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: Tuesday, November 4, 2008

Work Order No.: NRC-2521 Pages 1-140

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

+ + + + +

US-APWR SUBCOMMITTEE

MEETING

+ + + + +

OPEN SESSION

+ + + + +

TUESDAY,

November 4, 2008

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B3, 11545 Rockville Pike, Rockville, Maryland, at 8:30 a.m., Otto L. Maynard, Chairman, presiding.

MEMBERS PRESENT:

OTTO L. MAYNARD, Chairman

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR., Member

WILLIAM J. SHACK, Member

JOHN D. SIEBER, Member

JOHN W. STETKAR, Member

STAFF PRESENT:

NEIL COLEMAN, Designated Federal Official

LARRY BURKHART

MIKE MAGEE

TERRY JACKSON

MICHAEL JUNGE

JEFF CIOCCO

ALSO PRESENT FROM MITSUBISHI HEAVY INDUSTRIES AMERICA, INC.:

KEN SCAROLA

AKAGI KATSUMI

MASAFUMI UTSUMI

MAKOTO TAKASHIMA

SHINJI KAWANAGO

TOM WILSON

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

PAGE

Opening Remarks

Larry Burkhart........................ 5

Status on Reviews of Topical Reports

Mike Magee............................ 8

OVERVIEW OF FOUR TOPICAL REPORTS RELATED TO U.S. ADVANCED PRESSURIZED WATER REACTOR (US-APWR) DESIGN CERTIFICATION APPLICATION

Ken Scarola..................... 31

Safety Instrument and Control (I & C) System Description and Design Process

Ken Scarola..................... 40

Human System Interface System Description and Human Factors Engineering Process

Ken Scarola..................... 82

Safety System Digital Platform (MELTAC)

Ken Scarola..................... 105

Defense-in-Depth and Diversity

Ken Scarola..................... 115

OVERVIEW OF HOW DIGITAL TECHNOLOGY WILL IMPACT PLANT PERSONNEL

Ken Scarola..................... 128

Wrap Up and Adjourn......................... 139

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

(8:30 a.m.)

CHAIRMAN MAYNARD: This is a meeting of the Subcommittee for the Design and Certification Review of US-APWR, the event PWR. I am Otto Maynard, Chairman of the Subcommittee.

And members in attendance today, we have Jack Sieber, John Stetkar, Bill Shack, Dennis Bley, and Charlie Brown. The Federal Designated Representative for today's meeting is Neil Coleman.

Today's meeting is an informational meeting only. We have four topical reports associated with INC, Human System Interface, Human Factor Engineering, Diversity and Defense In-depth that we will be going over.

Portions of the meeting will be closed to the public due to the discussions being proprietary. There are designated times on the agenda for public comment to give the public an opportunity to provide input, if they so desire.

As a reminder for the members, this is information only. The reports are still under review by the staff. We are not being asked to write a letter or to make any final conclusions or anything. This is for our information. So if we get hung up on a point, it is not that critical that we get everything resolved. We will be moving on so we can keep the agenda moving. However, our discussions benefit the staff. They can listen to some of the items of interest to us and factor that into our review. And then at some future date we can discuss what we do.

And so with that, I am going to turn it over to Larry Burkhart, let him introduce it from the staff's perspective and then we will move on to presentations.

MR. BURKHART: Thank you Mr. Maynard. Yes, I am Larry Burkhart, the chief of the US-APWR projects branch. And I would like to thank you, the ACRS Subcommittee for hosting this meeting and thanks to MHI for coming as well as NRC staff and any members of the public.

Just a little introduction to make sure you know some of the folks here. To my left is Mike Magee who is one of our chapter project managers specifically for the Instrumentation and Controls area, and Human Factors area. Our lead design project manager is Jeff Ciocco and we have a few of our key technical folks here. Mike Junge in the Human Factors area and Terry Jackson who I know here but he might have stepped out, from the I and C area. So, I would like to welcome them, too.

Yes, we think that these meetings are very beneficial and we definitely saw that two weeks ago when we met on fuel design. Because the staff gets some insights and some perhaps help in formulating some RAIs, MHI gets to hear your perspective, as well as any member of the public. So we think these are very important meetings.

Just getting into these areas that the topical reports address, Instrumentation and Controls, on Human Factors, Human System Interface. These are probably two of the most challenging areas with respect to level of detail, what we think we need to see to satisfy the safety requirements. And specifically because in the past in these areas for design search, we have used, applicants have used what we call design acceptance criteria in lieu of providing detailed design information. And that, in general, not to get too deep, but design acceptance criteria tell us how they are going to implement the design, rather than giving us a 100 percent complete design. They gave us enough information for us to make a safety finding.

But these designs that are coming in now and Mitsubishi has told us that they do not intend to use any design acceptance criteria. So, we are on the spectrum of determining where and we will wait to see if that actually happens. We will wait to see. And we are on the spectrum of determining what is the level of detail we need to have 100 percent complete design and to support our safety finding. So, we think these meetings are going to be very useful in helping us get to that answer. So, I know there is a lot of effort on the staff's side in determining that.

Another interesting aspect to these topical reports are that Mitsubishi has asked for most of these topical reports to be applicable to operating reactors as well as new reactors. In general, there should be no difference in the requirements but as we get more into the review, we are seeing perhaps there is a different perspective on that. So, just something to throw out there, some unique aspects to these topical reports.

So, I would like to sum up again by thanking everybody for supporting this meeting. We think they are very important for everybody involved. And with that, I would like to turn it over to Mike Magee, our chapter PM to start a discussion, a very brief discussion of where we are in our reviews.

MR. MAGEE: Good morning everyone. As Larry introduced, I am Mike Magee, Project Manager for Chapter 7 and Chapter 18. And these topical reports are referenced heavily in both of those chapters. Today, I am going to give you an overview of where the NRC staff is in the review of each one of these topical reports.

The purpose of today's meeting. Provide the status of the review on the following topical reports. The Safety I and C Description and Design Process, the HSI System Description and HFE Process, the Safety System Digital Platform, MELTAC and the Defense-in-Depth and Diversity. In addition, we will also address any questions that the committee may have.

Again, this presentation is not, it is specific to the review status and the not the technical material. We do have technical staff available to answer any questions. However, Mr. Ken Scarola is going to give us an in-depth presentation on each topical report. And at that point, it would be an opportune time to ask the technical questions. However, if any questions come up, we will attempt to address them.

Topical report Defense-in-Depth and

Diversity. The topical report requests approval of the D3 approach to US-APWR. The staff's review focused primarily on MHI's design-based approach to D3, including the Diverse Actuation System for I and C system applied to its US-APWR nuclear power plant design.

We are currently in revision two in response to RAIs. RAIs have been reviewed and we are preparing a safety evaluation report, which we expect in late November.

CHAIRMAN MAYNARD: Just to make sure we are all on the same page. Could you just briefly describe the D3 option? You say the approach to D3. I'm sorry to D3. Just explain a little bit what that is.

MR. MAGEE: I would ask Terry or Royce, if you guys could give a good, better --

MR. JACKSON: Basically -- this is Terry Jackson with the staff. And basically in this topical report, with regards to the D3, it is a Defense-in-Depth and Diversity methodology. It doesn't include all of the components for a Defense-in-Depth and Diversity analysis, which would include other aspects. But this is basically where MHI is proposing certain ways to address Defense-in-Depth and Diversity, including architecture for their Diverse Actuation System and how they plan on using automatic and manual means to address a software common cause failure.

CHAIRMAN MAYNARD: Okay. That's fine.

MR. MAGEE: Are there any other questions on Defense-in-Depth topical report or the review status?

MR. BURKHART: So this is the most near-term safety evaluation report that we will complete before that we are talking about today.

MR. MAGEE: The next topical report, Safety System Digital Platform MELTAC. This topical report requests approval of this platform for an application to the safety systems of the US-APWR and for replacement of current safety systems in operating plants.

Staff are reviewing both aspects. Review is focused on the design of the Mitsubishi Electric Total Advance Controller MELTAC Platform and its conformance to safety requirements. Revision two has been received. RAI responses are under review by both offices for new reactors and operating reactors. We expect a safety evaluation report on this topical report in June of 2009.

MEMBER SHACK: Now this wouldn't be a

stand-alone report for the replacement. Right? I mean, they would have to deal with, presumably, the Diverse Actuation System sort of argument also on their own, if an operating plant came in and wanted to adopt this platform.

MR. BURKHART: That is something very interesting. There are, of course, other topical reports that are associated with what would be needed to replace an existing operating plant. And we are working with NRR to determine what kind of different processes/steps/requirements there might be for operating plants.

MEMBER SHACK: I am just sort of wondering what you approve when you approve this.

MR. BURKHART: That is a very good question. And are probably not 100 percent clear exactly what we are going to approve. I will let Terry discuss that.

MR. JACKSON: Terry Jackson again. The multi-platform is, essentially, the computer platform that they are planning on implementing some of the safety INC systems, for example, reactor trip and engineering safety features actuation using this platform. So, it is a key component but, like you said, it doesn't fully address all of the aspects for a safety-related INC system. So there are other aspects that have to be addressed, either if it is an occurring operating plant at the time that the licensee comes in with the license amendment request or even for US-APWR, the design certification will address aspects that the MELTAC Platform doesn't cover.

MR. BURKHART: It is usually from a process standpoint. The question that I am concerned with is, as NRO, our priority is finishing the review, getting the information we need for the design certification. There may be an instance, and let me back up by saying that there is no licensee who has referenced this platform to be replaced in an operating plant. Not like Oconee with the AREVA system.

So, and I only say that because there may be a divergence.

MEMBER SHACK: But if you guy write an SER on this one, it might.

MR. BURKHART: Well, our SER could --

MEMBER SHACK: It would depend on how you --

MR. BURKHART: Good point. Our SER though could be limited to only the US-APWR. So, I throw that out there as when you do see an SER on this, we don't know exactly what it is going to apply to. We may have one SER for the US-APWR. There might be certain different requirements for operating plants. There might be a supplement to the SER or a different SER for our operating plant. So, we haven't gotten there yet.

I can say that from this office's perspective, we are focusing on what we need to do to write an SER for our operating reactors. Right now, we want to do them together, consolidate SER for operating reactors -- I'm sorry. We want to focus on new reactors. Right now the plan is to address it together with NRR. We are working with them to try to do that.

MEMBER BROWN: Question. Brown. Are we supposed to give our names today?

CHAIRMAN MAYNARD: You don't need to. You've got a name tag on.

MEMBER BROWN: All right. I just want to make sure I am clear today. I have several questions.

In a couple of these reports, this platform was referred to in two different ways. One is MELTAC. Then there was another listing of it is called MELCO. That was in the INC system description.

Are they the same thing or are they different?

MR. BURKHART: I think MELCO is the company.

MEMBER BROWN: But they call it a MELCO platform.

MR. BURKHART: Okay.

CHAIRMAN MAYNARD: We are going to have an opportunity. They are going to be up presenting --

MEMBER BROWN: Oh, okay. Do you want me to wait?

CHAIRMAN MAYNARD: -- the company will.

MEMBER BROWN: Okay, that's fine.

CHAIRMAN MAYNARD: So, wait until they get up and present.

MEMBER BROWN: All right. I'm happy. I've got 20 pages of questions.

MR. BURKHART: Okay. Again, we are focused on just the status. I kind of went off base so I apologize. We are focusing on just the status of where we are in our reviews, which is pretty much almost the beginning on most of these.

MR. MAGEE: Thank you, Larry.

The next topical report HSI System Description and HFE Process. This topical report requests approval of the HSI System design and its design process for the application to HSI System of the US-APWR and replacement of current HSI Systems in operating plants.

This review has been focused or it was conducted using the elements of NUREG-0711, Human Factors Engineering Program Review Model. Review emphasis was placed and is placed on the six planning and analysis elements, as these elements are used as a basis of the HSE's design of the control room. We are currently in revision two in response to RAIs. RAI responses have been received and they are currently under review.

Safety Evaluation Report for this topical report due date is under evaluation. Some of the RAI responses have requested additional documentation. And until we received that additional documentation that we are expected sometime the second half of next year for a safety evaluation report.

MEMBER BLEY: So in this case, you have decided that the single SER will cover both operating plants and --

MR. MAGEE: That is the way we are reviewing it, yes.

MR. BURKHART: Yes, I would just throw out there, not being a technical expert but a process expert, I think that is the intention. But I think, depending on what happens in the reviews, it could diverge. That is my opinion from having worked here on these very difficult issues for a while. But the intention right now is address them together.

MEMBER BROWN: And the US-APWR and other plants where this may want to be applied?

MR. BURKHART: Yes.

MEMBER BROWN: Cover them both in one?

MR. BURKHART: That is what they have asked us to do and that is what we were intending.

CHAIRMAN MAYNARD: There are several of the topical reports where they have asked for both. Our focus for our meetings need to be on the design certification review for the US-APWR. The staff is going to have to struggle with some of these as to whether that gets all done in one SER or whether it gets --

MR. BURKHART: We are interested in hearing if you have any thoughts on the issue of operating reactors and new reactors, too. Because right now, that is our plan is to address them sufficiently for both. So, we are interested in hearing.

MEMBER SIEBER: Oh, I think if we write a letter though, we ought to address the way that the staff intends to certify as opposed to restricting ourselves to the APWR.

MR. BURKHART: I would agree with that.

MEMBER SIEBER: If those incidents come up, we have to think about them and, if necessary, comment on them.

MR. BURKHART: Yes, and if we think this warrants us coming to you for this SER by itself, you will certainly have a very good heads up on where we are going on that. So, we will keep communications open on that.

MEMBER SIEBER: I think we can handle it either way.

MR. BURKHART: But we are really interested in getting your feedback and any thoughts you might have on the, might there be any differences in operating reactors and new reactors, definitely.

CHAIRMAN MAYNARD: Okay.

MR. MAGEE: Any other questions?

For the fourth topical report, Safety I and C System Description and Design Process. This topical report requests approval of the MHI design and design process for application to the safety systems of US-APWR and replacement of current safety systems in operating plants. This review is focused on the design of the MHI digital safety systems and the design process used for the application of these systems to specific nuclear power plants.

Revision one has been issued. RAI responses are being received and reviewed by both offices for new reactors and for operating reactors.

Safety evaluation. This topical report and the MELTAC Platform topical report are closely linked and its safety evaluation report is also due at the same time in June of 2009.

Are there any questions on the safety I and C review status?

To summarize, the topical report, the review status --

MEMBER BLEY: I'm sorry.

MR. MAGEE: Yes?

MEMBER BLEY: Can I back you up --

MR. MAGEE: Absolutely.

MEMBER BLEY: -- to the HSI one.

MR. MAGEE: Absolutely.

MEMBER BLEY: I have two questions on that one. Is NUREG-0711 the one that was developed at Brook Haven that talks about process rather than detailed review?

MR. JUNGE: I'm sorry.

MEMBER BLEY: Was 0711 the NUREG, the one that was developed at Brook Haven that looks --

MR. JUNGE: Yes.

MEMBER BLEY: -- at a review of process?

Well, if they are not coming in for DACs on this and they are going to have the complete program, would that be the right basis for the review?

MR. BURKHART: Well remember, this is their topical report that lays out their approach. And the detailed design information would come in those part of the --

MEMBER BLEY: Okay, so that will come later. That makes sense. Thanks.

MR. BURKHART: So, that is a good question because that is where we are in this review. So, in theory yes, we should see all the detailed design information.

MEMBER BLEY: Eventually, okay.

MR. BURKHART: In my opinion, having dealt with designs that have used DAC before, having only experience with using DAC before in these areas, I really want to see how we get to 100 percent complete design in these areas. Because I don't, again, I am not a technical expert, really don't see how that can happen. Is it going to be more detailed that what we have seen before? Yes, that is for sure. Is it going to be what we consider 100 percent detail? MHI says yes. So I would say, we will see. So, that is just an opinion from having worked in this area before.

MR. BURKHART: Okay, Mike.

MR. MAGEE: You had two questions. So, your second question?

MEMBER BLEY: I did, yes. Thank you for reminding me. The other one was the HSI is the only one that you don't have a planned date yet for completion. Is that due to some details of what they have submitted or you haven't reached that point yet?

MR. MAGEE: We haven't. We need to address, this week we are addressing some documentation that we need in order to complete the review.

MEMBER BLEY: Okay.

MR. MAGEE: And when that documentation comes in, we will have a much better framework for which to establish a schedule to complete.

MEMBER BLEY: Okay.

MR. MAGEE: But we are anticipating that, in conjunction with some technical reports that are being submitted, that we will be able to get an SER out in the second half of next year but this is as close as I can approximate right now.

MR. BURKHART: And you will hear more about the basis of their HFE, HSI program in their presentation. And we just had some questions about how they did their up-front and basically using their Japanese plant as some experience in their HSI/HFE development. So, right now we are just asking some questions on how did they plan and design that, you know, the original plant and then to get to where they are with their US-APWR HFE program. So, you will see that in their presentation.

MEMBER BLEY: Okay.

MR. BURKHART: But there is just some information we need. And once we get that information, we can establish a more concrete schedule.

MR. MAGEE: To continue with the summary, we are actively reviewing these four topical reports. Currently the safety evaluation report is being prepared for Defense-in-Depth and Diversity topical report. The MELTAC and Safety I and C SER reports are due in June of 2009. And as we just discussed, the due date for the HSI/HFE topical report is under review.

MR. BURKHART: And just to throw something out there, this issue of these topical reports and platforms being applicable to operating plants and new reactors is not unique to Mitsubishi. AREVA has some similar requests into the staff. In fact, referenced in an Oconee license amendment request to replace the I and C System for an I and C System with a digital I and C System. So, you may not have heard a lot of details about that but just don't go away from here that MHI is the only one who has asked us to do this. AREVA has also. There may be different issues but, in general, there is --

MR. JACKSON: Terry Jackson again. Just a little clarification point. On the Oconee, they initially did come in with one of the AREVA topical reports referenced but then they subsequently removed it.

MR. BURKHART: Oh, I thought they had submitted another request. No?

MR. JACKSON: No, they removed it.

MR. BURKHART: Okay. I stand corrected.

MEMBER STETKAR: I have a question just for my own personal knowledge, because I haven't been through much of these.

I have a TRA background, guys, so I tend to be sensitive when I see the letters PRA in documents. And I noticed in several of the topical reports, without going into detail, there are several issues that the topical reports refer to the PRA as a basis either for allowed outage times or justification for levels of redundancy, or independence and diversity, or minimum inventory of alarms and indications and things like that.

How does the review of the topical reports mesh with reviews of the PRA? In other words, if you approve the topical report in the SER, is that implicitly approving the quality of the underlying PRA where it used as a reference document and analysis? I was a little bit confused about how that process worked.

MR. BURKHART: From someone from our process standpoint, I would say no, it doesn't implicitly approve anything about the PRA. From approving that topical report it may say your approach in this topical report is approved but we are reviewing, and Mitsubishi has submitted the generic PRA for the US-APWR. So, I would say, in general, no, we are not approving necessarily the quality of the PRA.

I know that you probably know more details about a PRA than I do --

MEMBER STETKAR: No, no. I don't want to get into the details. I was trying to keep this at the kind of higher level process area, in the sense that there are specific, in the topical reports, there are specific numbers in there for allowed outage times, frames of equipment and things like that are ostensibly derived, somehow from the PRA analyses or at least justified by them.

So, if you approve the topical report, including those times as a generic basis for the licensing of that design, does that -- how does that work with that underlying analytical basis?

MR. JACKSON: I think as we go through in our reviews and stuff, we will need to really consider closely where MHI is proposing the basis for certain designs or techniques and so forth based on PRA. And if there is a sufficient basis here, then we can recognize that. But if there is not, then that is something we would need to call out in safety evaluation.

MR. BURKHART: And maybe for the purpose of this meeting we can ask MHI when they give their presentation to highlight those areas.

MEMBER STETKAR: I was going to but as I

said, in terms of the general process, I wanted to look at --

CHAIRMAN MAYNARD: But aren't the applicants also required to if you find information about availability that you are no longer covered by what was assumed in the topical report? To use a topical report, you have to demonstrate that you fall within the criteria in the topical report.

So, I think if they found out later, they are either going to have to improve the availability --

MR. BURKHART: That is an important thing is that we have to address that in the SER, that aspect of use of PRA, however we think that is appropriate in the topical report.

MEMBER SIEBER: Could you give me an example where in these four topicals that there is a reference to the PRA?

MEMBER STETKAR: Yes, there are several. And I was going to bring them up during the --

MEMBER SIEBER: Yes, just give me one.

MEMBER STETKAR: Identification of minimum inventory of alarms and displays for the HSI/HFE. So there was --

MEMBER SIEBER: Well, let me ask you a

question. I am at the head table now. Most PRAs that I have seen do not get to the details to what the inventory of instruments needs to be from a risk standpoint. So, it is not clear to me how you get from those instances. And I thought about this.

MEMBER STETKAR: Oh, that is -- yes.

MEMBER SIEBER: How do you get from the PRA to that?

MEMBER STETKAR: I agree with you, Jack. And that is why I asked the question because, indeed, there are examples in that HSI/HFE topical report that have a relatively detailed, a summary but a relatively detailed summary of a THERP-type HRA PRA analysis that evaluates the quality of the indicators and things like that.

So, you are led to the belief that they actually did it. And if they did it, then it comes back to the second part of how did they do it and how well it was done.

MEMBER SIEBER: My rudimentary knowledge of PRAs sort of told me that standard PRAs don't get to that depth. Maybe they did something special. Those are good questions.

MEMBER STETKAR: They usually don't but there are methods.

CHAIRMAN MAYNARD: I think that those are good questions for discussion.

MEMBER STETKAR: Yes. I just didn't want to get into the detail. I was more curious about the --

CHAIRMAN MAYNARD: I just think it is important for the staff, it is going to be important on the SERs clearly what they do address and don't address.

MR. BURKHART: I agree and this is a great example of why we are here early to get these inputs. So, thank you.

CHAIRMAN MAYNARD: Any other questions for the staff?

MR. MAGEE: I wanted to -- Ken Scarola, did you have a comment that you wanted to share?

MR. SCAROLA: Ken Scarola, MHI. I just wanted to say that the entire minimum inventory subject will be addressed. And I think we can hit that PRA issue when we address that.

MR. MAGEE: Okay, thanks.

CHAIRMAN MAYNARD: Okay. Any other questions for the staff? Did you have any other --

MR. MAGEE: No, I did not, sir.

CHAIRMAN MAYNARD: Okay. Well I think we

are ready to transition then. Ken are you going to be leading the next discussion?

