Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Advisory Committee on Reactor Safeguards Open Session
Docket Number:	(n/a)
Location:	Rockville, Maryland
Date:	Thursday, March 6, 2014

Work Order No.: NRC-622 Pages 1-224

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

+ + + + +

612TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

THURSDAY

MARCH 6, 2014

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

COMMITTEE MEMBERS:

JOHN W. STETKAR, Chairman

HAROLD B. RAY, Vice Chairman

DENNIS C. BLEY, Member-At-Large

J. SAM ARMIJO, Member

RONALD BALLINGER, Member

SANJOY BANERJEE, Member

CHARLES H. BROWN, JR. Member

MICHAEL L. CORRADINI, Member

COMMITTEE MEMBERS: (Continued)

DANA A. POWERS, Member

JOY REMPE, Member

PETER RICCARDELLA, Member

MICHAEL T. RYAN, Member

STEPHEN P. SCHULTZ, Member

GORDON R. SKILLMAN, Member

DESIGNATED FEDERAL OFFICIALS:

ZENA ABDULLAHI

CHRISTINA ANTONESCU

GIRIJA SKUKLA

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

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

8:33 a.m.

CHAIRMAN STETKAR: The meeting will now come to order.

This is the first day of the 612th meeting of the Advisory Committee on Reactor Safeguards. During today's meeting the Committee will consider the following: Selected chapters of the Safety Evaluation Report with open items associated with the United States Advanced Pressurized Water Reactor Design Certification and the Comanche Peak combined license application; Diablo Canyon Power Plant Units 1 and 2 digital replacement of the process protection system and portions of the reactor trip system and engineered safety features actuation system; pellet cladding interaction fuel failures during anticipated operational occurrences; biennial review of the NRC safety research; and preparation of ACRS reports.

Portions of today's sessions may be closed to discuss and protect proprietary information.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act.

Mr. Girija Skukla is the designated federal official for the initial portion of the meeting.

We received no written comments or requests to make oral statements from members of the public regarding today's session.

There will be a phone bridge line. To preclude interruption of the meeting, the phone will be placed on a listen-in mode during the presentations and Committee discussion.

A transcript of portions of the meeting is being kept and it is requested that the speakers use one of the microphones, identify themselves and speak with sufficient clarity and volume so that they can readily heard.

Before we begin, I have one sad comment to make. Dr. Sam Armijo, who has been with us for 8 years is participating in his last meeting as a member of the Committee.

And, Sam, we're going to be really sorry to see you go. You're going to be really missed. Thank you very much for your long service and active participation and energy and everything you've brought to the Committee.

MEMBER POWERS: The trouble is he's going to be spending his time with more mature people. His granddaughter.

(Laughter.)

CHAIRMAN STETKAR: And people who know the difference between 8 and 18 probably already.

(Laughter.)

MEMBER ARMIJO: No, John, she's three-and-a-half.

(Laughter.)

CHAIRMAN STETKAR: Oh, doing partial differential equations by now.

(Laughter.)

CHAIRMAN STETKAR: And with that, we will begin our first topic, that is the US APWR and Luminant Comanche Peak COLA. And I will lead that discussion.

As a matter of introduction, this is another of our chances to provide some interim review comments on the DCD and COLA applications. As the Committee is well aware, we have been doing that over the course of the year. This particular session will cover most of Chapter 3 and most of Chapter 14 for both the DCD and the COLA, and all of Chapter 9 for the COLA. We had Subcommittee meetings on Chapters 3 and 9 back in November of last year. And just very recently, Tuesday of this week, we had a Subcommittee on Chapter 14.

And with that, I will ask the staff if they have any introductory remarks. Perry?

MR. BUCKBERG: No thanks.

CHAIRMAN STETKAR: Okay.

MR. BUCKBERG: No remarks.

CHAIRMAN STETKAR: Good. So I'll turn it over to MHI. Ryan?

MR. SPRENGEL: Good morning, everyone. I'm glad to be back yet again. We will be covering the majority of Chapters 3 and 14. The exceptions are noted in the slide.

With me today are Masatoshi Nagai and Rebecca Steinman, and they'll be covering the two specific chapters that we're looking at.

The first bullet here gets a little busy, and it's getting to the point Chairman Stetkar highlighted earlier in the week. We're talking about the remaining chapter because it's easier. So we actually are down to a few areas after today of remaining chapters or sections to bring to the Full Committee, and those being Chapter 1, the Section 3.7, 3.8 with associated sections of 14 and Chapter 18. So we're getting close in terms of our kind of interim interactions with the Committee.

The next two portions are a reminder, a

carryover from the last time we met with US APWR is going through some adjustments in our review and where MHI is focusing their energies right now. So we are nearing the end of our kind of slow down adjustment. And we'll be starting a new period where we're focusing on still getting our design certification but in a reduced number of areas at any one time, the first areas being Chapter 18 and defines topical report. So those will be our initial focus areas. And we will be working with the staff to complete the -- or for the staff to complete their SER and then we do it just bringing those to the ACRS Subcommittee and Full Committee.

With that, I will turn over the presentation to Masatoshi Nagai for Chapter 3.

MR. NAGAI: Thank you, Ryan.

Good morning. I am Masatoshi Nagai, the licensing engineer for Chapter 3. DCD Chapter 3 is titled, "Design of Structures, Systems, Components and Equipment." Last October the NRC issued Safety Evaluation Report with open items for this chapter except 3.7 and 3.8. MHI and the NRC staff presented that chapter to the ACRS Subcommittee on November 20th and 21st last year.

In t Safety Evaluation Report there are 24 open items. Seven of them are considered closed at this moment. The areas that require further review and interactions with the staff include the DCD sections listed on this slide. There are two outstanding RAIs in Section 3.9.2 regarding US APWR steam generator design methodology and criteria. So responses to the RAIs have been prepared and provided to the staff and the staff has been reviewing the responses.

MHI recently submitted revised responses to two RAIs in Section 3.9.4 regarding seismic design of CRDM reflecting the latest seismic input. The responses are available on the docket for the staff's review. MHI also submitted a revision to Technical Report MEUAP 10,023 initial type test result of class 1 mini gas turbine generator system, which includes discussion on seismic qualification of the system. There's one open item in Section 3.10 to track the status of the review of the report.

In Section 3.11, the environmental qualification, there are several RAIs that have been closed including ones regarding environmental qualification of non-metallic parts and the use of the term "important to safety." And we have been working with the staff to identify the path forward.

There are a few other open items in the Safety Evaluation Report to track the audit of design specifications for ASME 613 components for specifications and quote the seismic qualification -- I'm sorry, seismic and quality group classification. The audit was conducted last month, February 2014. There are several follow-up items from the audit which I committed to address by revising some of the specifications and the supporting documents and making them available in future follow-up audit for the staff to review the changes. Finally, reviewing responses to the questions from the ACRS Subcommittee meeting held last November will be submitted on the docket by the end of this month.

Okay. The next slide will be presented by Rebecca Steinman.

MS. STEINMAN: Hello, my name is Rebecca Steinman and I'm the licensing engineer responsible for Chapter 14 on verification programs. As Chairman Stetkar mentioned, we were just here on Tuesday to talk about that. And several of the members who are today got to listen to that discussion on an area of our initial test program and our ITAAC areas.

During that meeting on March 4th we presented all sections of Chapter 14 except for

14.3.2, which is the section of Chapter 14 that goes with the seismic information that we just heard about, the open items associated with that. And then we also did not include Section 14.3.9, which is associated with HFE, which is our next topic that would be coming in terms of the DCD chapters to the ACRS Committee.

In both cases the relevant Chapter 14 tests that are associated with those two technical areas would be presented at the same time that the technical topic came back to the ACRS. So you would expect to see that Chapter 14 discussion included in those presentations.

The remaining review areas for Chapter 14 are a little more limited than what was in Chapter 3. We only had one open item in our SE and that was tied to a Chapter 7 RAI. There was a follow-up that was submitted and MHI just at the end of February submitted their response to that. We believe that we have adequately addressed it, but of course the staff has not had an opportunity to completely review our response and come to the same determination, but we hope that we have a closure path for that one open item kind of already in the pipeline so that we'll be closing things up.

There are no additional RAIs that are open in Chapter 14 right now. We are making a couple of editorial types of corrections that have been found by the staff in terms of specific English word usage and some of the Tier 1 material that we're moving forward with as we close out confirmatory items in Chapter 14.

During our meeting on Tuesday we received approximately 10 questions from the ACRS and we'll be providing a written response to those hopefully within the next couple of weeks, but definitely by the end of March.

And this completes my part of the presentation, and I think our entire presentation for that matter.

CHAIRMAN STETKAR: That is efficient. As usual, we had a number of questions. I was going through my notes from the Subcommittee meetings. A lot of the questions during the Subcommittee tend to touch on rather detailed information that is probably not necessarily appropriate for discussion, especially because you're planning to provide written responses to most of our questions. MHI has been very, very good in the past about following up on the questions from the Subcommittee.

Recognizing that, I'll ask do any of the Committee members, especially Subcommittee members who attended the Subcommittee meetings, have any questions for MHI on these topics, Chapter 3 and Chapter 14, recognizing that the remaining sections of Chapter 3 will be the structural design and seismic analyses which tend to be somewhat more meaty topics. Put it that way.

(No audible response.)

CHAIRMAN STETKAR: If not, thank you very much for the summary and we'll have the staff come up.

MR. SPRENGEL: Thank you.

MR. BUCKBERG: Good morning. My name is Perry Buckberg. I'm the lead project manager for review of the US APWR Design Certification Application. I'll be presenting the staff's evaluation of Chapters 3 and 14, to follow MHI.

The current public schedule reflects the pending slow down of the review of US APWR since we have certain chapters that have been issued with open items, partial Chapter 3, Chapter 18 and a couple other areas, exercising phase discipline, if you will, Phase 2 is TBD along with the rest of the review. We've been working with MHI to coordinate the slow down process and how to reach a logical point for each of the chapters that are still under review regardless of what phase the chapter may be in, but TBD applies because we're not sure when the slow down period will end. Hasn't quite begun yet, but we're not sure when it's going to end. So the schedule will change some time, our estimate two to three years from now.

MEMBER SKILLMAN: Perry, let me this question, please.

MR. BUCKBERG: Sure.

MEMBER SKILLMAN: How does the staff ensure that there's continuity in review? Let's just theorize that the slow down is 24 months, 36 months. The cast of participants change or changes. New eyes and new concerns arrive with new reviewers.

MR. BUCKBERG: Yes.

MEMBER SKILLMAN: And the work that has been parked for 24 or 36 months now is exposed to new challenge, yet 24 months ago the work was essentially parked. What is in place to ensure continuity so there isn't a redoing of work that has been closed?

MR. BUCKBERG: The process is more or less unprecedented. Once the slow down was announced informally in October and then formally in November, we internally started working on that process. Specifically we designed a spreadsheet, an Excel sheet where the current reviewer, the current project manager would document each open area where there is possibly an RAI response to be reviewed or an open item that hasn't been resolved to document and put in writing certain aspects of that item and in data and in text.

That spreadsheet, one for each chapter, will be peer reviewed by their project managers to make sure it makes sense to another reader. Everything that's not represented on the spreadsheet should be represented in an updated draft Phase 4 chapter. You either have an evaluation in the chapter that's going to sit for a couple years, or you have itemized documentation of what needs to be done.

That was the best plan we could come up with. And the easy answer is I'll let you know if it works.

(Laughter.)

MR. BUCKBERG: There's going to be some re-review, but hopefully each technical branch to whatever extent is possible will own up to what review was done presently. And there may be a couple steps backward. That's just going to be part of the process. And one of the main reasons is each of the new reviewers, which it could be several, it could be a complete new branch, will have to sit up in this chair and present their evaluation. They're going to have to take ownership of what was done before them or redo the work before they sit up here. It's very stressful up here sometimes.

So that's the process of how we've planned it. And we think it makes sense and it ought to work. But anytime there's a delay of a couple months, or even if a reviewer himself has been out of the office, him or herself, for some period of time, there's a readjustment period. And two or three years from now there's going to be a couple steps backward before we start moving ahead again.

MR. LEE: Let me add to Perry's comments here, if I may. This is Sam Lee, the branch chief for Licensing Branch 2 that's overseeing this particular design and also APR-1400.

What we are envisioning is is that not knowing how long the slow down period will last, although Ryan has indicated that Chapter 18 will be covered initially during the slow down period and then there will be kind of a trickle-down approach and it will be a very -- smaller fraction of the staff resources dedicated to continuing the review during the slow down period.

Having said that though, that's hard to justify a staff of a good size of large -- a number of

PMs dedicated to this project during the slow down period. So what we're envisioning is is that we're going to try to package the chapters and the sections in such a way that if they're not addressed during the slow down period, whether it be two, three years down the road, that the records will indicate, you know, where the reviews have been, what has been done and what needs to be done and what are the next steps to be taken? So we're making sure that those road maps are clearly identified and recorded at this juncture.

We're also envisioning that there may be a new project manager and perhaps even a new technical reviewer down the road. And so we're making those assumptions in planning for how the work can be picked back up in a couple of years. So we're giving our best shot to make sure that we're leaving a good record for whoever comes along next to pick up the work.

MEMBER SKILLMAN: Thank you.

MR. SPRENGEL: This is Ryan Sprengel with MNES. We do need to clarify that there is no committed time period and we'll adjust our efforts and kind of ramp back up depending on other conditions outside of our control right now. So the two to three-year time period is nothing that we're actually specifically targeting.

MR. BUCKBERG: Any more questions on the slow down?

MEMBER BLEY: Let me ask one more question about the slow down. I don't know any details of it, but tell me if I'm correct in assuming that any responses to RAIs that are submitted before we really stop this for awhile, you will complete your reviews on those before finishing the flow charts and all of that of where you stand, right?

MR. LEE: So when MHI informed us of their plan back in November -- the staff has been trying to package up, you know, close the issues, you know, whether it's in Phase 1 or Phase 4. We saw a good ending point by March 31 was to have an SE with updated information and then so forth.

So, but as you might imagine, for every chapter, and perhaps sections, too, we're all in different places, right? And so it's important. For example, where is that particular RAI, you know? You know, if the RAI responses have been submitted, has the staff had the opportunity to review it? And not only have they reviewed it, but have they documented the review?

And so we're trying to get to a place

where documentation is the end. And so this road map that I spoke of specifically addresses each RAI, each confirmatory item so that when the review is picked back up, whenever, is that we have a clear sense of where that RAI was, where that confirmatory RAI -- what was in that SE?

MEMBER BLEY: Just to help me a little bit on this, it sounds as if March 31 -- after that date you have no more money for the review. So there might be some things that are --

MR. LEE: Yes.

MEMBER BLEY: -- some responses that are partially completed but not all the documentation. That would leave us in a tough spot, I would think.

MR. LEE: Well, so the goal here is is for every chapter and every section we -- there is a plan that MHI has been following. And we've been talking with MHI on a weekly basis on where are we specifically on each chapter. And so we're going to try to practice redundancy and diversity ourselves in such that we have records within the SE and the road map and the records that we keep by the technical reviewers and the PMs to make sure that where we are, where we leave this is exactly, you know -- that all parties agreed to that.

MEMBER BLEY: Okay.

MR. LEE: And that has not been easy. That's been a challenge. And we're in close dialog with MHI to do that.

Now, I just want to say that nothing is being shut down as far as I understand. It's being called slow down because there are some resources dedicated to this review. And as Ryan said, Chapter 18 is kind of next on line after, you know, April 1. So projects will have some resources dedicated to continuing the efforts, but obviously not at the level that we are currently doing.

MEMBER BLEY: Thank you.

MR. SPRENGEL: I'll take a moment to expand a little bit, maybe add some level of comfort hopefully.

The chapter status reports I mentioned that we'll be submitting at the end of March are doing many of the same things that Sam spoke of, but it's from the applicant's perspective and it will be sent in and available on the public record. So it does give a good snapshot of where everything stands in the review of the individual chapters at this time.

And we'll also treat those as living documents that we will update. So Chapter 18 is one of our first starting points. And as we've progressed with Chapter 18, staff finalized the SER. We come to ACRS. We would update that document to show where we stand at that time. So we are trying to keep a good communication and keep a good public record of where we stand in the review and what is happening over time. Like Sam mentioned, you know, we are slowing down, but we're remaining committed. And instead of focusing on all 19 chapters at a time, we're trying to just work on one main area at a time.

MR. BUCKBERG: If I might, in the case of the example of the one RAI response, if an RAI response was issued, we would have come to an agreement with MHI that in most cases the staff would review the RAI and at least give a preliminary acceptance of non-acceptance. In many cases we would have also discussed SE input being drafted to really close it out because we found in the past that unless SE input is drafted, even what looked acceptable may turn out to not be. But we didn't arrive to that point for every RAI, for every question. But we tried to. We tried to get to a logical point, and that's the process we're in right now through the end of the month. And we have a plan, MHI has a plan, and we're hopeful that it's efficient. That's about the best we can do, I think.

CHAIRMAN STETKAR: That's important. You know, I've obviously been following this for -- I said earlier Sam's been here 18 years. It seems like I've been following this for about 36 years.

(Laughter.)

CHAIRMAN STETKAR: But, you know, there are RAI snapshots, and some are very focused on, you know, one specific topic. Some of them are part of a chain of evolving questions. And those, I think, are a bit different. I hope the staff and MHI have been sensitive to those issues where there are initial RAIs issued and perhaps two or three subsequent iterations of RAIs to successively refine an understanding of a particular topic. Those are the ones where the continuity, especially the knowledge base of the current review staff, is probably more important than just a specific RAI on, you know, an isolated, if you will, topic.

MR. BUCKBERG: Right. And there are RAIs as you described that affect several chapters.

CHAIRMAN STETKAR: Right.

MR. BUCKBERG: And there's one reviewer that may be central in monitoring the whole thing like the head coach. There's not much we can do but document what the process was, what the status was and move on.

CHAIRMAN STETKAR: Okay.

MR. SPRENGEL: We do actually have a very good understanding and very good tracking of the kind of sequential RAI question. So that issue is important, and we've recognized that. And working with the staff over really a couple years now, we've kind of looked at the entire history of our RAIs and we've linked the series of questions so that we do understand the connection between them and that we're really at this point focused only on those most recent ones or any of them that are open for whatever reason. So those linkages are very well aware of and documented. So we're in good alignment with the staff and we're following those.

CHAIRMAN STETKAR: Okay. Thank you.

MR. LEE: May I just add one thing just to clarify here, because I don't want to create an expectation that I didn't mean to create here. What I said was that we were working toward making sure that we document as much as we can and the end goal being, you know, delivering a phase product via SER. I also just want to say that, you know, that because the chapters and sections are at various places in the review phase, there are RAIs that we have yet to review, RAI responses that we have yet to review. And so for those, you know, we're making sure that those are the next steps to be tackled, you know, when the full review is resumed.

I also want to say that, yes, the slow down that we're speaking of officially starts after March, but we've kind of been in an initial slow down period for the last three months. So with that, you know, there have been some reduced effort on the staff's part to work on this. So just to make sure that not all chapters have ended with an SER, with reviews of all the RAIs. They're in different places.

MEMBER BLEY: Not to beat a dead horse, but to say things that are so obvious. You know, you are taking care of them. But one thing I do want to just -- I know in this process of RAIs and the reviews of them there's a lot of verbal discussions and things that are worked out. And I hope you're somehow trying to get that documented so that whoever takes this over sometime has the best understanding they can of where things really stood, because I know it's tough to do.

MR. BUCKBERG: It's going to be tough. And one thing that hasn't been mentioned yet is we planned a public meeting on the 20th of March with MHI to compare notes chapter-by-chapter, line-by-line. And that will add some documentation to our side for sure; possibly to MHI, and some of those notes that need to be recorded will be. And that's part of the process. That's an important part of it.

MR. SPRENGEL: But it's a good question. And one of the key parts will be the upcoming meeting. And actually over the last couple months we've identified several areas and worked with the staff on items that were kind of floating, maybe concerns, maybe not and actually working with the staff we did get them documented as RAIs issued out to us. Now how that's resolved and how we respond to it, that's something that we'll deal with over time.

The other part is the chapter status reports that we're developing there is a section that looks into the future. And if it's kind of a key area that we know we still have some interactions and still have some, I don't know, maybe development of a response to go, we're giving an indication in that section of where we intend to go for that area. So again, it's meant to communicate with the staff and it's also documenting on a public record where we stand from the applicant perspective.

MR. BUCKBERG: Next slide? Reflected in

this slide are the chapters that have been issued and by the close of this meeting will have been through the ACRS Full Committee as well, which as MHI represented is the vast majority of the chapters, though there are some difficult areas yet to make it through Phase 2 even.

During the November Subcommittee meeting for Chapter 3, 20 open items were presented by the staff. The current status of those 20 open items is reflected in these three slides for Chapter 3. If there are any specific questions, I hope we can answer or take for action on these.

CHAIRMAN STETKAR: Perry, you noted -- never mind.

MR. BUCKBERG: Chapter 14 was presented on Tuesday to the Subcommittee. One open item was discussed. And no surprise, the status hasn't changed since Tuesday, so it's just reflected on this slide as well.

One ACRS question regarding steam generator internals and vibration testing we had sort of an interim answer that the staff is still considering where to go with that and how it affects Chapter 14 verification programs.

CHAIRMAN STETKAR: Yes, just for clarity

for the other members, there was some discussion during the Chapter 14 Subcommittee meeting. And I noticed -- the reason I said never mind was I looked ahead to this slide. But there's a previous -- one of the RAIs on -- I think slide 6 mentioned -- no, it wasn't slide 6. One of the long list there someplace that I can't find quickly mentioned continuing review of the steam generators.

It was my understanding from the Subcommittee meeting regarding the steam generators -- we had some questions about vibration testing of the steam generators during the start-up program and its resolution in the context of Chapter 14. And I thought that I understood from staff -- is that you've not yet completed -- I want to make sure that I understand it and the other members who were not present at the Subcommittee meeting have an opportunity to gain the same understanding. You've not yet completed your review of the steam generators, is that correct?

