

- Watchdog timer ensures that a locked-up controller is shifted to the fail-safe mode

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Independence
(Continued)

- **NRC Audits**
  - Reviewed un-docketed documents
  - Confirmed key design features described in the DCD
  - Witnessed demonstrations on actual MELTAC controllers to address the staff's concerns

United States Nuclear Regulatory Commission
Protecting People and the Environment

Independence
(Continued)

- **Open Item**
  - ➢ The applicant is asked to justify the use of non-safety component to operate safety equipments
    - \- Sufficient evidence associated with the HFE full scope simulator testing or a quantitative analysis to demonstrate that the use of O-VDU to operate safety equipment enhances the performance of the safety function
    - \- Provide an ITAAC to test normal and abnormal data transmission conditions for all non-safety to safety interfaces

Determinism

- **Regulations and Guidance**
  - 10 CFR 50.55a(h)
  - IEEE Std. 603-1991, Section 4.10
  - SRP BTP 7-21

Determinism
(Continued)

- **Staff's Review**
  - Software failures or system malfunctions are accommodated by the MELTAC internal diagnostic functions and the built-in watchdog timers
  - All functions execute with cyclical single task processing
  - Cycle times are pre-determined and fixed for all MELTAC processors with the same sequence of processing steps in each cycle
  - Message sizes and communication rates are constant, resulting in constant communication loads under all circumstances

Determinism
(Continued)

- Communication independence features ensure deterministic processing, that cannot be disrupted by other PSMS trains or the Unit Bus
- No external interrupts exist. There are two internal interrupts; CPU module & peripheral
- Processing is monitored for deterministic cycle time performance by a hardware based external watchdog timer, which detects anomalies and forces fail safe processing termination

Note: In safety evaluation Section 7.1.4.2.3, real-time performance is evaluated using SRP BTP 7-21 guidance

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Determinism
(Continued)

- **Response Time Analysis**
  - MUAP-09021, “US-APWR Response Time of Safety I&C System,” is evaluated using SRP BTP 7-21 guidance in Section 7.1.4.7 of the safety evaluation
  - Safety system response times in Chapter 15 are the analytical limits and are specified as allocated response times for each safety function
  - Total MELTAC response time accounts for all network components and data communication interfaces

Determinism

(Continued)

- Maximum and minimum controller response times are calculated to demonstrate compliance with allocated times
- In test phase, system response time is confirmed by measurement
- Final response time is verified through ITAAC

Defense-in-Depth and Diversity

- **Diverse Actuation System (DAS) Design Features**
  - Non-safety analog hardwired system that is independent from the PSMS and PCMS to cope with potential software common cause failures
  - Four diverse automatic actuation cabinets designed as Seismic Category I are located in separate Class 1E electrical rooms; and powered by Class 1E UPS power source
  - Uses a 1-out-of-2 taken twice voting logic
  - Automatic/manual actuation functions and indications included on the diverse HSI panel located in the main control room

Defense-in-Depth and Diversity
(Continued)

- **Policy and Guidance**
  - SRM on SECY-93-087
  - DI&C-ISG-02
  - DI&C-ISG-05
  - SRP 7.8
  - SRP BTP 7-19

Defense-in-Depth and Diversity

(Continued)

- **Staff's review**
  - MHI previously submitted Topical Report, MUAP-07006, "Defense-in-Depth and Diversity," which has been approved by the staff with the Application Specific Action Items (ASAIs)
  - For the US-APWR design, the applicant referenced MUAP-07006 and submitted MUAP-07014, "D3 Coping Analysis"
  - Functions performed by DAS are based on a best-estimate D3 coping analysis
  - Review of the D3 coping analysis is coordinated with the experts in human factors and reactor systems

Defense-in-Depth and Diversity
(Continued)

- **DAS design changes**
  - Changed diverse ECCS actuation from manual to automatic
  - Upgraded seismic classification to Category I
  - Changed DAS cabinets from two to four
    - Actuation logic changed from 2-out-of-2 to 1-out-of-2 taken twice
  - Upgraded other design features to address internal and external hazards

Defense-in-Depth and Diversity
(Continued)