While they are transitioning, I want to remind the members, this next segment is an overview that is open to the public. And it will be an overview that covers all four of the topical reports but it is going to be a public version of it.

We are then going to go through each one of the topical reports individually in closed session. So, some of your questions may be more appropriate to wait for the closed session. If you have general questions and stuff, I think that is fine. But if it is going to get into a level of detail that gets into the proprietary information, we will probably be asking to save that until that portion.

MEMBER BROWN: You mean you want us to be quite?

CHAIRMAN MAYNARD: No. Just don't push them for proprietary answers in this part of it. We won't get into that one.

MR. SCAROLA: Well let me just say that we will certainly do our best to answer all of the questions during the open session. But if we feel that we are getting into more detail than is appropriate with, then we will simply ask you to save your questions.

While they are bringing up the presentation, let me just introduce myself. My name is Ken Scarola. I am a technical advisor in the I and C, the Instrumentation and Control, I and C, and Human Systems Interface, HSI, areas for MHI.

I will be, over the next two days, the lead presenters on all of the material on these four topical reports. But as you can see in our room, we have brought many people that are much more capable and knowledgeable than I am and they will support us where we need to get more detailed answers.

I would like to thank the ACRS for giving us the opportunity to make these presentations. As was stated before, the I and C and HSI areas tend to be very complex areas. This is the basic reason why we submitted these four topical reports about nine months in advance of the US-APWR DCD. Our hope was that we would get a longer period of time for the staff to review these, due to the complexity. And, I think we are getting that review. So, we are very happy about that.

Okay, we have the slides up. We will be presenting first an overview in this open session. Then we will go into closed session and present the details of each one of the reports.

I do want to, I would like to introduce the key players that are here or will be here throughout the day. The first one is Shinji Kawanago. Shinji is actually not here this morning. He will be joining us this afternoon. But he is the MHI representative for I and C licensing.

We do have Makoto Takashima here. Makoto is responsible for all of the I and C design in the HSI design areas for MHI.

We have Masafumi Utsumi, who is responsible for safety systems. And we have Akagi Katsumi, who is our lead representative from MELCO. MELCO is Mitsubishi Electric Company. MELCO builds the MELTAC Platform. So hopefully we can avoid that confusion. And if we do confuse those two in our topical reports, then we will fix it.

But very clearly, MELCO is the name of the company.

MEMBER BROWN: But will you use them interchangeably? That is all I wanted to know.

MR. SCAROLA: You know, we try to use MELTAC Platform. In some cases we have probably said the MELCO Platform. It was certainly not intended to confuse you in any way but we will fix it.

MEMBER BROWN: At my age, I am easily confused.

MR. SCAROLA: Okay. Oh, just a little bit on my background. I was the lead I and C and HSI designer, manager, whatever you call us, for the System 80 Plus certified design. So for me, this is very much dé·jà vu. The last time I presented to the ACRS, you were in Bethesda in a very, very tiny building many, many years ago.

But what is very interesting is that the US-APWR and the I and C systems for the US-APWR that are the subject of these four topical reports are very, very similar to what the staff certified for System 80 Plus. So, there is a lot of background here that is applicable here. And I will be bringing some of those points up as we go through this presentation.

The purpose of these topical reports is first and foremost to describe MHI's I and C and HSI System designs. In addition, the intent is to describe the design process past, current and future. Now, what that means is the design process that was used for the development of the designs as you see them today in the topical report, the design process that we are now applying to apply those designs to the US-APWR so that is current, and the design processes that we expect to apply if we are fortunate enough in the U.S. to get a U.S. operating plant to select these platforms or these designs for a digital upgrade in the U.S.

So the design processes, in many cases are written in present tense. And they are written that way because they are applicable to both past, present, and future.

Finally, we are seeking NRC approval of both the designs and the design processes.

Now, we talked about the four topical reports. And when they were introduced, the staff said that three of the reports are applicable or that MHI has requested approval for both the US-APWR's operating plants. But the D3 report, the review process is only for the US-APWR.

I do need to clarify that a little bit. The D3 report, as it is written, states that it is applicable to both new plants and operating plants. But there was an interaction with the staff that basically said that was probably impractical and would likely delay the US-APWR. So, MHI has accepted that the staff's review, at least initially, right now, would be exclusively for the US-APWR.

It is very likely that MHI will come back sometime in the future and say, okay, would you now conduct the same review for an operating plant on the same topical report because the topical report is written generically. So, just a point of clarification.

MEMBER STETKAR: When I think about the general, the Safety I and C Design topical report, that does indeed make reference to the DAS design, to some extent, at least as far as the interface.

Does that mean that when we think about the Safety I and C, whatever it is called, the topical report on Safety Systems Design and Process, when we think about the D3, the Diverse Actuation System impact within the context of that topical report, we should think about it in some generic term when we are thinking about operating plants.

MR. SCAROLA: Yes. Very clearly --

MEMBER STETKAR: Because when I was reading the two, I had to bounce back and forth between the two to think about it is going to work.

MR. SCAROLA: It would never be HMI's intent to apply the Safety System Design, which is a digital design, to an operating plant without a strategy for Defense-in-Depth and Diversity to address common cause failure.

So, it is very, very difficult to unlink these two. You clearly must have a Defense-in-Depth strategy. That is reference in the safety system. It does reference the D3 report. So, I think we have a disconnect.

MEMBER STETKAR: But your message is that at the moment the D3 report is strictly for the US-APWR.

MR. SCAROLA: Well, at the moment it is written to be applicable to both. The staff is reviewing it only for the US-APWR.

CHAIRMAN MAYNARD: What I intend -- what you believe will probably come out is an SER that is applicable only to the US-APWR, at this point. But the topical report, you believe, can be applied with further review to all of them.

MR. SCAROLA: Right. I think what would happen here is the SER for the safety system is going to have to say that this safety system can only be used with an appropriate D3 strategy. Because that would only make sense. You have a digital safety system, you must have some strategy for common cause failure.

So, I think it is going to have to be an open item in the safety system SER that would have to be addressed for operating plants, either by an LAR referencing that D3 topical report and having it reviewed during the LAR process. But hopefully we can just come back in and put that open issue to bed before an LAR comes in because we would clearly like to see it done generically.

So, we have a little bit of a schedule problem here but I think we have addressed it. Okay, next slide.

The intent of this meeting is to provide the ACRS a better understanding of what the content is, to provide details of what we call the key technical issues, to focus on some of the key issues. We obviously, there is probably 400 or more pages of topical report. We can't get into everything. We are going to discuss what we think are the key issues. Clearly, if you have questions in any areas, we are here to answer those questions. But recognize that we had to select certain things for this meeting.

MEMBER BROWN: Will you be able to make reference to certain sections of your topical report, in response to questions if they reference those?

MR. SCAROLA: I will try.

MEMBER BROWN: For instance, a question that says, hey, on this page in this section, whatever it is that addresses this function, --

MR. SCAROLA: I think so.

MEMBER BROWN: -- will you be able to answer that question?

MR. SCAROLA: I think between me and all the people here, we should have enough knowledge of the topical reports. So on that level --

MEMBER BROWN: Well sometimes that is a little hard if you don't have a copy of -- I hate to read the words. I am prepared to do that.

MR. SCAROLA: When we get into the closed sessions --

MEMBER BROWN: One of the --

MR. SCAROLA: -- I will have my computer here. I just didn't set it up now. So I will be able to go right to the paper.

MEMBER BROWN: Well, I have got them also.

MR. SCAROLA: Okay.

MEMBER BROWN: So, it is just a matter of if other people want to see them. And that's just a methodology question. That is all.

CHAIRMAN MAYNARD: I think wait until we see if we get into those questions and see.

MEMBER BROWN: Okay.

MR. SCAROLA: And of course, finally, we

are anxious to hear your feedback. We welcome the opportunity to present to the ACRS and to hear what you think about these designs.

I think one of the things that I have seen in working with MHI is it's a pleasure to work with them. There is no sense of "not invented here, we are not doing that." They are open to discussion, open to comments, and very clearly open to change, if that is necessary. So, we welcome your feedback.

Okay. The way we will do this is we will provide an overview of the topical reports, rough design description, key issues. And again, this is an overview.

What we thought we would also do, depending upon timing, is if we have the time, we would like to present actually something that is not in the topical reports. And that is the way we see operations and maintenance in power plants today changing because of this digital technology. Now, if we don't have the time for that, we won't do it. But it is something we are always asked. So, we thought, if we had the time, it might be worthwhile to go through some of these things. Because it will help you get a better perspective on why we think this digital technology is so valuable and why we are trying to get it approved.

Okay. Then, of course, we will go through the closed sessions and we will present each one of the topical reports in detail. We will present the four topical reports in the following sequence.

First, the Safety I and C System Description. The reason is that really presents an overview of the entire MHI design.

Then we will present the HSI. Again, the HSI is from a broader perspective. It really helps you understand what we are trying to achieve in both the architecture underneath the HSI and what we are trying to give to the operators themselves.

Then we will talk about the MELTAC Platform. The MELTAC Platform is the fundamental building block that makes all this work. It is the digital controllers, the IO, etcetera.

Once you get an understanding of how all of these pieces are arranged, then we can get into Defense-in-Depth and Diversity because, in order to understand D3, you really need to look at the entire design in aggregate. So that is why we plan to present these in this order.

Okay. Just a little bit about what MHI is doing in the licensing arena. A very important part of digital I and C licensing are the recent task working groups that the staff has organized and which NEI is leading the industry participation. MHI participates in all of these task working groups, cyber security, D3, risk informing, digital I and C, data communications, human factors, licensing process, and also new reactor operator licensing. These are all related to digital I and C or digital HSI. MHI participates in all of these and we believe that the topical reports reflect the interim staff guidance that has come out of all of those task working groups.

Now of course, the staff is going to review against that. But at least it is clearly our intent to comply with the interim staff guidance and we think we have done that.

CHAIRMAN MAYNARD: I take it in some of your discussion, you have talked a little bit about your simulator facility.

MR. SCAROLA: Yes, absolutely. We will talk about it. And so let me just say right up front, we would like to give you an open invitation if you haven't gotten one already to come visit our simulator. We would love to have you there and see what we have done.

CHAIRMAN MAYNARD: Yes, we have received

one and we will be talking about that.

MR. SCAROLA: Okay. So, let me go on to the first topical report, which is the Safety I and C System Description and Design Process Topical Report. This slide simply presents the table of contents. We will get into this certainly section by section when we go through the details. Let me just say that the purpose of all of these topical reports is certainly to achieve an SER from the staff that is applicable, as we said, either to both operating plants and US-APWR or, in some cases as we pointed out before, possibly only to the US-APWR. But as documented in all of them, it says both.

We get into the scope of what is in the topical report. For example, in this one, the scope is primarily the safety systems but we do talk about the interface of the safety systems to the non-safety systems. Because certainly those interfaces and the isolation, the data communication between safety and non-safety is significant.

Section three identifies all of the applicable regulatory criteria. And we will go through some of the key criteria later. Section four is really the meat of the document in terms of describing the design. Section five addresses the key design basis issues. Section six speaks to this idea of design process. What is the process that was used for developing this? What is the process? What are the key points of the process that we need to apply going forward, when we apply this safety system to any specific power plant? Things like qualification analysis, response time analysis, etcetera, we will get into that.

Section seven really is intended to help the staff understand what we are asking them to approve here and what is not there and must be addressed in plant-specific licensing documents. So this is what we call future submittals. So, in the case of the US-APWR, the US-APWR is a plant-specific application of this safety system design. So what this section, section seven says is these are all the things you should expect to find in the US-APWR documentation that you are not finding in this topical report. Things like the response time analysis. That is a plant-specific thing. It would be done on a plant-specific basis.

So these are, it is really intended to help the staff understand what we are expecting approval for and what we are saying you are going to see later.

CHAIRMAN MAYNARD: And they basically have an example of that right now. They have the topical report. They have the DCD and actually even a COLA now.

MR. SCAROLA: Right.

CHAIRMAN MAYNARD: So, they can say what you are saying is in here and what should be in the DCD.

MR. SCAROLA: Correct. Now, in addition to those topics, we have some very detailed appendices, one focusing on IEEE-603, the other focusing on IEEE-7432. These two IEEE standards are essentially what the industry thinks about as the bible for safety system design requirements. They are the key requirements. 603 applies to all safety systems, whether they are digital or analogue. 7432 essentially supplements 603 for computer-based safety systems. In the appendices, we go through each paragraph and we address how we comply with each paragraph of these issues.

Appendix C gives more detail on something that we call spurious actuation, which is a very important issue when we look at non-safety systems and what they can do regarding causing plant transients that are either within or possibly outside the bounds of the safety analysis. So, Appendix C essentially gives our position on spurious actuation. And we will talk more about that because it is an important issue.

Okay. This is a drawing that I will use several times throughout the next two days. It provides an overview of the overall I and C System. I will walk through it at a high level now and then we will get into it in more and more detail as we go through each one of these topical reports.

The layout of this drawing is that the bottom of the drawing represents the I and C interface into the plant. This would be the instrumentation that is monitored by the I and C and the pumps and valves, heaters, breakers, that the I and C controls. So, these are all, the plant interfaces are at the bottom. The very top of the drawing represents the human systems interface.

This section of the drawing is what we call the PSMS, the Protection Safety Monitoring System. This is really the key subject of the safety system topical report. The safety system topical report describes the architecture of the reactor protection system, which is a key component of safety systems in nuclear power. It describes the architecture of the engineered safety feature actuation system, another key component, and the architecture of what we call the safety logic system. The safety logic system is where we do the combinational logic, combining manual signals, automatic signals, process interlocks for the actuation of each individual pump and valve in the plant.

So, if this valve gets manual control signals from the main control room, manual control signals from the remote shutdown panel, automatic signals from engineered safety features, interlocks from sensors, all of those things that are typically combined in relay logic, in existing power plants, are now combined in digital control logic in this design.

So, the topical report focuses on this boundary. Now, in understanding that boundary, the topical report also describes all of the interfaces into the non-safety system, what we call the Plant Control Monitoring System. The PCMS is where you will find systems such as reactivity control systems, pressurizer level, pressurizer pressure, steam generator water level control, turbine control systems. All the non-safety systems in the plant exist in this boundary.

When we move up in the hierarchy, we get to the human systems interface. Now, the human systems interface has both safety components, which are part of the PSMS, as we see here. These are safety-related ESF actuation and reactor trip system-level manual actuation switches that interface from the main control room down into the safety systems. We also have on this other side safety video display units which are part of the HSIS but are in an extension of the protection and safety monitoring system.

Similarly, we have non-safety man-machine interfaces that you see here in this pink color. And these are an extension of the PCMS. These are all of our non-safety man-machine interfaces. This will make a little more sense when we go to the next slide, where we show the control room.

MEMBER SIEBER: I have a simple question. I see you have a manual reactor trip that bypasses all the digital systems. As far as pump starts and stops, valve opening and closing, do manual switches override the digital?

MR. SCAROLA: For individual pumps and valves, we do not have, in the normal man-machine interface, we do not have the same type of bypass of the digital systems as we do for reactor trip. But we do have reverse actuation.

MEMBER SIEBER: Well --

MR. SCAROLA: Let me explain that.

MEMBER SIEBER: Let me just refine my question just a little bit.

This probably would never happen but the digital system may say start that pump and open the suction and discharge valves. And the operator would say, I don't want to start that pump. If he trips it, will the automatic system try to start it again?

MR. SCAROLA: Inside existing control rooms, manual switches have functions such as pull-to-lock on pumps.

MEMBER SIEBER: Okay.

MR. SCAROLA: Are you familiar with a pull-to-lock function?

MEMBER SIEBER: Yes, I was an operator.

MR. SCAROLA: We have a software-based pull-to-lock that an operator can actuate from the VDUs. So, if the safety system were to actuate, the operator can decide, no, I don't want that actuated. I can go through a series of steps and put that pump in the pull-to-lock mode so it shuts off.

MEMBER SIEBER: And he does it through the digital system --

MR. SCAROLA: Through the digital system.

MEMBER SIEBER: -- as opposed to locking it out by hand.

MEMBER STETKAR: Through the operational digital system.

MR. SCAROLA: The operational digital system. Now, --

MEMBER STETKAR: The non-safety.

MR. SCAROLA: -- let's take the case --

MEMBER SIEBER: So if it did fail, you may not --

MR. SCAROLA: Let's take the case where the digital system has actually failed --

MEMBER SIEBER: Okay.

MR. SCAROLA: -- and I go to pull to lock and I can't do it.

MEMBER SIEBER: Right.

MR. SCAROLA: Okay. Now we rely on what we call the Diverse Actuation System. The Diverse Actuation System is our analogue backup to address common cause failure. The Diverse Actuation System has both an automated part that will automatically actuate systems and it has a manual part that allows operators to manually actuate systems. This manual part is conventional hard-wired switches and hard-wired controls.

MEMBER SIEBER: Does it override the digital system?

MR. SCAROLA: It does not override the safety directional commands of the digital system.

MEMBER SIEBER: Thank you.

MR. SCAROLA: We'll talk about that. But we will talk about that more as we get into the details. What we have is what we call state-based priority. And we will talk about state-based priority as we get into this in a little more detail.

So now we have addressed the three major parts of the I and C architecture. The safety side, the PSMS, the non-safety side, the PCMS, as well as the interfaces into the man-machine interface or what we call the human systems interface. And we have addressed our Diverse Actuation System, which is the analogue part of the system to address common cause failure. Those are the three major echelons that we have in this design.

Let's go to the next slide. Here we show the architecture of the human systems interface. And we do describe this in the safety system topical report only to give a perspective of where safety interfaces are inside the control room. We have a large display panel, which is a non-safety function. We have VDUs for both alarming as well as operational VDUs that allow you to monitor instruments and take control. The operational VDUs are all non-safety. The alarm VDUs are non-safety.

But on the right side of the panel here --

MEMBER BROWN: Could you say that again?

MR. SCAROLA: The alarm VDUs are non-safety --

MEMBER BROWN: Not that part. You ran through a series of statements. You said that they -- you ended with the alarm VDUs. Something was safety, something was non-safety.

MR. SCAROLA: Everything I spoke about so far is non-safety. If I said safety, I am sorry.

MEMBER BROWN: Including the alarm VDUs?

MR. SCAROLA: The alarm VDUs, the operational VDUs, the large display panel are all non-safety --

MEMBER BROWN: I understood the large display panel part. I guess I didn't realize the alarm VDUs were non-safety.

MR. SCAROLA: These are all non-safety devices. Now, later I will talk about a capability of the operational VDU, which is what we call multi-division control, where we will use a non-safety man-machine interface to control both non-safety and safety components. But the interface itself is a non-safety interface.

And the backup for that non-safety interface is the safety interface inside the control room, which is what we call the safety video display units. The safety VDUs are part of the protection and safety monitoring system.

MEMBER BROWN: But do they include the alarms as well?

MR. SCAROLA: No. The alarm system --

MEMBER BROWN: The alarms are on a system that is non-safety.

MR. SCAROLA: The alarms are on a non-safety.

MEMBER BROWN: It is non-1E.

MR. SCAROLA: Non-1E, which is consistent with all operating power plants today and consistent with all of the regulatory guidance.

The alarms are, typically, aids to the operators. They are not credited in any of the safety analysis.

MEMBER SIEBER: They don't do anything. They are just there.

MR. SCAROLA: We will use them to the extent that they are available but we do not take credit for them. The EOPs are essentially written --

MEMBER BROWN: Yes, I understand that, except from the standpoint just I am not saying one way or the other, it is just that the standpoint now, the operator doesn't, something may be going on and yet he doesn't have an indication of what may be triggering that. So, he is blind, in a manner of speaking.

Now, I don't want to go into detail. It's just when I read this and I thought I had -- you just clarified something that I had read. So I appreciate that.

MR. SCAROLA: It just seems to be a little bit out of sorts to have the operator somewhat blind relative to what is going on. Why is it happening? What parameter triggered it? What did this? What did that? Because all he sees is some stuff starting or some actuations occurring.

One thing I will --

MEMBER SIEBER: -- are not safety but the indications are.

MEMBER BROWN: But if you know. I mean, all of a sudden, you have got to start flipping your eyes all over the place instead of something saying, hey, this system didn't work.

CHAIRMAN MAYNARD: The U.S. emergency operating procedures are not based on -- the operator doesn't have to know what the accident is. The EOPs are lined up to go by the --

MEMBER STETKAR: Be careful because these are event-based emergency operating procedures in this plant. So, as I understood it, we will probably get into that when we talk about the --

MR. SCAROLA: Well actually, we have both types of operating procedures, as do all Westinghouse CE Plants and PWRs in the U.S. have both function-based operating procedures as well what was call the optimal recovery, which are event-based. We have two types of operating procedures.

MEMBER STETKAR: And stop me if this gets into more of the proprietary stuff. Probably not but I was going to bring this up when we talked about the HSI/HFE.

As I understand it, what you classify as your function-based -- if I go back to the early 1980s in the United States, your function-based procedures are the function restoration guidelines. Your emergency operating procedures are strictly event-based. They are not symptom-based procedures. They are not integrated, symptom-based procedures. Are they?

MR. SCAROLA: Function-based procedures are considered part of the EOPs. As you execute an optimal recovery EOP and you get to a point in the EOP where the EOP or where the symptoms cannot be clearly diagnosed, the EOP directs the operator to go to the functional-based recovery procedures.

MEMBER STETKAR: I understand that. Although there is in newer plants, not in the United States, necessarily, but internationally a move toward fully symptom-based procedures where you are, you start out with symptoms of plant response and eventually fall out into a specific emergency. It is a different philosophy. It is a different hierarchy compared to what I understood for your procedural philosophy, if we want to call it that.

MEMBER BROWN: Let me, I wanted to ask for a clarification because my background is more on the symptom-based response. If you look at our operators in the Naval Nuclear Program, our procedures are fundamentally-based on UC. There is a set of symptoms to which the operators respond. There may be alarms going off or an indication doing something. So, I am not familiar with the term that you used event-based or function-based aside from symptom-based. So I am a little bit off track relative to that.

MEMBER SIEBER: Well one of the keys to the U.S. plants, the alarms aren't safety-related. They are using the indication, the actual plant parameters not an alarm that went off.

MEMBER SIEBER: There is a methodology that you go through to tell you what indicators to look at.

It seemed to me when I read this that it was consistent with U.S. PWR practice today, as opposed to the boilers who are symptom-based.