MR. BUCKBERG: That's our understanding.

CHAIRMAN STETKAR: And when you complete that review, you may revisit possible start-up testing requirements for the steam generators. Is that an accurate understanding?

MR. BUCKBERG: That's an accurate understanding.

CHAIRMAN STETKAR: Okay. Thank you.

MR. BUCKBERG: We're good?

CHAIRMAN STETKAR: (No audible response.)

MR. BUCKBERG: The RAI at the top of slide 5 is the one I believe you're referring to.

CHAIRMAN STETKAR: Yes.

MR. BUCKBERG: Just for the sake or argument.

That being said, that's the last for Chapter 14 and the end of my presentation. Any questions?

CHAIRMAN STETKAR: Do any members have any questions for the staff?

(No audible response.)

CHAIRMAN STETKAR: No? Thank you very much. And thanks a lot for the summary on the slow down information. That was helpful.

MR. BUCKBERG: Well, we appreciate the questions. We field lots of questions. We have a branch chief meeting today where we present and we take a lot of notes. And there are a lot of opinions and a lot of good suggestions on how to move forward with this. So we're trying to take it all in.

CHAIRMAN STETKAR: With that, we'll have Luminant come up. They have a little bit more material to cover than MHI and the staff.

John, you up first? Don?

MR. WOODLAN: I'm up first.

CHAIRMAN STETKAR: Okay.

MR. WOODLAN: Good morning. My name is Don Woodlan. I'm the manager of Nuclear Regulatory Affairs for Luminant and for the Comanche Peak, Units 3 and 4 projects. I want to thank you for letting us present today, squeezing us into your schedule, especially for Chapter 14.

With me today are John Conly and Bob Reible. They're both from Luminant as well.

First slide. The agenda of what we intend to cover today. Briefly an introduction of the various topics. And the chapters we're looking at are Chapter 3, less the seismic and structural sections; Chapter 9; and then Chapter 14. And as mentioned in the DCD presentation, that does not include the human factors or the seismic structural aspects of Chapter 14. Those will be covered when those sections are covered.

And some general topic information which we presented in most of our briefings hasn't changed much at all. The entire COLA uses the IBR, or incorporated by reference, methodology. In the chapters we're covering today, 3, 9 and 14, we take no departures --

(Laughter.)

MR. WOODLAN: -- from the US APWR DCD. In fact, we take not departures at all in the entire COLA at this point in time.

MEMBER SKILLMAN: SKILLMAN: Don, as you proceed do you anticipate taking departures based on the final 3.7 and 3.8 for the DCD?

MR. WOODLAN: No, but I will say that we have a list of potential departures that we would consider after we got the license mostly for economic reasons that there may be alternate ways of doing some things that we may consider doing. But it's just a list that we've maintained just in case and that we want to evaluate at that point in time.

MEMBER SKILLMAN: So there are potential departures --

MR. WOODLAN: Yes.

MEMBER SKILLMAN: -- awaiting the DCD and the final deposition of this application?

MR. WOODLAN: Yes.

MEMBER SKILLMAN: And that will be based

on economics at the time?

MR. WOODLAN: I believe so.

Do either you recall exactly?

I think that's what they are.

MEMBER SKILLMAN: Okay. And those will be based on Tier 1 information and Tier 2* information, is that correct? If it's not that, it's supplement, so it's Tier 1 or Tier 2*.

MR. WOODLAN: Yes, it could be either Tier 1 or Tier 2*

MEMBER SKILLMAN: Okay. Thank you.

MR. WOODLAN: We have no contentions pending before the ASLB. I will mention that we are one of the plants that was mentioned in the Waste Confidence Rule activities that are ongoing. And so we are part of that evaluation that the staff is completing. I believe they intend to complete that later this year.

All confirmatory items that have been provided to us have been incorporated into the FSAR. And I say FSAR Rev 4. And I believe that's true for these chapters. There are a couple confirmatory items that will be in Rev 5 when it gets issued.

Luminant has responded to all the open items in these chapters and all outstanding issues have been identified in the SERs that have been provided.

Okay. With that, we'll move into kind of a summary of the ACRS Subcommittee discussions and we'll each take turns covering a chapter. I'm going to turn Chapter 3 over to John Conly.

MR. CONLY: Thank you, Don. My name is John Conly. I'm the COLA project manager for Luminant's Comanche Peak Units 3 and 4.

In November of last year we presented Chapter 3. And at that time we discussed with the ACRS Subcommittee a couple of items in detail. One is the military air crash probability, the assumptions and numbers therefore. And the second item was the turbine missile probability calculation, again numbers and assumptions made during that calculation. Those were the major items discussed.

Are there any further questions?

CHAIRMAN STETKAR: My recollection, again for the members who were not present at the Subcommittee meetings, the issues that we raised that are noted here, the military aircraft crash probability, there is a military air traffic corridor within -- you'll have to correct me of the exact distance of the center line of the site, but it's within close enough that they need to actually quantify a crash frequency. And we had some questions about the military aircraft crash frequency data that they're using, because military aircraft have different crash frequencies than commercial aircraft. So that's that item.

Turbine missile probability calculation was more in terms of the completeness of the analysis looking at all of the -- not just the turbine stop valves and control valves and their associated hydraulics, but all the way out through the signal processing to get the trip signals into the solenoids that open the hydraulic fluid valves and things like that. I think there's a clear understanding. We haven't received any feedback yet on either of those items. Seem to be well under control. I don't know where you're going to get the military aircraft crash frequency data, but that's a different issue.

(Laughter.)

MR. CONLY: If there are no further questions, I will ask Bob Reible to pick up Chapter 9.

MR. WOODLAN: No, I'm doing that.

MR. CONLY: I'm sorry, Don Woodlan.

MR. WOODLAN: Yes, this is Don Woodlan again. Chapter 9, we have several topics that we've listed here that were discussed during the Subcommittee meeting. One was the use of wet bulb temperature and especially using that in calculating evaporative losses, whether or not the value we were using was in fact a conservative representation of the site. We talked about the duct heaters in the HVAC system. And that came up because the duct heater values, and actually in the presence of duct heaters was different in the four trains. And it wasn't obvious why they were different, so we discussed the differences.

We discussed the sharing or the fire brigade between Units 3 and 4 and how well that was going to work. We discussed the term of incident commander. And that also goes along with fire brigade leader and exactly what that term meant as we were applying it in the FSARs.

And the final topic was on flooding in the emergency service water pipe tunnel and whether or not that flooding had the opportunity to flow back into other areas that had safety-related equipment. Unfortunately we had some incorrect information in the FSAR that looked like the tunnel was vented into one of the safety-related areas and therefore flooding would have been a concern. In fact, that is not a vent path.

CHAIRMAN STETKAR: It is not open?

MR. WOODLAN: No, it's not open. That was incorrect in the FSAR. We're increasing that.

CHAIRMAN STETKAR: So it's sealed?

MR. WOODLAN: It sealed. So there will not be flooding into that area from the pipe tunnel. And those were the issues --

CHAIRMAN STETKAR: The reason we discussed that last item, and I'm glad -- I don't think we had feedback that it was sealed, did we? My notes were still open on that.

MR. WOODLAN: I don't know. We always depend on your comments to the staff and then the staff asks us and --

CHAIRMAN STETKAR: Okay. Well, we're closing the loop today, so --

(Laughter.)

MR. WOODLAN: Okay. All right. Good.

CHAIRMAN STETKAR: But those are flood protection sealed piping penetrations --

MR. WOODLAN: Yes.

CHAIRMAN STETKAR: -- into the reactor building?

MR. WOODLAN: Yes.

CHAIRMAN STETKAR: The reason this came up, for the other Committee members' benefit, is that the internal flooding analyses, if you want to call them that, for the certified design which includes all of the safety-related equipment areas in the -- I always get the names wrong, the reactor building and the power supply building are documented in the design certification document. So anything that has to do with internal flooding sources; pipes, pumps, valves, that kind of thing, within the scope of the certified design is handled in the DCD.

Luminant is responsible for the ultimate heat sink and the piping connections between the design of the piping connections from the ultimate heat sink, which in their case are mechanical draft cooling towers, into the normal plant and any associated flooding analyses with their site-specific scope of the design. And there's an interface where the pipes from the service water system enter the reactor building.

And there was some question, at least when we had our review, about whether or not those pipe tunnels were physically open to the reactor building such that a break in the piping tunnel could spill water into the reactor building, which was not considered in the internal flooding analyses because it was from a source outside of their scope. And in principle, if they were open should have been considered in the flooding analyses done by Luminant, but it wasn't addressed there.

So that's the whole reason for that last bullet there. And I'm glad to hear that those are closed.

MR. WOODLAN: And the reason for the confusion is when we were addressing freezing in the tunnel, we had mentioned that this was a vent path that would help assure no freezing. And that was incorrect.

CHAIRMAN STETKAR: That was incorrect?

MR. WOODLAN: Yes.

CHAIRMAN STETKAR: Okay. That's the problem? Okay.

MEMBER SKILLMAN: So now it can freeze but it can't flood?

(Laughter.)

MR. WOODLAN: Well, it could flood. The flood just won't flow into the other room.

MEMBER SKILLMAN: Yes.

MR. WOODLAN: And it does not freeze.

(Laughter.)

MEMBER SKILLMAN: Thank you.

MR. WOODLAN: You're welcome.

CHAIRMAN STETKAR: It is open to the ESW pump rooms, or are they sealed down there also?

MR. WOODLAN: I believe they're sealed at both ends.

CHAIRMAN STETKAR: Okay. Thank you.

MR. WOODLAN: All right. And we'll go to Chapter 14. And you'll notice there are no bullets here, but there are bullets on the handout that we gave you, because it just happened Tuesday. And I'm going to turn it over to Bob Reible to cover Chapter 14.

MR. REIBLE: My name is Bob Reible. I'm a project on the Luminant team and I'll address the discussion topics for Chapter 14. The discussion topics were also addressed with DCD and there were no follow-ups for the COLA with regard to these topics.

One of them was on design air flows. And the second one was the PRA success criteria versus the testing requirements for the ultimate heat sink. That concludes --

MR. WOODLAN: Both of which will work with MHI and the DCD in preparing responses.

CHAIRMAN STETKAR: Yes, again, for the

benefit of the other members who weren't here, the design airflow is -- part of the testing acceptance criteria measures air flow from ventilation systems, not necessarily the ability of the ventilation systems to maintain temperature in a room. So we had questions about whether the functional acceptance criteria for those tests should also be measuring the ability of the ventilation system to maintain design temperatures rather than just measuring the flow through the fans. And as Luminant mentioned, that applies both for tests that were specified within the scope of the certified design and for the essential service water building ventilation system which is part of Luminant's design responsibility.

The PRA success criteria, also a common topic that's shared between the design certification and the COLA because most of the -- or many, let's say, of the testing programs confirm the operation of systems to support the licensing basis of the plant, which -- and the licensing basis of the plant is the plant is nominally four 50-percent-capacity trains. So in many cases the tests confirm the fact that any two of the trains can support a safety function.

However, in the PRA there are many cases where the PRA has done analyses to support the notion that any one of the trains can support the PRA success criteria. So we had questions about whether or not the testing program would indeed confirm the PRA success criteria. In other words, that one and only one train operating would indeed support the success criteria as evaluated in the PRA. The PRA success criteria may be different than the licensing basis because the PRA best estimate heat loads and the timing at which the heat loads would be applied to the various systems.

So that's the genesis of the second bullet that we can't see on the screen up there, but that we all have in our handout here. And as I said, that also requires coordination between Luminant and the DCD because the shared nature of some of their responsibilities.

MR. WOODLAN: I was going to sneak in here and type it in, but you went too fast.

CHAIRMAN STETKAR: There you go.

(Laughter.)

CHAIRMAN STETKAR: With that, do any of the members have questions for Luminant? If not --

MR. WOODLAN: Well, let me just make some closing. You discussed earlier about the slow down on the DCD. Just to refresh everyone's memory, when MHI announced the slow down on the DCD, Luminant evaluated our status and we can't move any faster than the DCD moves. So Luminant was to actually suspend review. So as of March 31st we're suspending all reviews of the COLA to be restarted whenever. Again, we don't have a schedule either. We're very dependent on the progress that MHI makes on the DCD.

But we have worked very well. The staff has been extremely cooperative with us. We've gone thoroughly through what's still open on the COLA docket to get them to, as Perry said, a good closing point to get all the SERs updated as much as possible. We only have a handful, maybe five or six questions that we have now responded to and three of those were just issued last week. And the others are questions that we can't respond to because we're dependent on the DCD to give us information before we can respond.

And of questions under evaluation and review, again there's only a handful, I don't know, maybe five or six that are -- maybe more than that, maybe a dozen that are in the evaluation category that the NRC is reviewing. And most of those again are dependent on the DCD activity. Chapter 19, for example, they're focused on the DCD first. We always come second. So that's the reason they're pending.

It's not because there's any open issues.

Everything that could be responded to we have responded to. Almost all the confirmatory items have been closed out. There's only a couple that haven't. And Perry said, the SEs are being updated as they do that so that when we end this on March 31st they'll be as clean as possible going out.

And with that I'd like to thank the ACRS members, especially John and the Subcommittee and everybody that participated in the Subcommittees for the many briefings that we've had over the last several years. Because of the suspension Luminant probably won't be back here in front of the Committee for a good period of time. And this is probably my last time I'll be, unless something very unusual happens.

I'm very much a firm believer in the process, both the NRC reviews and the ACRS involvement. I believe ACRS makes a good contribution to that process and I believe the questions and the comments and the feedback that we've gotten over the years has been beneficial and has helped us to do a better job and produce a better project. And then that's all I have. Thanks, John.

CHAIRMAN STETKAR: Don, thanks a lot. We

appreciate your comments. And it's going to be sad if we don't have any interactions at least with the team in front of us in the future, because it's been very useful. Luminant has taken a real interest. They're knowledge people, good response and be sad if this is the last time we see you, at least with all the faces on both sides of the table. So thanks again for all of your interactions and responsiveness to our questions and things like that. It's been a good process.

MR. WOODLAN: You're welcome.

CHAIRMAN STETKAR: And with that, we'll have the staff come up for Comanche Peak.

MR. BUCKBERG: Hello again. My name is Perry Buckberg. I'm the lead project manager for the staff's evaluation of the Comanche Peak combined license application. I'll be presenting the staff review of Chapters 3, 9 and 14.

As Don introduced, the Luminant will be suspended. And this is what that looks like in black and white. Much like the MHI schedule, everything from Phase 2 on is TBD and will remain that way until the review is restarted at some period.

The review of COLA chapters has followed closely the review of the design certification chapters. So this slide looks much like the slide that I presented previously where most chapters as of the close of this meeting will have been through the ACRS Full Committee. And there are some interesting areas left, but a lot of progress has been made.

Chapter 3 was issued in October of 2013 and presented in November to the Subcommittee. The current status of the three open items discussed are reflected on this slide. And there's been some progress, but still open items at this point.

MR. GALVIN: Perry, if I could just mention, the staff -- this is Dennis Galvin. I'm the Chapter 3 project manager. Sections 3.7 and 3.8 of course were not presented, but also 3.41 was not presented here to ACRS because there was a link to the hydrology review which had not been completed. So you'll be seeing that at a --

CHAIRMAN STETKAR: That's right.

MR. GALVIN: -- future date.

CHAIRMAN STETKAR: Because we haven't reviewed those sections of Chapter 2 of the COLA, right?

MR. GALVIN: Yes. I think those are still being reviewed, yes.

CHAIRMAN STETKAR: Right, right, right,

right.

MR. BUCKBERG: Thanks, Dennis. Any questions on the status of the open items?

(No audible response.)

MR. BUCKBERG: Chapter 9 was issued in July of 2013 and also presented in November. One open item was discussed during the presentation and its status is changed to a confirmatory item where an acceptable response has been provided and the staff is awaiting the next update of the FSAR to verify the change. Any questions?

(No audible response.)

MR. BUCKBERG: Moving on to the last chapter. Fourteen was just issued a couple weeks ago. And again we appreciated the opportunity to present so soon after. There were no open items presented on Tuesday and the staff did field one question regarding license conditions being somewhat redundant with other requirements and regulations. And all the staff needed to discuss and come to an answer for that aren't present this week, but we're looking into it. It looks like it was a decision that was made a couple of years ago. And it's being revisited and there's a possibility of some change. We want to do what's logical and if we can't find justification for it now, it's a good opportunity to change it. So no promises, but that's going to be revisited and discussed internally.

Any questions on Chapter 14?

CHAIRMAN STETKAR: Any members have any questions?

(No audible response.)

CHAIRMAN STETKAR: If not, thank you. This was very efficient, but as all the participants mentioned, there are a number of -- not many really difficult open items, let's say, at least from our perspective, and that's a little bit why we have this efficiency meeting.

Before I go back to the Full Committee, let me ask if there are any members of the public or any people in the room who would have any comments.

(No audible response.)

CHAIRMAN STETKAR: And I don't know if we have anybody on the bridge line. Girija, can we get the bridge -- we do not?

(No audible response.)

CHAIRMAN STETKAR: Okay. I'm informed that we do not have any participants on the bridge line.

And with that, thanks very much to MHI and

Luminant and the staff; appreciate your participation, and again, very much for the cooperation earlier this week with the Subcommittee. It was a difficult process, but we actually got it all done in terms of logistics of the meeting. And again, I'd like to thank everyone for their cooperation earlier this week.

And with that, we will resume the Full Committee meeting.

Now, for planning purposes we are about an hour ahead of schedule. What I would like to do is -- let me ask the members. Would we prefer to take a break now, or do we want to just go into the next item that I'm going to propose?

MEMBER CORRADINI: What is the next item? It all depends.

CHAIRMAN STETKAR: What I'm going to propose is we have an initial read-through of our letters for both US APWR and Comanche Peak, only because we have the time to do that. The letters are relatively short and it's kind of fresh in our minds. So I think we --

MEMBER POWERS: And they seem to be bold-faced lies.

CHAIRMAN STETKAR: And they could be bold-faced lies.

MEMBER POWERS: Yes, because it says we're going to review these chapters during our meetings and we haven't really reviewed these chapters.

CHAIRMAN STETKAR: We've reviewed these chapters. We just did that.

MEMBER POWERS: No, we conducted a wake.

(Laughter.)

CHAIRMAN STETKAR: Anyway --

MEMBER CORRADINI: I hope that's not on the record.

CHAIRMAN STETKAR: It is on the record. What I'd propose, given the time; it's probably too early for a break, if we can just read through these letters, get an initial read-through. I may need some feedback on the -- you'll see on the Comanche Peak letter based on information that we just received during this meeting.

MEMBER CORRADINI: We're at your disposal, Mr. Chairman.

CHAIRMAN STETKAR: So let's try to do that. And we do that in open session, so you know anyone --

MEMBER CORRADINI: Everybody can sit here and watch us.

CHAIRMAN STETKAR: -- is welcome to participate.

Now, should we keep this on the record? We don't normally do that.

MEMBER CORRADINI: No.

CHAIRMAN STETKAR: So let's close the transcript record. It is still an open meeting. We don't normally deliberate on the transcript record. We'll reopen the transcript when we go back in Full Committee session for the next presentation.

(Whereupon, at 9:34 a.m. off the record until 10:44 a.m.)

CHAIRMAN STETKAR: We are back in session. The next topic that we'll hear about is Diablo Canyon Units 1 and 2 digital replacement project, and Mr. Charles Brown will lead us through that discussion. Charlie, it's yours.

MEMBER BROWN: Okay. This is a briefing. Obviously, I'm going to use the title here. Diablo Canyon process protection system is being replaced from its current Eagle System with a new digital protection system, and it's for the reactor trip and safeguards.

We had a subcommittee meeting on this on, I believe it was February the 18th. We had a very thorough and comprehensive subcommittee meeting where all the aspects of this particular replacement were covered pretty comprehensively and with a lot of detail. And we've taken a little bit of that detail out but not all of it. Hopefully, we've got the key pieces here. The staff did an excellent job of giving us the presentation, and I'm sure they'll do the same today.

So we've got about two hours. They have to take less than that because there will be some questions. You've got 40-something slides, so just be aware, as you're going through, get the sense, and when it's ready to move on, move on, okay? And other than that, I'll turn it over to John, if you have any comments, to make to light off.

MEMBER POWERS: The easiest thing is just ignore questions from Charlie.

MR. THORP: That's hard to do. He makes himself known. So that's fine, that's fine. We won't ignore those questions. I'm John Thorp, Chief of the Instrumentation and Controls Branch in the Division of Engineering in the Office of Nuclear Reactor Regulation. Our staff was requested to provide an informational briefing to the ACRS on several topics related to the digital Canyon process protection system upgrade license amendment request that Charlie has described to you.

So I just wanted to start off with a few introductory remarks, and then we'll move on into the briefing. I'm just going to briefly describe the regulatory history of the Tricon and ALS platforms, i.e. the Tricon and ALS topical reports. You'll get more detail a little bit later in the presentation. And the Diablo Canyon license amendment request, Rich Stattel and Rossnyev Alvarado are principal technical reviewers for this evaluation, but you also see Steve Wyman up here, up front with me, and he's going to speak to the Tricon platform topical report. Samir Darbali, who I believe was here this morning, is also one of my staff members. He's assigned as a reviewer for this evaluation.

So I think we have some members from Pacific Gas and Electric, the utility, that are here. And I'll allow them to introduce themselves, if they would like.

MR. SCHRADER: I'm Ken Schrader. I'm responsible for obtaining the license amendment for this application, and I work at Pacific Gas and Electric, Diablo Canyon Nuclear Plant.

MR. PATTERSON: Scott Patterson. I work

at Pacific Gas and Electric. I'm the project lead for this project.

MR. WILSON: Allen Wilson. I work for Pacific Gas and Electric. I'm the project manager for this project.