- **Open Item**
  - Outstanding RAIs are related to the review of the D3 coping analysis
  - Reactor Systems is evaluating or awaiting responses to the RAIs

Simplicity

- **Staff Review Approach**
  - ➢ Staff guidance discusses simple means to address hazards for specific design aspects like data communications
  - ➢ More complex design alternatives require a more in-depth and detailed review by the staff
- **Design Changes**
  - ➢ The applicant proposed multiple design changes to reduce design complexity

Simplicity
(Continued)

- **Design Attributes**
  - A single platform (MELTAC) is utilized for the entire plant
  - DAS is a hardwired analog system
  - All functions are executed with cyclical single task processing and no external (outside of the PSMS) interrupts
  - All the software modules are executed during a fixed cycle time in a predefined order
  - Application software is written in a graphically symbolized manner, so that functions can be easily understood, verified and validated
  - No dynamic allocation of memory exists

Software Program Manual

- **Background**
  - US-APWR SPM describes the software life cycle processes used to develop PSMS software; this description is provided through 12 software plans in the SPM
  - Majority of software plans in the SPM are also applicable to PCMS (augmented quality)

Software Program Manual
(Continued)

- **Regulations and Guidance**
  - 10 CFR 50.55a(a)(1)
  - GDC 1
  - 10 CFR 50 Appendix B
  - RG 1.152 (IEEE Std. 7-4.3.2-2003)
  - SRP BTP 7-14 (IEEE Std. 603-1991)

Software Program Manual
(Continued)

- **Staff Review**
  - Reviewed 12 software plans in the SPM against SRP BTP 7-14
  - Reviewed secure development and operational environment against RG 1.152, Revision 3
- **Open Item**
  - The staff requested applicant explain or describe the process it plans to use to ensure that its vendor’s safety software development process and the resulting software conform to NRC regulation and guidance. In addition, the staff requested that the applicant include an ITAAC to provide verification of such a process

Post Accident Monitoring

- **Background**
  - MHI decided to identify performance based list of PAM variables in the DCD
  - Function of PAM variables is to aid the operator in rapid detection of abnormal operating conditions
  - PAM variables represent a minimum set of plant parameters needed to asses plant safety status
  - Staff is working closely with experts in Human Factors, Reactor Systems, Technical Specification, and Containment Design for reviewing the list of PAM variables
  - Audited draft US-APWR Emergency Response Guidelines used as one of the bases for the PAM list

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Post Accident Monitoring
(Continued)

- **Regulations and Guidance**
  - 10 CFR 50.34(f), “Additional TMI-Related Requirements” applies to accident monitoring instrumentation
  - RG 1.97, Rev. 4 (guidance for selecting performance based list of PAM variables)
  - SRP BTP 7-10 (guidance on application of RG 1.97)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Post Accident Monitoring
(Continued)

- **Open Item**
  - ➢ Revised draft RAI response received in April 2013 is being reviewed
  - ➢ Staff is working with the applicant in resolving limited number of remaining issues
    - Use of alarms for credited manual operator actions
    - Adequacy of using containment pressure to determine containment integrity
  - ➢ Staff is working with experts in Human Factors, Reactor Systems, and Containment Design for reviewing this open item

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

PCMS Failures' Impact on Safety

- **Background**
  - SRP Section 7.7 states, in part, that failure of any control system component should not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the DCD
- **Open Item**
  - To assure that this concern is addressed, the staff asked the applicant to provide additional information on the effects of control system failures (including software common cause failures) on the safety function

Non-Concurrence

(NCP-2012-007)

- **Background**

  Employee submitted non-concurrence on Chapter 7 safety evaluation raising issues with:

  - Commercial grade dedication of MELTAC System
  - MELTAC Basic software lifecycle development process
  - US-APWR data communication system

Non-Concurrence

(Continued)

- **Actions taken**
  - Followed the non-concurrence implementation guidance outlined in NRC MD 10.158
  - Asked applicant to verify that all MELTAC technical and quality requirements are identified in the DCD; and provide ITAAC to verify and validate the as-built safety I&C system in conformance with the specified technical and quality requirements