MEMBER STETKAR: Well, and internationally most plants are going to a more integrated system. Granted, we are in the United States. The difference is the operators need to decide that they have a steam generator tube rupture and they go to a steam generator tube rupture procedures, as opposed to the fully symptom-based procedures are that you start out with making sure that you have all of your critical safety functions satisfied. The reactors trip, you have core coolant. You don't care whether it is a LOCA, you don't care whether it is a tube rupture. You don't care whether it is a reactor trip. You do the same thing for everything.

MEMBER SIEBER: That's not the practice.

MEMBER STETKAR: That is not the practice here.

MEMBER SIEBER: Okay.

MEMBER STETKAR: I just wanted to make sure.

MR. SCAROLA: And it's important. It is not the practice by PWRs in the United States.

MEMBER STETKAR: That's true. That is correct. Current PWRs.

MR. SCAROLA: This design is an evolutionary design that follows the practices of the PWR owners group. So there are both event-based procedures as well as function-based procedures.

MEMBER BROWN: What is an event? Tell me what an event is as opposed to --

MR. SCAROLA: And event is something you can actually diagnose. So therefore you take -- in CE plants, they call them optimal recovery versus functional recovery. The optimal recovery is more efficient. It works faster and it puts the plant in a safe condition with less investment challenge.

Functional recovery is when you can't diagnose the event and, therefore, you are only worried about critical safety functions. And you can end up pouring a lot of aerated water into the plant. You can end up venting water onto the floor of the containment. So, it is an investment challenge. Not a safety challenge, but it is an investment challenge.

So, PWRs today try to avoid going to functional recovery by using optimal recovery. They always will attempt to use optimal recovery first.

MEMBER SIEBER: In PWRs in the U.S., I was going to say today but when I was in there isn't today, you actually ran both symptom and event-based procedures at the same time. The operating crew would do event-based and the engineering staff on duty would do the symptom-based. The engineering staff would say to the operating staff, you have this issue and your recovery is not quite working. You may have two faults in the plant, for example.

CHAIRMAN MAYNARD: Well, today's U.S. procedures, it is a symptom-based. You start out, you don't care what the accident is. You care but the procedure leads you down a path based on your indications. And then you get to a point where it leads you into either the optimal recovery for a steam generator or optimal recovery for LOCA or whatever. But it is based on the symptoms that you get there by.

On the side, you have function restoration procedures that if you have got things going on outside of that, then it will lead you into a functional restoration there. But it is kind of a combination. But you start out in a symptom-based to get you let into the optimal recovery procedure.

MEMBER SIEBER: Yes, we might see better as we go on. Why don't we go on?

MEMBER BROWN: And we are interested in keeping submarines and aircraft carriers operating, as opposed to shutting the plants down. So there is a slightly different mind set when you have got 25 and 55 million dollar jets in the air, that you really want to keep that carrier moving.

MEMBER SIEBER: Well, we have got 55 million people living around --

CHAIRMAN MAYNARD: Now, let's move on because we will probably come back to this again later anyway. Let's go ahead and move on.

MR. SCAROLA: One of the man-machine interfaces that you don't see in this photograph is the diverse HSI panel which I will show you later in other photographs when we get into the simulator that we have here in the U.S.

MEMBER STETKAR: Just a quick question

because you had the pretty picture up here.

When I was reading the topical report, you talk about the whole plant is designed for one RO, one SRO and this is a single RO station. But I thought there was a discussion that there could be a two RO version that essentially, I don't know whether it duplicates everything that you see within the operator console there. Is this the standard? And the two RO is for, or is this the two RO?

MR. SCAROLA: I can understand your confusion.

MEMBER STETKAR: Because it seemed to be like the operational VDUs were duplicated.

MEMBER BROWN: Two chairs.

MR. SCAROLA: Two chairs but this photograph that is in the safety system topical report is intended only to be representative of the control room to show the distinction between safety man-machine interfaces and non-safety.

When we get to the HSI topical report, that is where you will see the actual U.S. control room that has the capability for two ROs.

MEMBER STETKAR: So it is duplicate sets of at least the operational VDUs.

MR. SCAROLA: And it has got more VDUs.

MEMBER STETKAR: Okay.

MR. SCAROLA: It duplicates these VDUs --

MEMBER STETKAR: Okay.

MR. SCAROLA: -- in a second RO station.

MEMBER STETKAR: Okay. Thanks. Thanks.

MR. SCAROLA: I'm sorry for that confusion.

MEMBER STETKAR: No, that's fine. That's -- thanks. Thanks.

MR. SCAROLA: I can understand why you are confused. Okay, so let's move on.

Now, this slide just summarizes what I have already said. So we can move on from that. Okay, the next slide.

Now these next few slides talk about some of the key INC features that allow us to achieve some of the key goals of this design. We are using plant-wide digital technology. We use digital technology everywhere, with the exception of addressing common cause failure, which we say we use analogue technology.

The reason for digital technology is to achieve goals of maximum reliability, maximum stability, minimum maintenance. Maximum reliability is basically because digital components have demonstrated higher reliability than analogue components. It is essentially because they are less heat producing. As a result, they have more longevity.

In digital systems, we also have a significant amount of redundancy, even in the non-safety system. So when we do get failures, those failures essentially don't manifest themselves to system-level plant disturbances. So we can have an alarm for a failure. We can repair it before it causes any sort of transient.

Stability is the issue of all of our set points. Constants are all in digital values. Digital values don't drift. So we have more stability. All of this leads to less frequent need to touch the equipment by humans, which ultimately is an enhancement to reliability as well. Because what we find historically is that we have more problems because of maintenance errors than we actually have because of equipment failures.

MEMBER SIEBER: How do you address the issue of processing speed? For example, at TMI, the alarm monitor was about an hour behind in processing and printing out alarms at one point and guaranteed that that was a 1960s system. How do you demonstrate in this system that the processing units can keep up with all the stuff that is going on?

MR. SCAROLA: The simple answer is that this system uses a method of monitoring and data transmission where all of the instruments are monitored every cycle and all of the data is transmitted every cycle, whether it changes or not.

So every cycle, we are sending pressurizer level okay, pressurizer level okay, pressurizer level okay. Then all of a sudden some time later we send the same signal but it says pressurizer level not okay. So, the bus loading, the CPU loading, the bus loading, the loading of the alarm VDU processor, is constant at all times.

MEMBER SIEBER: It is not okay. It goes, the computer goes into some subroutine that says this, this, and this. That is where the bottleneck occurs.

MR. SCAROLA: But in this system, we actually process those subroutines all the time anyway, even when things are okay. We execute all of those subroutines.

MEMBER BROWN: Okay, that was one of my questions I had later. So, I will just ask it now, since you guys brought it up. You talked about, I forgot what the words were, a cyclical deterministic, I have forgotten what the exact words were. And I wanted to translate that into my language from my past experience where it was all done on what we called a main operating loop. Every function was, every calculation, every data from every sensor was sampled, every calculation was done, every alarm was generated or not generated within every operating cycle, whether it be 50 milliseconds or ten milliseconds, however fast you could run the thing to do all of that, such that, and you had a timer, watchdog timers both hardware and software to monitor that all of those functions were done and you didn't overrun your sample time.

MR. SCAROLA: Correct.

MEMBER BROWN: And is that what this does?

MR. SCAROLA: That is what this does.

MEMBER BROWN: I mean everything. I mean, I am talking about in the MELTAC Platform now. I am not talking about the distribution bus. That is --

MR. SCAROLA: Even the distribution bus sends all of the data all of the time, every cycle.

So, what I would like to do, since that gets into a lot of detail, I would like to hold that.

MEMBER BROWN: That is fine. I just wanted that momentary clarification.

MR. SCAROLA: You have summarized the method of addressing his problem. But I would like to wait and get into it in more detail later.

MEMBER BROWN: Not good enough? Jack's still not happy with me.

MEMBER SIEBER: Let me ask one question and I will hold a question for later. What is the cycle time?

MR. SCAROLA: Cycle time varies depending upon the requirement. Some things have a cycle time --

MEMBER SIEBER: Oh, okay.

MR. SCAROLA: -- of 100 milliseconds.

MEMBER SIEBER: Okay.

MR. SCAROLA: But that 100 milliseconds is repetitive every cycle. Some things have a cycle time of two seconds. For example, there is no reason to monitor temperature, RTDs faster because they just are slow things.

MEMBER SIEBER: Okay.

MR. SCAROLA: So we can have varying cycle times.

MEMBER SIEBER: Well that broaches some additional discussion. Okay. Never mind.

The statement that you know every routine and scan every instrument every cycle is not correct. You have a lot of different cycles going on inside and it is all timed out, to give you a relatively constant CPU.

MR. SCAROLA: Right.

CHAIRMAN MAYNARD: Why don't we go ahead and move on because I think we will discuss this later, too.

MR. SCAROLA: Okay. We also use digital technology to achieve --

MEMBER BROWN: Can I make one more -- you talk you one of the reasons. I don't disagree with going to digital microprocessor type technology. Don't take my question any other way. That is all I did for the last 22 years or 32 years.

MEMBER SIEBER: 52 years.

MEMBER BROWN: Pardon? Since 1978. You talked about one of the reasons because you get less heat. And I don't know how you all do it in the commercial world, okay, in this world but all I know is when I went from analogue cabinets that performed a specific function to the same size digital base, microprocessor-based cabinet, I had more heat that I had to deal with in the microprocessor-based systems than I did in the analogue systems.

Now, I performed more functions. I took advantage of the microprocessor technology, ran them harder, but they were hotter and I had to deal with that. And it was a lot more heat relative that we had to deal with.

So, I take it, maybe if you have got bigger cabinets and you have fans running, that is a different issue. You can get rid of, we didn't have any fans, all that kind of stuff.

MR. SCAROLA: We have fans.

MEMBER BROWN: But that is a touchy --

MR. SCAROLA: And of course, it depends on the digital technology that you are using. If you are using bipolar digital technology, it is very heat producing. If you use CMOSS or NMOSS technologies, --

MEMBER BROWN: It was all CMOSS.

MR. SCAROLA: -- it is much less heat reducing.

MEMBER BROWN: I don't disagree with that.

MR. SCAROLA: I can tell you that certainly we have to get rid of whatever heat is in it.

Yes, all right. I just, it was just the same, that was a basis. There is a lot of other bases and reasons for using the digital technology, other than because it is cooler.

MEMBER BLEY: And we do have a little more room.

MEMBER BROWN: And you have got lots of room. Absolutely, relatively.

CHAIRMAN MAYNARD: Why don't we move on.

MR. SCAROLA: I think the realty is that we are using it because it is demonstrated higher reliability.

MEMBER BROWN: I don't disagree with that.

MR. SCAROLA: And that is really the key.

MEMBER BROWN: I don't disagree.

MR. SCAROLA: We also use it because we can get very high coverage of self-diagnostic testing, which means it can automatically test itself to a very large degree. That doesn't mean that we can eliminate all manual tests. There are some manual tests. We still retain them. We will talk about them.

MEMBER BROWN: Sorry I asked the question. Go ahead.

MR. SCAROLA: Okay. In this architecture, we have a four train architecture. And in terms of what is required, the tech specs, you will see this for the US-APWR. In most cases, there are a couple of exceptions, but in most cases, the tech specs require only three divisions to be operable, even though we have four divisions. So, if we lose a division, unlike operating plants today, the tech specs do not have LCOs on loss of those divisions.

So, that facilitates online maintenance which essentially leads to shorter outages. So rather than doing a lot of testing during outages, we can do that testing with the plant online because we can take divisions out of service, put them into tests, run them, put them back in service. And that is really a fundamental key in compressing refueling outage times.

MEMBER SIEBER: Short question, short answer. To what extent do you still use independent analogue control rooms like a feedwater heater level? None?

MR. SCAROLA: Essentially none. Everything is in the digital controllers.

MEMBER SIEBER: You don't have anything that runs separately?

MR. SCAROLA: Well, we have nothing that runs separately that is within the context of the DCD. There may be some things --

MEMBER SIEBER: Yes, --

MR. SCAROLA: -- that are in the balance of plant that we haven't gotten to the detailed design yet that we may conclude we will have a single loop controller but we just have not gotten to that part of the design. But within the scope of the DCD, no. Everything is in the control rooms.

MEMBER SIEBER: You have not made an effort to limit the amount of wiring going back by using independent channels.

MR. SCAROLA: We will talk about wiring in the next slide.

MEMBER SIEBER: Okay.

MR. SCAROLA: Because we certainly have made an attempt to limit wiring.

MEMBER SIEBER: Okay.

MR. SCAROLA: In addition to a four train safety INC architecture, we have a fully redundant non-safety INC architecture. So one of the concerns about well what happens when the alarm VDU fails is addressed by the fact that we have several alarm VDUs in side the control room. They are all running with redundant processing, redundant data communications. So even though things are non-safety in this design, we build in redundancy, self-testing, etcetera, so that there is no single component failure that can challenge plant operation either because it might cause a transient or because it could result in loss of HSI.

There is no single component failure that can challenge plant operation. Now, that is a pretty broad statement but it is a statement that MHI adheres to very rigorously.

Moving on. This next slide is going to talk about remote multiplexing. And this is a key to minimizing cabling. We do use remote multiplexing to minimize the amount of field cables coming back into the central control room. This not only reduces cables but it benefits us with regard to aging issues, as well as fire issues. There is just less cable that we have to worry about.

Multiplexing also improves reliability. Now, some people think that hard wire is more reliable than multiplexing. But the problems with hard wires is you don't know that your connections have failed until you put a demand on those connections. So, until I try to start the pump, I don't know that I have a bad cable. Until I try to open the valve, I don't know that I have a bad terminal block connection. Whereas, with digital multiplexing, we are continuously testing that data communication all the time.

MEMBER SIEBER: So when everything goes

blank, you know you have got a problem. All your digital readouts and --

MR. SCAROLA: I would hope that we know we have a problem before everything goes blank. Because every place we have multiplexing, we have redundancy. So we can fail one day to communication path --

MEMBER SIEBER: You have multiple channels.

MR. SCAROLA: We have multiple channels.

MEMBER SIEBER: Okay.

MR. SCAROLA: We have multiple data communication paths. So, if we fail one, we will get an alarm but we won't have a plant upset condition.

MEMBER SIEBER: Okay.

MR. SCAROLA: In that picture that I showed you before, where we have the safety systems and the non-safety systems, it is important for me to emphasize that all of those systems utilize the MELTAC Platform that we will be talking about later.

So we do have a common digital platform. The reason for that is that we want to minimize engineering so that the engineers in the plant can get trained on one technology. They don't have to be trained on multiple technologies. The maintenance people can be trained on one technology not multiple technology. And the spare parts industry can be carried once for all systems in the plant. So, we have the same spare parts for both the safety system and the non-safety systems and then people say, well does that mean that your non-safety parts meet all the Appendix B requirements? And the answer is for this plant, yes. We are using the same hardware everywhere.

So, again, when we talk about reliability of the alarm system, even though this alarm system is non-safety, we do have safety quality components in the non-safety systems, which is very important.

MEMBER BROWN: Well, actually your document stated that the same platforms are used but they would use lesser standards of QA methods for design and manufacturing than used for the safety platforms. And so that is mentioned, that is stated several times on the document.

MR. SCAROLA: It is meant to refer to the software quality process. It is not meant to refer to --

MEMBER BROWN: So is it a less quality software in the --

MR. SCAROLA: In the non-safety system. In the non-safety system, we do not apply IEEE-7432 quality standards to the software development process. We have non-safety software and safety software. On the hardware side, we are using the same equipment across the board.

So, from a spare parts perspective, it makes the hardware interchangeable. From a software perspective, no. You have to load safety software and safety controllers and non-safety software and non-safety controllers.

MEMBER BROWN: So that is another management problem with software.

MR. SCAROLA: Well, not a frequent management problem. Certainly something that you would have to have under control --

MEMBER BROWN: Is it only a software issue or just, in other words, in the hardware itself is designed, manufactured, tested, etcetera, to the same standard and that the only -- because that is not stated in the documents in any of them.

MR. SCAROLA: I think we need to clarify. We could probably clarify that.

MEMBER BROWN: But I would think that that would just, the idea of having non-safety software utilized for non-safety of whatever, a lower standard of verification or validation that that software is satisfactory, I know, that is hard to swallow. But I mean, I understand what you are doing. And I understand. I mean, I read several statements where you all provided a basis for that but it was not overwhelmingly satisfying as to why we would.

MR. SCAROLA: Well --

MEMBER BROWN: I'm not asking you to justify it right now.

MR. SCAROLA: We'll talk about it a little bit more later but let me just say that the standards for software testing coverage and software documentation requirements, traceability, etcetera, for safety-related software are extremely rigorous. For us to try to apply those same standards to non-safety software is not economically practical due to the complexity of the non-safety software. What it would force us to do is make the non-safety software as simple as the safety software.

MEMBER BROWN: What is wrong with that?

MR. SCAROLA: Because then we would have very unfriendly man-machine interfaces. We would have very primitive automated control systems. But remember, safety system automation is very primitive. I monitor level. When I get to a set point, I actuate. Whereas non-safety control systems have proportion interval derivative controllers inside. There are lead lags. There are many, many feedback networks in non-safety control systems. To attempt to verify and validate that software to the same degree that we verify and validate the simplistic safety software is just beyond the capability of the industry today.

MEMBER BROWN: So my control of a turbine generator or my control of reactivity addition devices like control rods or my control of any other feedback type control system is less important than the reactor's safety function.

MEMBER SIEBER: Yes.

MR. SCAROLA: Well, it is less important form a safety perspective. It is extremely important from an economic perspective. So utilities do encourage suppliers to demonstrate high reliability of their non-safety standards.

MEMBER BROWN: Let me expand on that a little bit. I used the TG set as an -- because I can look at your picture. Say that is a little box down here that is controlling a throttle or a valve or something like that. But there is a lot of other non-safety hardware. A software up in some of these other systems that interface with the safety software from your displays, alarms, etcetera, that is all non-safety software also.

So, I wouldn't really argue with you or disagree -- not argue. That is the wrong word. I would not disagree with you relative to a supervisory instrument for the TG or some other feedback control system or continuous control system that you would have to utilize. But from the standpoint of interfacing the safety system with its operating display, alarm, and indication functions, that software and having that non-safety grade --

MR. SCAROLA: Well realize we do have --

MEMBER BROWN: -- that is just a problem.

MR. SCAROLA: -- safety grade human systems interfaces with very simplistic screen designs, very simplistic control designs and we will be showing those. Simplistic to the point that we can put them through the 7432 V and V process. That is why they are simplistic.

MEMBER BROWN: Yes, but you are not going to be using those all the time.

MR. SCAROLA: Well that is why --

CHAIRMAN MAYNARD: I think we are going to have to move on. First of all, I don't think the key issue is whether it is safety or non-safety. It is what level of controls are put on. Just because it is non-safety doesn't mean that there are absolutely no controls or anything put on it. So, I think we need to get into that.

MEMBER BROWN: Well, I understand that.

CHAIRMAN MAYNARD: But we are running behind and I think we need to move on because we are going to revisit some of these subjects later, too. So, let's go ahead.

MR. SCAROLA: Okay. Finally, as I spoke about a common digital platform, we do have to consider that that common digital platform that is used throughout this has some hidden software defect. A hidden software defect can lead to a common cause failure. So we address that by the Diverse Actuation System.

And within the Diverse Actuation System again we really strive for simplicity. We have simple analogue comparator functions, manual actuation functions so that this results in a design that is simple to test and simple to maintain. Again, striving for simplicity so that we can reduce O and M costs. So that is a fundamental basis of that Diverse Actuation System as well.

And we will talk later about our drive to keep that system as simple as possible and some other drivers that would encourage us to make it more complex. So, we will talk about these issues.

Okay, next slide. Here is some history of this whole design. This design in Japan started out in its application to non-safety systems. The MELTAC Platform was originally applied to non-safety systems. What you see on the right side of that architecture drawing, the PCMS functions, reactivity control, turbine control, steam generator, water level, etcetera.

We have been operating now in non-safety systems for about ten years in five operating plants, 50 different applications of non-safety functions, over 20 million hours of operating experience. And to date, there has been no system malfunction. System malfunction. There have been component failures, board failures, etcetera, but because of the architecture of the design, the redundancy, none of those have become system failures that have impacted the plant.

MEMBER STETKAR: But your 20 million operating hours you use, this is just sort of a comment, use that in several places to justify the very high reliability of this system. And yet, if I do the math, you actually have something on the order of probably 400,000 system operating hours. You might have 20 million individual function operating hours. If you do the math, if you multiply five plants times ten years, --

MR. SCAROLA: Times 50 applications.

MEMBER STETKAR: -- times 50 applications, you get 20 million operating hours.

But many of those applications --

MR. SCAROLA: Well, at least our math is good.

MEMBER STETKAR: Well, it is a little misleading --

MR. SCAROLA: Okay.

MEMBER STETKAR: -- because you say you have never had a reactor trip from a system malfunction and more than 20 million operating hours. Well, I think a lot of those functions --

MR. SCAROLA: Oh, okay.

MEMBER STETKAR: -- wouldn't lead to a reactor trip, if you really had a failure of the function.

MR. SCAROLA: Okay.

MEMBER STETKAR: So I am curious how many hours you have with no function malfunctions, if you will, or channel malfunctions that caused an alternate, you know, switch-over to the alternate feedwater control, you know, the redundant feedwater control or something like that. That is a more, you know, you have two parallel processors. So for feedwater control, for example, and have you ever had any malfunctions that demanded the alternate feedwater control function to take over, which it did successfully, did not result in a plant trip. But you know, if you are using this 20 million function operating hours as a basis for your reliability, you have to be a bit careful about what that means.

MR. SCAROLA: When we say system malfunction and we say we have never had a system malfunction, what we are saying is we have never lost a function in the plant.

MEMBER STETKAR: Oh.

MR. SCAROLA: Feedwater control is a function. Feedwater control is a system. Yes, we have failed some of the components within feedwater control but we have never had a system-level malfunction for feedwater control. That is what we refer to as a system.

MEMBER STETKAR: A failure does not cause a system to stop.

MR. SCAROLA: Right. The failure has not caused loss of function of that system.

MEMBER STETKAR: But did it invoke the standby control? You know, you have the parallel standby controllers.

MR. SCAROLA: Sure.

MEMBER STETKAR: So that is --

MR. SCAROLA: We have had CPU failures that have forced --

MEMBER STETKAR: Okay.

MR. SCAROLA: -- to fail over to the redundant CPU.

MEMBER STETKAR: We should keep going. I just wanted to try to understand what the 20 million applies to.

MEMBER BROWN: But the point here, John, is that he flexibility of the microprocessor-based systems allow you to build in automatically transferred functions that aren't achievable very easily with analogue functions. This really adds to plant reliability.