MR. HEFLER: John Hefler. I'm with Altran, and I've been supporting the PG&E project for some years now.

MR. THORP: Okay, thank you. In October of 2011, Pacific Gas and Electric submitted a license amendment request to replace the Eagle 21 digital process protection control system at Diablo Canyon Nuclear Plant's 1 and 2 with an improved digital plant protection system. The new plant protection system will be comprised of two plant protection subsystems, one of which is based on the Invensys Tricon platform and the other is based on the Westinghouse Advanced Logic System, or ALS as it's known.

Now, the Tricon system is a computer-based PLC or programmable logic controller type system. The NRC issued a safety evaluation report for the Tricon V10, which means Version 10, platform topical report in May of 2012.

For the Advanced Logic System, the ALS, it's a field-programmable gate array, an FPGA-based system that includes diverse features that you'll hear a little bit more about later to address the NRC guidance for diversity in digital protection systems.

MEMBER BROWN: One comment on that for those who don't know what FPGAs are relative to computer-based systems. That's the fundamental difference. Tricon is a software-based system, PGA is a, literally, burned-in gate logic. That's a simplified version, but it's not software based. It does have timers with a clock that runs it and all that kind of stuff, but it is not software controlled. So once you've set it in, it's there. The software is there. The design stage is where the software comes in.

MR. THORP: Right, right. Software is used in the design and construction of FPGAs, and those instructions are then burnt in, as Charlie described, to the chip. So we issued the safety evaluation report for the ALS topical report in October of 2013, and we accepted the LAR for evaluation in January of 2011 for the overall digital PPS. And we identified several issues that could present challenges to approving the license amendment request, and they were deterministic performance of software, software planning documentation, equipment qualification testing plans, and set point methodologies.

Since we raised those particular concerns or issues, Pacific Gas and Electric Company has provided several license amendment request supplements. And they've responded to all of our RAI questions to date. Now, we've sent out another set that Rich can speak to, and they're working on that.

We've had two audits at the vendor facilities of Westinghouse and Invensys. Those have been conducted, and the results are publically available.

So next will be just a very brief discussion on the process protection system overview. This figure shows the Diablo Canyon, it's a very simplified diagram obviously, process protection system architecture, how it fits in with the plant design.

You'll see the red box on the screen. That, essentially, is the scope of the digital process protection system or plant protection system being modified. The white boxes that you see all around it, the various other systems and components, are existing plant components and systems that are not being modified.

The digital plant protection system consists of four protection sets to support reactor protection system and the engineered safety features actuation functions with either two of four or two of three coincidence actuation logic. Now, the integration of RPS and ESFAS, as you may have heard it called before, reactor protection system and engineer safety features actuation system, combines two of the four echelons of defense layers that are described in the NUREG report 6303 for protection against software common-cause failures, or CCF. We'll discuss that aspect in a little bit more detail in our discussion of diversity.

At this point, I'd like to turn over the presentation to Rich Stattel for a more in-depth look at the replacement process protection system.

MR. STATTEL: Thank you, John, and good morning, everyone. I'm the lead reviewer, and, actually, I'm just going to punt it right over to Steve. He's going to discuss the platform reviews. So what we try to do, the vendors of the platforms that develop and design these platforms, they provide us with information and topical reports. We try to evaluate them at a generic level with the understanding that many of the applications, many of the regulations that we're evaluating against are really dependent, we really have to know what the application is, what the specific application is.

Here's a case where we know what the application is. However, we do reference back to the platform evaluations, and there are many characteristics of the system that were previously evaluated. Now, Steve was the lead reviewer for the Tricon platform evaluation. And Bernie Dittman who's in the back of the room here, he was the lead reviewer for the ALS system evaluation. So there are some important characteristics that were reviewed during those applications, and Steve will talk about those first. Go ahead, Steve.

MR. WYMAN: Slide, please. Okay. First, the ALS platform. ALS stands for Advanced Logic System. This is a depiction of a typical ALS platform. It uses a standard form factor rack. It's configurable. Each rack can host a variety of input and output boards, and any combination of boards can be placed in any given rack.

There's a single configuration constraint in that a single logic board must be used to coordinate the processing of signals from all the other boards that are connected in the rack. So we'll show a block diagram in the next slide, and you can see that a little bit better. Back up because I'm not finished talking about the chassis. Thanks.

The system is capable of using multiple racks, and this gives them greater opportunity to use more field signals. What's unique about this platform is that the processing engine of each board is a single FPGA device. Although each board contains unique programming, a common model FPGA device is used on every board. Furthermore, the platform provides two design variants of FPGA programming for each board as a means to increase built-in diversity within an application. Rich is going to talk about diversity a little bit later in the presentation.

MEMBER BROWN: Can I ask one question that I forgot to ask during the subcommittee meeting? The back plane for this, I presume there's a back plane that these all plug in to.

MR. WYMAN: Yes.

MEMBER BROWN: Is that a wired back plane or a printed wiring board style back plane?

MR. WYMAN: I'll let Bernie answer that.

MR. DITTMAN: Bernie Dittman, Office of Nuclear Reactor Regulatory Research. It's a PC copper back plane --

MEMBER BROWN: Printed circuit. It's a printed --

MR. DITTMAN: It's vertical. It's a printed circuit board.

MEMBER BROWN: Okay.

MR. DITTMAN: The cards mount to the front, and the field signals mount on the back.

MEMBER BROWN: Okay. That's all I wanted to know. Thank you. I appreciate that.

MR. WYMAN: Okay. Slide, please. It's a block diagram of the ALS platform. If you notice the parenthetical values, we didn't have a chance to label them, represent number of inputs or outputs on each one of these. I just wanted to point that out.

These signals enter and exit the instrumentation via connectors at the rear of the chassis. As the block diagram is shown here, we have inputs on the left and outputs on the right. Each input and output board requires configuration parameters but does not require changes to its FPGA programming. The board shown on the bottom is a communication board, which may be used to implement interdivisional communications for voting purposes. The board also requires configuration parameters without requiring any changes to its FPGA programming.

Once configured, a communications board acts only as a unit directional receiver or unit directional transmitter. In either case, the serial data communication does not require handshaking.

MEMBER BROWN: This is one division, right? It's one protection set? It's not, when you say interdivisional communication, or, no, you said for voting purposes, and that's a comment we didn't make in the subcommittee meeting. Is that internal to the division?

MS. ALVARADO: He's presenting the generic platform.

MEMBER BROWN: Okay, got it. Okay, fine. Thank you very much. I appreciate that.

MR. STATTEL: In actuality, the Diablo Canyon application does not use any ALS 601 boards.

MEMBER BROWN: Thank you.

MR. WYMAN: My next line, yes.

MEMBER BROWN: I apologize for being ahead of the game here.

MR. WYMAN: The board shown on the top is the logic board and the brains of the ALS platform. The board controls the safety signal bus. As part of the safety signal path, communication between the logic board and the remaining boards occurs through the motherboard over redundant serial bus, shown here as RAB 1 and RAB 2. RAB stands for reliable ALS bus. The use of multiple racks extends this bus.

The logic board acquires conditioned inputs, performs logic functions, and commands the control of outputs. The logic board is the only board that requires application-specific programming. Part of its application-specific programming is the knowledge of the required configuration of all boards connected to its bus. The logic board also provides a limited amount of onboard input and output capability. The signals shown as TxB1 and TxB2 provide unit directional outbound-only serial data communications without handshaking.

The platform has connection for an auxiliary service unit, shown here as the ASU connector. The connection supports communication between the maintenance workstation and each board. These communications occur over another serial bus shown here as TAB for test ALS bus. The test bus operates similar to the safety signal bus but independent of it. The maintenance workstation itself is not part of the ALS platform.

MEMBER SKILLMAN: If I could, you didn't present slide four. May I ask you to show that one, please? No, back to slide four, please.

MR. STATTEL: Oh, that was just an introductory slide.

MEMBER SKILLMAN: Let me ask my question.

MR. STATTEL: Oh, four was just, that's just like a partition --

MEMBER SKILLMAN: It's a cartoon. But let me ask my question. How are the four channels powered? When they did the upgrade at Diablo, did they use the same foundation with the same power supplies? I'm assuming this is DC vital or AC vital. Was there a change to that while you were going through the change to the digital equipment?

MR. STATTEL: I can answer that. They're installing the new digital protection system in the same cabinets as the old protection system, the Eagle 21 system. It is AC vital power, and it's basically the same power that powered the divisions of the Eagle 21 are powering the new digital equipment.

MEMBER SKILLMAN: Understand. So the configuration control for the power supplies is unchanged. You're really changing the brain.

MR. STATTEL: That is correct.

MEMBER SKILLMAN: Got it. Thank you.

MR. WYMAN: The approved ALS platform. So the approved platform from the review defines the architecture and internal communications approach upon which to build an I&C system. The approved platform specifies seven boards, and all board functionality and functional allocations programming, with the exception of the allocation application-specific logic of the core logic board, ALS 102.

The approved platform uses diversity attributes to create two design variants of each board and establishes the development process for the boards, their programming, and verification and validation. The approved platform also establishes qualification boundaries for the platform and design features support implementation of safety function for a plant's application-specific system.

MR. STATTEL: Okay. We're going to move on to the Tricon system now.

MR. WYMAN: Okay. This is a Tricon V10 chassis. I've actually got a nice real picture. So if I stand up and point --

MEMBER BROWN: As long as you can talk loud enough.

MR. WYMAN: I can talk loud enough. Thank you. I just kind of wanted to go over, since we've only had block diagrams before, the key switch that we talked so much about last time for positions, run/stop program, and remote. Each unit has redundant power supplies built in. So for two separate independent power inputs that power both of the independent power modules, up here we have extension bus connectors. If we want to extend the IO bus further, we can do this with regular plain copper cables for local expansion.

Down here, we have the in-processor boards. So a little bit different than ALS where they have single processors doing all the thinking, the Tricon uses three boards running in parallel, all making the same decision at the same time and then they vote on the outputs. It's a redundancy to improve reliability and availability.

In a normal system, you would see this here filled with a communications module. I even asked Tricon about this. This was just an opportunity, so they actually have two communications modules stuck in this slot over here. So you can see where they have four, one, two, three, the top four are serial bus connections. This is a diagnostics connector down here, and these two connections here are for diagnostics.

Now, on the V10, we do not have -- I'm sorry. These are not for diagnostics. These are for, these are the ethernet connections right here, two channels of ethernet, four channels of serial, and one diagnostics connector. The lights up on the top would indicate status realtime, and the remainder of the rack here is filled with IO parts.

Here they have, I believe, an input card, a 32 point input card. And I'm not familiar with these, but all their cards use LED lights on the surface to indicate status.

The box up here contains two redundant batteries that would support saving information, data and the control program, on the loss of power. So there's redundant batteries. Each battery is capable of holding up the information for a six-month period.

Over here, all these blue connectors are simply just extensions of the IO points so you can put terminations on. That's the D10 chassis and all the components described.

Slide, please. Okay. The block diagram for the V10. This diagram is shown left to right, input to output. So this would be a standard termination panel. The V10 uses a set of standard panels that were part of the approval process that go in the back of the chassis. When we bring a signal in on termination panel, internally it goes to three different legs. So for each input module, it actually has three identical circuits that are independent of each other. Each one has its own processor, its own clock. It processes the input signal, which then communicates on the IO bus -- I'm sorry, I can't see over here. It communicates on the IO bus to the three independent main processor boards. The IOC processor on the main processor module controls all the communications on this serial clearance IO bus, and all the safety communications are on just the IO bus.

The same processor also controls communications on the comm bus, which speaks to the communications module that I pointed out earlier. The communications module has single outputs for the communications outside the unit and then internally splits them to three separate channels separately to each of these three cards.

MEMBER BLEY: And that's just a redundancy issue?

MR. WYMAN: Yes.

MEMBER BLEY: And then some kind of selection to make sure you're picking the good signal coming out?

MR. WYMAN: That's right. And the Tricon product, I think, was originally developed commercially to support applications where availability was an issue. We couldn't get to the unit, and we wanted to live a long time, so high reliability and redundancy give them a longstanding availability.

So information comes in. We have a dual port RAM between the communications processor and the application processor where we make our decision. Each individual branch makes its own determination. And if you're familiar with the TriBus, they vote the information among the three independent channels. Each one takes the input information in. It assesses the information, decides if it's good. It votes between the three. They determine whether or not anybody is out of sync and has bad information and, if they do, they throw that information away and that individual channel is given a good answer from one of the other two cards. And then they all run the algorithm based on the good information that they have, and then they write the output back to the IOC comm. Down here on the IO bus again, it will write them out to the output modules. And where we voted inputs over here in the processor, outputs are voted in the output card. I know that was a point that we discussed --

MEMBER BROWN: We vote on the voting and then we vote on the voting and on and on and on.

MR. WYMAN: And then back to our termination panel on the output. And that's the basic operation of a V10. Next slide, please.

MEMBER BROWN: Go back to that one for just one second --

MR. WYMAN: Sure, absolutely.

MEMBER BROWN: -- because it's the first time we've really seen, you've modified the slide to be a little bit more --

MR. WYMAN: I like it. This is the drawing that I learned --

MEMBER BROWN: Yes, that's fine. I guess one of the questions was where is the output to the SSPS?

MR. STATTEL: Well, the answer to that is --

MEMBER BROWN: The primary RXM module, according to one of them.

MR. STATTEL: There's an output forward that plugs into all three of the IO bus -- this is actually triplicated, right, this bus here? So there's an output board that plugs into this. Now, it receives the decision, so, basically, the actuation decision, it receives that from all three processors. Then it does -- the voting takes place on the output board. There's only one contact output here, so, basically, it's a solid state, so the trip decision, the on/off decision of whether to actuate the trip circuit are not, is made on that output board and that is fed, basically, by a copper wire down to the existing solid-state protection system.

MEMBER BROWN: Okay. That's an important point that we had great discussions on because it was not clear. So you had clarified that very well, and this is a good picture to illustrate that. Thank you, Rich.

MR. WYMAN: Okay. Let's go for the Tricon platform review. Obviously, this was an update from V9. A significant number of the components changed. Most of the changes were in the MP3008 main processor boards and the communications module. The V9 unit used three different individual communications modules that were optional, and, in this one, they have an altogether new different TCM, Tricon communications module. A major part of our review focused on these two modules.

The Tricon platform review establishes guidance for communications and compliance with ISG-

04. I believe we only approved two of the individual points, generically, for the system. Everything else is application specific, but we do offer up some guidance in the SE that would help on the application-specific reviews.

The platform report also establishes development process for the boards and their programming and verification and validation. And similar to the ALS, it establishes qualification boundaries of the platform, the design features to support implementation of safety functions for the plant's application-specific system.

MR. STATTEL: Okay. Well, thank you, Steve. What we're going to do now is we're going to step back a little bit, and I'm going to give you an overview of how these two platforms have been incorporated into the Diablo Canyon application-specific project here.

So this diagram here, this is an expanded view of the existing Eagle 21 process protection system. There's a couple points I'd like to emphasize on this slide. As we mentioned before, as John mentioned, both the trip system, reactor trip system, and ESFAS systems share this sensor input, but the sensors are isolated between divisions, as you can see here.

The voting logic for the ESFAS and the reactor trip function is performed by the solid state protection system, which is shown as the gray box below the blue box there. And that's not being modified as part of this license amendment.

The actuation signals to the SSPS voters are hardwired connections. They do not use digital communications technology at all. There are no interdivision communications being implemented in this design.

Okay. This is a view of the replacement process protection system. And like the previous drawing, both the RTS and ESFAS systems will share the same sensor inputs. There's no changes there. The voting logic will continue to be performed by the SSPS system, which is not being modified. The actuation signal to the SSPS voters will remain hardwired connections, and there are no interdivision communications being implemented.

The maintenance workstation boxes that are shown on this diagram, these are these gray boxes that are within the Tricon and ALS subsystems here, those are maintenance workstation computers. Those are non-safety related, and they will be installed within the

PPS cabinets.

MEMBER BROWN: One comment just to amplify, there's no connection between the Tricons and the ALS's? Those are two separate connected processing systems for the data?

MR. STATTEL: Yes. Later on in the presentation, we'll be talking about communications aspects.

MEMBER BROWN: Yes, there's one exception to that, but it's not a, it's more feeding data that is not processed -- I apologize for that confusion. There's a temperature signal that's fed out of the ALS that that's where you've computed, and then it's sent to the Tricon within the division? So there's no interdivisional, but that's the only connection between them, roughly.

MEMBER SKILLMAN: Rich, what is the KVM, the --

MR. STATTEL: Okay. KVM just stands for keyboard, video, and mouse. So, basically, this is the operator interface. Both the ALS and the Tricon chassis that you saw pictures of earlier are going to be mounted in the same cabinets as the existing Eagle 21. They have, each has an individual maintenance workstation, basically a PC that's installed in that cabinet. But there really wasn't room in the cabinet for the licensee to put two separate monitors, two separate keyboards. So what they do is they put one switch in, and that just switches those peripherals between the ALS maintenance workstation and the Tricon maintenance workstation.

MEMBER SKILLMAN: Thank you.

MR. STATTEL: Okay. One other thing I'd like to point out on this figure, at the top of the figure you'll notice between the sensors and the process protection system are a series of isolators. And these are basically qualified analog devices, analog isolators, that send signals over to non-safety related systems, such as the AMSAC system which is being used for ATWS protection.

Okay. The figures in this and the next set of slides represent varying levels of detail how the safety functions are accomplished by the process protection system. All of these slides are going to be laid out in the same format. On the left side are the inputs to the system, in the center are the processes being performed by the process protection system, and on the right are the outputs from the system.

So as an example, on the left side of this figure are the monitored plant parameters. The blue boxes represent parameters that are used to perform reactor trip functions. The pink boxes are parameters that are performing engineered safety features functions, such as safety injection actuation. And the purple boxes are parameters that are used for both reactor trip and ESFAS functions.

On the right side are the functions supported by the PPS system. The top box is a red box. That's the reactor trip. And all of the other ones are ESFAS functions.

Okay. As you can see here, the replacement system basically splits from what was previous just a single Eagle 21 processor. Now we're going to have two subsystems, one is Tricon and one is ALS.

This figure basically shows you which functions are being performed by the Tricon system. The determination of functions, function allocation for the PPS systems were made based on the results of a D3 analysis that had previously been performed.

All functions for which automatic --

MR. THORP: By D3, we mean diversity and defense in depth analysis.

MEMBER CORRADINI: He was talking to

Charlie.

MEMBER BROWN: You just answered his question.

MR. THORP: Yes, I have a little bit of ESP. I got the memo from the Chairman of the Commission that said we should not try to speak in acronyms, so I'm trying to do the best we can to explain any acronyms that pop up without having further . . .

MR. STATTEL: So the basis for the function allocation was all functions for which automatic diverse backup actuation signal could already be credited in the analysis were assigned to the Tricon subsystem. I'll point out and we'll mention it later on, as well, there was an original D3 analysis performed in 1993 for the Eagle 21 system. That was updated in, I believe it was 2010.

There were three signals for which no existing automatic diverse actuation function was available in the Eagle 21 design. Those are reactor coolant flow, pressurizer pressure, and containment pressure, and you can see those three signals on this diagram have inputs to the ALS system. So those were allocated, those functions were allocated to ALS. As the next few slides will show, all the remaining signals are allocated to ALS.

Okay. So this is the opposite slide, which shows the ALS functions. Now you can see which process signals are provided and which functions are being performed by the ALS subsystem. For functions associated with these signals, manual operator actions needed to be credited for the original Eagle 21 design. The D3 analysis, the original D3 analysis postulated a loss of all safety functions for the entire PPS on a common-cause failure.

For these three functions, there basically was not automatic diverse coping means for those. And, therefore, they relied on manual operator actions.

So, essentially, if you think about it, this figure also represents what the PPS functionality becomes when a CCF failure of the Tricon system occurs. So, basically, these are the functions that are retained on the postulated common-cause failure.

And as the figure shows, there are only two functions that are, that become unavailable on the CCF of the Tricon. And those are the turbine trip feedwater isolation and ultra feedwater initiation. However, both of those functions, the D3 analysis, had identified coping means for them.

CHAIRMAN STETKAR: Rich, before we leave that, we had some discussion at the subcommittee meeting about function allocation between Tricon and ALS. And I just want to make sure that I left the subcommittee meeting understanding that correctly. We talked about auxiliary feedwater initiation, which is one of the functions you just mentioned that is not allocated to ALS, and I believe that the conclusion was that the AMSAC logic would provide a diverse signal for auxiliary feedwater actuation. At least that's what my notes say here.

MR. STATTEL: That's correct.

CHAIRMAN STETKAR: Mean steamline isolation for steamline breaks outside containment, not steamline breaks inside containment but steamline breaks outside containment, I believe we were left with the impression that that function is only performed through the Tricon platform.

MR. STATTEL: That's correct. The D3 analysis covers all of the accidents that are covered in the safety evaluation for the plant. It's not just these two. I really just pulled these two up as examples.

CHAIRMAN STETKAR: I understand. Let me finish, let me finish my observations, just for the record and --

MR. STATTEL: Okay.

CHAIRMAN STETKAR: -- edification of the other members who weren't present. And that all of the safeguards actuation signals for a LOCA are now processed only through the ALS platform. We were told that, well, for the steamline isolation for steamline breaks outside containment, that still could be mitigated by manual operator actions to isolate the steamlines. And for safeguards actuation for a LOCA, if the ALS platform were to become unavailable, the operators could manually initiate safeguards actuation. Is that --

MR. STATTEL: That is true. That is true and correct.

CHAIRMAN STETKAR: I just wanted to make members aware of the fact that we've, this change has provided diversity for common-cause software failures in the Tricon platform. It has not necessarily provided diversity for all conceivable common-cause failures.

MEMBER CORRADINI: But it's better than what was there?

CHAIRMAN STETKAR: It's different from what was there.