United States Nuclear Regulatory Commission
Protecting People and the Environment

Non-Concurrence
(Continued)

- Asked applicant to ensure that its vendors' safety software development process and resulting software conform to the NRC regulations and guidance; and provide ITAAC to verify such a process
- Asked applicant to demonstrate that multi divisional control of safety components from O-VDU result in enhancement of safety function performance; and provide ITAAC for testing normal and abnormal data transmission conditions for all non-safety to safety interfaces

Note: All actions taken to address non-concurrence are being tracked as Open Items

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Discussion / Committee Questions

List of Acronyms

APWR	Advanced Pressurized Water Reactor
ASAI	Application Specific Action Item
BTP	Branch Technical Position
CCF	Common Cause Failure
CGD	Commercial Grade Dedication
COM	Communication System
CPU	Central Processing Unit
D3	Defense-in-Depth and Diversity
DAS	Diverse Actuation System
DCD	Design Control Document
DCS	Data Communication System
DI&C	Digital Instrumentation and Control
ECCS	Emergency Core Cooling System
ESFAS	Engineered Safety Features Actuation System
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array

List of Acronyms
(Continued)

F-ROM	Flash Electrically Erasable Programmable Read Only Memory
FSAR	Final Safety Analysis Report
GDC	General Design Criteria
HFE	Human Factors Engineering
HSIS	Human System Interface System
I&C	Instrumentation and Control
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
ISG	Interim Staff Guidance
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MHI	Mitsubishi Heavy Industries, Ltd.
O-VDU	Operational Visual Display Unit
PAM	Post Accident Monitoring
PCMS	Plant Control and Monitoring System

List of Acronyms
(Continued)

PRA	Probability Risk Assessment
PSMS	Protection and Safety Monitoring System
QA	Quality Assurance
RAI	Request for Additional Information
RAM	Random Access Memory
RCS	Reactor Coolant System
RG	Regulatory Guide
ROM	Read Only Memory
RPS	Reactor Protection System
SE	Safety Evaluation
SLS	Safety Logic System
SPM	Software Program Manual
SRP	Standard Review Plan
S-VDU	Safety Visual Display Unit
UPS	Uninterruptible Power Supply

Reference Slides

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Descriptions of Open Items

Open Item	Brief Description
RAI 993-7027, Question 07-56	Oversight of vendors’ safety software development process
RAI 995-7024, Question 07.01-45	MELTAC platform and CGD issues
RAI 996-7040, Question 07.07-33	Impact of PCMS failures’ on safety functions
RAI 992-6999, Question 07.09-26	Bases for manual control of safety components from O-VDU, and testing of normal and abnormal data transmission conditions for all non-safety to safety interfaces
RAI 568-4588, Question 07.05-18	Bases for PAM variables
RAI 753-5742, Question 07.08-17 to 22 RAI 988-7021, Question 07.08-26 to 30 RAI 7045 Question 24724-24727 RAI 7066 Questions 24764-24767 & 24771	D3 coping analysis

LUMINANT GENERATION COMPANY

Comanche Peak Nuclear Power Plant, Units 3 and 4

ACRS, US-APWR Subcommittee

FSAR Chapter 7 – Instrumentation and Controls

April 25, 2013

Agenda

- Introduction
- Site-Specific Aspects
- Summary

Introduction

- COLA uses “Incorporated by Reference” methodology
- No departures from the US-APWR DCD for FSAR Chapter 7
- CPNPP COLA Revision 2 submitted in June 2011 and Revision 3 in June 2012
- No contentions pending before ASLB

Sections That Are 100% IBR

Sections 7.0 - 7.3 and 7.6 - 7.9 are IBR with no departures or supplements

7.4 Systems Required for Safe Shutdown

- CPNPP COLA FSAR Summary
  - Addresses site-specific component control and indication to achieve safe shutdown as related to UHS
- NRC SER Summary
  - No outstanding issues

7.5 Information Systems Important to Safety

- CPNPP COLA FSAR Summary
  - Addresses site-specific type D PAM variables related to UHS
  - Addresses site-specific type E PAM variables for monitoring meteorological parameters
  - Describes CPNPP Units 3 and 4 EOF