MEMBER STETKAR: I understand that. It is just if we are doing reliability analysis, we have to be careful about consistently understanding what the numerator and the denominator mean.

MR. SCAROLA: Now, we are now extending the application of this technology to safety systems, reactor protection and engineered safety features. And over the next several years, there will be several safety systems coming online in Japan, the first of which will be the digital safety system upgrade at Ikata 1 and 2, which will be operational the summer of 2009. Then we have an -- that is a digital upgrade project.

Then we have a new plant that is under construction that will go into commercial operation in November of 2009. And then from that point moving forward all the way to about 2013, there are several digital upgrade projects that will apply this to the reactor protection systems. And then ultimately the Tsuruga project which is an APWR that is under construction, that is a 2015 commercial operation date.

So, we started in non-safety applications, had very good success and have now moved into safety applications. So what you see in our topical report represents everything.

Okay. I am going to go on to the next topical report, although maybe we --

CHAIRMAN MAYNARD: I am not familiar with the Japanese regulatory process. Have these been approved for safety related applications in these plants or do you have to get approval? I am not sure what your process is.

MR. SCAROLA: Has there been Japanese regulatory approval?

MR. TAKASHIMA: It is approved. The first one is the Tomari number 3. That plant will start commercial operation next year. We are already approved by --

CHAIRMAN MAYNARD: Okay.

MR. TAKASHIMA: -- Japanese.

CHAIRMAN MAYNARD: Very good. Thank you.

MR. SCAROLA: Okay, we will move on. We are now going to talk about -- oh, excuse me. I just wanted to list for this topical report, I am not going to go through these now. I will be going through each one of these key issues when we get into more detail later. But I wanted to point out that each of these topical reports does identify key issues and we get into them in a little more depth than we get into anything else. So, that is the point of this list and we will be hitting all of these later.

Now we will go on to the HSI System Description and HFE Process Topical Report. This topical report is structured very similar to the safety topical report, a purpose section, a scope section. In section three, we identify the codes and standards that are important to the design of HSI systems. Section four describes the HSI design.

Now before during the NRC's presentation, somebody was talking about DAC and design process. And that shouldn't we, excuse me, I think it was -- I'm not sure where the question came from. But the point was, shouldn't we be reviewing the design, if there is no DAC and not just the process. And that is exactly what we have provided within section four is the actual design of the HSI systems.

We break the HSI systems down into building blocks. A building block is the large display panel. A building block are soft touch controls. A building block is the alarm system. Section four describes each one of these building blocks in a generic sense. And of course, we have to apply those building blocks to each specific plant, such as the US-APWR and that is a design process for the US-APWR that is addressed in the US-APWR HFE program. But the intent of the topical report is to describe the building blocks and we have requested staff approval of those building blocks. We will get into that a lot more later.

Section five then describes the design process. And again here, we talk about past process, which is how did we develop those building blocks. The current process for the US-APWR and the future process would be the application of those building blocks to any future operating power plant as a digital upgrade project.

Section six has additional references that go beyond regulatory criteria. And then section seven again tries to present the perspective okay of this is what we are asking you to review now. We are not asking you to review these things that will come later. And please understand what these things are. So again, it is kind of the roadmap.

MEMBER BROWN: You made the statement in all of these that what is presented in here is typical. And I presume then that the DCD would provide the specifics --

MR. SCAROLA: For a particular plant.

MEMBER BROWN: -- for -- all right.

MR. SCAROLA: Right.

MEMBER BROWN: Now, I think you said that once before and it kind of went in and exited out the other side. So I thought I wanted to make sure I understood that.

MR. SCAROLA: What is not typical is the design basis for each one of these elements. We define the design basis for the large display panel.

MEMBER BROWN: I understand that.

MR. SCAROLA: We do give an example of how that design basis results in a design. So we put a typical large display panel in the topical report, simply to help the staff understand what that means and what the content is.

But clearly, each large display panel would meet the same design basis but may have some slightly different content, depending upon the plant that it is being applied to.

There are three appendices in this document. Appendices A and B focus on what we call the reference design, which is the Japanese standard HSI design. This is the same design that is being applied in Japan. Appendix C basically explains the process we are using to take the Japanese design, phase by phase an apply it to the U.S. And we will talk about that entire process.

CHAIRMAN MAYNARD: I hate to break it here but I think -- I am going to go ahead and break, take a short break here. I look at the schedule and we weren't scheduled for a break until almost right before lunch. And I would rather take a 15 minute break here. We will come back and finish up.

So we will come back at 10:25.

(Whereupon, the above-entitled matter went off the record at 10:13 a.m. and resumed at 10:26 a.m.)

CHAIRMAN MAYNARD: Okay, let's go ahead and get started. We will resume. We have a member or two that will join us when they -- let's go ahead and get started.

MR. SCAROLA: Very good. Okay, whereas the Safety INC Topical Report focuses on the digital architecture behind the control room, the HSI Topical Report focuses on the functional design of all of these man-machine interface building blocks.

These basic HSI design features are expected to improve operator performance and efficiency. And I will just say that we have just completed Phase 1(a) of our U.S. V and V Program using our simulator that has been built in Pittsburgh. And we are, in fact, seeing that, that operator performance has been very good. Operator efficiency looks good.

All of these things are to enable staff reduction compared to conventional control rooms.

Although the US-APWR will accommodate the staffing that we have in existing control rooms, excuse me, the basic HSI will accommodate the existing staffing, which is essentially two ROs inside the control room and an SRO, it enables the reduction down to one RO in the control room.

These are through features such as the large display panel, which is a fixed display to enhance overall plant situation awareness, soft controls that allow us to bring all of the information to the operator, rather than have operators walking around the control room to get information and take controls.

That reduces task burden as well as it allows a more functional or a more cohesive distribution of functional responsibilities when you do have multiple operators. Because in existing control rooms today, we often divide responsibilities by okay, you take that side of the control board, you take that side. Well, you know, the inventory control functions exist on both sides. Well, wouldn't it make more sense to give one guy inventory control? Well, now we can do that.

And lastly, we computerize the data processing, to just help the operator understand what is happening in the plant. A big part of that is distinguishing I and C failures from real plant problems.

In the old control rooms, if I got an instrument failure, well it shows up as pressurizer low pressure. Well now, through my computer processing, I can look at that and say well what are the other instruments doing? The other instruments are not telling me that I have a low pressure. So now I tell the operator that he has an instrument failure, rather than a low pressurizer pressure, which is a huge improvement in the way we present data to the operator and allow that data to help him prioritize his actions.

So the whole point of this topical report is to address these building blocks and explain, essentially, how they enhance the performance inside the control room.

CHAIRMAN MAYNARD: You may have mentioned that the control room staff you were using at the simulator in Pittsburgh, was that a U.S.-staffed operators?

MR. SCAROLA: Yes, U.S. staff. We will talk about that in more detail. You can flip slides.

Now, while all these enhancements improve operator performance, the design also needs to emphasize and does emphasize coping with degraded HSI conditions. Because all of these things are wonderful when they are functioning but we need to train the operators for the cases, the situations where they are not functioning correctly. And that, very honestly is the major challenge of advanced digital main control rooms.

So, included in our design process and included in our V and V Program is the consideration of failures such as complete non-safety VDU freezing or blackout. That means an operator loses that large display panel. He loses all of the non-safety glass in front of him and he is faced with managing the plant and managing accidents with just the safety related things.

We even go beyond that and address common cause failure. All of these MELTAC controllers that are behind the control room, that are doing all the data acquisition, we must assume that we have a common cause failure, they freeze, and therefore we don't get any of that information into the control room anymore. So now we have to rely on the Diverse Actuation System, the diverse HSI panel. So we need to design for that condition, as well as train the operators for that condition.

Finally, we have to deal with evacuation of the main control room. Fire in the control room forces the operators to go to the remote shutdown facility and safely shut down the plant from the remote shutdown facility.

MEMBER BLEY: I'm sorry. Go ahead and finish what you were saying.

MR. SCAROLA: Well I was just going to say that while this computerized HSI is a huge enhancement, we can't forget that we might be putting ourselves in a comfort zone that operators may not be fully prepared for when these things fail. So we have focused our design process to specifically address that concern.

MEMBER BLEY: The kind of things you mentioned here, and it is good to see you are doing that, are kind of, from my point of view, the easier things for an operator to deal with compared to cases that have occurred, and I can't say in the nuclear business but in other places with automatic control, where input data or something else takes things out of the expected and tested range and all of a sudden maybe you register overflow somewhere, and you just start getting anomalous behavior.

MEMBER SIEBER: It sounds like a refinery.

MEMBER BLEY: It has happened there. It has happened in electric power control. It has happened in medical applications.

Have you thought about that and is there any way that you have thought of trying to deal with that to help the operators?

MR. SCAROLA: It happens in analogue control systems as well and we train operators very well for those conditions today. And so we will certainly continue to train with them. And we will continue to do task analysis for those situations. But those are not new situations imposed by digital systems.

The new things imposed by digital systems are the more catastrophic global types of problems that we didn't have before. Because before we had all these individual instruments and individual loops. So failures might affect pressurizer level but they wouldn't effect pressurizer pressure. Now we have the potential for a failure on our data communications network. That means none of the displays are getting, or none of the non-safety displays are getting refreshed. Or a common cause failure that says none of the displays are getting refreshed.

MEMBER BLEY: Let me give you an analogue to what I am concerned about. And it is in between the case you are talking about and the case we used to have. And the only place I have seen it happen with old style systems are with instrument air systems. And there you thought of global failures if you lose all air for some reason.

But the ones that were really difficult were the things where you got moisture into a system or something. And now all of a sudden there are multiple things, kind of widespread but not global, going wrong. Things moving in wrong directions that are linked in a way nobody understands for a while. And that can happen through a system like this. So they are wider spread than you used to have but they are not the complete, it is there, it is gone, kind of thing. It is all of a sudden hunks of it are behaving differently. And I am just wondering if, I know that is really hard to address. I am wondering if you have given that kind some thought.

MR. SCAROLA: Clearly we have, we view it as a problem with analogue systems that we will continue to have in digital systems. We don't necessarily view that digital systems expand that problem. We clearly have that problem.

MEMBER BLEY: But integrated systems expand that problem. But go ahead.

MR. SCAROLA: Okay.

MEMBER BLEY: I mean, somehow I am not communicating the kind of problem I thinking of.

MEMBER SIEBER: Well, let me ask a question that goes all the way back to slide eight. And slide eight, don't go back, but it shows seven CPUs doing different things. Alarm monitors, plant procedures, non-safety systems and so forth.

Since all of the computers in the CPUs have access to the same data, they could operate independently. But I would think that what you want to do is coordinate some of these things.

MR. SCAROLA: Absolutely not.

MEMBER SIEBER: So, one of them has to be in charge. Right? Which one is in charge?

MEMBER BROWN: There are multiple opinions on that.

MEMBER SIEBER: Well, I would like theirs.

MEMBER BROWN: I agree with you but I don't think they are going to answer it the way you think they ought to answer it.

MEMBER SIEBER: Yes, well, if you aren't going to give me a good answer, then we can move on.

MR. SCAROLA: I think for the most part, we see them as parallel processors with nobody in charge.

MEMBER SIEBER: Okay, thanks.

MEMBER BROWN: They run asynchronously.

MR. SCAROLA: They all run asynchronously. They all operate on the same data. They all do different functions with that data.

MEMBER SIEBER: Okay, that answers my question.

MR. SCAROLA: To the extent that the output of an algorithm in this one is an input to an algorithm in another one, yes, there are functional dependencies. But --

MEMBER SIEBER: You mean, they don't calculate the same algorithm independent of one another. They will pass data?

MR. SCAROLA: Well, the redundant parts do. For example, we have redundant alarm VDUs. One is running, one is basically in a hot standby mode.

MEMBER SIEBER: And is all represented in the same box.

MR. SCAROLA: It is all represented in the same box in that picture.

MEMBER SIEBER: Yes, I got that part.

MEMBER BROWN: But the four RPS trains have four separate computation platforms.

MEMBER SIEBER: There is one box.

MR. SCAROLA: No.

MEMBER BROWN: No.

MR. SCAROLA: That is four boxes.

MEMBER BROWN: That is four boxes.

MR. SCAROLA: Well, in the RPS, you have four different divisions. Right? A, B, C, D divisions.

MEMBER SIEBER: Right. Got it.

MR. SCAROLA: We will talk about that more later.

MEMBER SIEBER: Right.

CHAIRMAN MAYNARD: Yes, we need to be moving on.

MR. SCAROLA: All right. Go to the next slide, please.

The HSI system design features that we described in the topical report are directly applicable to the main control room, the remote shutdown room, and the technical support center.

The HSI design process extends to the EOF and local areas of safety significance. So, we are not trying to say that all the building blocks that we are using in the main control room are the same things we are going to use locally. Locally we may, in fact we will, use conventional hand switches and in some cases local analogue meters. The design process will extend to those. The HSI building blocks that we describe in section of this topical report will not. I just want to make sure that is understood.

The reference design for the U.S. basic HSI system is the Japanese standard HSI system. We are extending that with additional consideration for U.S. operating methods and procedures. We found out through engaging U.S. operators in our V and V program that U.S. procedures are quite different from Japanese procedures. And as a result, we are having to make some design changes. And we would have not seen that until we brought U.S. operators into this V and V program, which has been very effective.

Of course we have ergonomic differences between the populations. We have cultural differences in the way we structure things like alarm messages. Very simple things like deviation from set point in Japanese culture is actually written exactly opposite. Set point deviation. Well we say, well gee, the set point should never deviate. The process deviates from the set point. So we have had issues where the operators read alarm messages and they don't get it because we did a direct Japanese translation and now we have to massage those. These are very simple things.

We are also updating the operating experience review that was originally conducted for the Japanese system. We are now extending that for U.S. operating experience. So we are going through U.S. LERs and event reports and making sure that we have everything covered.

Finally, we take what we call the basic HSI, which are the basic features of the design and we apply those on a plant-specific basis through the analysis methodology and the design process that is defined by NUREG-0711. So, this is basically what we start with and where we take it to.

The Japanese standard HSI system is the foundation. It is the foundation of everything that is in this topical report. That was developed using the NUREG-0711 design process. Everything from function analysis to human reliability analysis, V and V activities, including approximately 200 Japanese operators. The same process that is defined as the standard in the U.S. was used for Japan.

And this Japanese HSI system will be

operational in nuclear power plants in Japan in the near future. First Tomari Unit 3, which is a new construction plan, Ikata Unit 1 and 2, which is a main control room modernization program, and it will also be operational in the Japanese PWR training center, which is a new facility. So this is the foundation of what is done in the US-APWR. That foundation is described in this topical report.

Now, when we take that reference design and we apply it in the U.S., we are applying it in a three-phase program. Phase 1 demonstrates overall human performance improvement from the Japanese HSI system compared to conventional HSI. We are also, in Phase 1, demonstrating conformance to U.S. requirements.

Ultimately, the goal of Phase 1 is to identify any changes from the Japanese HSI system that might be needed for the U.S. We are doing this by evaluation using both U.S. HFE experts, Human Factors Engineering experts, and U.S. operators. The Phase 1 report will be submitted for NRC review December of this year. And all of the Japanese development documentation that is the basis of all of this is available for NRC audit.

And I know we are having discussions with the staff now with regard to what Japanese development documentation should be translated, so that the staff can do a more rigorous review of that.

Phase 1 is intended to take that Japanese design and put it through a rigorous V and V program with U.S. personnel, both U.S. HFE experts and U.S. operators. To do that, we are using a dynamic simulator facility that we have built in Pittsburgh, and I will be showing a picture of that next. So, when we get back to this idea of are we asking the staff to approve a design process or a design, we are clearly asking the staff to approve a design, not just a process.

Extending this further. The end of Phase 1 is expected to result in some revisions to this topical report that we are talking about. If we find that some of the basic HSI features need to be modified for U.S. operators, we will reflect those modifications in the revision to this topical report. At the end of Phase 1, we will say this is our U.S. basic HSI design. This is what will be applied to the US-APWR. This is what will be applied to all future applications in the United States.

The application process is what we call Phase 2. Phase 2 applies this HSI system to the US-

APWR. And what we mean by application, it means we do all the function analysis, all the task analysis, all the human reliability analysis that is specific to the US-APWR that will result in the specific display for the large display panel. The specific displays for the 250 displays that are in the display inventory.

In other words, the displays will reflect the piping mimics for the US-APWR. The displays will reflect the specific alarms for the US-APWR. Whereas, Phase 1 describes the method of navigating, Phase 2 describes what you are navigating to. It gives you the inventory of all of the pictures. Phase 1 describes the method of alarm presentation. Phase 2 identifies the actual alarms that are applicable to a US-APWR.

All of the Phase 2 activities are conducted over the next several years. Some of the analysis reports, function allocation, task analysis, and human reliability analysis will be submitted to the staff in June of next year. Subsequent reports after that will be submitted over the next two years.

So, we go from Phase 1, which is a basic HSI design to Phase 2, which is the application of that to the US-APWR. Phase 3 then becomes the site-specific design. So when we go from a generic US-APWR to a site-specific Comanche Peak Units 3 and 4, there may some additional changes. For example, in Phase 2, we would design what we think is the ultimate heat sink but the ultimate heat sink is a site-specific system. So Phase 3 may adjust that ultimate heat sink for the site-specific applications.

MEMBER BLEY: Let me ask a question about that process. When that happens, is there a resulting update to the DCD or amendments to the Tier 1 or something or it is all --

MR. SCAROLA: No.

MEMBER BLEY: What is it?

MR. SCAROLA: These are site-specific activities. So they would not affect the DCD at all. They would not affect Tier 1 in any way.

All of the basic HSI features, the method of navigation, the icons that we use throughout the system, the way we present alarms, are generically applicable. Now we are applying them to the ultimate heat sink, which is a site-specific design system. So, I would see no upgrades or no revisions to anything in the DCD. I actually think that this is a level of detail that is not even addressed in the COLA.

MEMBER BROWN: Are the icons consistent

with what other type stuff that U.S. operators are used to looking at? I mean, you --

MR. SCAROLA: Does a pump icon look like a pump?

MEMBER BROWN: Well I don't know. You said you were translating them from -- I don't know. I have never seen a screen that showed some icons for the Japanese-style systems. You know, whether they use circles with little lines or whether they use a box with a pipe coming in, I have no idea.

So, you get used to see certain icons and all of a sudden your mind connects to them when you are an operator. And that I just wondered if they are the same or whatever --

MR. SCAROLA: They are the same --

MEMBER BROWN: -- or close enough.

MR. SCAROLA: -- thus far. They are the same. Okay? But I also have to say --

MEMBER BROWN: I would think they would be universal but --

MR. SCAROLA: -- that there is no U.S. standard for what icons have to look like for different things.

MEMBER BROWN: I understand that.

CHAIRMAN MAYNARD: That is what I was

going to say. They are all different and even like colors mean different things and stuff.

MEMBER SIEBER: They all look like P and IDs.

CHAIRMAN MAYNARD: We need to move on here.

MR. SCAROLA: Okay.

CHAIRMAN MAYNARD: Again, this is an overview of the overview. We are going to be going each one of these topics again, here.

MR. SCAROLA: This is the Pittsburgh simulation facility that we are using in Phase 1, will use in Phase 2. Phase 3 is somewhat up in the air as to whether or not that might be at the Comanche Peak site versus a central facility. But this is a fully dynamic simulator. It models all of the basic HSI features. The plant model that is actually behind this is a conventional Japanese PWR. It is not the US-APWR. We don't have the US-APWR plant models yet. So this is actually representative but it will become the US-APWR plant-specific over time.

MEMBER SIEBER: He gets them back at Costco.

CHAIRMAN MAYNARD: We'll move on.

MR. SCAROLA: The topical report addresses many things. A number of key issues. We will be hitting all of these when we get to the proprietary section. But you will see things in here like computerized procedures, which is a generic TWG issue. You will see soft controls, another generic TWG issue, multi-division VDUs, as we talked about before. So there are a number of issues that we address in the topical report that are essentially generic industry TWG issues and we try to address each one of them.

That's all I had on the HSI. We will hit it in more detail later. If there are no questions, we will move on to the MELTAC Topical Report.

MEMBER BLEY: One quick question on the slide you had before. In a Phase 1, and I guess that is where it be, it sounds as if there is thorough documentation of the delta between the Japanese version and what is going on in the U.S. design. But some of the detailed underlying design documents are only for the Japanese design and not all of them have been or probably will be delivered to NRC and maybe unless they ask for it. Is that right? That is what I think I heard you say.

MR. SCAROLA: Okay. Let me take a good example. At the end of this year, we will generate an operating experience review report that takes the Japanese, that takes the OER that was done for the Japanese and now extends it for U.S. applications. That report will have a section that summarizes all of the Japanese OER activities and the key things that came out of that.

It is our intent for every one of these reports that we produce, and there are about 12 reports, the first one is OER, then we do function allocation, task analysis, staffing, HRA, etcetera, every one of those reports, we intend to include in those reports a summary of all of the Japanese activities and how those are pertinent to the US-APWR. That was our intent.

The staff has recently asked us to make submittals of some of that Japanese documentation. So what we are now doing is we have to meet with the staff, get some neutral agreement on what they really need to see, and then we have to go through a translation process.

MEMBER BLEY: Fair enough.

MR. SCAROLA: Okay, any other HSI questions? We will move on to MELTAC.

Okay. The MELTAC Topical Report is entitled Safety System Digital Platform MELTAC. It has a similar table of contents, purpose, scope, relevant codes and standards.

Section four, as in other topical reports, is the description of the platform, including before we talked about HSI building blocks, now these are the building blocks for the digital systems behind the HSI. So, we have the digital building blocks such as input modules, output modules, central processors, data communication building blocks, etcetera.

Section five describes all of the equipment qualification that has been done. Environmental qualification, seismic, electromagnetic interference qualification, etcetera.

Section six describes the lifecycle process which, for digital systems is essentially a description of how the software was developed and the overall quality program for that software.

Section seven describes equipment reliability. The reliability of the individual components and how we take component reliability and ultimately develop system reliability numbers. So it describes the processes for analyzing equipment reliability.

Appendix A provides the hardware specifications for each one of the modules in the design. The input modules can handle zero to ten volts at so many milliamps and those types of specifications. Appendix B describes all of the software building blocks that are available to the designer for building-specific applications.

So, for example, in Appendix B you will find that there is a building block which is an AND-gate, another building block which is an OR-gate, or a flip-flop, or a latch, or a counter, whatever it might be, all the building blocks. The whole library of building blocks are described in Section B.

MELTAC stands for Mitsubishi Electric Total Advance Controller. So when we say MELCO, that is what we mean. Mitsubishi Electric Company. MELTAC is -- I think you know.