MEMBER BROWN: Well, I would call that, I would expand that a little bit. I mean, they do provide some automatic operation for stuff that was only manual before.

CHAIRMAN STETKAR: They provide automatic actuation for stuff that was only manual before for a software failure in that particular platform.

MEMBER BROWN: Yes, in that Eagle 21 platform. Yes.

CHAIRMAN STETKAR: There are still manual requirements for software failures in the Tricon platform, and there are still manual requirements for what, at the moment, I'll call unspecified common-cause failures in the ALS platform.

MR. STATTEL: Right. And these are all considerations that we're taking into account in our safety evaluation. We recognize that the Eagle 21 is an approved platform. The plant is operating today with that. This modification does reduce the reliance on manual operator action.

CHAIRMAN STETKAR: And that I absolutely agree with. It's reduced the reliance, it hasn't -- I want to make the -- there's still a need for manual operator action under certain conditions.

MR. THORP: Mr. Corradini's observation

that it's better than the Eagle 21 is in that sense, is in that respect.

MEMBER CORRADINI: Yes, but it's hard to extract a better than out of --

MR. THORP: Right, right.

CHAIRMAN STETKAR: My experience is new, this is different. Better than requires a pretty thorough reliability assessment, and I don't think that's been done.

MR. THORP: Right. And as Rich pointed out, I don't know that I mentioned that in the beginning, but we are still in the process of conducting our safety evaluation. This is not a completed evaluation yet, so it's an informational, this is where we are right now, presentation.

MR. STATTEL: Now, of course, in performing our review, we're using our guidance, right? So we have Chapter 7 guidance from the standard review plan. Part of that guidance is BTP 7-19, which is the diversity defense in depth. And in that guidance, there is a preference for automatic diverse actuation instead of manual actuation. And we've had discussions with the licensee, and this was the basic premise that they were pursuing --

CHAIRMAN STETKAR: And I'm not, you know, I'm not trying to, I'm just trying to make sure that the members here who didn't have the benefit of the subcommittee discussions aren't led to necessarily believe that this change has eliminated completely the need for any manual operator actions, that, essentially, it's not, they aren't left with that impression.

MR. STATTEL: That's correct.

CHAIRMAN STETKAR: Those operator actions is true, are approved under the existing design, given the time available and the indications and, you know, that approval, in a licensing perspective, would be carried through, you know, your current guidance, I presume.

MR. STATTEL: Yes, that's correct. So at this point, this completes the system overview. So if any of the members have questions about the general layout of this system, now would be a good time for that.

The next session, we'll be talking about communications, so we'll talk about the communication interfaces and we'll talk about the review criteria that we're using for that.

MEMBER SKILLMAN: Let me ask this question: with the change to these two different subsystems, are the response times that are modeled or that are assumed in the analyses for the various accidents and conditions unchanged?

MR. STATTEL: The specifications for response time are basically being carried from the Eagle 21 system response time numbers to the new system. We are evaluating, there's a specific section in our safety evaluation for both deterministic performance and for response time performance characteristics of the systems. That is, there is an application-specific aspect of that that we're evaluating, and I will talk in more detail about that later in the presentation.

MEMBER SKILLMAN: Thank you.

MR. STATTEL: So what I'd like to do now is turn it over to Rossnyev Alvarado, who is also a lead reviewer for this license amendment review, and she'll be talking about communication aspects of the system.

MS. ALVARADO: Hi. I'm Rossnyev Alvarado with the Office of Reactor Regulation, Division of Engineering, Instrumentation and Controls Branch. I am responsible for the review of the Diablo Canyon PPS system communication.

This slide that we have here list the

guidance that we have available for communication. 603 provides criteria for independence between redundant portions of a safety system and between safety systems and other known safety-related system. Then 7-4.3.2, in addition to the requirements described in 603, states that data communication between safety channels or between safety and non-safety systems should not inhibit the performance of the safety function.

To clarify these two guidance, the Digital Instrumentation and Control Steering Committee formed the task working group. This task working group prepared ISG 4, which provides adherence points for evaluating a digital safety system compliance with NRC communications guidance. We're using ISG 4 to evaluate the Diablo Canyon PPS replacement system.

Next slide. I know Rich presented this slide, but I just want to emphasize the description provided regarding communication. The first thing is that the PPS system consists of four independent protection systems. You can see it here identified as PS-I, II, III, and IV. The PPS system does not use any means of interdivisional data communication. The licensees maintain interdivisional independence by not including any cross-divisional communication. This means that there's no communication between the vertical wall, so nothing goes between one protection system to another one.

In addition, data communication doesn't occur between the Tricon and the ALS system within a division. As Member Brown points out, even though this looks like they're together, they're not communicating. So no communication link, in this case, again, crosses the horizontal walls that you see in this slide.

Rich points this out, but I just want to emphasize that there are no communications between the PPS and the SSPS. The lines shown in the figure only represent the signal trip decision sent from the PPS to the SSPS. And last but not least, the same level of communication separation is provided for all four protection sets.

CHAIRMAN STETKAR: Rossnyev, just for clarity again, you said there's no communications between ALS and Tricon. There is --

MS. ALVARADO: I go --

CHAIRMAN STETKAR: You'll have slides on those? Okay.

MS. ALVARADO: What I mean, communication means data communication.

CHAIRMAN STETKAR: Okay.

MS. ALVARADO: But I will show that in detail because there is a transfer of signal, yes. This is a slide that shows the replacement communication architecture. This slide was provided by the licensee in the license amendment request. This slide shows the links and pathways supported by the Diablo Canyon PPS design. Again, these are just data communication I'm talking about.

Each protection set has the same communication pathway. The PPS communication architecture is designed to ensure communication between safety and non-safety equipment within the protection set adhered to the guidance described in ISG 4.

Like I said, again, this slide shows the ALS and the Tricon together. But as I mentioned before, they do not communicate with each other.

Within each protection set, the PPS incorporates safety-to-non-safety communication. The non-safety components are towards my right, to your right, sorry, the other right, the non-safety components that they communicate.

I will talk about the Tricon and ALS in subsequent slides, but I want to use this slide to introduce and describe the components that are non-safety related. In this case, we're talking about the plant computer system, which is down to your right; the maintenance workstation; the KVM switch; and the Tricon remote RXM non-safety chassis, which is not shown here but I will show later in the Tricon.

So Rich point out that we have the maintenance workstation. This is on the right of the slide. We have a maintenance workstation for each one of the systems. In other words, one for the Tricon and one for the ALS.

This maintenance workstation support maintenance calibration and surveillance functions. The maintenance workstation are stand-alone computers that cannot connect to the internet, nor with the plant computer system or network.

These workstations are in a division set, and they cannot communicate with other workstations in a different division. In addition, the workstations cannot communicate with workstations in other redundant protection sets or communication with safety-related equipment, like ALS or Tricon, in other protection sets.

Then we're going to move into the KVM switch. The KVM switch, it's a switch that provides access to peripheral devices, such as keyboard, video displays, and mouse, for authorized personnel to perform maintenance and calibration activities. One KVM switch is provided for each protection set. So authorized personnel would select with a KVM switch what safety system they want to perform the activity.

The maintenance workstation and the KVM switch will be located inside a locked cabinet in the cable spreading room, minimizing the possibility of the inadvertent action. Use of the maintenance workstation and KVM switch is subject to site-specific procedures and physical access control.

And last but not least is the plant computer system, which is the one at the bottom to the right. Both the Tricon and the ALS communicate data to the plant computer system. The plant computer system is part of the existing system and is not part of our review.

Communication with the plant computer system is one way. The Tricon transfer this data to the port aggregator tap and the ALS does it through the transmit TxB communication ports. I will talk about them when I talk about each one of the systems. Next slide.

MEMBER SKILLMAN: Before you go, I've got a question. Rossnyev, you say the KVM switch and that gear is in the cable spreading room. One would assume that's highly protected through plant security.

MS. ALVARADO: Right.

MEMBER SKILLMAN: But if somebody were to find access to the cable spreading room and into that locked cabinet, is there any way use of that equipment in that locked cabinet could take control of any of the channels?

MS. ALVARADO: First of all, there is, like, password-protected access to the maintenance workstation. So besides getting access and getting the key to access to that, you need to have the right password to access that. And Samir will talk about that.

And second is you have to select which protection set you want to do, you want access to. But access is, if, for example, you were to alter the ALS, it's not so simple, and I will describe that, because it's not just logging into the maintenance workstation. You also need to connect a cable to do such a thing because the communication from the ALS to the maintenance workstation through normal operation is just to monitor. You cannot do anything. To do any of your maintenance activities, you need to connect what is identified as a TAB, a test ALS bus, to be able to communicate two-way with them.

With the Tricon, it's slightly different because with the Tricon the port aggregator tap permits two-way communication. However, there are means inside the Tricon that you need to tamper with to be able to do such a thing. For example, there are different access level and they have a key switch that you need to modify, to do something like that.

So it's not as simple as I break in and I go into the KVM switch and I can go on and alter that. I mean, it's a complicated series of steps.

MR. STATTEL: I'd also like to add, clearly, it's feasible that someone could, a knowledgeable insider could get access to the equipment and they could break through all of these measures if they know the password and they can connect the ALS bus, they can turn the key switches on the Tricon. However, all of those activities would alert the operator because any of those activities would cause an alarm in the control room.

So the answer is it is feasible for an insider to get access and take control of the system in the cable spreading room. However, it's really not conceivable that he could do that without the operator being aware of that.

MEMBER BROWN: Could they access -- that's only one protection set, though.

MR. STATTEL: That's correct.

MEMBER BROWN: You still can't get through the -- if you're accessing one, can you access another one? I don't remember that from the previous --

MR. STATTEL: They're in different cabinets. If you had more than one person accessing them, I guess it's theoretically possible.

MEMBER BROWN: Okay, all right.

MR. STATTEL: But there would be multiple alarms in the control room, as well.

MEMBER BROWN: Yes, thank you very much.

MS. ALVARADO: Actually, whenever you're doing modifications in the ALS, an alarm will be enunciated and then a second alarm will be enunciated for the Tricon.

MEMBER BROWN: Before you leave this slide, from the previous meetings we've had and the discussions relative to control of access to external internet type functions, that would be through the plant computer if anybody was going to do that. So there's three lines: the ethernet line and the TxB1 from ALS A and the TxB1 from ALS B. Those are the three lines that somebody, if they made access to the plant computer, could come back.

Now, you're going to discuss why those are hardware type one-way, as opposed to software based, correct? So those are the key lines from a control of access and external tampering via particularly the software in the Tricon.

MS. ALVARADO: Right. Okay. What I did was a cartoon to try to identify better the different components that we have. And this slide shows the communication architecture for the ALS system. There are no communication paths between redundant safety divisions or protection sets in the ALS portion of the PPS replacement. It means that ALS and other protection sets cannot communicate with this protection set in particular. I'm using protection set four for these description, but all of them are exactly the same.

In previous slide, we mentioned that there is no communication between the Tricon and the ALS. However, you can see that this figure shows these green lines here. I want to clarify that these lines represent analog temperature signals processed in the ALS system that are used by the Tricon system to perform the over power differential temperature and over temperature differential temperature reactor trip safety functions. So these are not communication links. These are just analog signals that are sent from the ALS to the Tricon.

Regarding communication with the workstation, the ALS used the transmit TxB ports.

MEMBER BROWN: Rossnyev, can I make, I want to make sure I understand one thing. The ALS A and B are the same --

MS. ALVARADO: Yes.

MEMBER BROWN: -- but independent, and they are both sending the same signal over the, you still have that system? So you can move one of those. That's my memory anyway.

MS. ALVARADO: Yes, I apologize I didn't explain that. I guess I forgot.

MEMBER BROWN: That's okay. No, you're fine, you're fine.

MS. ALVARADO: No, because in the presentation that we did before, we went into this. ALS has two cores. It's core A and core B, and this is part of the redundancy that they have. Both cores perform the same functions, so that's what I'm talking about.

MR. STATTEL: One minor correction,

Charlie, I'd like to make. They're not the same temperature signal being processed by ALS A and ALS B. There are actually two elements in each RTD, and one of the elements goes to A and one of the elements goes to B.

MEMBER BROWN: It's the same temperature signal to --

MR. STATTEL: Same signal, yes.

MEMBER BROWN: I'm very familiar with that process. Yes, okay, thank you. It's a good clarification.

MS. ALVARADO: Okay. So we're talking about the transmit TxB port. As you can see, ALS A and ALS B, each one of them has two transmit ports, one goes to the maintenance workstation and the other one goes to the plant computer system. These communication ports are customized so they can only transmit data to these connections, and this is done in hardware.

Communication for the TxB port is only directional and does not require the use of handshaking signal. These ports are physically and electrically incapable of receiving information from external sources, in this case from the maintenance workstation and the plant computer system.

MEMBER BROWN: The TxB1 and each one of them, is that the one where you've got the open circuit, so it's a physical open line, whereas the transmit line is closed, obviously?

MR. STATTEL: That's correct.

MEMBER BROWN: Thank you.

CHAIRMAN STETKAR: You have a very resonate voice.

MEMBER BROWN: I pushed my microphone as far away as I can.

MEMBER CORRADINI: Everybody else is not as forceful. Stop using your command voice.

MS. ALVARADO: These ports provide a barrier between class 1E and non-class IE. The use of the transmit TxB ports was reviewed and approved for the ALS platform.

Then regarding testing and maintenance of the ALS, the test ALS bus, which you can see at the top there, it says disconnect, needs to be connected to the maintenance workstation and to the ALS core that you want to perform activities to to provide direct two-way communication. Normally, this tab is disconnected and all you have is information that is coming to the TxB.

MEMBER BROWN: Can I ask one other

question to make sure I still remember what you told us in the subcommittee meeting? The ability to communicate back to either one of the cores does not allow changing the fundamental program, that it only allows you to change set points, calibration data, that type of information; is that correct?

MS. ALVARADO: Correct. Because as you mentioned before about the FPGA, that's one of the benefit of using FPGA. You need to burn the core in the device itself. If you want to change it, you need to remove the board to do that.

MEMBER BROWN: Put a new piece in?

MS. ALVARADO: Right.

MEMBER BROWN: Yes, thank you. That's a good clarification. Thank you.

MS. ALVARADO: Maintenance and calibration activities for one of the ALS core, it's required the TAB is physically connecting, allowing two-way communication between that core and the maintenance workstation. Only one core can be connected to the TAB, and this is restricted by process procedures.

There is no associated with disconnecting or connecting this communication link. A TAB connection is provided for each core.

If a diverse ALS subsystem or the core

that is not connected to the TAB will be performing the regular functions, the one that has the TAB connected to it will be taken out of service, with the exception of the RTD signal, the temperature processing functions that are needed to be sent to the Tricon. An ALS trouble alarm will be initiated in the main annunciator system when the TAB is physically connected so the operators will know that someone is performing activities in the ALS.

Next slide. The Tricon communication architecture. This is presented in this slide. So what I did was just try to focus in the different components for the Tricon.

There are no communications again between the Tricon in one protection set to the Tricon in another protection set. All Tricon communication with external devices for the Diablo Canyon PPS is via the Tricon communication modules and their remote RXM. The remote RXM is a new component that was not shown before but still a slide pointed out.

These remote RXMs are used to acquire and transfer non-safety related signals to support functions that are not safety-related PPS functions. In other words, what they represent is an expansion chassis that is located several miles away from the main chassis. There is no data exchanged between the RXM chassis in other protection sets. In addition, one remote RXM can just communicate with the primary RXM.

The use of the RXM communication was described in the Tricon platform topical report and was evaluated by the NRC in the associated safety evaluation. As a result, we have one of these plant-specific application items in which it is required that we confirm that data received from a non-safety remote RXM is not used to perform required safety functions. So as a part of our review, we need to confirm that, for Diablo Canyon, signals acquired by these RXMs are not used to support mitigation functions for a common-cause failure of the Tricon. We did that and the last slide from my presentation identifies this. I just wanted to point out.

Then let’s go back to the Tricon communication module. Inside the Tricon, there is this Tricon communication modules that allows the Tricon to communicate with the maintenance workstation. To do such a thing, communication has to occur through the dedicated one-way port aggregator network tap. I will talk about the port tap in the next slide just to show how it works, but the TCM uses psychic redundancy checks, handshaking, and other protocol-based functions to ensure data communication integrity.

In addition, the Tricon uses dedicated memory location for communication. In this model, there's no direct communication between the application processor and the TCM interface with the maintenance workstation. So if I were to lose the TCM, the main processor will continue to function. The TCM was qualified under the Invensys Appendix B program, and our evaluation is described in the safety evaluation report.

The next slide. So in this slide, what I'm trying to show is what we're talking about, this port aggregator tap. We have three ports. If you can see, there is port A, B, and 1. I tried to put arrows so you can see to what configuration, how they're used in the Diablo Canyon. And what I want to point out is that port 1 is one-way communications. Ports A and B are two-way communication. This tap aggregator is a hardware device that provides this communication TABs and it does not rely on computer software.

The port tap was previously evaluated and has been approved as an acceptable mean for isolating safety system. The NRC performed a safety analyses to confirm such a thing. This analyses, what they did was that for data signals to flow from the TCM, the Tricon TCM, towards the plant computer system, which means for port A to port I, electrical signals pass to a buffer amplifier integrated circuit component.

The NRC staff evaluated this proper amplifier where the potential of electrical signals to flow in the opposite direction, meaning coming from the plant computer system to the Tricon TCM. And what the staff found is that the amplifiers were not capable of passing electrical signals in the reverse direction under any conditions, which means that they reckon a flow for port 1 to port A.

Regarding port B, which is the communications with the maintenance workstation as a set, there are different measures of protection to allow this access to the Tricon, and these are like the Tricon K switch that Steve was mentioning about. They have different operation modes that you need to change if you were to change the program inside the Tricon. And for calibration and maintenance, you also have to go to different layers of access in the maintenance workstation to change the set points.

And last but not least, next slide, this is the IO signals that are processed by the remote RXM chassis. The reason we decided to list that is just to show that, as a part of the application specific item that we had, we needed to confirm that these signals are not associated with systems required to be diverse from the PPS system.

This concludes my presentation of all the system communication, and now Rich Stattel will describe his evaluation of the diversity and defense in depth.

CHAIRMAN STETKAR: Rossnyev, I don't remember whether we asked at the subcommittee meeting. It is possible for personnel to use the Tricon maintenance workstation to update the programming software in the Tricon platform during power operation, right?

MS. ALVARADO: Well, yes. But you will want to have the specifics to do so, which is the Invensys TS 1311. And then you need to modify, with the key switch you need to modify to be in remote or program to do that.

CHAIRMAN STETKAR: Yes, I know about the things that people need to do that. But, indeed, the difference, you can't, because of the programmable gate arrays, you can't change the burned-in logic. You can change the set points. You can change the set points anywhere. But the question I had is are there any restrictions for Diablo Canyon to not change the programming during power operation to update the software? There have been events where people have updated software. Obviously, if you're going to operate software in one protection --

MR. STATTEL: We actually have not made that decision for Diablo Canyon.

CHAIRMAN STETKAR: Okay, okay.

MR. STATTEL: That will be, that will be documented in the safety evaluation.

CHAIRMAN STETKAR: Okay, thanks.

MR. STATTEL: I will mention, though, for the Oconee application, we had that discussion and they committed to never changing software while operating. So they basically have to shut down in order to load a new version.

CHAIRMAN STETKAR: To update the software.

MR. STATTEL: It becomes very complicated because if you allow that, so if you think about it, you have four changes. You basically have to do an operability determination for each configuration you go through in the process of --

CHAIRMAN STETKAR: Oh, because, in the interim, you're going to have different versions of the software --

MR. STATTEL: And we've began those discussions with the licensees, and they're like, yes, we're just going to shut down any time we load software.

CHAIRMAN STETKAR: I just didn't remember in the subcommittee meeting whether they talked much about that.

MS. ALVARADO: Now, I just want to add that if, for example, there was something to happen with your program and you just want to reload the program, you could do that. But then you will have to, like, check between all three processors to be, you know, like, are we all having the same configuration. And like Rich said, we're still in the decision part of it.

So Rich?

MEMBER BROWN: It would be a good idea to highlight that and document it. I presume you will do that in the SE, correct?

MR. STATTEL: Yes, we will. Typically, the way we document that is we'll write, either we'll have the licensee make a commitment, a documented commitment, or we'll write inspection items. So we basically list items to be inspected during the start-up, so the region would go out and do inspections during the site acceptance testing, and they would follow through with documenting that.

MEMBER BROWN: Yes. But once you finish that, now you're in operation. Somebody could try, so there's still a downstream effect if somebody wanted to go change the --

MS. ALVARADO: Well . . .

MEMBER BROWN: Now, but once you've finished the initial startup and all the initial testing and everything else, now you're back generating electricity for everybody. So the same concept would apply. You have to shut down before you go modify something. If the vendor, Invensys, comes up with an, uh-oh, we've got a little thing over here we need to fix, then you have to go through the shutdown process in order to do that to be consistent on all four channels, I would think.

That's why I'm suggesting that that thought process be carried clear through the operational phase, as well, in the SE so we understand what the final decisions are.

MR. STATTEL: Understood.

MS. ALVARADO: Okay.

MR. STATTEL: Okay. Thank you, Rossnyev.

I'm going to switch over, and we're going to talk about the diversity defense in depth characteristics of the system. In the first slide here, I talk about the guidance documents that we used for our diversity review. There are three primary documents that cover diversity. They're based on the direction provided by the Commission in the SRM, or staff requirements memorandum, for SECY-93-087.

The first one is a NUREG document, 6303, which describes a method for analyzing a common-cause failure, a software common-cause failure of a computer-based nuclear safety system and it's potential effects on the overall plant safety analysis. The second document is BTP, I mentioned before, Branch Technical Position, 7-19, which is part of the standard review plan. It provides guidance for evaluating an applicant's or a licensee's D3 analysis and the design of automatic and manual controls and displays for use as a diverse actuation system.