- NRC SER Summary
  - No outstanding issues

Acronyms

ASLB	Atomic Safety and Licensing Board
COLA	Combined License Application
CPNPP	Comanche Peak Nuclear Power Plant
DCD	Design Control Document
EOF	Emergency Operations Facility
FSAR	Final Safety Analysis Report
IBR	Incorporated by reference
PAM	Post-accident monitoring
R-COLA	Reference Combined License Application
SER	Safety Evaluation Report
UHS	Ultimate heat sink
US-APWR	United States Advanced Pressurized Water Reactor

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Presentation to the ACRS Subcommittee

Comanche Peak Nuclear Power Plant, Units 3 and 4
COL Application Review

Safety Evaluation Report

CHAPTER 7: Instrumentation and Controls

April 25-26, 2013

Staff's Presentation Order

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **Stephen Monarque** - Comanche Peak COLA Lead Project Manager
- **William Ward -** Project Manager
- **Eugene Eagle** – Instrumentation and Controls Branch

Chapter 7 Instrumentation and controls

- No Open items

LUMINANT GENERATION COMPANY

Comanche Peak Nuclear Power Plant, Units 3 and 4

ACRS US-APWR Subcommittee

FSAR Sections

2.0 Site Characteristics

2.1 Geography and Demography

2.2 Nearby Industrial, Transportation, and Military Facilities

2.3 Meteorology

April 26, 2013

Agenda

- Introduction
- SER Open Item
- Site-Specific Aspects

Introduction

- FSAR uses IBR methodology
- No departures from US-APWR DCD Sections 2.0-2.3
- All COL Items addressed in FSAR
- One SER Open Item
- No SER Confirmatory Items
- No contentions pending before ASLB

SER Open Item

Open Item 2.3.4 Changes to Sections 2.0-2.3

Luminant submitted changes to FSAR Sections 2.0-2.3 in February 2013 to provide atmospheric dispersion updates due to standard plant changes

Resolution – NRC Staff will review the change

Luminant

US-APWR

MNES
MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC.

Site-Specific Aspects

2.0 Site Characteristics

All key site parameters are enveloped by DCD

2.1 Geography and Demography

- Proposed CPNPP Units 3&4 site is co-located with operating CPNPP Units 1&2
- 7950-ac site located in north central Texas, 40 miles southwest of downtown Fort Worth
- Nearest population center is Cleburne, Texas located 24 miles east

2.2 Nearby Industrial, Transportation, and Military Facilities

- CPNPP Units 3&4 design is bounded by DCD Section 2.2
- Evaluated Design Basis Events for hazardous materials and activities in the vicinity of the site
- No additional mitigation required

2.3 Meteorology

- Hurricanes - One hurricane has been recorded within 50 miles of the CPNPP site since 1851: a Category 1 hurricane in 1900 with winds of ~65 mph as it passed within 50 miles of the site location.
  - Maximum hurricane site characteristics are bounded by the US-APWR DCD based on RG 1.221.
- Tornadoes are the more likely concern for the CPNPP site. In the 56-year period from 1950 to 2006, 3 tornadoes were reported in Somervell County (the location of the site).
  - Maximum tornado site characteristics are bounded by the US-APWR DCD based on RG 1.76.

Acronyms

ASLB	Atomic Safety and Licensing Board
CPNPP	Comanche Peak Nuclear Power Plant
DCD	Design Control Document
FSAR	Final Safety Analysis Report
IBR	Incorporated by reference
SER	Safety Evaluation Report
US-APWR	United States Advanced Pressurized Water Reactor

Presentation to the ACRS Subcommittee

Comanche Peak Units 3 & 4 Combined License Application Review

SER/OI Chapter 2

Section 2.1 –Geography and Demography
Section 2.2 –Nearby Industrial , Transportation, and Military Facilities
Section 2.3 – Meteorology

April 26, 2013

Staff Review Team

- Technical Staff
  - Tech Reviewer Name
    RPAC Branch: Seshagiri Rao Tammara
  - RHMB Branch: Kevin Quinlan
- Project Managers
  - Lead PM: Stephen Monarque
  - Chapter PM: Tarun Roy