MEMBER BROWN: Can I answer the question?

MR. SCAROLA: The basis, there are two fundamental principals in the design of the MELTAC Platform, simple design and high quality. And we will be talking about both of those as we get into this.

This slide simplistically represents all of the building blocks of the MELTAC Platform. The most fundamental one is the controller. And here we blow up the controller and we see that inside controllers we have CPUs, which are the brains, and

I/O chassis which are the data acquisition and results outputs. There are, in any system there are, multiple controllers. Here we see four represented. The multiple controllers intercommunicate via something we call the control network. This is a data communication network that allows one controller to send and receive data from any of the other controllers that are in the system. We also have --

MEMBER BROWN: Excuse me. A MELTAC is the controller box.

MR. SCAROLA: MELTAC is the aggregate. Let me explain. MELTAC includes the controller. It includes the control network. It includes the safety VDU processor which drives the safety VDUs inside the control room. The safety VDUs are part of MELTAC. All of the things that you see on this are all part of MELTAC, which the exception of the operational VDU. We don't actually -- I don't think we consider that part of MELTAC. Am I right in saying that?

MEMBER BROWN: Well, no, the reason I ask the question is that I go into reactor protector -- the RPS train. It says it has a MELTAC Platform. But if I look within the train, it has got the controller but the safety VDU is outside. It is somewhere else. It is after the distribution bus.

MR. SCAROLA: Yes, but it is train, though. If you look at one division of an RPS, of a train, you will see a safety VDU division A, a safety VDU processor, --

MEMBER BROWN: Okay, thank you. That wasn't clear from looking at the pictures.

MR. SCAROLA: Okay. Okay. We will have to try and clarify that through the presentations.

All of these components, including, for example, here we see what we are trying to represent here as inter-division data communication.

MEMBER BROWN: Is that --

MR. SCAROLA: So this might be the controller in one train talking to a controller in another train. And we do that via data links.

MEMBER BROWN: In your little picture, you show one giant bus going across all RPS, all PCMS.

MR. SCAROLA: That is this guy, what we call the control network.

MEMBER BROWN: Okay but is that part of MELTAC?

MR. SCAROLA: Yes, it is part of MELTAC also.

MEMBER BROWN: But there is not ten of those. There is just one.

MR. SCAROLA: Well, there is five of these control networks, division A, B, C and D. No, excuse me. Four of those, A, B, C, and D.

MEMBER BROWN: So that is the bus --

CHAIRMAN MAYNARD: You have five fingers.

MEMBER BROWN: That is the bus within the train.

MR. SCAROLA: Within the train.

MEMBER BROWN: Okay.

MR. SCAROLA: Now we have the intertrain bus, which is this one. Same technology.

MEMBER BROWN: And that is the bus up here?

MR. SCAROLA: That is the bus up there.

MEMBER BROWN: Okay.

MR. SCAROLA: Same technology. Still the control network but used at a different hierarchical level in the architecture.

MEMBER BROWN: There is only one of those.

MR. SCAROLA: Only one of those that goes across the entire plant. Non-safety, safety.

MEMBER BROWN: Okay. All right.

MR. SCAROLA: Okay. Now, in addition to all of those, we also have this dotted line here that we call the maintenance network and the engineering tool, which basically allows us to do more detailed diagnostics of failures and also, if we need to, upgrade the software. So, we will talk about all of these features of the MELTAC Platform.

Moving on. A fundamental part of the MELTAC Platform is the basic software architecture. What we are trying to simplistically represent in this picture is that the software executes one function block at a time deterministically. It never changes. And we will get into this in a lot more detail as we get into the proprietary section.

This slide summarizes the operating history as well as projections. Ah, I needed my proprietary information for this. Let me just say that the development began in 1985. As I said before, we started in non-safety applications and moved to safety applications. The first installations of non-safety were in 1991. The first safety installations will be occurring next year, 2009.

To date, refresh me with the memories, with the numbers, we have approximately 80 controllers in operation, 70 or 80 controllers? Excuse me, 70 controllers that are in operation today doing various functions. By 2011 we will have about 200 controllers and by 2015, which will be when the US-APWR goes into operation, help me with the number, over 2000? Over 1000. Over 100 controllers.

All of these controllers utilize the same basic software. The application software in every controller is, of course, unique. But the important thing is we are rapidly gaining operating experience with this Platform. And as you gain more and more operating experience with the same basic software, you get more and more confidence that you don't have hidden software defects. And that is an important point that we will be raising as we go through this whole discussion.

MEMBER BROWN: So you don't integrate the application code with the operating, --

MR. SCAROLA: Absolutely not.

MEMBER BROWN: -- the fundamental loop operating system. You don't --

MR. SCAROLA: They are completely independent. Actually in separate read-only memory.

MEMBER BROWN: That was another question.

MR. SCAROLA: We use different types of memory for the --

MEMBER BROWN: I will ask you that question later.

MEMBER BLEY: In these, and I think you

called them now I forget what you called them but operating experience reports that it sounds like you are doing every year from, as you gather more and more experience. It sounds as if those will be available to NRC to read. And do they go down to explain where you have had problems and failures functionally what went wrong, what were the modes of what happened so that they can understand what problems have existed and how they have been --

MR. SCAROLA: Let me clarify what I think is a misunderstanding.

MEMBER BLEY: Fine.

MR. SCAROLA: OER, Operating Experience Review, is a program element of NUREG-0711 applicable to the HSI. It is not applicable to the operating experience of the platform, of the digital platform. It is an HSI/HFE function. Okay?

The way we manage operating experience in the digital platform is through the Appendix B quality program, which requires problem reporting and then corrective action documentation. So, the end result is essentially the same but it is done through a different process. It is done through the Appendix B quality program, as opposed to a NUREG-0711 program element.

MEMBER BLEY: Okay.

MR. SCAROLA: But clearly, we do record all of our operating experience. When we have operating problems in the field, we document those problems. We evaluate the problems. If the problems are related to something that requires a design change, then we document that design change through the corrective actions program. And the topical report does describe that corrective actions program as part of the process. Part of the lifecycle process.

MEMBER BLEY: Okay. And these Appendix B reports, even though right now they are not for experience with failures in the U.S., are those going to be available for the review process?

MR. SCAROLA: Yes. I think we actually had some of those available in the audit that was recently conducted by the staff. The staff recently did an audit on the MELTAC Platform. And I believe we had corrective action reports in that audit. Maybe the auditors can tell me. Do you recall seeing any corrective action issues?

MR. WILSON: No, I don't Ken.

MR. SCAROLA: All right.

CHAIRMAN MAYNARD: You need to stand up

and identify yourself for the record. And you need to come to a microphone, too.

MR. WILSON: I'm Tom Wilson, Oak Ridge National Lab. I participated in the staff audit that Ken is describing. Now, I don't recall seeing that particular thing but that was not the area I was looking at. I don't think we actually audited that particular feature of it.

MR. SCAROLA: If the staff would like to see that, we could make it available to them.

MEMBER BLEY: Thank you.

MR. SCAROLA: It's not a problem. Okay, let's move on.

In this topical report the key issues that we address are in this list. We will be talking about all of those when we get to the proprietary section.

CHAIRMAN MAYNARD: Let's stop here just a minute. I just want to check. Is there anybody in the audience from the public that is going to want to make any comments? Okay, let's go ahead and move on.

MR. SCAROLA: Finally, the last topical report is the Defense-in-Depth and Diversity Topical Report. We have a similar table of contents here.

When we get to section four, we basically present the I and C overview similar to what has already been presented in the safety system topical report. It is simply repeated here for convenience.

Section five talks about the basic principles of our Defense-in-Depth strategy, which we will talk about. We have a strategy that looks at the risk significance of the events, basically the event frequencies and provides Defense-in-Depth in accordance with the frequency of that event. And we will be talking about those things as we get into this.

Section six describes specifically the design of the Diverse Actuation System. Now, we do describe specific functions of the diverse actuation system and specific sensors that it monitors. But we explain that these are typical. The actual functions and actual sensors are in plant design documentation, which is for the US-APWR, it is all described within Chapter 7.9 of the DCD.

Section seven analyzes the diversity between the analogue Diverse Actuation System and the digital PSMS, which is kind of a trivial analysis because it is kind of hard to find a lot of commonality between an analogue system and a digital system. But nevertheless, we analyze it because it is a requirement of NUREG-6303.

Section eight describes the analysis methods that we use for demonstrating that we can cope with a plant accident concurrent with a common cause failure. BTP-719 calls this best estimate analysis. Well, best estimate is not well defined in BTP-719. So, we define it. We say this is what we mean by best estimate and we explain the analysis methodology. Now, we don't provide the analysis in this document. The analysis for the US-APWR is actually in a separate technical report for the US-APWR. Every plant will have its own D3 coping analysis but every plant will use this same methodology. So we are asking the staff to approve the methodology, not the specific analysis. The analysis is done separately.

Section nine has the key technical issues. We will be going through those. And then of course, section ten is like all of the other documents. It gives the map of what we are asking the staff to approve versus what we expect to have in future submittals. One of those, for example, being this D3 coping analysis.

MEMBER SIEBER: The D3 coping analysis method description, do you set out what is acceptable and what is not?

MR. SCAROLA: We define the acceptance

criteria, yes.

MEMBER STETKAR: Can I just make sure? We have the technical report for the --

MR. SCAROLA: US-APWR?

MEMBER STETKAR: -- US-APWR. So that technical analysis, in combination with this topical report should cover everything that we need to know for certifying the US-APWR. Is that correct? Each plant is different.

MR. SCAROLA: Yes.

MEMBER STETKAR: Now, I was wondering where the interface between because I haven't read this technical report yet.

MR. SCAROLA: Okay. If we look at the topical report as kind of the mother document, this is the representation of the functionality. Now, a sub-tier to that is the technical report for the US-APWR. Another sub-tier is section 7.9 of the DCD.

MEMBER STETKAR: Okay.

MR. SCAROLA: But the 7.9 describes the specific DAS functions for the US-APWR. The analysis then takes credit for those functions.

MEMBER STETKAR: What I was trying to get to and probably not being very clear is that I don't need to worry about specific COL ITAACs for example.

MR. SCAROLA: Not --

MEMBER STETKAR: Because the level of detail and scope of information for understanding how you satisfy the D3.

MR. SCAROLA: You are correct.

MEMBER SIEBER: For the topical report.

MEMBER STETKAR: Okay. Thanks.

MR. SCAROLA: Now, there may be some construction ITAACs.

MEMBER STETKAR: Yes, okay. Yes.

MR. SCAROLA: But not designs. But not DACs.

MEMBER STETKAR: Okay. Not DACs.

MR. SCAROLA: Not DACs.

MEMBER STETKAR: Not DACs.

MR. SCAROLA: Okay, let's move on.

MEMBER SHACK: You have many ITAACs.

MR. SCAROLA: Yes. But -- okay.

MEMBER STETKAR: People tend to use DAC and ITAAC interchangeably a lot. I have somehow gotten into that.

MR. SCAROLA: What we are talking about in this topical report is essentially this section of this big architecture drawing, where we call this the Diverse Actuation System. The Diverse Actuation

System has a diverse HSI panel, which is a conventional panel, switches, analogue indicators inside the main control room. It has a cabinet that interfaces to that. The cabinet also supplements the manual actuations with automated actuations for certain functions. And then finally the interface into the plant.

In our Pittsburgh simulator facility, the diverse HSI panel is this panel that is on the side of the control room. We were not able to get that panel fully instrumented and tied to the simulator for our Phase 1 activities. It will certainly be tied to the simulator for Phase 2.

Phase 1 actually has two parts, 1(a) and 1(b). 1(b) is starting in March of next year. I think the jury is still -- are we going to have it?

MR. REMLEY: The operational.

MR. SCAROLA: Wonderful. So we will have that DHP for what we call Phase 1(b). And we will be talking about 1(a) and 1(b) in more detail later. So we will have it shortly, which will be very helpful to us.

MEMBER SHACK: Given its own picture, I mean, all I can see is a corner of it behind.

MR. SCAROLA: Yes, well, let me explain to you why.

MEMBER SHACK: It's cardboard.

MR. SCAROLA: The reason it doesn't have a picture is right now it is a cabinet with sheet metal on it. It doesn't have switches and indicators. It won't have that until March. So that is why it -- we didn't want to give you a close-up.

CHAIRMAN MAYNARD: Do you also have a remote shutdown panel?

MR. SCAROLA: Yes.

CHAIRMAN MAYNARD: And that may not be the topic of these but is it more similar to your diverse panel or is it --

MR. SCAROLA: The remote, if you go back one, I will just hit it very, very quickly. The remote shutdown panel essentially looks like this right corner of the reactor console. It has got safety VDUs and a couple of operational VDUs. It assumes the digital system is functioning. We do not take a common cause failure with a fire in the control room, with evacuation of the control room. Common cause failure is an event unto itself.

MEMBER STETKAR: Okay. Just to make sure that I understand it. That means the DAS has no controls at the remote shutdown panel. Is that correct?

MR. SCAROLA: Correct.

MEMBER STETKAR: Okay.

MR. SCAROLA: Correct. Because again, the design basis for common cause failure is not concurrent with fires or not concurrent with evacuation of the control room.

MEMBER BROWN: Okay. Let me make sure I understand exactly. So, the DAS is a function that only can be utilized within the main control room.

MR. SCAROLA: Correct.

MEMBER BROWN: There is not a DAS, a remote DAS similar to the remote control station --

MR. SCAROLA: Correct.

MEMBER BROWN: -- or unit or whatever.

MR. SCAROLA: Correct.

MEMBER BROWN: Okay, I didn't quite understand that. Thank you.

MR. SCAROLA: Okay. Let me just an overview of our strategy for D3. First and foremost, we do everything we can to minimize the potential for common cause failure in the PSMS. Our key strategies there are both functional diversity and design simplicity. So, the first and foremost is to minimize the potential for common cause failure. We believe we have actually eliminated the potential for common cause failure but, of course, you can never prove that. It can never be proven so all we can say is we have done everything that industry technology allows us to do. We have taken every precaution that we know how to take. And we will talk about all of these things, simplicity, diversity, etcetera.

Then, despite all of that, we assume we have a common cause failures and now we demonstrate that we can cope with that common cause failure. We provide a Diverse Actuation System which is immune to that common cause failure. And the immunity comes through this diverse analogue technology. Now, we look at --

MEMBER SHACK: Well actually, in you diversity report, it could be a diverse digital system.

MR. SCAROLA: Well, that is very true. If you look at the D3 report, is it the D3, yes. If you look at the D3 report -- no. I'm sorry.

If you look at the safety system report, it simply says that the diversity is defined in the D3 report.

MEMBER SHACK: Yes.

MR. SCAROLA: Okay? It doesn't say what

the technology is. It could be analogue or digital, as long as you demonstrate sufficient diversity. But the D3 report that we have submitted describes an analogue system. So that is all we are asking the staff to approve.

MEMBER SHACK: It does. Yes, you are right. It does.

MR. SCAROLA: The D3 clearly states it is an analogue system. So that is all we are asking.

MEMBER SHACK: Clearly, the APWR intends to have an analogue system.

MR. SCAROLA: APWR references that D3 and it will have an analogue system.

We just wanted to leave the door open in the safety system so that if a future customer who is doing a digital upgrade decides they don't want an analogue system, they could design a separate DAS. It meets all the same functional requirements but they would have to demonstrate adequate diversity for whatever technology they select.

As the staff often tells us, you can take the easy path or the hard path. The easy path would be use an analogue system. The harder path would be, okay, use something else but you have to demonstrate diversity.

Okay, so now we get back to our strategy. And our strategy looks at the frequency of these events and we provide commensurate Defense-in-Depth based on the frequency.

For example, for anticipated operational occurrences, we have automated DAS functions in accordance with the ATWS rule. The ATWS rule says you must have the following automated functions. For different PWR types, we basically follow the Westinghouse PWR type because this is, essentially, an evolution of a Westinghouse-style plant.

For postulated accidents of moderate frequency, we have automated or manual DAS functions to achieve the acceptance criteria defined in BTP-19, which is the most fundamental one is no offsite releases that exceed the 10 C.F.R. 100 limits. And we demonstrate that through best estimate analysis.

So, we look at each one of these events. We do a best estimate. We say we have met the criteria.

Lastly, we have large break LOCA. Large break LOCA is where we have looked at this the same way it was looked at for System 80 plus during that design certification process. We analyze the potential frequency of the common cause failure. The frequency of the postulated accident. And we conclude that the best thing that we should do here is to balance prevention and mitigation. So we do what we can to prevent the accident based on leak detection, where we have diverse leak detection capability. We have diverse manual shutdown controls such that if we detect a leak, we can diversely shut down the plant. And we ultimately have diverse ECCS actuation capability. In the event that there really is a large break, now we give the operator the ultimate defense.

So, depending upon the frequency of the accident, our strategy varies. And we will talk more in depth about that varying strategy.

CHAIRMAN MAYNARD: We have about ten minutes to go over about 20 slides. So --

MR. SCAROLA: Okay. I understand. Okay, if we can move to the next slide.

This basically is a simplified representation of the safety system, which is the normal half from sensor all the way to actuation. In this case, we are showing the reactor trip breaker. And here you see we isolate those sensor signals, take them in their analogue form over to the diverse actuation cabinet. Here we have conventional logic where we monitor that same set point in an analogue or that same parameter in an analogue bistable. The output of the analogue bistable is used to trip, in this case, the motor generator sets. So, we basically have a parallel function but diversity all the way from the output of the sensor, all the way down to the actuation. And that is fundamentally how the DAS works throughout.

The DAS design is based on conventional analogue technology that is currently operating in analogue protection systems in Japan. So the DAS technology is well proven. Its analogue technology has been around for years. And the same strategy that we are applying in the U.S. is the strategy that is being applied to all of these plant in Japan that will have digital reactor protection systems.

The topical report addresses all of these key issues, including our strategy for each one of the event frequencies.

Okay, that is much as I had to say about the topical reports. The next section which I said we would address if time permits, it looks like time does not permit. So we could stop right here, unless there are specific things in this following section that you have looked at previously because you had a draft of this that you would like me to address. But I was hoping we would have time. It looks like we are not going to have time for it.

CHAIRMAN MAYNARD: About how much time do you think it would take to do it right?

MR. SCAROLA: I can hit the high points in probably ten minutes and then we could go back if we want to get into any specific areas.

CHAIRMAN MAYNARD: I think that might be worthwhile.

MR. SCAROLA: Okay.

CHAIRMAN MAYNARD: If that is not enough time, then we will just put it off. But before you do that, let me check one more time and make sure there is no members of the public that are here that want to make any public comments.

Okay, go ahead.

MR. SCAROLA: Okay. Now this section is intended to give an overview of how this digital technology will impact plant personnel. The first one speaks to the issue of information and control accessibility. In existing control rooms, we send the operator to the information. He has to traverse a large real estate of boards. In this design, we bring the information and the controls to the operator. This is the fundamental thing that enables staff reduction. And I will just leave it at that. We will move one.

This is just an example of the navigation scheme. This is a high-level screen menu that allows the operator to access roughly 250 displays. This is the highest level in the information hierarchy. There are various levels. So, by making a touch on this screen, the operator can get to any information in the plant. Let's move on.

Another important feature, before I touched on it very briefly, and that is computerized data processing. One of the things that we use this computer for is to continuously cross-check redundant instruments. Existing control rooms do that once a shift, once every eight hours, the operators are required to manually compare all of the instruments in the redundant safety channels. This system does it continuously and automatically. Operators don't have to do it. If the computer sees a problem, it sounds an alarm.

MEMBER STETKAR: I hope when you talk more about the detailed system design you are going to talk about the, I have forgotten, there is an acronym SSA, the signal select --

MR. SCAROLA: The signal selection

algorithm. SSA.

MEMBER STETKAR: Is there part of -- okay thanks.

MR. SCAROLA: We'll talk about it later.

Next one, automated actuation checks. One of the most time consuming things for operators to do during the execution of the emergency operating procedures is the verification that if the ECCS was demanded, that all of the components of the ECCS actually responded and lined up correctly.

Containment isolation. I get a containment isolation signal, have all 150 valves actuated correctly. Extremely time consuming tasks, something that takes a matter of seconds for the computer. We automate it. Simply tell the operator everything is okay or something is not okay and then they can drill down to see what is not okay.

MEMBER BLEY: Do any of the operators you have run through this get a little uncomfortable with that?

MR. SCAROLA: Actually the operators have responded extremely well to this. They think this is great. This is the greatest thing since sliced bread. Because this information is shown on our large display panel. It is one of the highest level situation awareness features that we have. And at a glance, the operators can see every safety function that is actuated and whether the actuation was successful or the degree of degradation. We display things like "not okay" in various colors. Red color means it is really not okay. Yellow color means, some things didn't go but don't worry about it. Move on and do something else. You can worry about this later.

So, the operators seem to have adapted extremely well to it. And I think it is because if they want to drill down, they can drill down. If they want to look at every pump and valve and they have the time to do that, they can look at every single pump and valve and they can see where it has gone. We automate the process.

MEMBER STETKAR: Ken, is that -- I missed it. Is that display one of the ones that you can pull up on the safety VDUs? Is the okay, whatever you call it --

MR. SCAROLA: No. No, it is not.

MEMBER STETKAR: It is not. Okay, thanks.

MR. SCAROLA: And this all gets back to the complexity of the software.

MEMBER STETKAR: I know there were some

things that you can pull up on the safety VDUs.

MR. SCAROLA: What we try to do on the safety VDUs --

MEMBER STETKAR: That's okay. --

MR. SCAROLA: -- is keep it as simple as possible.

MEMBER STETKAR: We will get into it. That's --

MR. SCAROLA: Okay.

MEMBER STETKAR: I just didn't -- thanks.

MR. SCAROLA: Similar to verifying automated actuation, we also want the operators to be continuously aware of the availability of their safety system. So, there is an acronym in the industry, bypassed or inoperable status indication or some people refer to it as BISI.

BISI is automated in this design. We use the computers to continuously look at the availability of the things that may need to be actuated in the future. And if something is not available, we have logic that determines the effect at the system level. And if the system function of ECCS or the system function of containment spray is not available, then we say not okay. And the operator can drill down.

Again, we use the computer for the --

MEMBER SIEBER: Does it check the tech specs for operability requirements and say you have got to shut down, for example?

MR. SCAROLA: When you say does it --

MEMBER SIEBER: Or does it just say not okay?

MR. SCAROLA: Well the tech specs will often go beyond lineups.

MEMBER SIEBER: Right.