The ACRS has reviewed that latest version. I believe it was a couple of years ago. And, finally, there's an Interim Staff Guide 02 document that was developed as a result of direction we received from the Digital I&C Steering Committee to provide clarity for the established expectations for D3 analysis.

I mentioned the ISG-02 document. It's criteria have been incorporated into BTP-19. However, the D3 analysis for this project was evaluated prior to that, so it is a relevant document. We're actually using the Revision 6 BTP-19 for our application evaluation.

Okay, next slide. Okay. So what BTP-19, what the criteria states is that there should be a coping strategy to be developed for digital safety systems to address the effects of a software common-cause failure when the potential for a common-cause failure cannot be eliminated. So, basically, they have two options. They either make a case that there is no potential for a common-cause failure, or they do the analysis and play it through and apply that to every accident situation that's in the FSAR and determine how the plant responds and what coping mechanisms are available.

A D3 analysis was initially performed for the existing Eagle 21 system back in 1993. That analysis postulated an entire failure of the PPS system, the Eagle 21 system. So if you think back to the first diagram I showed you, that entire green box fails and all of the safety functions on the right side of that basically fail to perform. So the reactor doesn't trip, the ESFAS doesn't actuate. That's what was postulated.

The result of that, there were several accident scenarios where manual operator actions were required to be performed in a given time frame. And there were also other scenarios where there were existing diverse system, such as the AMSAC system, that were available and could be credited for mitigating the accident.

Prior to this license amendment or receiving this license amendment, the licensee performed an update to the D3 analysis to address the changes being made for this license amendment. The NRC staff completed an evaluation of that updated analysis in 2011. It was basically an update to the previous tables that were done in 1993. It involved the postulation of the software common-cause failures for all plant accidents and AOOs described in the FSAR.

The safety functions associated with these parameters that were relying on manual operator actions were allocated to the ALS. We talked about how the functions were allocated on the earlier slide.

The D3 analysis does not make a case for that software common-cause failure of either Tricon or

ALS is not possible. Instead, for the ALS, it determined that the effect of the postulated common-cause failure does not cause a loss of the safety functions, and that's because they have a means of basically adding diversity into the system. And I'll discuss that in the next slide.

So for the Tricon, basically, they just postulated loss of all the functions, so there's really nothing to discuss there. It's no different than what was analyzed for the Eagle 21 system.

But for the functions performed by the ALS, they've designed two important redundancy features that are being considered in the evaluation we're performing. They are core diversity. As implemented in Diablo Canyon application, they generate two redundant logic implementations for placement within each FPGA for each standard circuit board. So the two redundant logic implementations are represented in this figure as the relation between core A1 and core A2 and between B1 and B2 in this slide.

So both of these implementations use the same hardware descriptive language, so the same set of instructions to program the FPGA are used. However, the logic implementation is produced using different synthesis directives. What that means is the tool that they're using to actually program the FPGA, they set the, they change the settings on that tool and they force the implementation to be different. And that's something we call core diversity. This means was previously used in Wolf Creek application as a means of establishing some form of diversity.

Now, during the Wolf Creek application, it was recognized for more complicated functions, such as what we're dealing with with the Diablo Canyon application, additional means of diversity would be required.

CHAIRMAN STETKAR: Rich, to help the other subcommittee members, Wolf Creek was a digital feedwater control system.

MR. STATTEL: No --

CHAIRMAN STETKAR: I mean feedwater and steam isolation.

MR. STATTEL: It was a very simple system. It basically took digital input, and it actuated main feed isolation and main steam isolation.

CHAIRMAN STETKAR: Thank you.

MR. STATTEL: That's all it did. Okay. The second form of diversity I'll talk about is called embedded design diversity. This provides an additional level of diversity that's provided to that that's provided by the core diversity. Embedded design diversity requires the production of two versions of ACL files. So there's two different diverse sets of instructions that are used to program the FPGA cards. This is represented as the relationship between the A cores and the B cores in this figure.

The Diablo Canyon application defines the configuration and arrangements of the PPS system and creates two different sets of FPGA design variants. And you can see there are two sets of code, there are two sets of requirements that are used to generate that code. Is there any question about the embedded diversity?

Okay. The next slide. Just also mention the A and B design variants are housed in separate and different chassis in this system.

I'll mention -- thanks, John. Somehow I missed that in the notes, but another difference between the A and B design variants is they use completely design development teams. They're both the same vendor, but they have different teams using different instructions and different program directives to develop different sets of instructions.

MR. THORP: And just to add to that a little bit, part of our audit process was to kind of examine how well they did that, how independently they, how did they assure independence between those two teams and to look for any potential cross pollenation.

MR. STATTEL: Okay. So, now, this figure, it basically shows the functional architecture for the ALS portion of the PPS. The postulated logic implementation for CCF failure of the ALS would only affect one of the cores within each protection set. So only the As would lose functionality. The Bs would still perform, successfully perform the safety function.

Okay. Each of the core logic blocks shown on the figure includes two diverse cores. This was also shown on the previous slide. You can see the or gate there. You might ask the question, well, isn't that a software implementation, and the answer to that is no. I couldn't think of any other way to represent this or function. The way it's actually performed is on the next slide.

MEMBER BROWN: In the old days, if you wanted to develop a combinational logic digital circuit, that or gate was the symbol you used and/or/nor/neither and all that kind of stuff. And that was when you didn't use software. You were just building the FPGA with discrete components, so an or gate was an or gate.

MR. STATTEL: That's correct. So even though it's performing an or function, there's no software involved with that. And the next slide shows that. This is a de-energized trip function. This is a diagram that's right out of the license amendment request. So you can see here there's 120-volt AC source on the right side, and it's used to energize the relays. The SSPS train A and train B figures there are relays within SSPS system.

So when it's going through the ALS A and ALS B digital output cards, so think of those as contacts, so it's de-energized to trip. So, normally, those contacts are closed during plant operation. So to actuate the signal, basically, you'd need to drop out those two relays, and that's performed either by the A or the B. If either one of those contacts opens, those relays will clearly drop out.

And you can also see the manual trip switch simply opens the circuit, and it's in series with the other contacts. So it's obvious that that, that the manual trip function is retained and that it’s not dependent on any of the software that’s being performed in the PPS system. So no matter what happens with the software that goes into isolations, the output fails open, fails closed, if the operator wants to drop out those relays, he opens that switch, and they’re going to drop out. And then you can also see how the bypass functions are affected there, as well.

Next slide. Okay. I’ll talk a minute about the ATWS system because part of our evaluation is verifying that the new system doesn’t create any dependencies or violate any of the independence that was established with the AMSAC system. This figures shows the functional relationship between the PPS and the AMSAC. As you can see, the steam generator level and turbine impulse pressure signals are shared signals. However, that’s really the only interface between those systems.

The steam generator level and turbine impulse pressure signals used for the AMSAC actuation are derived from the same sensors. However, those sensors are not digital devices, so they would not be subject to common-cause failure.

MEMBER SKILLMAN: Rich, what is turbine impulse?

MR. STATTEL: It's an indication of loading of the turbine.

MEMBER SKILLMAN: Okay, thanks.

MR. STATTEL: Okay. So the staff is confirming through review of the interface requirement specification that the input signals used for the AMSAC actuation are independent and isolated from the PPS system.

Okay. Next slide. Okay. PG&E has shown the existing ATWS system remains diverse from the replacement system. And these are some of the characteristics listed on this slide that we're looking at.

The staff performed the evaluation of these differences or is performing evaluation of these differences. This is the list. I will note both the ALS and the AMSAC system are currently supplied by the same vendor, Westinghouse. However, the ALS was not, when it was developed, it was not developed by Westinghouse Corporation. It was an independent vendor that was later purchased by Westinghouse, so we consider it to be an independent vendor.

Okay. Any questions on this? Okay. A couple of words on manual operator actions. The new system will reduce, as I mentioned before, will reduce operator reliance on manual operator actions as a means of coping with software common-cause failure. The modification does not affect the ability of operators to perform manual operator actions of safety functions. So the existing component and division level actuation capability is being retained, and these capabilities are not changed at all as a result of this PPS upgrade.

The manual initiation signals are provided directly to SSPS system, which is not being modified. Previously credited manual operator actions will still be available to the operators and existing component and division-level actuation from the main control boards will be retained.

Okay. Are there any questions with regard to the diversity of the system? All right. With that, I'm going to turn the presentation over to Samir Darbali, who is also one of our technical reviewers, and he's evaluating the secure development environment.

MR. DARBALI: Thank you, Rich. So I'll be talking about SDOE, or secure development and operational environment, which we already talked a little bit about in the communications section.

The staff is reviewing the secure

development and operational environment to ensure reliable system functionality. Applicable guidance is Reg Guide 1.152, Revision 3, criteria for using computers in safety systems of nuclear power plants, which endorses 7432 2003.

This reg guide is not intended to address the ability of protective features to thwart malicious cyber attacks. Secure development environment is defined as the condition of having appropriate physical, logical, and programmatic controls during the system development phases to ensure that unwanted, unneeded, and undocumented functionality is not introduced into the digital safety system.

Secure operational environment is defined as the condition of having appropriate physical, logical, and administrative controls within a facility to ensure that the reliable of operation of digital systems are not degraded by undesirable behavior of connected systems and events initiated by a access to the system.

Next slide. As part of the Tricon and ALS topical report reviews, the staff evaluated the secure development environments used by Invensys and Westinghouse to develop the respective generic digital platforms. The staff is currently evaluating that these secure development environments are maintained for the development of the Diablo Canyon application.

The vendors control access to the development environments by performing vulnerability assessments, which identify both physical and life cycle vulnerabilities. Control of access to the development environment is accomplished by the use of access security cards and by controlling development areas, including computers, workstations, network service, and portable medium.

The vendors have established procedures for controlling access to signed documents and materials, as well as for software development, configuration management, testing, and non-conformance reporting. PG&E will not be developing or modifying the software at the plant. And once the PPS replacement --

MEMBER BROWN: Excuse me, Samir. Thank you. I've just forgotten something. On the code reviews, to detect and prevent the use of unintended code or code functions, I mean, by that I think friends, inheritance, things of that nature. I'm thinking C or C plus or whatever it is. Is that the vendors doing that, or does NRC, does the staff actually do a code review to determine whether they've used unintended code or code functions?

MR. DARBALI: The staff audits the vendors' procedures for --

MEMBER BROWN: Just the process reviews.

MR. DARBALI: Yes, yes.

MEMBER BROWN: So if their process misses it, then that's the way it goes?

MR. STATTEL: Well, let me talk about that a little bit. Here's how it goes. So we perform threat audits, so we pick -- one of the aspects that we cover during our audits is configuration management. And configuration management, we'll typically go to the vendor and we'll ask them this question: how do you make sure that no unintended functions or unintended software is introduced in this system? And it's very closely related to configuration management because it has a lot to do with who has access and who has the capability of modifying the code and how that's managed and how you make sure two people aren't modifying the same code at the same time, things like that.

And so we haven't completed our audits yet, so let me state that. We have performed audits at the vendor facilities, but that was prior to them having developed the software. So we plan on doing audits at the vendor facilities this summer and continuing on with these.

So the way the conversations go is, when we ask those questions, they walk us through, well, here's how a software engineer is going to modify the code, here's the steps he has to go through. And they'll show us the procedures, and they'll describe the controls that are in place to make sure that the software isn't inappropriately checked out or, if it's checked out, it doesn't get to be checked out by another software engineer.

Then the other thing is the check-in process. So once the code is modified, what approval processes and what protections are in place to make sure that that change in the code doesn't introduce a function that's not called for, it's unintended, or it's not documented. And this ties back in with the traceability process because that's another aspect of the audit that we pay very close attention to.

So, in other words, if there's a function in there that's not described by a requirement, an approved system requirement, and an engineer goes to check that function in, the requirements traceability process, and they perform audits on this, we review those audits reports, as well, would catch that.

That's our expectation.

So we review that process. We have them walk us through the process for developing the code. In addition, we review their problem reporting documentation, as well. So if anyone attempts to check in software inappropriately or that hasn't been, hasn't been tied to an official approved requirement, that should show up in their corrective action program, right? So we look for that, as well.

So that's kind of the process we go through. We're talking, you know, many thousands of pages of code to go through. We expect the vendors V&V process to do those code reviews.

MR. DARBALI: Okay. Thank you, Rich. For secure operational environment, once the PPS replacement project is completed and the PPS system is in the operations and maintenance phases, several modifications to the Tricon and ALS platforms will be controlled by the PPS replacement software configuration management plan. Modification to the PPS replacement components produced by the vendors will be performed by the vendors, not the licensee.

Like we mentioned in the communications portion of the presentation, the PPS replacement system will be located in the cable spreading room, which is a plant vital area. The PPS will be housed in the same cabinet as currently houses the Eagle 21 system. These cabinets are locked, and the keys are administratively controlled by operations personnel.

Also, access to the maintenance workstation --

MEMBER BROWN: Excuse me, Samir. By operations, you mean in the main control room?

MR. DARBALI: In the control room. That's correct, yes. And access to maintenance workstations is password protected. An annunciator will inform the control room if a maintenance workstation is accessed. And during a visit we had last August at Diablo Canyon, we did have operations personnel guide us through the process.

MEMBER SKILLMAN: Let me ask this. Rich raised the point that, if there are issues, one would think that they would show up in the corrective action program. If there is an error that the licensee in software modification and there is a violation, is that a violation of criterion 3 design control? That's an absolute ignorant question. It's just curious to me. I understand how the SSCs are --

MR. STATTEL: We're not able to do, you know, a 100-percent code review, so we're really, we really consider the V&V personnel and the processes the vendor has in place to be as kind of our agents. So we want to test those processes. So when we go to perform these audits, we run these hypothetical situations. We say, okay, now that I've checked -- if possible, we actually run through, let's check this piece of software out, let's modify it, let's add a function block in there that doesn't, that's not called for by a requirement, and let's go try to check it back in. What's going to catch that? And, if possible, they should be able to demonstrate, you know, this is the thing, this is the measure that we have put in place to prevent that from occurring.

And we have them kind of walk us through that process. We interview the personnel that are involved in all of those processes: the engineers, the software librarian, the V&V engineers, because there's always a V&V step in the process of checking that back in. So there's a signature that goes in. So we ask, well, what does that signature mean? What's behind that signature? And what we're looking for is some procedural step in some procedure they have that we can read that will tell me, oh, this guy isn't going to sign this unless he knows that there's a requirement associated with every function that's being added to that piece of software.

MR. THORP: Now, you had mentioned if the licensee changed the software, just to be clear, the licensee itself is not going to change the software on-site. They're not going to do that.

MR. STATTEL: Well, they're not completely off the hook either, let me tell you.

MR. THORP: Well, they're responsible, they're responsible. But I think they're going to use the vendor for software changes; is that right?

CHAIRMAN STETKAR: Just if you answer things, make sure we get you on the record who you are.

MR. THORP: Right. So that's Ken. Go ahead and speak in the mike.

MR. SCHRADER: This is Ken Schrader, PG&E. And the answer to that question is -- ask the question again.

MR. THORP: Well, the question was if the licensee had caused a change to the software that created some inadvertent condition that wasn't appropriate, would that be a violation of criterion 3 design control? Certainly, if the licensee did that somehow, I would think, yes, we'd be looking at the 10 CFR 50 Appendix B criterion. The folks in the inspections area, the resident inspectors and whoever else would get involved would be examining whether that criterion would be what they would apply in terms of a violation. But in terms of process itself --

MR. SCHRADER: Well, the last statement I heard was is that PG&E would not be modifying the software, and that is a true statement.

MR. THORP: So your point is well taken. Yes, that would be --

MEMBER SKILLMAN: Let me explain why I asked the question. It's because this is from a world I really don't understand. I understand the old analog and how we handled 10 CFR 50 Appendix B with old equipment, but it seems like this is a new, a new atmosphere that we've moved into where the vendor is actually the adopted leader for the portion of the licensee's control system and the licensee is depending on that vendor. And so there is a, at least as I see it, a different relationship than the old environment in which we operated where the licensee really owned everything.

In this case, the licensee certainly owns it but is fully dependent on this vendor to give the licensee --

MR. THORP: And, nonetheless, we would

still, as an agency, hold the licensee accountable for any issues or impacts on their systems and equipment. And so as we'll find, Rich has been talking about the audits that we do, we also are looking at the licensee and looking at what kind of audits do they do. They've got their vendor quality assurance program that they have to follow, and they're, I would think, perhaps even more intensely interested in what's going on in terms of the vendor's controls for the software design and configuration management even than we are. But if you would like for them to speak to that, I'd be happy to . . .

MR. PATTERSON: And this is Scott Patterson, Pacific Gas and Electric. We do review every piece of software that the vendor produces. I mean, we've gone through all their software design descriptions, and we validate that there's no code that's not supposed to be there. We also do a site acceptance test once we get the code and validate that everything works as expected --

MEMBER BLEY: Could you say the end of that again? I couldn't quite hear you.

MR. PATTERSON: When we get the equipment on site, we do a site acceptance test and validate that the equipment works as desired for our requirement specifications. So that's kind of a back-up to the factory acceptance test that the vendor does. Do you want to talk about the audit that we're going to perform --

MR. STATTEL: Well, it is a different paradigm. I recognize that. When I was on the licensee side myself, when I was a system engineer, believe me, I wasn't comfortable with this either. I didn't like passing this responsibility to the vendor. So like Scott mentioned, we did perform some very comprehensive site acceptance testing before we would declare a system operable. And that's our expectation, as well.

Now, going back to the original point with regard to the corrective action program and whether entry into that is a Category 3 event, not necessarily. You might think that we review the corrective action and we never find any violations in terms of unintentional code. But, in actuality, we find many instances, but it's usually not intentional. It's usually, inadvertently, there's some piece of code that wasn't properly documented. So it might just be an administrative thing to correct that and update the requirements in order to make sure that the code is appropriately documented and it belongs there.

It's not actually unintended.

And that's really part of a process working, and that's what we're really looking for when we perform these audits. We want the process to be adaptive, and we want it to be, you know, to provide high assurance and they're achieving the correct software. And if there is something that goes wrong or some code that gets inadvertently introduced, they have a way of recognizing that and correcting that. And that's why we review the corrective action documentation.

MEMBER SKILLMAN: Thank you. Thanks.

MS. ALVARADO: Just for further clarification, also we review the plans and process that both the vendor and the licensee have in place to catch this kind of, you know, software that is not working right or doesn't meet our requirements. So we do evaluate in this part of our safety evaluation.

And the last thing I wanted to add was that the vendors usually have different layers of corrective action programs. So it just depends of what phase you are. But before they release it to the licensee, they have different ways to document this before reaching their corrective action program. And we do look at those records to see how, you know, they found it and how they address it. And usually it requires not just the design engineers to fix it, but it requires, you know, like a group of people or a team to approve those changes. So it's not as simple as just like I'm going to fix this.

MR. STATTEL: Final topic for today is going to be deterministic performance of the PPS. And we'll be talking about the attributes of both of the subsystems. So both the Tricon and the ALS platforms are designed to process every piece of plant input data and every plant protection and safeguards function, including process of all system outputs during each program cycle.

Each of the platform evaluations determined that there are application-specific parameters which could influence the systems ability to perform in a deterministic manner. The staff is, therefore, evaluating the deterministic behavior characteristics for each subsystem within the context of the Diablo Canyon application, and I'll go into a little bit more detail on what that entails.

Okay. Our guidance, the standard review plan guidance advises that an evaluation should confirm the system's realtime performance as deterministic and known. What does that mean exactly?

So BTP 21 discusses design practices to be avoided for computer-based systems. And those practices include non-deterministic data communications, non-deterministic computations, use of interrupt multi-tasking, dynamic scheduling, and event-driven design.

So we're reviewing these design processes and looking to see that these are not incorporated. So it's kind of like a reverse criteria that we're applying here.

However, during the platform evaluation, that's exactly what we did. So we followed this guidance. So each of the platform evaluations concluded that there are application-specific parameters that I mentioned. The staff, therefore is reevaluating deterministic behavior characteristics for each subsystem for Diablo Canyon.

Let's go to the next slide. So first I'll talk about the ALS subsystem. It's an FPGA design. It does not embed microprocessor cores, which is something that's used in some other FPGA designs. And it does not use interrupts.

The staff is in the process of confirming the Diablo Canyon application operates on fixed, it does operate on fixed cycles, which are deterministic sequence of acquire inputs, perform logic operations, and generate outputs. That has to be followed without the use of microprocessor core or interrupts, and we're confirming that now. This is consistent with the ALS platform's approved topical report.

The staff is evaluating deterministic performance of ALS. There are parameters which are application specific and require separate evaluation. In this case, only the ALS 102 core logic boards are subject to application-specific response time. So as you can imagine, the more functions and the more complicated the logic is, the longer that process is going to take. So that's why there's an application component of this.

So part of our evaluation is we look at the safety analysis. We understand what the expected performance characteristics are for maintaining plant safety. We look at the specifications for the system that PG&E has developed and provided to the vendors, and we look at the actual application in terms of the logic that's performed and the time that it takes to perform that logic.

With Diablo Canyon, we know exactly the number of inputs, we know what the processes are, and we know the exact number of outputs. So with that in mind, we can calculate, the applicant calculates what the expected response time is. And what we've seen so far is that it's much shorter than what the required response times are provided by the licensee.

Okay. The Tricon system is a little bit different. Its performance characteristics are dependent on the specific application design. As part of the application development process, a timing analysis calculation is performed after the application program is written. So we don't get to see this until pretty late in the design process. However, that calculation takes into account the complexity and the extent of the application that's being developed. So the more functions that are being performed, the longer this calculation that time will end up being.

Actually, go to the next slide. This kind of represents our approach to this. So the variables, the things that affect the time response are the number of input and output parameters, the number and types of function blocks utilized, and the architecture of the design system.