2.1 Geography, Demography

- DCD Incorporated By Reference
  - Site specific information
    - Site Location
    - Exclusion Area Boundary (EAB)
    - Population Distribution, Projections, Population Center and Population Density
  - Conclusions

2.2 Nearby Facilities

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

2.2.1-2.2.2 Location and Description

- DCD Incorporated By Reference

- Site specific information
  - Nearby Industrial, Transportation, and Military Facilities
  - Pipelines
  - Gas wells
  - CPNPP Un its 1 and 2
  - Onsite chemical storage facilities

- Conclusions

2.2 Nearby Facilities (Con'd)

2.2.3 Evaluation of Potential Accidents

- The evaluation of potential hazards to new units 1 and 2 due to potential accidents from nearby facilities, pipelines, and transportation routes.
- The evaluation of potential toxic chemical releases from nearby facilities, transportation routes and onsite storage for the control room habitability of new units 3 and 4.

- DCD Incorporated By Reference
  - Onsite storage of Chemicals
- Site Specific Evaluations
  - Explosions
  - Fires
  - Gas Pipelines
  - Collision with intake structures
  - Aircraft hazards
  - Liquid Spills
  - Toxic Chemicals (Control Room Habitability)
- Conclusions

Meteorology

United States Nuclear Regulatory Commission
Protecting People and the Environment

- **2.3 – Meteorology**

- FSAR Chapter 2.3 incorporates by reference Revision 3 of the US-APWR DCD.

- COL items and Supplemental Information
  - CP COL 2.3(1) – Site Meteorology
    - Addressed in Subsections 2.0, 2.3.1, and 2.3.2
  - CP SUP 2.3(1) – Comparison of Site Parameters Versus Site Characteristics
  - CP COL 2.3(2) – Short Term Atmospheric Transport and Diffusion
    - Addressed in Subsections 2.0 and 2.3.4
  - CP COL 2.3(3) – Long Term Atmospheric Transport and Diffusion
    - Addressed in Subsections 2.0 and 2.3.5

Meteorology

- **Technical Topics of Interest**
  - **2.3.1 Regional Climatology**
    - All CPNPP site characteristic values presented in FSAR Section 2.3.1 have been found to be acceptable
      - 50-year/100-year Wind Speed (3-second gust)
      - Extreme Wind Speed (other than in tornado)
      - Maximum Tornado Wind Speed
      - Maximum Roof Load (Winter Precipitation)
      - Air Temperature and Humidity
  - **2.3.2 Local Meteorology**
    - Provided detailed information showing that the CPNPP onsite meteorological data are representative of the site area
    - Addressed cooling tower-induced effects on ambient temperature, moisture, and salt deposition

Meteorology

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **Technical Topics of Interest**
  - **2.3.3 Onsite Meteorological Measurements Program**
    - COL applicant described the existing onsite meteorological measurements program and provided a copy of the resulting meteorological data
    - Applicant met RG 1.23, Revision 1 criteria for siting of the tower in relation to Units 3 & 4

Meteorology

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **Technical Topics of Interest**
  - **2.3.4 Short-Term (Accident) Diffusion Estimates**
    - All CPNPP site characteristic values presented in FSAR Section 2.3.4 have been found to be acceptable
      - EAB & LPZ χ/Q values
      - Control Room χ/Q values
    - Minor changes expected to Control Room χ/Q values due to Integrated Seismic Closure Plan
  - **2.3.5 Long-Term (Routine) Diffusion Estimates**
    - All CPNPP site characteristic values presented in FSAR Section 2.3.5 have been found to be acceptable
      - CP COL 2.3(3) verified release points and receptor locations

Meteorology

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- **Conclusion**
  - All CPNPP site characteristics presented in FSAR Section 2.3 have been found to be acceptable and bounded by the corresponding US-APWR site parameters
  - All regulatory requirements for Section 2.3 have been satisfied
  - No open items related to Meteorology
  - No exemptions or departures
  - One confirmatory item (updated Control Room χ/Q values due to Integrated Seismic Closure Plan)