MR. SCAROLA: It basically checks the ability to actuate and the ability to achieve the lineup.

MEMBER SIEBER: Right.

MR. SCAROLA: If the tech spec goes beyond that, no. It may not be checking all of the tech spec parameters.

MEMBER SIEBER: But does it tell the operator that, based on what it knows, whether it is complying with tech specs? Like if some system is unavailable and tech specs say it has to be available?

MR. SCAROLA: Oh, okay. This is very interesting. This system will tell the operator that the system is available or not available.

MEMBER SIEBER: Right.

MR. SCAROLA: Whether or not that is a

tech spec violation may be mode dependent. It may be the tech specs require two divisions in this mode but four divisions in this mode. No, the system does not go that far. But I believe there is an offline system. Maybe you can --

MR. TAKASHIMA: Maybe some will be some way of checking of the tech spec or a checking system will be provided but it is not fix it.

MR. SCAROLA: Yes, but we don't describe that in the topical report because --

MEMBER SIEBER: That's not a bad feature.

MR. SCAROLA: -- it is not a standard feature of the design. It is clearly something Luminant has asked for. They said, look, your system tells us the availability of systems but would you take it the next step and tell us whether we are violating a tech spec or not. Yes, that might be something we do in the plant computer but we don't think it is critical to the staff safety determination of this design because --

CHAIRMAN MAYNARD: I would be a little cautious about integrating that into the program. Running computerized tech specs may be fine but you may want to consider running that.

MR. SCAROLA: Which is exactly what is

being considered. This is something we would run in a separate IT computer, an information technology computer, not the online system that we are running in the plant.

MEMBER STETKAR: I am assuming, I didn't see it in there but I am assuming that the bypass inoperable status indication extends down to all of the support systems for each train. So, if you have a ventilation fan out of service or a cooling water valve shut, it will fold back up in. So you have got the full end-to-end.

MR. SCAROLA: Right, end-to-end.

MEMBER STETKAR: Okay.

MEMBER SIEBER: Well, BISI usually doesn't got to ventilation. It goes to cooling water.

MEMBER STETKAR: That is why I wanted to ask.

MR. SCAROLA: But it will go to cooling water and ventilation if those are required for the operation of this RHR pump or this safety injection pump.

MEMBER STETKAR: Required functionally or administratively?

MR. SCAROLA: No, functionally.

MEMBER STETKAR: Because sometimes they

are different.

MR. SCAROLA: Functionally.

MEMBER STETKAR: Well --

MEMBER SIEBER: Yes, there is a difference. Air conditioning is administrative.

MR. SCAROLA: Okay. Another important feature of the design is alarm management. We do a number of things to minimize nuisance alarms. We will be spending more time on that later. Let's go on from that.

And lastly, I think we spoke a little about this before, all of these advance features are very good in helping the operators perform better, perform more efficiently. But we really need to recognize that the failure modes can be different and we need to train operators to respond to those failure modes. And we need to design so that we have accommodated those failures modes.

So, in this new control room, we employ redundancy everywhere so that we minimize the frequency of large catastrophic integrated failures but we still have to recognize that they can happen.

So, for example, some of the things that we did in Phase 1 for the operators from Luminant is we put them through degraded HSI conditions and we looked, we monitored how they responded. And some responded better than others. And we have some things we have to do in the design to improve it but we clearly have good data now. I would say that the biggest challenge we have for operator training is degraded HSI in these control rooms.

If we look at this next picture -- oh, did I miss one? Okay, let's just go to channel calibration. That is fine.

Okay, everything that we talked about so far pertains to the operators. Now, we are going to talk a little bit about the technicians. A big thing that technicians do is calibrate instruments and all of the modules that relate to the instrument loop, for example, signal conditioners, filters, computational lead lags. Technicians calibrate these things every 30 days. And it is a tremendously labor-intensive activity.

In the digital system, the calibration is limited only to the field instrument. When we calibrate the field instrument, we calibrate the entire loop right up to the HSI as one string. Once we see the appropriate digital values at all of the various measurement levels, we typically do five levels across the entire range of the instrument. We know that everything is calibrated. So that encompasses the signal conditioning, the A to D conversion and, once we see a digital value on one VDU, we can be confident that the same digital value is going to show up on every VDU. So, all of the calibration is greatly simplified.

The next one is operability testing. In existing analogue designs, we have an enormous amount of segmented tests. We will test each segment of a loop separately with overlap. We test both the interfaces to the analogue I and C systems, as well as what is going on inside the systems. In the digital system, we rely on self-testing for everything that is inside the digital boundary. The manual tests are limited to verifying that the analogue signal gets into the digital system correctly. And then we have a manual test that verifies that the signal from the digital system will, in fact, move the valve or start the pump.

So, that is effectively where we do manual tests on each end but what is inside the digital system, we test automatically.

MEMBER STETKAR: Are you going to talk more about that this afternoon? Thanks.

MR. SCAROLA: I think I actually spoke

about the last slide already. The same subject.

So, finally, since we have a lot of extra time, I will go through each of these acronyms one-by-one. No.

(Laughter.)

MR. SCAROLA: I noticed you looked up.

CHAIRMAN MAYNARD: You can do that with your colleagues over lunch.

MR. SCAROLA: I don't know that we clarified the acronym list in the presentation. I'm not sure where it came from.

CHAIRMAN MAYNARD: You can go over those at your lunch table today while you are at lunch.

One of the challenges, I think, for the operators is all of the advantages of this is one thing but what are they going to be doing when nothing is going on. And I think one of the challenges for the plants is keeping the operators awake and not complacent and stuff like that. But that is a topic for another discussion.

But anyway, let's go ahead. I want to take a break. But before we do here, though, I'll make sure one more time nobody from the public.

When we come back, we will come back and go into closed session. The next open session for the public will be tomorrow at 12:00, I believe it is, at noon. So with that, let's go ahead and we will break for lunch and come back at 12:30 and we will come back into closed session.

Thank you.

(Whereupon, the above-entitled matter went off the record at 11:34 a.m. for a closed session, adjourning the open session to continue on Wednesday November 5, 2008.)

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

NRC Review of Mitsubishi Topical Reports

To:
Advisory Committee on Reactor Safeguards

By:

Mike Magee, Project Manager
U.S. Nuclear Regulatory Commission

November 4th, 2008

Purpose

- Provide status of the NRC staff review of the following Topical Reports
  - Safety I&C System Description and Design Process
  - HSI System Description and HFE Process
  - Safety System Digital Platform MELTAC
  - Defense-in-Depth and Diversity
- Address the Committee's questions

Defense-In-Depth and Diversity (D3)

- Topical Report requests approval of the D3 approach for the US-APWR.
- Review focused on MHI's design basis approach to D3, including the Diverse Actuation System, for I&C systems applied to its US-APWR nuclear power plant design.
- Revision 2 submitted in response to RAIs
- Safety Evaluation Report expected late November.

Safety System Digital Platform - MELTAC

- Topical Report requests approval of this platform for application to the safety systems of the US-APWR and for replacement of current safety systems in operating plants.
- Review is focused on design of the Mitsubishi Electric Total Advanced Controller (MELTAC) Platform and its conformance to safety requirements.
- Rev 2 received, RAI responses received and under review
- Safety Evaluation Report expected June 2009

HSI System Description and HFE Process

- Topical Report requests approval of HSI System design and its design process for application to the HSI System of the US-APWR and replacement of current HSI systems in operating plants.
- The review was conducted using the elements of NUREG-0711, "Human Factors Engineering Program Review Model." Review emphasis was placed on the six planning and analysis elements, as these elements are used as the basis for the HSI design of the control room.
- Rev 2 received, RAI responses being reviewed.
- Safety Evaluation Report due date under evaluation.

Safety I&C System Description and Design Process

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Topical Report requests approval of MHI Design and Design Process for application to the safety systems of the US-APWR and for replacement of current safety systems in operating plants.

- Review is focused on design of the MHI Digital Safety Systems and the Design Process used for the application of these systems to specific nuclear power plants.

- Rev 1 issued, RAI responses received and under review

- Safety Evaluation Report expected June 2009

Summary

- Safety Evaluation Report being prepared for Defense In Depth and Diversity Topical Report
- MELTAC and Safety I&C SER’s due in June 2009
- HSI/HFE SER due date under review.

US-APWR
ACRS Review Meeting

Overview of Four Topical Reports

Safety I&C System
HSI System
Digital Platform
Defense-in-Depth and Diversity

November 4-5, 2008
Mitsubishi Heavy Industries, Ltd.

Meeting Attendants

- **Shinji Kawanago** (Representative of I&C Licensing)
  - ✓ Engineering Manager
  - ✓ Mitsubishi Nuclear Energy System, Inc. (MNES)
- **Makoto Takashima** (Responsible for all I&C Design)
  - ✓ Deputy Chief Engineer
  - ✓ Water Reactor Engineering Department
  - ✓ Mitsubishi Heavy Industries, LTD. (MHI)
- **Masafumi Utsumi** (Responsible for safety I&C Design)
  - ✓ Engineering Manager
  - ✓ Instrumentation & Control Engineering Section
  - ✓ Mitsubishi Heavy Industries, LTD. (MHI)
- **Katsumi Akagi** (Responsible for Digital Platform)
  - ✓ Project Manager
  - ✓ Mitsubishi Electric Corporation (MELCO)
- **Ken Scarola** (Technical Adviser for I&C Design)
  - ✓ Senior Technical Manager
  - ✓ Mitsubishi Nuclear Energy System, Inc. (MNES)

Purpose of Topical Reports

- Describe the MHI I&C/HSI system designs
- Describe the design process that was used to develop those designs
- Describe the design process that will be used to apply the design to specific nuclear plants
- Seek approval from the US Nuclear Regulatory Commission for the use of the MHI I&C/HSI system designs and design processes for new nuclear plants and for operating nuclear plants

ACRS Meeting Objective

- Provide the ACRS a better understanding of the content of the MHI Topical Reports (TRs)
- Provide detail discussion of Key Technical Issues related to the MHI Topical Reports
- Discuss completeness and future submittals
- Obtain ACRS feedback on MHI I&C/HSI system designs and design processes

Topics

- **Overview of Topical Reports**
  - ✓ Design description
  - ✓ Key issues
- **Effects of Digital Technology**
  - ✓ On operations and maintenance
    - As time permits
- **Presentation of each Topical Report in detail**

Topical Reports

Part 1: MUAP-07004

Safety I&C System Description and Design Process

Part 2: MUAP-07007

HSI System Description and HFE Process

Part 3: MUAP-07005

Safety System Digital Platform -MELTAC-

Part 4: MUAP-07006

Defense-in-Depth and Diversity

Digital Licensing Evolution

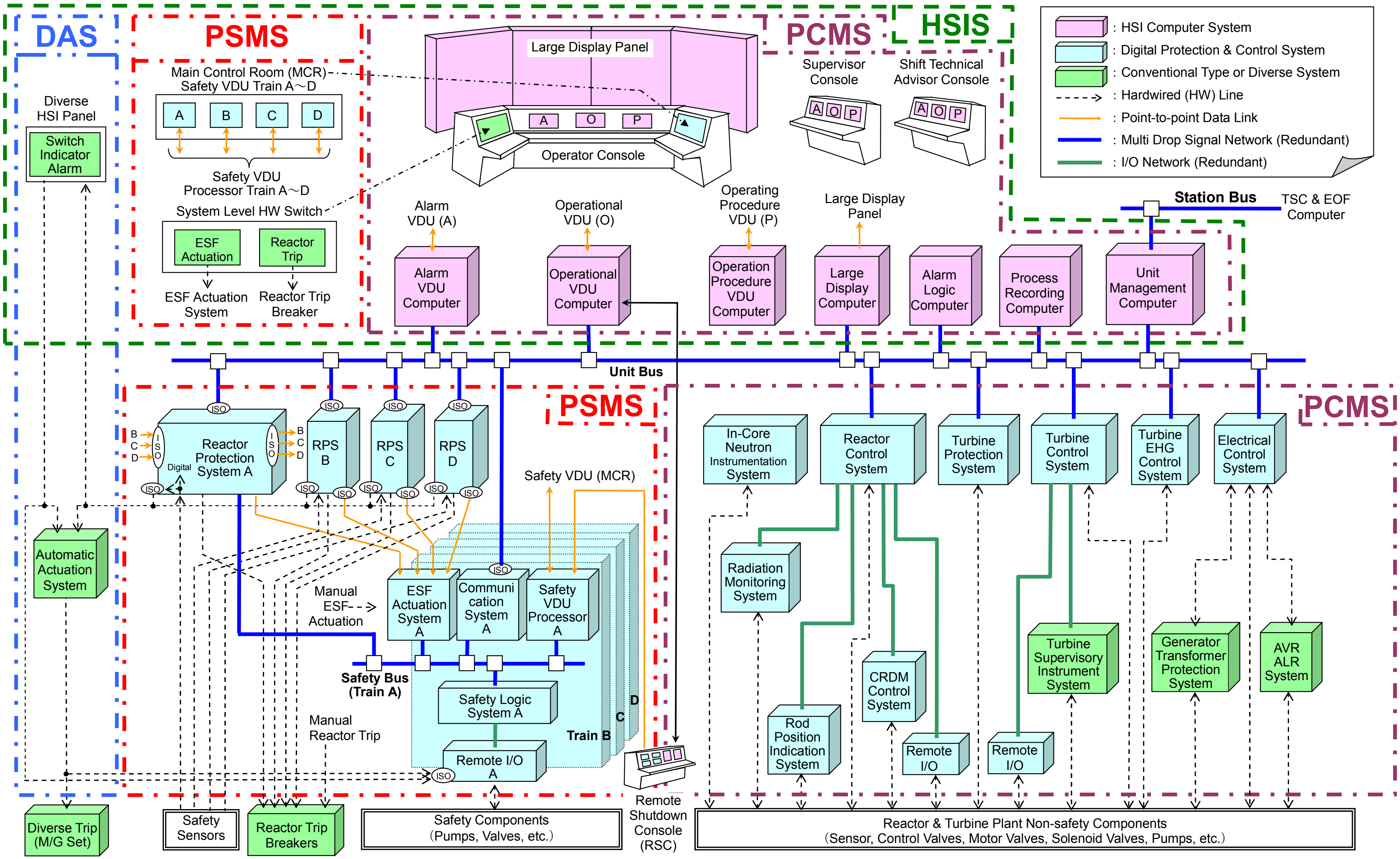
- **MHI participates in the following Digital I&C task working groups:**
  - ✓ Cyber Security
  - ✓ Diversity and Defense-In-Depth
  - ✓ Risk-Informing Digital I&C
  - ✓ Highly Integrated Control Room - Communications
  - ✓ Highly Integrated Control Room - Human Factors
  - ✓ Licensing Process Issues
  - ✓ New Reactor Operator Licensing
    - This group visited MHI's Pittsburgh simulator facility August 2008
- **The topical reports reflect the Interim Staff Guidance generated to date**

Table of Contents

1. Purpose
2. Scope
3. Applicable Code, Standards and Regulatory Guidance
4. System Description
5. Design Basis
6. Design Process
7. Future Licensing Submittals
Appendix A: Conformance to IEEE 603-1991
Appendix B: Conformance to IEEE 7-4.3.2-2003
Appendix C: Prevention of Multiple Spurious Commands and Probability Assessment

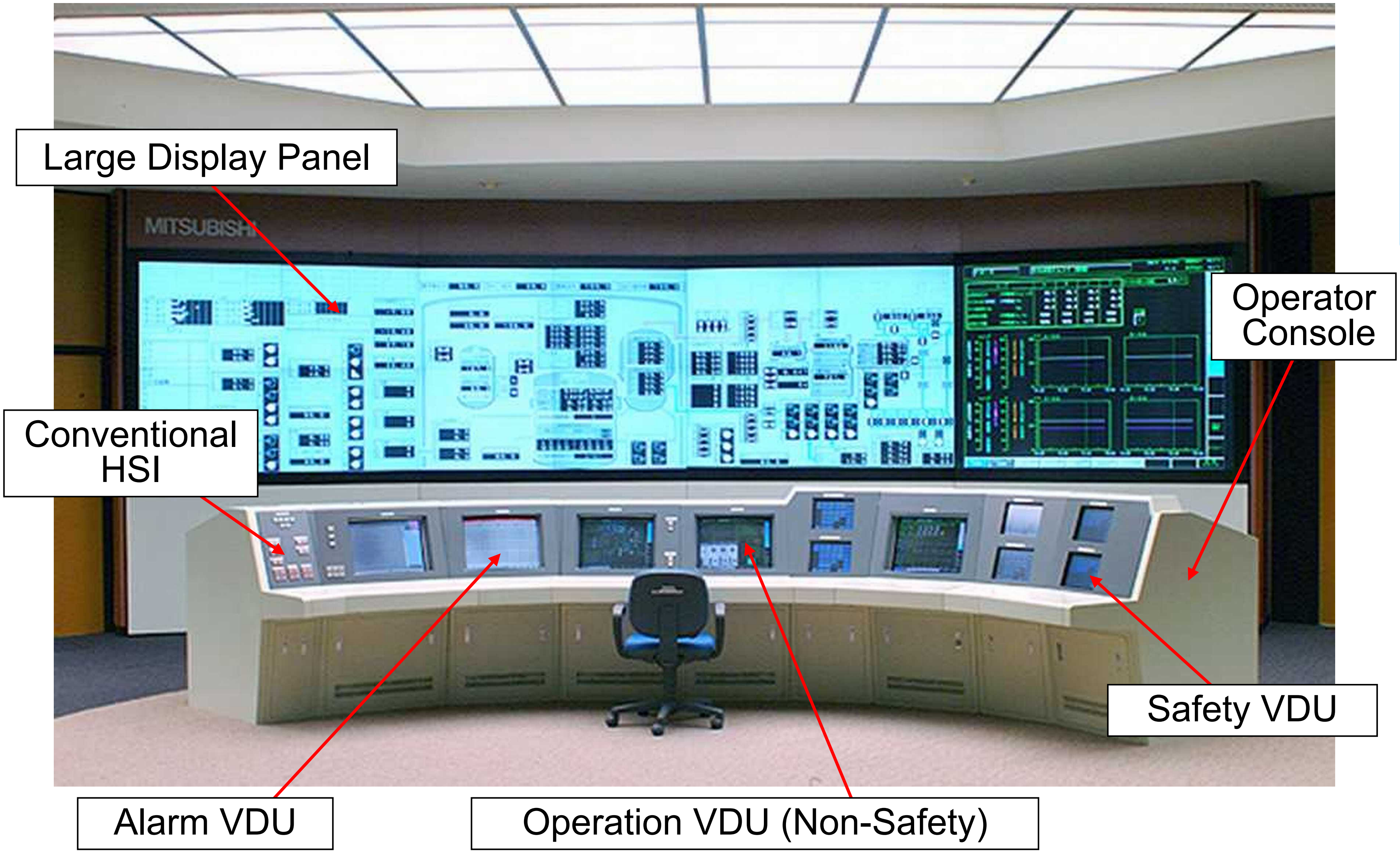
Overall I&C System Architecture

US-APWR



DAS : Diverse Actuation System PSMS : Protection and Safety Monitoring System HSIS : Human System Interface System PCMS : Plant Control and Monitoring System

HSI System Architecture in MCR



VDU: Visual Display Unit

HSI/I&C System Interface

- The complete set of safety and non-safety HSI components is referred to as the HSI System
- The safety-related HSI elements are part of the PSMS
- The non-safety HSI elements are part of the PCMS or the DAS

PSMS – Protection Safety Monitoring System
PCSM – Plant Control and Monitoring System
DAS – Diverse Actuation System

Key I&C Features

- **Plant-wide digital technology**
  - ✓ Maximum reliability & stability, minimum maintenance
  - ✓ High coverage of self-testing, minimum manual testing
- **Four train safety I&C**
  - ✓ Technical Specifications require only 3 trains for many functions
  - ✓ No Limiting Conditions of Operation due to single train failures
  - ✓ Unlimited On-line Maintenance (OLM)
- **Fully redundant non-safety I&C**
  - ✓ For all Central Processing Units (CPUs), critical instrumentation, critical outputs
  - ✓ No single component failure challenges plant operation

Key I&C Features

- Redundant remote multiplexing for input/output (I/O), intra & inter system digital data communication
  - ✓ Reduces cable & related aging issues, fire issues
  - ✓ Improves data communication reliability
  - ✓ Minimizes undetected latent failures
- Common plant-wide digital platform
  - ✓ Reduces engineering/maintenance training & personnel
  - ✓ Reduces spare parts inventory
- Diverse Actuation System for coping with Design Basis Accident (DBA) and concurrent Common Cause Failure (CCF) in common digital platform
  - ✓ Simple analog comparator functions and manual actuation functions result in simple testing and maintenance

History and Future Applications

US-APWR

- ➢ **The safety system design has evolved from experience with the same digital platform in non-safety applications**
  - ✓ Average 10 years operation for five operating plants
  - ✓ Applied to all non-safety I&C, 50 applications per plant
  - ✓ Over 20 million hours total operating experience
  - ✓ No system malfunction caused by software or hardware failure
- ➢ **Current application for Reactor Protection and ESF Actuation System in Japan**
  - ✓ Ikata #1/2 (Digital upgrade operational July 2009)
  - ✓ Tomari #3 (Under test, C/O November 2009)
  - ✓ Takahama #1/2/3/4 (Digital Upgrade 2009 – 2012)
  - ✓ Ohi #1/2/3/4 (Digital Upgrade 2009 – 2013)
  - ✓ Tsuruga #3/4 (APWR) (Under licensing, C/O 2015)

Note: RPS/ESFAS basic architecture is the same as US-APWR

C/O : Commercial Operation

Topical Report Key Issues

- Integrated RPS/ESFAS
- Digital Data Communication
- Control System Failure Modes
- Unrestricted Bypass
- Credit for Self-diagnostics
- Software Quality Assurance Program
- System Analysis
- Cyber Security