The result of this calculation is used as a baseline, which is kind of shown as the pink bar on this graph here. That's the results of the calculation. And it's used as a baseline for establishing the program cycle time for the application, and that's the next bar up, which is the blue time. So they will basically add on a degree of margin to the calculated time, and they will set the processor to re-execute in the program scan time. So that gives us a level of assurance that at least the calculated, at least all functions will be performed in that scan time.

The program's scan time is always longer than the calculated execution time for the application. The scan time is also shorter than the required response time allocated to the Tricon system.

Another thing I'll mention is we talked about the temperature processing signals. And you might notice that the temperature signals are processed by the ALS system, and then they're fed as analog signals over to the Tricon system. So in that case, we consider the response time for those functions that are supported by that, we consider the response time of both systems in series, right? So there's an allocation for the Tricon and allocation for the ALS that are relied upon for performance of those functions, right? So we're evaluating that, as well.

Okay. And, finally, the purple bar on the top of this diagram represents the response time established by the plant accident analysis. And we're looking at that, as well.

And that's pretty much all I had planned on talking about with regard to deterministic performance. Do you have any questions on this topic?

MEMBER BROWN: Anybody?

CHAIRMAN STETKAR: The only question I had, before you get asked for comments, Rich, do you have -- the SE is still in progress. Do you have any estimate of when you might be finished?

MR. STATTEL: Well, when it was originally submitted, we were supposed to be completed in, I believe, October of 2013. That was our two-year metric. So we didn't meet that, but it was not a result of any, of the licensing reviews. The licensee has been very responsive to our questions. What, in fact, happened is the licensee made some schedule changes. They had some delays from the vendors in terms of vendors going through the design process. So those delays were factored in, and the licensee made a decision to push the implementation back by one refueling cycle. They informed us of that last year, and we adjusted our schedule.

Currently, we plan on completing our audits. The factory tests are scheduled for this spring, very soon actually. We plan on performing the final audits in, I think, like, June - July time frame. And once we receive the final test result reports, the final summary reports, we hope to complete our draft SE and have that to the licensing folks by, I believe, September of this year.

CHAIRMAN STETKAR: The only reason I ask is this is really the first fairly-detailed overview of reactor protection safeguards actuation replacement the Committee has been exposed to. We had kind of a briefing on the Oconee upgrade, but it was fairly high level and fairly short. And I think there might be an interest in following up, you know, as you get closer to finishing the SE, whether it's at the draft form or more finality among the Committee, have another briefing, especially to see how you've closed out some of these things.

MR. STATTEL: Sure.

CHAIRMAN STETKAR: Because it is kind of an innovative design. It's a little different than what the Committee has seen in the context of some of the new reactors that have used different ways of assuring diversity and things like that, and this may be, you know, a coming wave among several licensees. So I think there's some level of interest in it.

MR. THORP: Well, I can tell you that I do sense, in my interactions with the industry at various meetings, at ANS meetings, etcetera, that they're very carefully watching to observe how this, by the way, this pilot process is occurring. It's a pilot with respect to the Interim Staff Guidance number 6, which is the guidance that lays out sort of the expectations for what kind of information that should be submitted and in what phases it should be submitted so that the licensing process can go more smoothly. So we're learning things as we move through that process, and I think what other folks who are looking at possible protection system replacements and similar digital upgrades are trying to determine for themselves is whether this is going to be worthwhile for them to do in terms of the efficiency of the time it takes them to get it done, the predictability of when they can see a safety evaluation. So there are some folks on the sideline who are watching to see how this all comes out.

CHAIRMAN STETKAR: Thank you.

MEMBER BROWN: Okay. Is there any one on the phone line that would like to make some comments?

Is the phone line open?

CHAIRMAN STETKAR: The answer to that is no.

MEMBER BROWN: Is there anybody --

MR. LEWIS: Is the phone line open?

MEMBER BROWN: It is.

MR. LEWIS: Can you hear me?

CHAIRMAN STETKAR: Yes, thank you.

MR. LEWIS: My name is Marvin Lewis. I have been trying to get through every time you've opened the phone line supposedly. May I ask a question, please?

CHAIRMAN STETKAR: Go ahead.

MR. LEWIS: Okay. Actually, I did just ask a question, but that's all right. Answer it in the positive. Here's my problem. You seem to be doing various types of paperwork exercise. Let me explain --

CHAIRMAN STETKAR: Mr. Lewis, could you kind of keep a uniform distance from the microphone or something? You're kind of fading in and out.

MR. LEWIS: Is this a little better?

CHAIRMAN STETKAR: That is much better, much better.

MR. LEWIS: All right. I had my speaker

on. I'm sorry. Look, I know what's going on in labs, in scrap yards, nuclear power plants. It's one thing that the paperwork says, it's another thing that's put on the computer, and things go on like that. Let's say, let's say people are human, okay?

For instance, let me give you a couple of little for instances. One, a repair tag blocks the view of a warning light and Three Mile Island Number 2 goes down and is still down and will still be down. There's a place out in New Mexico, I think it's called Carlsbad. There's a waste site there, transuranic waste. Oh, the paperwork was beautiful. I looked at all the paperwork. I was sure that site would never give anybody problems. Two days ago, that site leaked radioactive big, and somebody put out an order, I don't know who, and every reporting field meter in the United States went down for maintenance. So I don't know much about that episode, but I do know it contradicts the paperwork.

That's my question. Is this paperwork that's going to get contradicted, like a Fukushima, like at Three Mile Island, like at Chalk River, like at a thousand other places, or is this going to be for real on the site, on the ground? I hope I'm making myself clear.

CHAIRMAN STETKAR: I think you have. Thank you very much for your comments. I'm sure the staff, I see them taking notes, so thank you very much for your comments, sir.

MR. LEWIS: Oh, look, if they're taking notes, let me give my email address.

CHAIRMAN STETKAR: Well, you're on the record, actually, and all of this is public information so . . .

MR. LEWIS: All right.

CHAIRMAN STETKAR: We're good. Thank you.

MR. LEWIS: Thank you. Bye.

MEMBER BROWN: Is there anyone else on the phone line that would like to make a comment? Hearing none, Christina, would you close the phone lines? I went to the audience, and nobody stood up. Is there anybody out in the audience would like to stand up and make a comment? Hearing no one, we will then proceed, and now we'll -- number one, I would like to thank the staff before I hang out here for a very thorough, comprehensive, again, discussion. There was a lot of meat you presented during this briefing. And based on response of the members, I think a lot of head shaking, up and down, by the way, not side to side. So I wanted to thank you all for a good presentation, and I will now turn this back over to the Chairman.

CHAIRMAN STETKAR: Thank you very much. And, again, I'd like to echo Charlie. Thanks a lot. You covered an awful lot of material. I didn't think you had a prayer, and you did it pretty well. So thank you.

With that, we will recess until 1:45. We have another presentation scheduled at that time. I will remind the PRA Subcommittee members that we have a noontime meeting in the conference room. Anyone who wants to attend, please do.

(Whereupon, the foregoing matter went off the record at 12:47 p.m. and went back on the record at 1:46 p.m.)

CHAIRMAN STETKAR: We're back in session, and this afternoon the first item on the agenda is we're going to hear from the Staff on pellet cladding interaction, and Dr. Armijo has one of his final --

MEMBER ARMIJO: My parting shot on this one.

CHAIRMAN STETKAR: He will lead us through that. So, Sam, it's all your's.

MEMBER ARMIJO: Thank you, Mr. Chairman. I'll just off with a little bit of history, and I'll refer to something -- I got into the PCI problem in the early ‘70s. Okay? Actually, what was really driving it was something that the NRC put out, and that was related to TCI-related cladding failures during off-normal events. And this is the report that was used to pretty much strong arm the BWR fuel manufacturers into trying to solve this problem, this PCI, pellet cladding interaction problem.

During normal operation we figured out how to take care of that by very careful power maneuvering, but NRC was concerned that if you had a transient that took you above your normal peak operating power you could fail a lot of fuel because this would be a whole core transient and a lot of fuel would be going up in power very fast. That was one of the big drivers in the GE program to develop barrier fuel, and that’s a program that I led. So, the way we tested, we tested the fuel to be PCI-resistant by taking it up to very high powers, much higher than our normal peak linear heat generation rate. Typically, we would test it 16 kilowatts per foot, sometimes as high as 18 kilowatts per foot before we were satisfied we had something that would work in transients, as well as during normal operation without any restrictions. That turned out to work very well, and that fuel was commercialized, licensed, and has been in BWRs around the world for 30 years.

In PWRs they didn't have such a serious problem because they've got a more favorable environment, higher pressure, higher temperature. They don't change power that quickly, but the materials are still susceptible to this stress corrosion cracking problem, so the PWR guys never had to implement any kind of a PCI remedy, although they talked about it and they fooled around with it in limited number of tests.

You had in 2007, I think, somewhere around 2009, we had several meetings. Paul was in, and we were worried that some of the BWR operators had forgotten why they were using PCI-resistant fuel, were starting to talk about just going back to convention cladding. And that was at the Susquehanna review. So, we put out a White Paper, we met and we wrote some letters. Dana, and I, and Sanjoy wrote some things recommending that the Staff should come up with an analytical tool, a regulatory tool to assess whether this was a real problem, and to do something about it.

It turned out so many -- the world using PCI-resistant cladding wasn't a problem for BWRs. More recently, the PWR question came up in a review of the MHI, the MHI certification, and we asked a lot of questions, but it wasn't really fair to them because it's really a generic issue. So, we asked the Staff, and we've been pressing the Staff to work on this some more. And the fundamental issue is if you have -- how much time do you have to correct the problem if you don't have an automatic system that will terminate a power transient very quickly, how much time do you have for manual action? And the other part of it is, can your fuel actually get to the powers that are necessary for this problem to occur? So, that's really the heart of the matter, you know, time, and power, and the system characteristics because if you'll ever go to very high powers in the times we're talking about, and is the system capable of terminating the event?

The other part of the problem is for years people in the industry have been relying on a cladding, pellet cladding mechanical interaction criterion to protect the fuel from this over-straining, and it works very well, you know. There's 1 percent -- you're allowed to have up to 1 percent cladding strain during a power transient, and that's a mechanical thing. And everybody designs their fuel so that they stay below that during all the transients for their system.

The trouble with that is that the PCI is not PCMI, has some parts of it but it’s a stress corrosion problem, and all of the data say stress corrosion happens well below 1 percent. And that’s in that little White Paper I sent around, and it happens for BWRs, and it happens for PWR fuel.

So, the Staff has been working on how to assess it for PWRs, and they’ve written a White Paper titled, “PWR Susceptibility to PCI Cladding Failure.” And we had a June 17 subcommittee meeting on that, and I think there’s been a lot more work done since that, maybe not. I see a lot more charts. But, anyway, Paul is going to give us an update on where they stand, what they’ve done. And we’re fortunate that we have a very large database on this subject of ramp testing, which is the key tool that you use to assess PCI susceptibility. So, Paul, with that introduction.

CHAIRMAN STETKAR: Before we get started, let me just remind that Sam and Paul, we’re in open session right now, so we’re open, so if you get questions during this period that start to tread on proprietary information either alert us and we’ll close it, or deflect those until we close the meeting for the proprietary part. Make sure that we’re alerted to that.

MEMBER BALLINGER: Part of this presentation has sensitive material label on the bottom.

CHAIRMAN STETKAR: That's correct. We will close the meeting, but I just wanted to make sure everybody was sensitized that if we start treading in the open session into anything that's proprietary to be sensitive to that.

MR. CLIFFORD: Okay, thanks. Dr. Armijo did a great job with the background material, and he's correct. The real purpose here is to kind of address this in a generic fashion because during several NRO reviews and NRR APUs the question kept coming up generically, what have you done with respect to PCI on these PWR reviews? So, we agreed to kind of take a step back and look at this at a generic level.

The agenda is as follows. We'll just talk about the Studsvik Cladding Integrity Program, talk about what we've done to validate the FRAPCON code, and how we've used the FRAPCON code to come up with a draft failure threshold. Then we'll talk about PWR operating characteristics, and identify AOO overpower scenarios that may be susceptible to PCI. Then we'll get into some FRAPCON calculations we did to calculate whether or not we would predict PCI cladding failure.

And then we'll have conclusions.

As I mentioned earlier, I'm not sure everyone was here, but my counterpart in research, Patrick Raynaud, he won't be joining us today. His wife is pregnant and she's due any second so he's at home waiting to drive to the hospital.

MEMBER CORRADINI: More important things.

MR. CLIFFORD: Exactly. But I'm prepared to answer any questions you have on the research portion, and we have Harold Scott from the Office of Research, too.

This is just general background. Obviously, pellet cladding interaction can lead to a variety of stresses and strains on the cladding, and there are three pronounced types of cladding failure mechanisms. That's classical strain-based hydrogen embrittlement, stress corrosion cracking which we're here to talk about today, and delayed hydride cracking. Each one of them would occur at a different time and different loading conditions.

MEMBER CORRADINI: Sam did this orally, but you have a cartoon, so can I ask you a question?

MR. CLIFFORD: Sure thing.

MEMBER CORRADINI: Is this a steady state issue, more of a ramp issue, or depending upon the ramp rate a little bit of both? That's what I didn't understand in the description.

MR. CLIFFORD: It's a ramp issue.

(Off the record comment.)

MR. CLIFFORD: But it's a change in power and the duration of the change in power which increases the stress loading. If you're at normal steady state for a period of time you get stress relaxation, so if you were operating at say 12 kilowatts a foot and you moved your way up to 14 kilowatts a foot, that's extreme condition, but after a period of time you get stress relaxation --

MEMBER CORRADINI: It's not X to Y, whatever X to Y is. It's the rate at which you go from X to Y, or is it the absolute X and Y?

MR. CLIFFORD: It's both.

MEMBER CORRADINI: Okay.

MR. CLIFFORD: It's both, but it's not necessarily a peak, it's the delta. In my view it's always the delta because that's the maximum --

MEMBER CORRADINI: So, it's the ramp rate and the magnitude that you end up at.

MR. CLIFFORD: Correct.

MEMBER CORRADINI: Okay.

MEMBER ARMIJO: It's all three. It's the

peak power, it's the higher the delta power is, and then the ramp rate. Just for perspective, the BWRs used to have to increase from 8 kilowatts per foot LHGR, and if they wanted to go to 13 kilowatts per foot, they had to cross that 8 kilowatts per foot line at a rate of .1 kilowatts per foot per hour. That's a long, long time, huge capacity factor loss. If they went a little bit faster, it would fail by PCI. If they went very fast it would still fail by PCI, so it's a very sensitive rate of change, and relaxation of the cladding is a key thing. That's how barrier works, it relaxes very fast.

(Simultaneous speech.)

MEMBER BANERJEE: Paul, so on that duration, so take a typical turbine trip event, where would that put us?

MR. CLIFFORD: We're getting -- there's specific slides on that.

MEMBER BANERJEE: Okay.

MEMBER CORRADINI: So, back to my original question.

MEMBER BANERJEE: It's SEC. Correct?

MR. CLIFFORD: Yes.

MEMBER BANERJEE: In that case. Okay, that's really what I wanted.

MEMBER CORRADINI: So, all of these that you talk about are chemical effects, not mechanical effects.

MR. CLIFFORD: No, the classical PCMI --

MEMBER CORRADINI: Is mechanical.

MR. CLIFFORD: -- is a mechanical loading strain-based capabilities that's affected by hydrogen embrittlement. PCI stress corrosion cracking is a combination mechanical and chemical interaction. Delayed hydride cracking a little more complex because you have reorientation of hydrides.

MEMBER CORRADINI: In the green boundaries.

MEMBER ARMIJO: No, not necessarily. Radiation hardening hardens the cladding. The fission build up during operation creates iodine or possibly cadmium that are the embrittlement chemicals, and the change in power creates stress, so you need three things, stress, susceptible material, and aggressive environment.

MEMBER BALLINGER: You have to maintain a certain crack tip strain rate. I don't want to get too technical, for a long enough period of time, and the ramp rate, and the condition of the fuel, and how fast you can relax stresses at a crack and all that kind of stuff contributes to this. You have to maintain a certain strain rate at the tip of a crack and then it will just --

MEMBER CORRADINI: Go ahead, Paul.

MR. CLIFFORD: Okay. So, GDC 10 requires that the fuel vendors define SAFDLs, Specified Acceptable Fuel Design when it's -- which encompass all known degradation mechanisms and define performance metrics of failure, where it fails, where it doesn't fail. And then demonstrate that during normal operation and all AOOs that they do not fail cladding.

There's many SAFDLs. The top three are what we would use to delineate failure from non-failure during an AOO.

I put this slide in here because there has been a lot of discussion about what the existing cladding experience SAFDL is versus a PCI, whether it's PCMI, or PCI. And the 1 percent as it's commonly referred to is strictly PCMI, mechanical loading. And the SRP clearly acknowledges that this 1 percent limit will not protect against corrosion-assisted PCI failure.

As you can see in this plot, this withdrawal event, low power, you can have a rapid power excursion. You're at low power so you have plenty of DNB margin so you’re not going to fail by DNB. You’re at relatively low fuel temperatures, you’re not going to fail by melt, but you may fail by just cladding strain. So, it’s an important --

MEMBER CORRADINI: And just walk me through, I’m sorry, but since we’re -- so that means the fission gases don’t get out, so I do some initial -- from a high ramp rate I’d have some sort of immediate swelling and contact, and then associated chemistry.

MR. CLIFFORD: No, in this particular case the chemistry aspect is irrelevant because of the time frame.

MEMBER CORRADINI: So, it’s strictly a strain --

MR. CLIFFORD: It’s strictly mechanical strain.

MEMBER CORRADINI: And the inability to absorb the rapid change.

MR. CLIFFORD: Correct.

MEMBER CORRADINI: Okay.

MR. CLIFFORD: So, the SAFDL is based upon separate effects testing on irradiated cladding segments. It specifically accounts for hydrogen embrittlement since it’s done as a function of hydrogen, a function of burnup. It's generally chosen as a lower bound of the uniform elongation data, and the empirical strain limit would then be compared against a predicted strain using conservative analytical models. So, this cladding strain SAFDL serves a purpose.

MEMBER ARMIJO: Oh, I agree.

MR. CLIFFORD: Okay. Now, how do we insure that we prevent AOO, prevent failures during AOO? Well, the power plants rely on many aspects including fuel design features, operating procedures, initial margin as preserved by their tech spec LCOs, automatic system actuations, manual responses to insure that they do not have fuel failure. The Chapter 15-type safety analysis is based on very conservative models, limiting initial conditions to the most unfavorable allowable, system responses, along with high confidence limits. So, if you're at 100 percent power and you increase power due to excess steaming or whatever is driving power up, in general, you're going to approach your DNB SAFDL first. And then second amount you would approach your fuel swelling, and then finally you'd approach fuel temperature, so that's kind of the order of things.

So, the question is in blue here, if you need to specifically model PCI failure would that require a change to the tech specs, or the operating limits, or the fuel design relative to the existing criteria for which they specifically evaluate?

MEMBER BANERJEE: So, they would sort of replace an OLM CTR or something, or what? What's the top there?

MR. CLIFFORD: That's BWR talk.

(Simultaneous speech.)

MEMBER ARMIJO: It would be another way of -- you'd have to find another way of handling it.

CHAIRMAN STETKAR: Paul, I'm sorry. You were careful to say if you were at 100 percent power. Suppose you were at 30 percent power, does PCI become -- in terms of your hierarchical color boxes there, does PCI ever overtake, for example, DNBR?

MR. CLIFFORD: At lower powers there's a significant amount of initial DNB margin, so it's never really the limiting factor.

MEMBER CORRADINI: So, what you're saying is the green box gets so big that the other boxes get within it.

MR. CLIFFORD: Right.

MEMBER CORRADINI: Simply because of where I'm sitting in pressure, and temperature, and flow.

MR. CLIFFORD: Correct.

MEMBER CORRADINI: Okay.

MEMBER ARMIJO: But no matter whether it's PCI or DNB, low power is a good thing. If you're at low power and go up a little bit, let's say 10 percent over your 30, big deal, from a PCI standpoint it's not a problem. It's when you --

CHAIRMAN STETKAR: I just think about the ramp -- you know, if you had a 50 percent power increase from 30 percent power.

MEMBER ARMIJO: That's going to hurt you.

CHAIRMAN STETKAR: Okay.

MEMBER CORRADINI: But, I'm sorry, this one I'm trying to learn, so I'm going to slow you down. So, if I'm at high power this graphic of what comes first, second, third makes sense, but as I shrink power the green box in terms of its allowable space gets bigger, so I could have other effects that will essentially become limiting, one being this -- the example you had of mechanical strain.

MR. CLIFFORD: Right. I mean, it's not that simple in the sense that as you go down in power your tech specs change, so your allowable operating ranges get wider.

MEMBER CORRADINI: Right.

MR. CLIFFORD: You can put rods in deeper, you're allowed to have more severe peaking factors and actually power shapes, so where they are in that, the box is bigger so where they maneuver the plant to can actually then bring DNBR back into the picture.

MEMBER BANERJEE: Can you explain what those colors mean again?

MR. CLIFFORD: It's more of a cartoon. I wouldn't take too much out of the colors. It just shows that as power is increasing you're approaching three different existing SAFDLs. Each one of them could be more limiting depending on what your initial conditions are. And it's really the question that's the real take-away, if you needed to consider PCI explicitly. Would that change tech specs, would it change set points, would it change fuel design? It would require something change.

MEMBER RICCARDELLO: So, each of those colors is a different SAFDL?

MR. CLIFFORD: That was the idea.

(Laughter.)

MEMBER ARMIJO: I think it's important, it's a very good drawing. And each of those axises represents a SAFDL.

MR. CLIFFORD: That's correct.

MEMBER ARMIJO: So, in the case of -- let's take the fuel swelling strain SAFDL, the horizontal one there. If you -- if the only two you had to handle PCI was a strain criteria, and PCI failures occur at lower strains than 1, you'd have to reduce that and have a new SAFDL for PCI.