HSI System Description and HFE Process Topical Report

Table of Contents

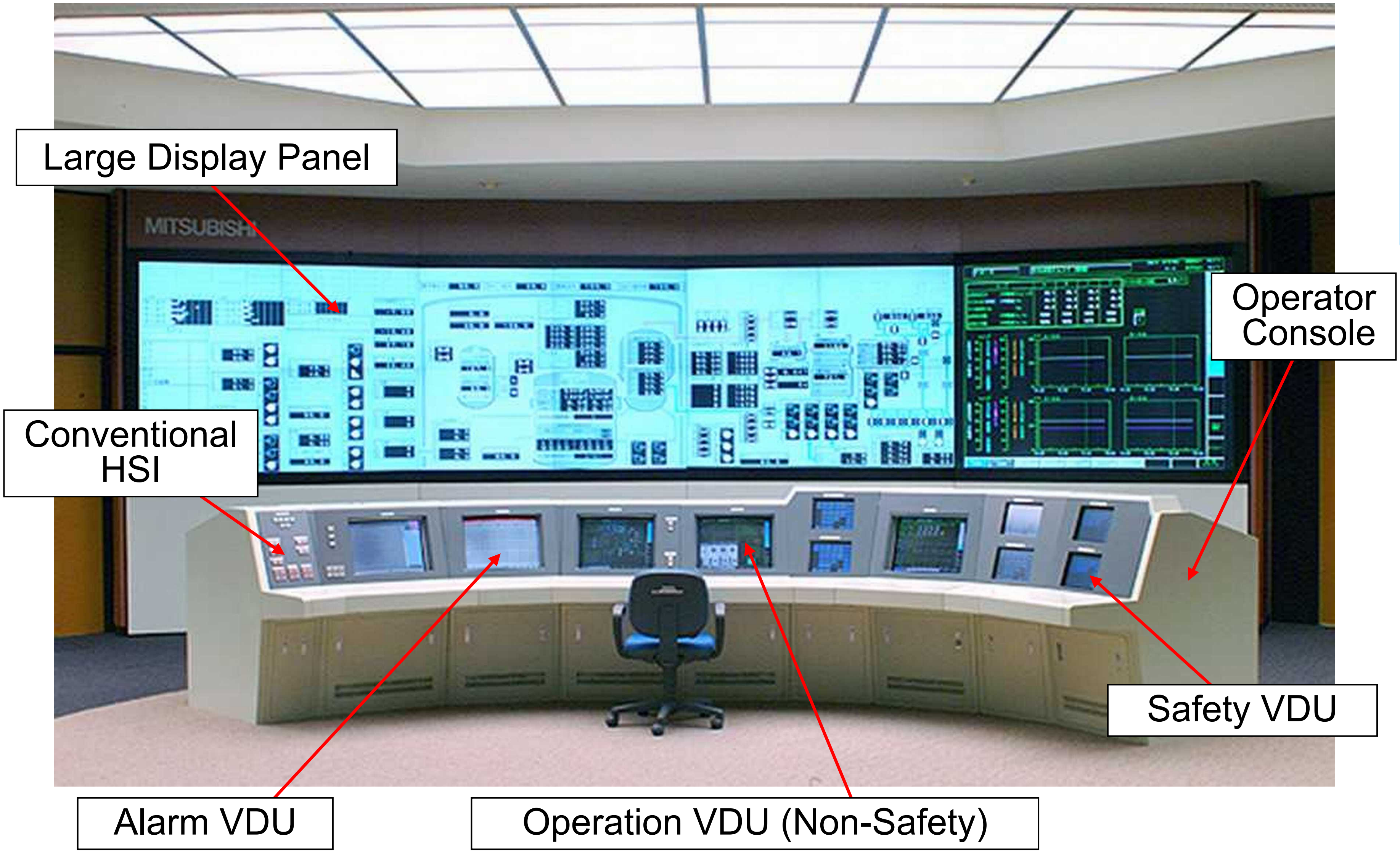
1. Purpose
2. Scope
3. Applicable Code, Standards and Regulatory Guidance
4. Design Description
5. HFE Design Process
6. Reference
7. Future Licensing Submittals

Appendix A: History of Development of Japanese PWR Main Control Room by Mitsubishi and Japanese PWR Power Utilities

Appendix B: HFE V&V Experience in Japan

Appendix C: Phased Implementation Plan

HSI System Architecture in MCR



VDU: Visual Display Unit

Key HSI Design Features

- **Basic HSI design features are expected to improve operator performance and efficiency**
    - Thereby enable staff reduction compared to typical staff in operating plants
- ✓ Large Display Panel
    - Fixed display to enhance situation awareness and crew coordination
- ✓ Soft Controls
    - To bring all information and controls to any operator, thereby
        - Reducing task burden for information/control access
        - Enabling more flexible division of responsibility among multiple operators
- ✓ Computerized data processing
    - To distinguish plant problems from I&C problems
    - To reduce operator task burden
    - To prioritize information and alarms

Key HSI Design Features

- **While modern computerized HSI can improve operator performance, the design also emphasizes coping with degraded HSI conditions**
  - ✓ Complete non-safety VDU freeze or black-out
  - ✓ Common cause failure effecting all computerized HSI
    - Non-safety

      and
    - Safety
  - ✓ Evacuation of MCR

HSI System Facilities

- The HSI System design features and design process described in the Topical Report are applicable to
  - ✓ Main Control Room
  - ✓ Remote Shutdown Room
  - ✓ Technical Support Center
- The HSI design process extends to the
  - ✓ Emergency Operation Facility
  - ✓ Local control areas
    - For operations, testing and maintenance activities significant to plant safety

Reference Design

- **US HSI System is being developed from MHI's Japanese Standard HSI System**
  - ✓ With additional consideration for:
    - US operating methods and procedures
    - US ergonomic and cultural differences
    - Updated US Operating Experience Review
    - Plant specific HFE analysis and HSI inventory design for the US-APWR

Reference Design

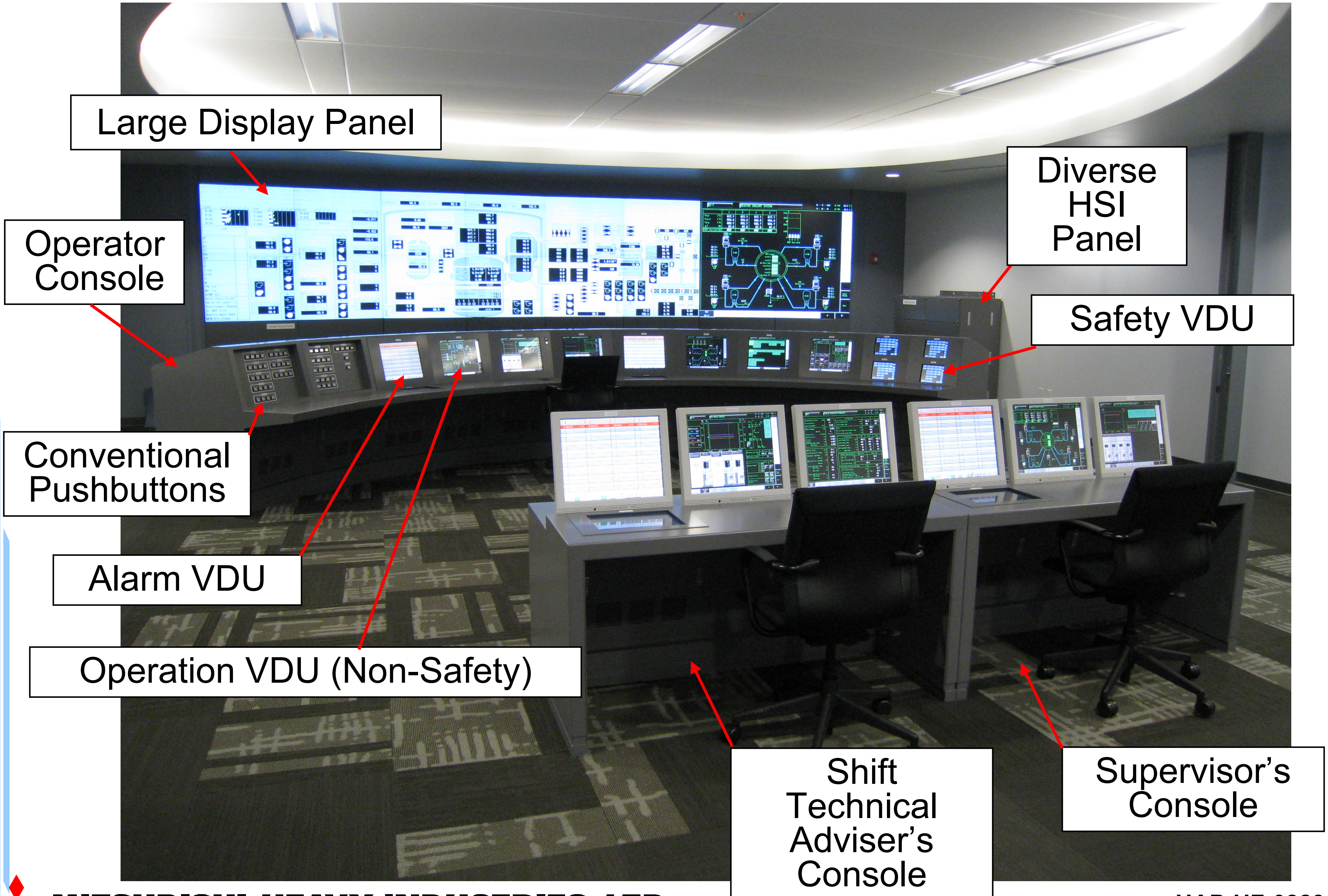
➢ Japanese Standard HSI System:

- ✓ Development process included all NUREG 0711 elements
- ✓ Including validation by approximately 200 Japanese nuclear power plant operators using a full scale MCR simulator
- ✓ Will be operational in several Japanese nuclear power plants in the near future
  - Tomari Unit 3 (New Construction Plant)
  - Ikata Unit 1&2 (MCR & I&C replacement/updating)
  - NTC-4 (New facility in Japanese PWR training center)

US HFE Design Process

- Phase 1
  - ✓ Demonstrate overall human performance improvement from Japanese HSI System compared to conventional HSI
  - ✓ Demonstrate conformance to US requirements
  - ✓ Identify any changes from Japanese HSI system needed for US
  - ✓ Primarily through simulator evaluation by US HFE experts and US Operators
    - Phase 1 report submitted for NRC review December 2008
    - Japanese development documentation available for NRC audit
- Phase 2
  - ✓ Apply US HSI System to US-APWR
    - Analysis reports submitted June 2009
    - Design and V&V ITAAC reports available 2011-2012
- Phase 3
  - ✓ Apply US-APWR HSI System to Comanche Peak
    - Very few changes expected from Phase 2
    - Primarily operator training

Pittsburgh Simulation Facility for HSI V&V



Topical Report Key Issues

- What is an HSI System
- Reference Design
- US-APWR HFE Program
- Minimum Inventory
- Alarm Management
- Computer Based Procedures
- Soft Control Methods
- Multi-division VDUs
- Degraded HSI
- Operator Staffing
- HFE Team Organization & Qualification
- Task Analysis & Human Reliability Analysis

Table of Contents

1. Purpose
2. Scope
3. Applicable Code, Standard and Regulatory Guidance
4. MELTAC Platform Description
5. Environmental, Seismic and Electromagnetic Qualification
6. Life Cycle
7. Equipment Reliability (analysis and operating experience)
Appendix A – Hardware Specifications
Appendix B - Functional Symbol Software Specifications

MELTAC Digital Platform

US-APWR

➢ Mitsubishi Electric Total Advanced Controller

✓ Simple Design

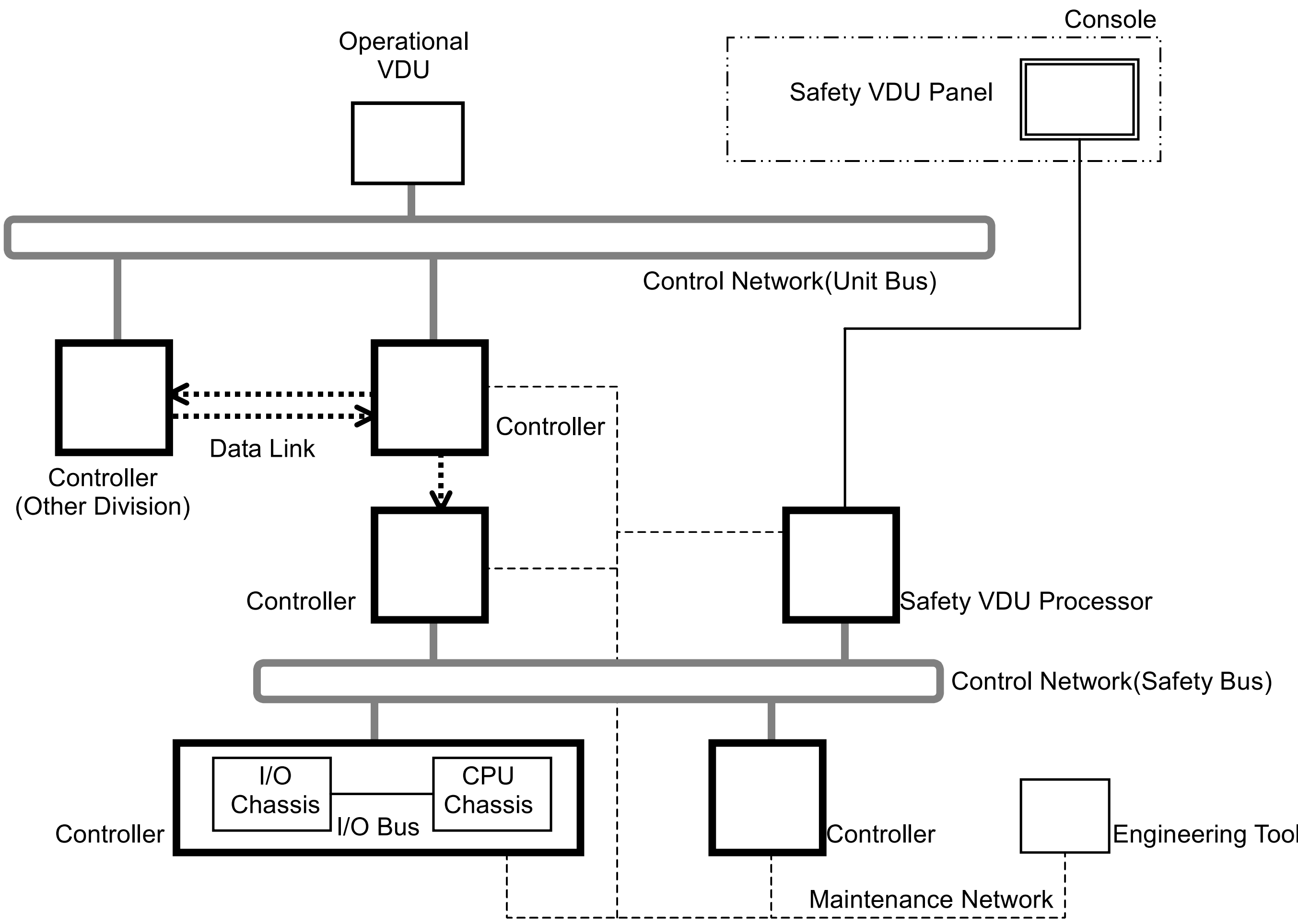
- Modular and Structured Architecture
- Single Task execution
- Cyclical Processing with No Interrupts

✓ Quality Assurance and Control

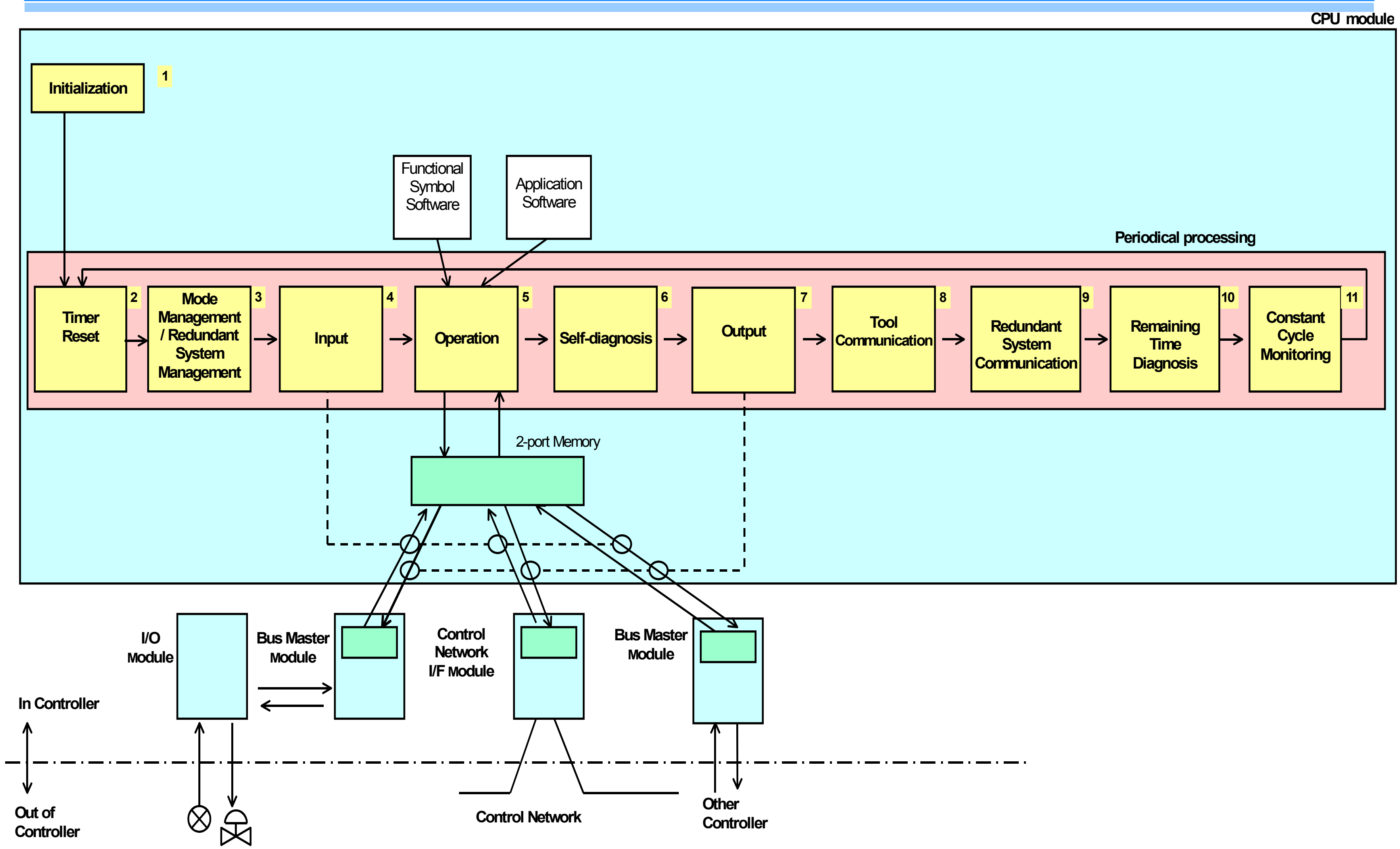
- Designed specifically for Nuclear Applications
- Under control of Nuclear QA/QC
- Fully owned and life cycle managed by Mitsubishi

Basic Hardware Architecture

➢ Building blocks to create plant systems



Basic Software Architecture



➢ Deterministic Performance

Operating History and Projections

US-APWR

- **Digital Platform Non-safety Application History**
  - ✓Development began in 1985 with long term goal of safety applications
  - ✓First installation for non-safety in 1991
- **Each controller includes identical basic software and unique application software**
  - ✓Safety and Non-safety

Topical Report Key Issues

- Obsolescence Management
- Quality Assurance Program
- Coverage of Self-diagnostics
- EMI Qualification
- Data Communication
- Prevention of Common Cause Failure

Defense-in-Depth and Diversity Topical Report

Table of Contents

1. Purpose
2. Scope
3. Codes and Standards
4. I&C System Overview
5. Basic Defense-in-Depth and Diversity Principles
6. DAS Description
7. Diversity Analysis
8. D3 Coping Analysis Method
9. Key Technical Issues
10. Future Licensing Submittals

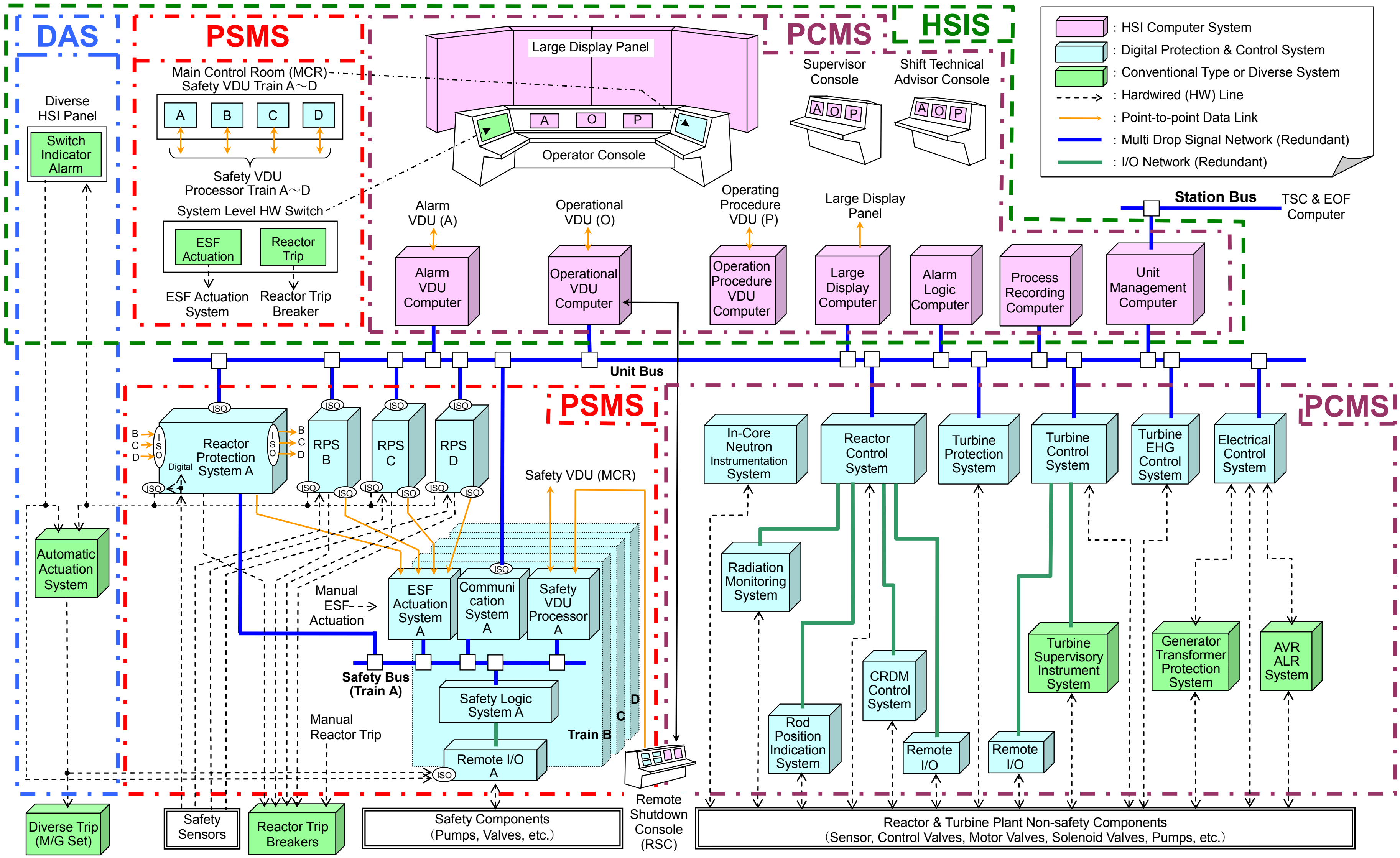
Appendix A: Conformance to BTP HICB-19

Appendix B: Conformance to 10 CFR 50.62

Appendix C: Functional Configuration of PIF module

I&C System Overview

US-APWR



DAS : Diverse Actuation System PSMS : Protection and Safety Monitoring System HSIS : Human System Interface System PCMS : Plant Control and Monitoring System

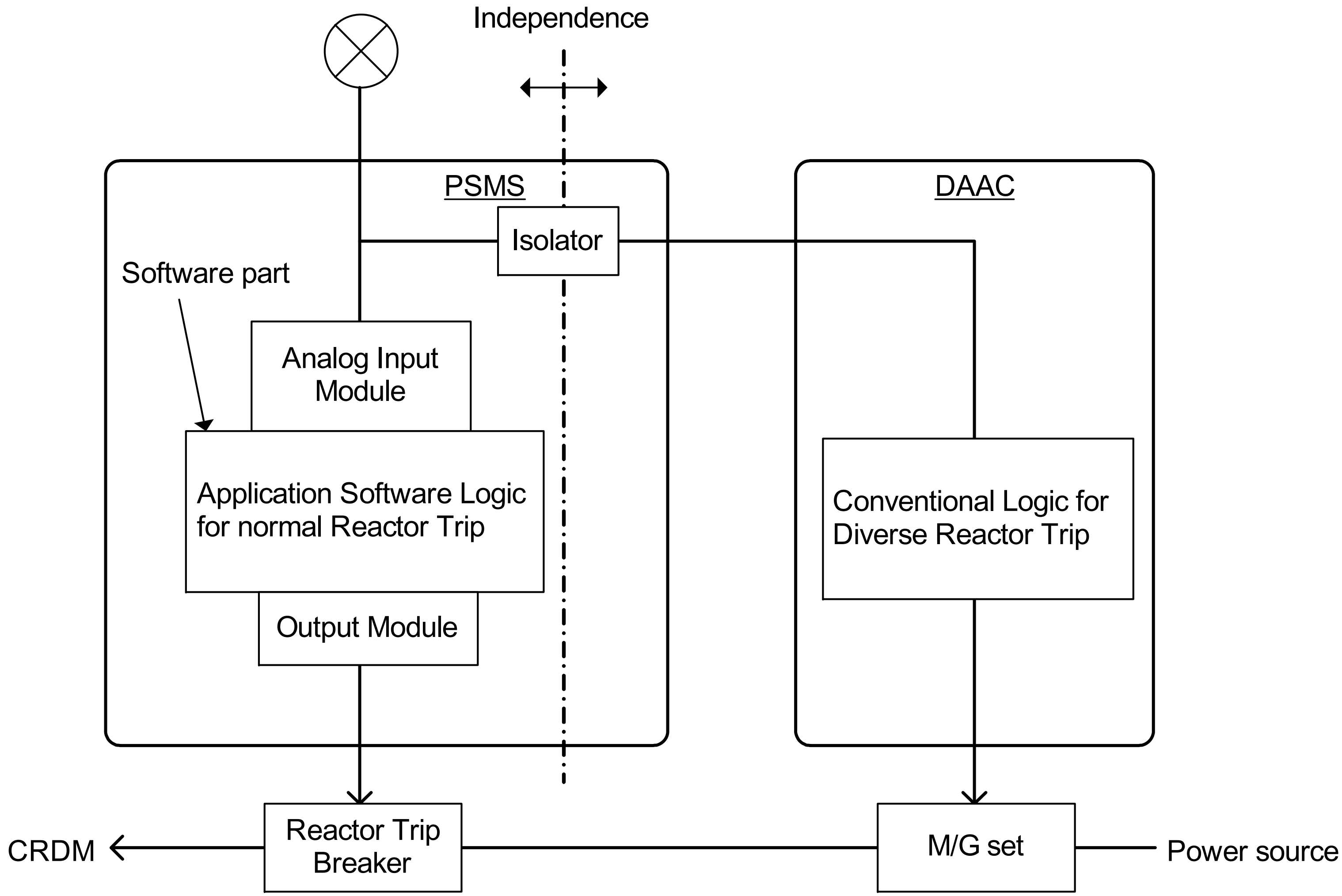
Pittsburgh Simulation Facility for HSI V&V

D3 Strategy Overview

- **Minimize the potential for CCF in the PSMS**
  - ✓ Through functional diversity and design simplicity
- **Provide DAS which is immune to PSMS CCF**
  - ✓ AOOs
    - Automated DAS functions in accordance with ATWS rule
  - ✓ PAs of moderate frequency
    - Automated or manual DAS functions to achieve acceptance criteria of BTP-19
      - Based on “best estimate” assessment of Time Available and Time Required
  - ✓ LBLOCA
    - Manual DAS functions for safe shutdown and ECCS actuation
      - Based on leak detection and RCS low pressure/inventory
- **D3 strategy is based on approved ALWR Design Certification**
  - ✓ Balances prevention and mitigation through adequate diversity and simplicity, depending on the event frequency

DAS Basic Architecture

- Complete hardware and software diversity between PSMS-RT and DAS-RT



History and Future Applications

- The DAS design is based on conventional analog technology used in currently operating in Japanese protection systems
- The D3 strategy and DAS are being applied to Japanese plants that will install digital protection systems
  - ✓Ikata #1/2 (Digital upgrade operational July 2009)
  - ✓Tomari #3 (Under test, C/O November 2009)
  - ✓Takahama #1/2/3/4 (Digital Upgrade 2009 – 2012)
  - ✓Ohi #1/2/3/4 (Digital Upgrade 2009 – 2013)
  - ✓Tsuruga #3/4 (APWR) (Under licensing, C/O 2015)

  Note: DAS basic architecture is the same as US-APWR

Topical Report Key Issues

- Minimize the Potential for CCF
- Coping with CCF for AOOs
- Coping with CCF for PAs
- Coping with LBLOCA
- Common PIF Module
- Effects of the Software CCF
- Coping Analysis Methodology

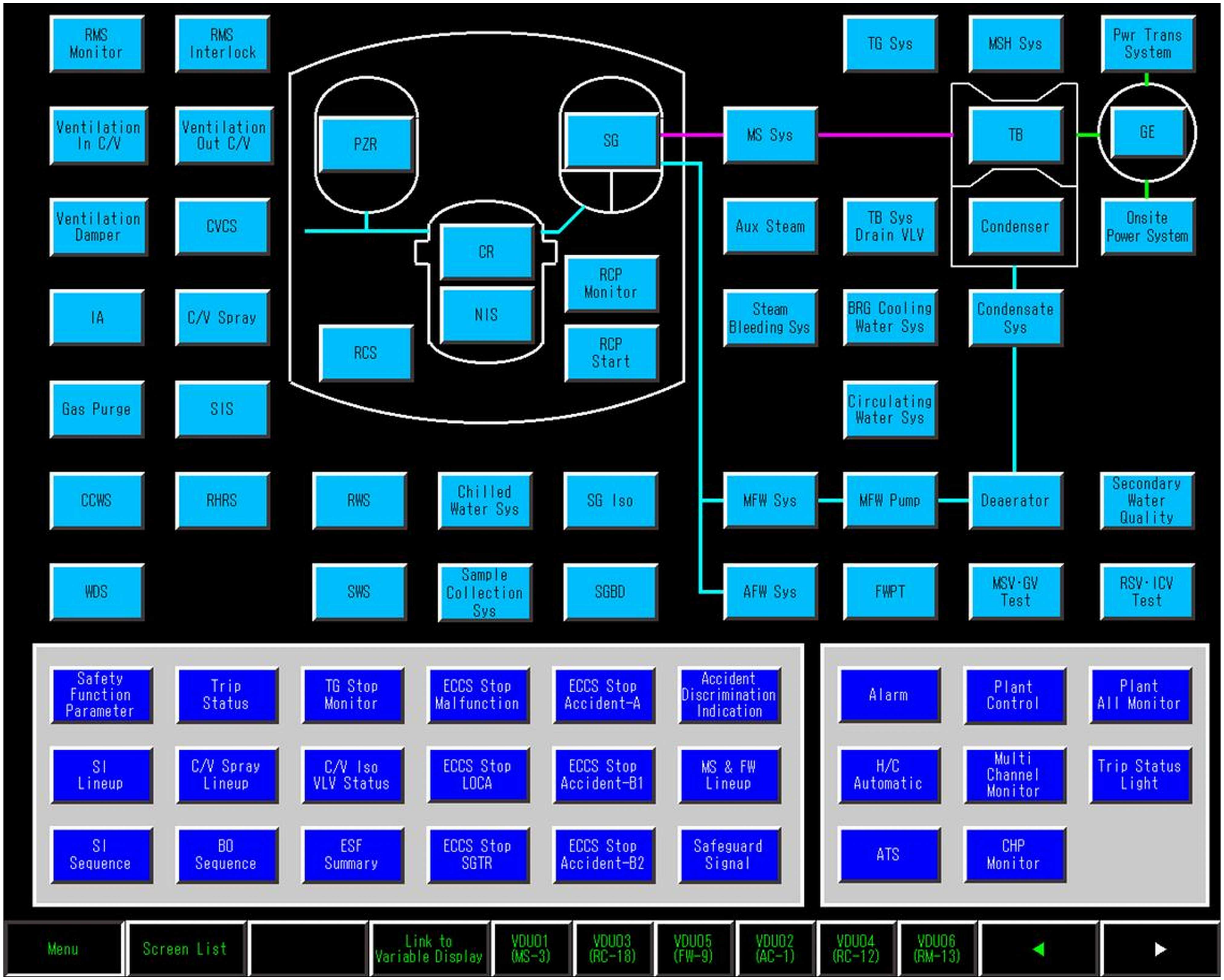
Effects of Digital Technology

- Digital technology will change some operator tasks and technician tasks

Information & Controls Accessibility

- **All information and controls are easily accessible to each MCR operator**
  - ✓ Visual Display Units (VDU) with hundreds of display pages
  - ✓ Multi-division VDUs allow control of safety divisions and non-safety from the same VDU
- **Very different than the geographic distribution of instrumentation and controls on conventional panels**
  - ✓ One RO can monitor and control all plant functions
  - ✓ With two ROs, the division of responsibility between ROs can be function based rather than system based
    - For example, one RO can be responsible for all systems (safety and non-safety) for controlling the same function (eg. RCS inventory)
- **No credited safety actions for Auxiliary Operators**
  - ✓ Safe shutdown achievable from MCR or RSR for all events, including fire

Operational VDU – Screen Menu



System display request area

Emergency display Request area

Automated Cross Channel Checks

US-APWR

- Computers continuously perform cross channel checks
  - ✓ Operators don't need to do this anymore
- Monitoring and control displays show one parameter, not four
  - ✓ Four are available on diagnostic level displays
- Control systems use all channels
  - ✓ No process effect from single channel failures
- Operators respond to channel deviation alarms
  - ✓ Check system level effect (usually none, Partial Trip)
  - ✓ Confirm deviation
  - ✓ Check Tech Spec LCOs
  - ✓ Longer term action
    - Maintenance work order

Automated Actuation Checks

US-APWR

- ➢ **Computers check correct actuation of all ESF system components**
  - Pump start, valve line-up
  - ✓ Operators don't need to do this anymore
- ➢ **Operators respond to "Not OK" alarms**
  - ✓ Confirm alternate train is "OK", including performance
  - ✓ Longer term action
    - Confirm "Not OK" status
    - Restore to "OK" status
    - Maintenance work order

Automated BISI

Bypassed or Inoperable Status Indication

- **Computers monitor components for inoperable or misalignment conditions**
  - ✓ While in standby mode
- **Computers determine and display effects at train level**
  - ✓ Operators don't need to do this anymore
- **Operators respond to "Not Ok" alarms**
  - ✓ Confirm "Not Ok"
  - ✓ Check Tech Spec LCOs
  - ✓ Longer term action
    - Restore to "OK" status
    - Maintenance order

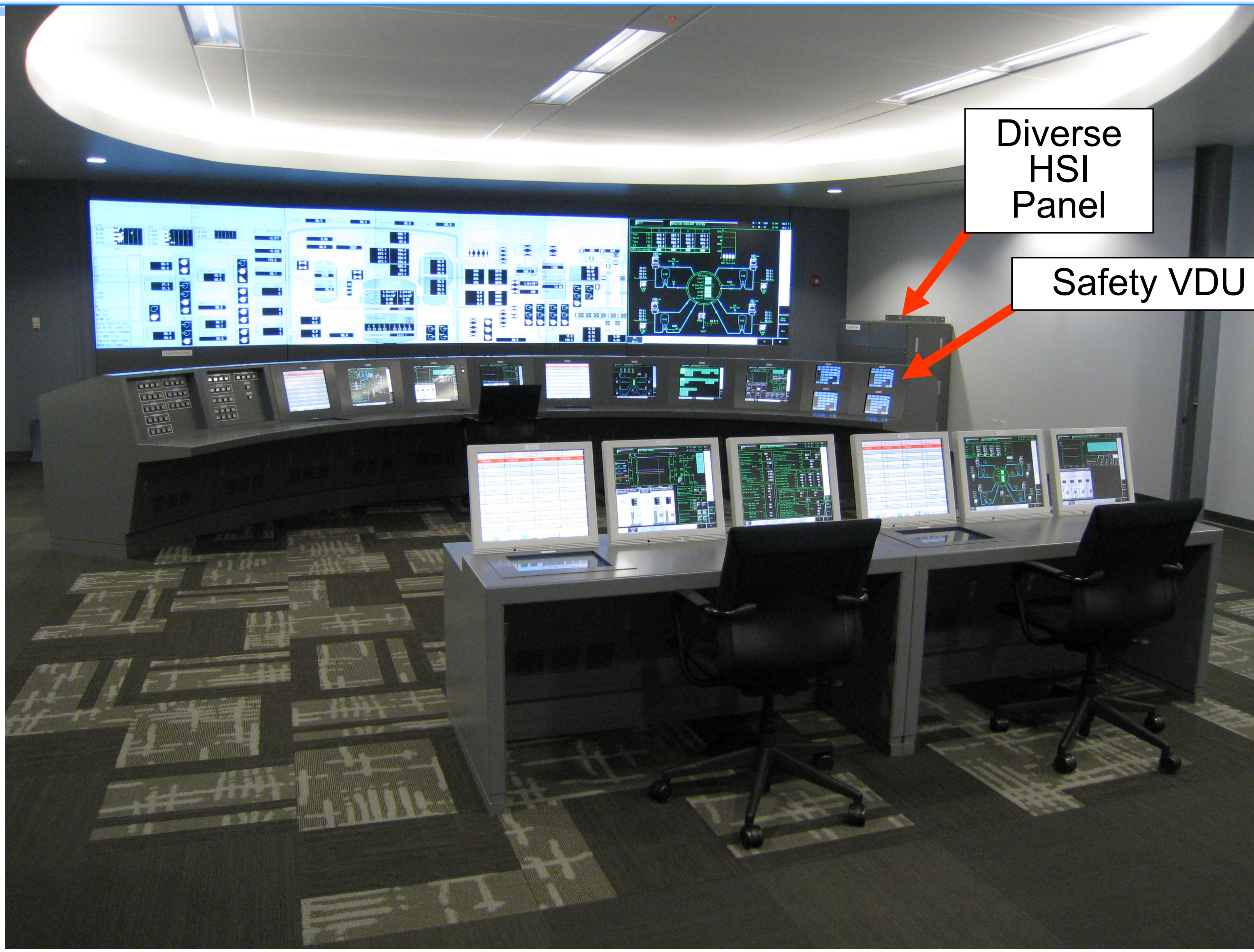
Alarm Management

- Alarm avalanche conditions are common in current alarm systems
  - ✓ EOPs and training do not credit the alarm system
- Alarm avalanche conditions are significantly reduced by
  - ✓ Signal validation
    - – based on automated cross channel checks
    - One process alarm, not one for each division
  - ✓ Cause-consequence dependency logic
    - Plant mode
    - Equipment mode
  - ✓ Prioritization logic
    - Highlights degrading conditions
- Allows the alarm system to be credited

Degraded HSI Conditions

- **Current control rooms**
  - ✓ HSI is an integral part of the plant systems and components (eg. pumps, valves, instruments)
  - ✓ Operators train primarily to cope with plant component failures, not HSI failures
- **New control room**
  - ✓ HSI redundancy to minimize the potential for failures
  - ✓ If an unusual failure occurs, the effect can be much more global (eg. complete VDU freeze)
    - In addition to training operators for plant component/system failures, we must also train them for HSI failures
    - This is further complicated by NRC criteria for consideration of common cause failure
      - Adds even more training for beyond design basis events
  - ✓ Degraded HSI is the most significant operator training challenge

Degraded HSI Conditions



Degraded HSI Conditions

- **Normal HSI**
  - ✓ LDP, Operational VDUs, Alarm VDUs, Electronic Procedures
    - Normal conditions, accident mitigation and cold shutdown
      - – Operational VDUs control all plant components
- **Loss of all Non-Safety HSI**
  - ✓ Safety VDUs, Paper Procedures
    - Continued stable operation, accident mitigation and cold shutdown
      - – Safety VDUs control safety plant components
- **Common Cause Failure**
  - ✓ DHP, Paper Procedures (special event EOPs)
    - Accident mitigation and hot shutdown
- **MCR Evacuation**
  - ✓ Remote Shutdown Console with Operational VDUs, Safety VDUs, Paper Procedures
    - Cold shutdown design basis (but same functionality as MCR)

Channel Calibration

- **Analog**
  - ✓ Technicians separately calibrate
    - Each field instrument
    - Each analog module internal to I&C systems
      - – Signal conditioners, filters, computation (lead/lag), comparators, output converters
    - Each meter and recorder
- **Digital**
  - ✓ Calibration limited to field instruments
    - Digital readout during calibration inherently checks
      - » Signal conditioning
      - » A/D conversion
      - – Wireless readout at transmitter allows one person calibration
    - HSI checked continuously through normal operation

Channel Operability Test

➢ Analog

- ✓ Technicians test all functions manually
  - Setpoints
  - Interlocks
  - Alarms
  - Combinational logic
  - Interfaces to plant components

➢ Digital

- ✓ Self-test continuously checks integrity of
  - Digital processing
  - Basic and application software memory
  - Data communications
- ✓ Technicians initiate automatic program memory check once per cycle for configuration management

Trip Actuation Device Operability Test

➢ Analog

- ✓ Operators test plant component actuation for several configurations and operational modes
  - Each ESFAS function and sequence
  - Each actuation interlock
- ✓ Results in multiple component cycles
- ✓ Most tests are conducted during refueling
  - Due to test complexity
  - Due to Tech Spec LCOs

➢ Digital

- ✓ Operators test plant component actuation one time
- ✓ Most tests are conducted on-line

List of Acronyms (1/2)

AOO	Anticipated Operational Occurrence
BTP	Branch Technical Position
CBP	Computer-based Operating Procedure
CCF	Common Cause Failure
CDF	Core Damage Frequency
COLA	Combined License Application
CPU	Central Processing Unit
C/O	Commercial Operation
CRC	Cyclic Redundancy Check
C/V	Containment Vessel
D3	Defense in Depth and Diversity
DAC	Design Acceptance Criteria
DAS	Diverse Actuation System
DBA	Design Basis Accident
DCD	Design Control Document
DHP	Diverse HSI Panel
DI	Digital Input
DTM	Design Team Manager
ECCS	Emergency Core Cooling System
EFW	Emergency Feed Water
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EOP	Emergency Operating Procedure
E/O	Electrical to Optical or Optical to Electrical
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FRA	Functional Requirement Analysis
FTA	Fault Tree Analysis
HED	Humanfactors Engineering Discrepancy
HFE	Human Factors Engineering
HFEVTM	HFE V&V Team Manager
HICs	Highly-Integrated Control Rooms - Communications Issues
HRA	Human Reliability Analysis
HSI	Human System Interface
HSIS	Human System Interface System
HW	Hardware
I&C	Instrumentation and Control
LBLOCA	Large Break Loss of Coolant Accident
LERF	Large Early Release Frequency
I/F	Interface
I/O	Input/Output
IR	Intermediate Range
IT	Information Technology
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
LAR	License Amendment Request
LCO	Limiting Conditions for Operation
LDP	Large Display Panel
LER	Licensee Event Report
LOOP	Loss of Offsite Power
MCR	Main Control Room
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
M/G	Motor Generator
MHI	Mitsubishi Heavy Industries, Ltd.
MNES	Mitsubishi Nuclear Energy System, Inc.
MTBF	Mean Time Between Failure

List of Acronyms (2/2)

OBE	Operational Basis Earthquakes
OE	Operating Experience
O/E	Optical/Electrical Converter
OER	Operating Experience Review
OLM	On-line Maintenance
PA	Postulated Accident
PCMS	Plant Control And Monitoring System
PIF	Power Interface
PFD	probability of failure on demand
PM	Project Manager
PR	Power Range
PRA	Probability Risk Assessment
PSMS	Protection And Safety Monitoring System
QA	Quality Assurance
QAP	Quality Assurance Program
RAM	Random Access Memory
RG	Regulatory Guide
RCP	Reactor Coolant Pump
RO	Reactor Operator
ROM	Read Only Memory
RPS	Reactor Protection System
RSR	Remote Shutdown Room
RT	Reactor Trip
RTS	Reactor Trip System
SER	Safety Evaluation Report
SDCV	Spatially Dedicated Continuously Visible
SG	Steam Generator
SLS	Safety Logic System
SR	Source Range
SRO	Shift Technical Advisor
SPDS	Safety Parameter Display System
SS	Shift Supervisor
SSE	Safe Shutdown Earthquake
SW	Software
TA	Task Analysis
TR	Topical Report
TT	Turbine Trip
UCP	US Conformance Program
V&V	Verification and Validation
VDU	Visual Display Unit
WDT	Watchdog Timer