MR. CLIFFORD: Right.

MEMBER ARMIJO: Assuming you got into that power range, but you have other tools. So, the question is how do you define the region where you're vulnerable, if any, and what's the right criterion to do it. That's a good drawing.

MR. CLIFFORD: That's really where we're going with this presentation. Is there an area where we're vulnerable considering that you've already had these systems that are tuned to protect against these other failure mechanisms. Is there a vulnerable part of operating space?

MEMBER BALLINGER: There's a second time variable, though. There's not only a time variable where they fix the strain rate, but there's a time variable that affects the conditioning of the fuel. So, if you operate the fuel at I don't know, 7 or 8 kilowatts per foot for a long period of time it gets conditioned, and then if you have a transient your cladding in relation to the fuel is set in a certain way and you get can this transient. So, the fuel can condition, if you will, at the beginning of the transient also makes a difference.

MR. CLIFFORD: Right.

MEMBER BALLINGER: Especially with BWRs. You know, this is a little bit -- you can't change power that fast during normal operation. Right?

MR. CLIFFORD: Yes, I think what you'll see —-

(Simultaneous speech.)

MR. CLIFFORD: The conclusion is for PWRs operating most all rods out have full power, you're not seeing that sort of issue. But let's move on with slides.

MEMBER CORRADINI: Yes, keep on going, don't look back.

MR. CLIFFORD: Okay, I've got two slides. Okay, so the NRC has been participating in the Studsvik Cladding Integrity Program which is a large multinational research program to evaluate various cladding failure mechanisms, and PCI stress corrosion cracking is one of the focal points of this large research effort. And I have a summary here.

The SCIP program has performed in depth

investigations to better understand stress corrosion cracking including hundreds, close to 1,100 power ramp tests on irradiated fuel. They've done separate effects testing and extensive characterization.

The PWR database exhibits a large scatter with respect to many variables, and as such there's no clear failure threshold. Generating a PCI criteria is very complex and at least two large international programs have failed to produce a unified criterion. And we expect that the level of effort and funding required to complete the work would be significant.

We continue to participate in the SCIP program and there are explicit research plans to further investigate PCI on the hopes of coming to some consensus on how -- what's the best way to model it, how do you develop a failure threshold?

The next slides are going to be going to be sensitive.

MEMBER ARMIJO: Okay. Let me ask you, just ask you a quick question. As I look through the database which is really very user-friendly to analyze that data, I recognized a lot of the BWR data seemed to be the data that you did, and was published. So, you know -- but I understand why people want to keep it proprietary because they pay money to be in the

SCIP program and they don't want other guys to be using the data.

MR. CLIFFORD: Well, the database that you looked at was made available to only the SCIP participants.

MEMBER ARMIJO: Right.

MR. CLIFFORD: That's why it's not --

MEMBER ARMIJO: There's a lot of data in the DOE public domain, the BWR data.

MR. CLIFFORD: Correct.

MEMBER BANERJEE: So, the BWR talking about this barrier fuel are subject to the same sort of behavior?

MEMBER ARMIJO: More subject, more sensitive.

MR. CLIFFORD: And we'll get to that.

MEMBER BANERJEE: So, you're going to tell us about that.

CHAIRMAN STETKAR: What we need to do now administratively, if it's okay, is we need to close the transcript, and we need to make sure that the bridge line is closed, and we need to make sure that there is nobody in the room who should not be here. I should not be here, not who doesn't want to be here.

(Laughter.)

CHAIRMAN STETKAR: When I say close the transcript it's proprietary. We're not off the record, we're just -- they mark the transcript that we're in closed session.

MEMBER ARMIJO: I think we're okay.

CHAIRMAN STETKAR: As long as we've got confirmation that the bridge line is closed. It is?

(Closed session begins at 2:10 p.m.)

CHAIRMAN STETKAR: I think we are back reoriented, so again we're in open session. And continue, Paul.

MR. CLIFFORD: Okay. The next --

(Phone dialing.)

CHAIRMAN STETKAR: That's just me.

MEMBER ARMIJO: We'll plunge ahead.

MR. CLIFFORD: Okay. So, this portion of the presentation we will talk about the Staff's efforts to develop a draft stress corrosion cracking cladding failure threshold based upon the data we had available.

With using the code FRAPCON, which is a well validated and well calibrated code and NUREG/CR-7022 Volume 2 documents the validation on this code which consists for ramp tests of a relatively large database where the code is tuned, the fuel swelling models are tuned to provide a best fit to the measured strains from the ramp testing.

We can run through these slides here. It's just predicted minus measured and it just shows you the best fit of the fuel swelling data. It was a function of burnup. Here's a function of ramp turn on level. And we went through these in more detail during the Subcommittee meeting. So, on to the efforts to develop a stress threshold.

There's a lot of scatter, as we have seen, on failure strain and time to failure as a function of power increases which make it difficult to develop a purely strain-based criterion. And more importantly, since this isn't really a macroscopic strain driven mechanical failure as shown by a lot of the tests that failed below .1 percent strain, it was difficult to develop a strain-based criteria, so in place we developed a stress-based criteria. And this is consistent with some of the approaches that have been started in the SCIP program. And that's where these cases that were run by the Office of Research as part of one of these investigations in the SCIP program.

They ran 16 Studsvik ramp tests including six failures. The predicted cladding hoop stress on the failed rods ranged from 229 to 297 megapascals with an average of 265.

MEMBER ARMIJO: Paul, you know, here's where I have a hangup. You could calculate stress all sorts of ways but you can measure strain after the -- see, so when they calculated these kinds of stresses did they also say okay, for that stress, you know, we have a stress strain curve, what was the failure strain? And I -- and the problem it's going to be, it's very localized. Everything is so localized, as you said, that it may be that you just -- you don't know what the stress is unless you have a really detailed stress concentration at the tip of a crack in the pellet pressing on the cladding. And that's well known to be where the problem starts, or it nucleates. You know, we've got great pictures showing exactly what's going on, so a global strain or a global stress is doomed to failure because it's all localized.

MR. CLIFFORD: I agree it's localized but, see, that's the problem, there are so many unknowns we're trying to predict whether there was a chip or a fine that was pressed up against the pellet wall, a gap between the pellet and the cladding. Whether that stress riser caused the nucleation. There's too many unknowns.

MEMBER ARMIJO: Well, don't -- just use a regular pellet with a crack in it, you know, as radial cracks and that geometry, at least, as other people have analyzed it.

MR. CLIFFORD: Right.

MEMBER ARMIJO: And I think FRAPCON could do it, too, but I don't know if you're -- that's what I'm pushing to --

MEMBER CORRADINI: I don't understand your comment, Sam. I apologize. Are you saying that you would rather have them measure strain, or have the threshold limit on strain?

MEMBER ARMIJO: I don't think --

MEMBER CORRADINI: I'm not understanding.

MEMBER ARMIJO: I don't think there's a strain limit that will work.

MEMBER CORRADINI: Oh.

MEMBER ARMIJO: I think it will be so low that it's impractical so you have to find some other criteria that says it's power and time, or delta power and time. And if you stay out of that regime you're going to be okay.

MEMBER BALLINGER: Yes, but that's what EPRI did 20 years ago, that power shock. What did they call it? What did they call -- you must know what the data talks about.

MEMBER ARMIJO: That was notably unsuccessful, but the concept is right. The principle is right, you know.

MEMBER CORRADINI: Well, they stopped --

MEMBER ARMIJO: There's a map of power and time and --

MEMBER RICCARDELLA: Sam, are you saying that a nonlinear stress analysis is not sufficiently accurate --

MEMBER ARMIJO: No, I think you can do it but you're going to wind up with some numbers that reflect -- you know, the measured strain on the cladding typically in these PCI failures is way below 1 percent, sometimes .1 percent, sometimes not even measurable. And it's real, it's not an error. It's real.

MEMBER RICCARDELLA: Running the analysis gives you stress.

MEMBER ARMIJO: Yes, but you do a localized stress analysis at the tip of a crack which you're capable of doing like a -- you get -- Joe Rashid does this. He did it on his code, and FALCON code. So, it can be done, and that gives you what the real stress is where the crack is going to nucleate. So, these generalized stresses, they're interesting but they won't save your bacon.

MR. CLIFFORD: No, I don't disagree. I think there needs to be more work that goes into this to develop more complex analytical tools with which to evaluate. But this was just our first attempt.

MEMBER ARMIJO: No. I appreciate you've got to start somewhere.

MR. CLIFFORD: Right, we've got to start somewhere. We used the tools we have.

MEMBER SCHULTZ: Paul, do you have a picture where you've shown the data associated? You talk about making predictions, but are you predicting successes as well as the failures?

MR. CLIFFORD: Yes, it's in the backup slides.

MEMBER SCHULTZ: Oh, okay.

MR. CLIFFORD: It's back here. I'm going to get to it.

MEMBER SCHULTZ: We don't have the backup slides. You have them.

MR. CLIFFORD: This is it right now. So, these 16 cases here you have predicted versus measured. The ones that are kind of shown, difficult to see but just look for the ones that have failure time.

MEMBER SCHULTZ: We can see them from here.

MR. CLIFFORD: Okay. You must be less color blind than I am.

(Laughter.)

MEMBER ARMIJO: Measured failure time and --

MR. CLIFFORD: FRAPCON doesn't have a failure model, so we're just predicting stress.

MEMBER ARMIJO: Right.

MR. CLIFFORD: And we're just getting stress distributions for the ones that failed and the ones that didn't fail.

MEMBER RICCARDELLA: Are they predicting local stress or just global hoop stress?

MR. CLIFFORD: Global hoop stress at a particular node.

MEMBER RICCARDELLA: Yes, I understand, but it doesn't see the concentrating effect.

MR. CLIFFORD: No, it does not. That's correct.

MEMBER BANERJEE: So, this is the RZ code. Right? It's not --

MEMBER BALLINGER: FRAPCON is not three dimensional. It's two dimensional.

MEMBER ARMIJO: Well, two dimensional will do a good job.

MEMBER BANERJEE: Well, that was Graham Wallis' question, actually.

MEMBER SCHULTZ: I'm trying to grab this. It looks like the code is predicting very high stresses for rods that did not fail.

MR. CLIFFORD: Well, it's almost representative of the database we saw earlier. I mean, there's blue and red up and down.

MEMBER SCHULTZ: Yes. I just wanted to know whether we've got something that's working. We're really don't, we're modeling. That's fine.

MEMBER RICCARDELLA: Has this also got creep effects in it, relaxation, or is it linear, these stress calcs?

MR. CLIFFORD: Harold, would this have creep?

MEMBER ARMIJO: Not for such short times. What's max -- we're talking minutes.

MR. CLIFFORD: Minutes.

MEMBER ARMIJO: Yes.

MEMBER RICCARDELLA: So you're saying the creep effects aren't important.

MEMBER ARMIJO: I mean, they could be but --

MEMBER SCHULTZ: They're not modeled. I mean, the model is not going to predict anything over a short time.

MEMBER ARMIJO: Yes, it's not a time dependent stress.

MEMBER BANERJEE: So, this is a -- if we remember it's a finite difference code. Right?

MR. CLIFFORD: Harold, that's true. Right?

MEMBER BANERJEE: And what is the state-of-the-art right now? Are there other quotes finite element right now? For example, the French.

MEMBER ARMIJO: The EPRI code, FALCON.

MEMBER BALLINGER: I think the MOOSE BISON thing is finite element. Right?

MEMBER REMPE: It is, but it's -- they're doing comparison calculations with FRAPCON for verification, so it's not validated is the bottom line. Okay?

MEMBER BANERJEE: So, the finite element codes are 3D, or --

MEMBER ARMIJO: 2D.

MEMBER BANERJEE: They're still 2D?

MEMBER CORRADINI: Well, they're all 3D in theory, but 3D calculations are quite expensive to do, so most of the simulations are 2D, the ones that I've seen presented.

MEMBER BANERJEE: Is this potential 3D then? It's just that you don't run it 3D.

MEMBER ARMIJO: No, this is a 1-1/2D I think. At least that's what Raynaud -- Patrick did, but I don't know what a 1-1/2D thing is anyway, so 2D, you guys have.

MEMBER BANERJEE: Yes, okay.

(Off the record comment.)

MR. PORTER: This is Ian Porter from Research. FRAPCON is a 1D one-half solution so it's a stacked 1D problem, so it solves only radial heat transfer recalculated at every axial node so the coolant conditions change axially, but the heat transfer is only radial.

MEMBER CORRADINI: But I thought the -- our question was on FALCON.

MR. PORTER: Oh, on FALCON?

MEMBER BALLINGER: FALCON is the EPRI code.

MEMBER CORRADINI: I know. That's what I --

MEMBER BANERJEE: A more general question I was asking, what is --

MEMBER CORRADINI: But in the simulations that have been presented at least in other venues they've only been two dimensional comparisons.

MEMBER BANERJEE: OCTATA?

MEMBER RICCARDELLA: RZ.

MEMBER BANERJEE: RZ.

MEMBER CORRADINI: And the ones that I've seen between FALCON and the animal guys are RZ.

CHAIRMAN STETKAR: Can I interject here? I said earlier we're not really constrained on time but I think --

(Laughter.)

CHAIRMAN STETKAR: I'd like to sleep tonight, and although I know you guys like to talk about codes, but Paul does have -- he's a little more than halfway through.

MEMBER BANERJEE: We have codes but don't delete them.

MEMBER ARMIJO: What are we doing after this? Working on letters?

CHAIRMAN STETKAR: It's all our's, so we're not constrained to a 3:15 time, but it's just --

MEMBER ARMIJO: Give Paul a chance to finish his --

CHAIRMAN STETKAR: No, no, no, that's -- I just wanted to give him a chance to finish.

MR. CLIFFORD: So, using the codes we have in place and comparisons to the Studsvik ramp we came up with a lower bound and a best estimate stress threshold to PCI failure.

Now, the next part of this presentation we will talk about PWR operating characteristics and AOO overpower, and that will then lead into the calculations that we chose to run to show whether or not we are susceptible to PCI failure.

As we touched upon earlier, BWRs have shown to be susceptible to PCI and that's really due to plant maneuvering with high worth control blades. Operating experience has now shown that PWRs are susceptible. The exception was a limited number of failures due to missing pellet surface and that problem has since been identified and resolved with improvements in manufacturing specifications and inspection.

Okay. So, there are 65 PWRs operating. Because there are 65 there is always exceptions to every rule, differences as they came up in the generations, so we'll talk about them in more general terms, just remembering that there are unique situations like Palisades that it's a PWR but it had control blades.

So, reactivity control in a PW -- well,

let me start off by saying there are obviously differences in operating characteristics between Ps and Bs. Sam alluded to this earlier, PWRs operate at higher temperatures and higher pressures, but there are other unique characteristics, specifically reactivity control. BWRs use deep insertions of the control blades to hold down excess reactivity to achieve long cycle lengths. PWRs employ boric acid dissolved in the RCS, so one is kind of a gentle global redistribution of our hold down of reactivity, and the other one is a little more severe with respect to local power densities.

BWRs can operate control blades individually which increases their worth and their impact on local power density; whereas, PWRs which normally operate all rods out move their control rods in assigned banks, and they are significantly restricted based upon their tech spec allowable PDIL, Power Dependent Insertion Limits. And the next page will show an example of a PWR PDIL.

As you can see, at 100 percent power they’re limited to, I thought I remembered this but it’s something like 20 inches or maybe less of insertion of Bank 5, and Bank 5 is, I believe, four locations in the core so it’s overall bank worth is very, very low when you're at full power. And they normally wouldn't even insert them at all.

We talk about reactor kinetics. In addition to negative fuel temperature coefficients, BWRs operate with a negative moderator temperature coefficient due to high concentrations of soluble boron to hold down excess reactivity. They may have a slightly positive MTC at the very beginning of cycle at very low power, but by the time they get to full power on day one they have a negative MTC.

Due to negative temperature feedbacks controls, PWRs are very stable with respect to increasing and decreasing power scenarios. In other words, they always fight to stay where they are. So, any increase in reactor power without a proportional increase in secondary demand will promote increasing reactor coolant temperature, which in turn would result in the additional negative reactivity. And the opposite would be true, also. So, in general terms, reactor power follows secondary heat removal.

Here is a typical tech spec limit on MTC, Moderator Temperature Coefficient. You know, the take-away here is it's negative, and it gets more negative as cycle goes, so at basically hot full power you could have -- the most positive would be a minus .2, and it could go all the way to minus 4 percent delta rho, 10 the minus 4^{th} percent delta rho 3 degrees Fahrenheit.

So, the reactor protection system. For any of the overpower scenarios, which is really what we're talking about here, the PWRs rely on a high neutron flux or a variable high-power trip safety grade reactor trip to provide a timely trip in order to protect the SAFDLs.

Additionally, PWRs have trip functions such as here is the overpower delta T, which is applicable to Westinghouse and MHI, and low DNBR which is CE and AREVA PPR.

MEMBER ARMIJO: Paul, are you saying that all of the AOOs are protected by some sort of automatic system, that there's no known AOOs where you have to rely on an operator to --

MR. CLIFFORD: Any power-based AOOs, that's true. There may be --

MEMBER ARMIJO: Power increase, that's all I'm worried about, power increase.

MR. CLIFFORD: Right. There may be an AOO like inadvertent charging where someone turns on a third charging pump and you start filling the pressurizer. You'll get an alarm but it's up to the operator to then secure that. That's not a power transient. Power transients are all protected against automatic response.

MEMBER ARMIJO: And in the control rod withdrawal error do they have such a thing?

MR. CLIFFORD: Control rod withdrawal?

MEMBER ARMIJO: Yes.

MEMBER SKILLMAN: That would be a rate limit.

MEMBER ARMIJO: A rate limit that trips it?

MEMBER SKILLMAN: Probably trip the reactor on rate.

MR. CLIFFORD: In general, when we analyze Chapter 15 events, Chapter 15 is part of the FSAR. I always refer to it as Chapter 15. We don't allow operator action, so they have to show that the system is in place with their response times, and their instrumentation, and their set points will provide a trip when needed to insure that you don't have fuel failure. We don't allow them to credit operator action for our pure Chapter 15-type analysis. That doesn't mean that during our actual event the operators wouldn't respond. It just means that they have to be failsafe.

MR. JACKSON: Right. For AOOs, the reactor trip saves you under all circumstances with very few exceptions, and that would be like the -- you know, inadvertent SI signal is an AOO, and they calculate 20 minutes before the operator terminates that. That would be one that would be terminated by operator action.

MEMBER ARMIJO: Okay.

MR. JACKSON: Safety valves protect you. The other one --

(Simultaneous speech.)

MEMBER ARMIJO: Is it different for the BWR? It's a different philosophy? You know, for example, loss of feedwater heater is the big one I worry about in a B in that you've got the whole core going up, and there have been instances where manual operator action was required to terminate it because the trip systems either didn't exist or were set too high. And I don't remember how high they went in power but I think Susquehanna had such a thing.

MR. CLIFFORD: I don't remember, but you always have to remember when a transient analyst chooses to show that the system can respond or ride through a transient, sometimes they ignore trips. And they say look, it can go up to a higher power and it can stay there for a period of time, and I don't violate my --

MEMBER ARMIJO: You don't shut --

MR. CLIFFORD: You know, CPR limits. So, they can -- it's the easiest way to get it through NRC review is to say look, I know there are trips that would help me here, but I'm just going to ignore them and show you that I don't fail my fuel.

MR. JACKSON: Right. And, typically, many plants don't credit the positive rate trip so that would be there to determine --

MEMBER ARMIJO: Okay.

MR. CLIFFORD: So, on this slide we just show you the set points, the allowable set points that are in the tech specs for these plants just to give you a feel that they're very similar. There's a high-power trip that occurs somewhere between 105 and 111 percent for the plants.

MEMBER ARMIJO: Paul before you leave that slide, just to get calibrated, they compare 110 percent. Let's pick the Westinghouse number. What is that in kilowatts per meter for the peak rod in an AOO that would generate the kind of a delta? Is it -- what I want to do is say where -- on your Figure 13 where would a transient that would take you to 110 percent put you on this ramp terminal power versus burnup failure plot?

MR. CLIFFORD: These are power as measured by their explore detector channels, so this -- these are continuously calibrated so it would be a 10 percent increase in neutron flux as seen by the explore detectors.

MEMBER ARMIJO: Right, but --

MR. CLIFFORD: That's not related to what local power can be.

MEMBER ARMIJO: But that's --

MR. CLIFFORD: Especially if you have an event that's not symmetric or global.

MEMBER ARMIJO: Well, that's what I'm looking for the rods that represent peak rods in the bundle, what's the nodal power that they achieve? Is it 30 kilowatts per meter, is it 40, is it more than that?

MEMBER SCHULTZ: Not for the delta, no.

MEMBER ARMIJO: No, no, for the actual, not the delta, the peak.

MEMBER SCHULTZ: Oh, for the terminal?

MEMBER ARMIJO: Yes, the terminal because that's where the action is as far as PCI. So, this number -- I'm just trying to say where does that put you on this -- on Figure 13 roughly?

MR. CLIFFORD: Well, I mean, it’s an impossible question to answer only because core loading patterns are such that, you know, as they design the core what’s the peak rod? But on average, the average liner heat generation rate is roughly between 5.6 and 6 in the PWRs.

MEMBER ARMIJO: And they’re very flat.

(Simultaneous speech.)

MR. CLIFFORD: Bring it up to the maximum rod would generally be about 9, 9-1/2 kilowatts a foot at the peak node.

MEMBER ARMIJO: Okay.

MR. CLIFFORD: I mean, they have higher limits, LOCA limits that they use to set their initial conditions and their stored energy for the LOCA analysis that could be as high as 13.1 I’ve seen.

MEMBER ARMIJO: But you see what I’m getting at. If your peak nodal power in whatever transient it is that’s protected by a trip is below threshold on this kind of a plot, you kind of made the case.

MR. CLIFFORD: It really depends on the type of transient. If it’s an asymmetric transient, in other words, if it involves control rods, either a drop of a control rod or withdrawal of a control rod, you're going to get very high local power distribution changes, so the --

(Simultaneous speech.)

MR. CLIFFORD: So, whereas, if you have excess steam demand it's not really local power driven. It's a global power event, so you're going to increase power uniformly across the core.

MEMBER ARMIJO: Small.

MR. CLIFFORD: No, I mean, you can go very high in power but it's still going to be a uniform increase in power because it's driven by cold water coming into the core. It depends on the type of events. When we talk about the AOOs, I talk about whether it's a local phenomenon or a global phenomenon.

MR. JACKSON: The AOOs throughout the cycle they calculate, they stay within all the limits for all the AOOs, so the kilowatt per foot limit, the peaking limits. So, if it's a global event the 110 percent trip will get them. If it's a local event, either that, or one of the other trips will get them. But they have to calculate for all three acceptance criteria that he described before throughout the cycle for all AOOs.

MEMBER ARMIJO: Right.

MR. CLIFFORD: So, if you kind of go back to Chapter 15 philosophy, you're defining your limiting initial conditions to maximize the consequences, in this case maximize say temperature increase or DNBR margin degradation. And often you choose to either try to avoid a reactor trip or to overshoot a reactor trip to get the maximum power you can before you scram the reactor. So, this strategy yields conservative analysis results with respect to margin of DNBR and melt, and your cladding strain, or it would maximize the predicted fuel failure.

It's important to note, as we mentioned earlier, stress corrosion cracking really requires both stress and time, so is there an AOO overpower scenario that exists which exhibits a prolonged power excursion of a significant magnitude to where your fuel rods would be susceptible to stress corrosion cracking? And that's what we'll talk about.

If you look at this slide, there's a survey of all the AOOs. I think this is a Westinghouse or a CE plant, but they're all pretty similar. And you just kind of identify which ones are a global power increase and which ones are a local power increase. And really when we started talking about this issue it was -- the concern was is there an event on a global scale that would result in a lot of fuel failures across the core, so we're really sticking to global changes.

MEMBER ARMIJO: Global ZED because, you know, what -- fuel rods from a local area is not a problem. And, actually, it started out with the issue of power uprate, now we're uprating the core, so that -- now we're going to be able to go to even higher power than we normally used to be able to do. That was at Susquehanna when it started.

MR. CLIFFORD: Right.

MEMBER ARMIJO: So, a global power increase is a threat in time and power, maximum power are the parameters.

MR. CLIFFORD: The PWRs, there's been a lot of power uprates of PWRs but they -- really have they achieved that power uprate by increasing local rod power? Done it by putting a higher feed -- number of feed batches so what happens is they flatten the power. We've seen peaking factors -- when I was doing fuel management, you know, we had peaking factors of one seven, now we're down to peaking factors of one five, so we're really -- things have changed. They really haven't gotten worse from a local perspective.

MEMBER BANERJEE: So the limiting case will be the rod withdrawal, I take it. Right?

MR. CLIFFORD: Right. There's two types of events here that we're going to go into, and that's the first one is the bank withdrawal, and the second is really the whole class of increased secondary heat removal. And all of the first five are from Chapter 15.1, increase in secondary heat removal. So, we'll start with the bank withdrawal.

CHAIRMAN STETKAR: Paul, just go back for a second. I love alphabet soup as much as anybody, and I understand all of it. What's ASGT? That's the only one I couldn't figure out.

MR. CLIFFORD: It's Asymmetric Steam Generator Transient, so you're operating at full power --

CHAIRMAN STETKAR: Oh, go on. Okay.

MR. CLIFFORD: You want to hear about it or not?

CHAIRMAN STETKAR: You can.

MR. CLIFFORD: You're operating at full power and say one of your main steam isolation valves inadvertently closes, so one steam generator output would go to zero, the other one would pick up the load and go from 50 percent to 75 percent, so you have the inlet flow distribution changes and the temperature in the --

CHAIRMAN STETKAR: I understand the concept. I've just never seen that acronym.

MR. CLIFFORD: Okay.

CHAIRMAN STETKAR: Or that kind of connotation. Thanks.

MR. CLIFFORD: Okay. So, we'll start with the bank withdrawal. The limiting CEA withdrawal scenario in the FSAR would be to maximize the power excursion, in other words, the overshoot of your trip set point by selecting the maximum bank worth, least negative MTC, least negative FTC, and minimum delayed neutron fraction.

It is possible to identify a CEA withdrawal event, say one that has a partially inserted bank, or a very low worth bank which could avoid the rapid trip. However, with no increase in secondary steam demand reactor power will eventually trend back down to match secondary removal, so power will go up, temperatures will go up, negative feedbacks will then just beat it back down. So, if the operators aren't doing anything on the secondary side this is an event that could challenge fuel failure, but it's not a prolonged event. It's a short-lived event.

MEMBER BANERJEE: So, what's the typical power pulse you could get in the -- in that scenario typically?

MR. CLIFFORD: Because the tech specs limit insertion at power it's a very benign transient. Here is a power trace at full power, because you're limited to Bank 5 and you only can insert it 22-1/2 inches or something like that. The worth is very low so it's really not even a significant event. But at low power where you're allowed to have say not just Bank 5, but Bank 4 and Bank 3 in, now you have a lot more worth delta rho per inch. So you can get a significant power increase. The previous -- previously I showed a trend of a rapid power excursion that went from zero to 70 percent rated power in two or three seconds. That was a hot zero where you're allowed to have a lot more deep insertion.

MR. JACKSON: Right. So, this is a situation where if a plant wanted to load follow and they wanted to keep their rods in, they would have to change their tech specs to allow bigger rod insertions and then they would have to redo this analysis with acceptable results. So, the way they choose to operate their plants and their tech specs is a --

MEMBER ARMIJO: But that 18 seconds that

puts my mind at ease, so this one I'm saying --

MR. JACKSON: You're done.

MR. CLIFFORD: So, if it's a primary driven power excursion it's going to turn itself around. I mean, that's kind of the take-away, the rule of thumb, and it's based on how much time it takes for the water to circulate around and to heat up a full bank, whatever is driving it. So, this is a benign event for two reasons. One, it turns itself around, which isn't shown here because it hasn't reached that point yet. And really it's just the tech spec's limit the worth of the rod.

So, this event is really susceptible to stress corrosion cracking because of the time duration. And you can argue that since you don't operate with rods in the core you really can't even have this event. The probability of that event is so low because they don't operate with rods in the core. The delta rho is very low, such peaking factors are minimized by tech specs. You've got your negative feedbacks, you've got your available trips, and the operators would take action.

So, the excess demand events are really the ones that -- of all of the AOOs would be more vulnerable. And it's really driven by how much excess steaming or how much excess heat removal is there, and what point of the cycle they're in, what's the MTC? So, if you had like an inadvertent opening of a steam generator atmospheric dump valve, that's roughly 10 percent steaming, full power steaming, so power is going to want to work its way up to 110 percent in the reactor. How quickly it moves up there depends on what the MTC is.

So, there's a wide variety of how this event -- what the scenario would look like, what the accident progression would look like based on the amount of steam releases, the MTC, et cetera. But there is a combination which will give you a prolonged power excursion. The question is, is the magnitude of the excursion such that you would have to worry about stress corrosion cracking? So, the time part can be achieved. The question is can the stress part be achieved?

Here is just a plot of OSGADV and it shows you that it can be at power for a long period of time. Here is a steam bypass.

MEMBER ARMIJO: These are seconds, huh?

MR. CLIFFORD: Yes, 360 seconds.

MEMBER ARMIJO: Three minutes, so that's long enough.

MR. CLIFFORD: So, this is the type of event where you could pick the right conditions where you could go up in power but you could avoid the ex core-driven high-power trip. Now, you're going to trip on something. In this case, you're probably going to trip on low steam generator pressures because once you open your atmospheric dump valve pressure starts dropping, and that's a safety grade trip.

MEMBER ARMIJO: Have these things ever happened an OSGADV?

MR. CLIFFORD: I'm sure they have.

MEMBER ARMIJO: Inadvertent -- what is it?

CHAIRMAN STETKAR: Somebody blew a safety valve off them --

MR. JACKSON: I'm mean they're not common.

CHAIRMAN STETKAR: These are not common, but I know somebody blew open a safety valve.

MEMBER ARMIJO: Would a steam break action do this, too?

CHAIRMAN STETKAR: Steamline breaks are not AOOs.

MEMBER RICCARDELLA: No, that's not an AOO. That's an emergency or fault --

MR. CLIFFORD: That scenario wouldn't -- that would be a very rapid power excursion, a very quick trip. And then you -- and what you're really worried about is the return -- if there's going to be return to criticality and return to power if you keep blowing down your steam generator if you can't isolate it.

MEMBER ARMIJO: Paul, now let's just stick with this thing so I can myself clear. If you were at 100 percent power and this happened, that means some rods, and I don't know PWR assembly, lots of rods will increase power. But the only thing I care about is does it -- from what LHGR in kilowatts per meter does it go, does it get -- your peak rods get up to 40 kilowatts per meter locally?

MR. CLIFFORD: During this event, it's a global increase. The only redistribution of power you really see is the colder water will tend to drive the actual power shift, will drive it down towards the bottom of the core, which is very benign from a DNBR perspective so we don't even allow them to credit that. But there's not a redistribution that you would see in a rod motion --

MEMBER ARMIJO: Let's just assume that the whole core goes up uniformly just -- if your peak rods are at 8 kilowatts a foot and they go up to 8.8, that's pretty benign. And if you look at your data of

PCI failures below a threshold, at least there's no data there. But if it was -- if you were operating at 10 and you went up to 11, you're getting into this borderline, if you were at 12 and went up to 13 or 14 kilowatts per foot, then you're in the problem range. But I don't know if you can get those powers in this event in a PWR.

MR. CLIFFORD: When we do EPU reviews we generally repeat -- and I've presented these results here before. We repeat the fuel mechanical design analysis where they'll identify the limiting rods, three or four of the limiting rod power histories, and we'll run our transient analysis, I mean our FRAPCON analysis to show that the rods meet all their fuel design requirements. And generally those are relatively benign because they're getting pretty flat with these power distributions. They're getting really good. You don't want to have them in a peaky core because you're not properly utilizing your uranium if you're discharging --

MEMBER ARMIJO: What's the number, what's the LHGR that --

MR. CLIFFORD: The only regulatory limit they have is the LOCA linear heat generation limit in their code ware. That's the only limit, regulatory limit they have. Where they actually fuel manage to is a different story.

MEMBER ARMIJO: What are they allowed to go to?

MR. CLIFFORD: That would be at 13.1 kilowatts a foot. I've seen that number.

MEMBER ARMIJO: Yes.

MR. CLIFFORD: Are they ever challenging that? I don't think so. Are they within three or four kilowatts a foot, probably not even, but they're allowed to be there.

MEMBER ARMIJO: That's the key.

MR. CLIFFORD: They're allowed to be there.

MEMBER ARMIJO: Okay.

MEMBER BANERJEE: I think you have to count on them being there.

MR. CLIFFORD: Absolutely.

MEMBER BANERJEE: You can't do anything else. In fact, this issue came up earlier, this was a BWR. That's enough.

MEMBER ARMIJO: Okay. Thanks, Paul.

MR. JACKSON: For our current limits, and the three criteria that he -- we look at all the times and cycle through all -- I mean, you look at it all, so we don't --

MEMBER ARMIJO: Yes.

MR. JACKSON: I mean, here's where he's speculating or he's working this if we apply new criteria to --

MR. CLIFFORD: Right. So, there are events that could you give you the time element you need for stress corrosion cracking. Here's another type event, this is a steam bypass control system malfunction. This would give you significant over-steaming, so you're going to get a rapid trip, so this particular scenario would show that's not an issue. So, if an event has a very high power and hence, a very high stress, it's going to be of short duration. So you really have to find the scenario that has a combination of time, which means it has to be a relatively low power, otherwise it would have gotten a trip.

So, here's just a summary here. Due to the high-power trip and the low steam generator pressure trip that's going to limit the magnitude and duration of the power excursion, and there's additional trips that also can be credited. And there's obviously going to be control room alarms that would alert the operators to take action. And then there's a whole class of non-safety alarms and trips that we don't credit but are there --

(Simultaneous speech.)

MR. CLIFFORD: So this event is something that needs to be looked at for stress corrosion cracking because, as I mentioned, you can have the time duration. The magnitude of the power, hence the magnitude of stress is going to be limited by the existing reactor protection functions.

MEMBER ARMIJO: Paul, is this the worst one that you found? Is this the transient that does --

MR. CLIFFORD: There's an infinite possibility of excess type events that could -- if your trip was 118 you could find an event that would get you to 118. If your trip was 104, you could find an event that would get you to 104. You know, there is really an infinite possibility, but they're -- from the traditional Chapter 15 they're never limiting. You want something that overshoots because that's one that's going to challenge your fuel design limits.

MEMBER ARMIJO: Yes.

MR. CLIFFORD: So, we ran some FRAPCON calculations, two different types of calculations. The first one we're answering the question do the existing reactor protection system trip functions provide adequate protection against stress corrosion cracking?

And the second set was how much margin exists between where we would expect them to be and when they would be expected to have stress corrosion cracking.

So, the inputs, as I mentioned, a rapid power excursion which overshoots the trip set point won't have significant time duration so they were scratched. So, as a result we're really looking at a prolonged power excursion event that stays below the existing trip set points. And as you saw earlier, they're all somewhere between 105 and 110 percent. We chose 112 percent for this exercise, so we chose three different power histories, and on each of those power histories we ramped power by 112 percent at different burnup points, and then we calculated what the change in stress was. And then we compared them against the thresholds that we had previously estimated, the lower bound and the best estimate.

So, at least from our calculations one thing we can take away from this is that at low burnups you have an existing gap. In an ideal world, you have an existing gap, so if you just do 112 percent ramp based on where they are, 112 percent higher than where they were, it's insignificant. Sometimes you won't even close the gap, so it's strongly dependent on power history, fuel design, et cetera. But for these three rod designs or power histories, we calculated the stresses. Let's see, what else can I say about this? The maximum stress stayed well below a threshold, below a threshold of 200 megapascals based upon our FRAPCON analysis of the SCIP data, and the maximum hoop stress here is 164. And this 164 is actually pretty aggressive in the sense that a fuel rod with a local burnup of 67 gigawatt days was still operating at 7.75. This radio falloff curve, as I mentioned, is not a power history. It's actually the worst composite power history that you could have. In other words, it's a line drawn above all the fuel rod power histories, so it's a very bounding case.

So, for that case where you already had a significant stress, pre-ramp you have a significant stress, and then you've increased that stress by 90 megapascals, you're nowhere near the stress threshold. But in this simple exercise we ran, we were just trying to answer the question, if you ramped up in power, stayed below your trip set point, what sort of stresses could you expect in your cladding? And would those stresses be of sufficient magnitude to cause this nucleation crack propagation stress corrosion cracking? And our conclusion is that because of the existing -- our conclusion is that the existing trip functions and set points are adequate to protect against this scenario, so we wouldn't expect there to be stress corrosion cracking because the power excursion is so minimal.

In the next set of calculations we used the same power histories, and instead of going up to 112 percent we iterated on power, so we changed the power increase until we hit either the 200 megapascal or the 250 megapascals thresholds. So, this shows what the maximum ramp could possibly be to get to that point where you may predict stress corrosion cracking. So, as with the previous analysis, at low burnups if there's a preexisting gap, you can have a relatively large power increase. But as burnup increases and the gap closes and initial stress is higher what you're seeing is the allowable power increase decreases.

MEMBER ARMIJO: And you're getting strains that are in the range of the very low strains, much less than 1 percent, if I'm reading this right.

MR. CLIFFORD: Correct.

MEMBER ARMIJO: Well, this one you actually worked backwards. Right?

MR. CLIFFORD: Right.

MEMBER ARMIJO: Okay.

MR. CLIFFORD: So, calculations show that you need a prolonged power excursion greater than 118 percent to achieve the lower bound, and 125 percent to achieve the best estimate threshold. And these calculations suggest that there is some safety margin to stress corrosion cracking based upon how these plants are operated, and what the existing trip functions are.

So, another way of looking at it is you set these trip -- you create these engineered safety features, these trip functions and you set the set points to protect you against other failure mechanisms. And by doing that, you're inadvertently protecting yourself against stress corrosion cracking.

MEMBER ARMIJO: But not the 1 percent SAFDL doesn't do it. Your other --

MR. CLIFFORD: Not for this class, right.

MEMBER ARMIJO: Not for this kind of mechanism, this failure mechanism. But what it says, if your threshold is 200 megapascals for failure and you go above it, you're taking from the SCIP data you estimate that that's -- you would be getting failures, but that calculates strains.

MR. CLIFFORD: Yes, 265 is the average. This is just a very lower bound.

MEMBER ARMIJO: Yes, at some point -- I really don't understand how you got your 265 but I'm going to let that sit and think about it a bit. But based on calculated strains and comparing that to the measured strains to failure from the SCIP data, you're in the failure regime.

MR. CLIFFORD: I mean, as we mentioned, I mean, you can -- it's not really a macroscopic strain-based failure, so it's -- you can have strains of close to 1 percent and not fail. That's what we expect on the data. You can get --

MEMBER ARMIJO: No, that's not correct, Paul.

MR. CLIFFORD: Not by stress corrosion cracking, but by -- so you're right. I mean, we don't have an SEC failure model in FRAPCON, but we're not predicting the actual propagation and failure, through wall propagation and failure. What we're predicting is just stress. We're kind of taking that leap of faith that the stress needed as a function of burnup is X as we calculate it, and we're just trying to show that —-

MEMBER SCHULTZ: But you apply FRAPCON to the test data, and that's where the numbers came from.

MR. CLIFFORD: Correct.

MEMBER ARMIJO: Okay. So, your bottom line is you're not going to get to the powers for a long enough time without tripping.

MR. CLIFFORD: Yes.

MEMBER ARMIJO: And it isn't the strain safe that's protecting you, it's just --

MR. CLIFFORD: Correct.

MEMBER ARMIJO: -- the engineering --

MR. CLIFFORD: It's a combination of the systems you have in place and the characteristics of operating hot full power all rods out. You don't -- you're not moving blades. I mean, what we're seen in the past is you got PCI failures because you were moving blades, high worth blades and exposing fuel which is causing an increase in local power density for a prolonged period of time. There's none of that in the PWR.

MEMBER SCHULTZ: The interesting thing is if you were operating -- if one was operating in a load follow mode you'd have to look at this all over again.

MEMBER ARMIJO: You might. You might have to do that, yes.

MEMBER RICCARDELLA: But the French experience indicates that that's not a problem, for whatever reason that doesn't seem to be a problem.

MR. CLIFFORD: They've evaluated that and they've set preconditioning guidelines, they've set maneuvering guidelines to avoid it.

MEMBER ARMIJO: As long as we stay out of there, as long as we stay out of that business in the U.S.

CHAIRMAN STETKAR: Maybe not.

MEMBER ARMIJO: It may not, we may --

MR. CLIFFORD: I can send you my presentation. It doesn't look good.

(Laughter.)

MEMBER SKILLMAN: Well, there was a time in the '70s where we did load follow with the Ps. I know B&W was 150, 100 in 10 minutes and it would do it. It wouldn't trip. ICS would keep it on line. And we did not have failures, so I know there was a time when the Ps in the United States were actually load following. And as time went on into the '80s and '90s we went to baseload and we did all shim with boron. We were trimming with actual power shaping rods or power length rods but we did load follow in the early days.

MR. CLIFFORD: I guess the conclusion is it's really a combination of the existing engineered safety features and operating restrictions that insure that PWRs are not susceptible to stress corrosion cracking during normal operation, and that's certainly backed by the operating experience we've had in this country.

With respect to the vulnerability during AOOs, the calculations show that there's margin to get to a stress regime or a magnitude of stress where you might become susceptible to stress corrosion cracking. As we mentioned, it's a difficult phenomenon to model and I agree with some of the recommendations in the White Paper that we should improve our analytical methods so that we can be ahead of the curve because change is upon us. And if, in fact, we start seeing plants coming in for load follow license amendment requests we want to have the tools available to evaluate stress corrosion cracking.

We will continue to participate in the SCIP program. And as I mentioned, there are ongoing tests as we speak, and then there's an additional set of tests in the SCIP-3 program which are upcoming, which are specifically designed to help us further understand stress corrosion cracking so that we can work with our international counterparts and kind of come up with a uniformed approach, you know, what's the stress intensity factor? How do I model it? What's the duration? I mean, we need to identify -- we need to increase our knowledge so that we can develop a regulatory framework around this failure phenomenon.

MEMBER ARMIJO: Okay. Well, look, first of all I go around the table and see if there's comments or questions, and then I'll wrap up with some comments. Mike?

MEMBER CORRADINI: Oh, you're going to start with me?

MEMBER ARMIJO: Yes.

MEMBER CORRADINI: I appreciate the time you took to explain it to those that aren't expert in it, but I don't have any comments. I guess my only observation is that I guess your final conclusion was the thing that I'll take away, which is by I won't say happenstance but let's just say by good fortune things apparently are covered. But your recommendation is given the fact where there'll be new activities, better modeling of this and maybe better coordinated analysis of it is necessary.

MR. CLIFFORD: Yes. We should spend the time and complete what research is necessary to validate future codes.

MEMBER REMPE: Well, I was part of the APWR Subcommittee when this was mentioned and I really think it was good to back it out of that and come and do this in a generic fashion and have a better perspective. And I appreciate your willingness to participate and educate us on it.

Listening to what's being done in other countries, I think it is a good place having a research plan to bring up the need for better tools perhaps, and to be anticipating what might happen in the U.S. I think that's a really good forum for us to provide comments, in my opinion.

I know that before this meeting started we talked about some emerging other issues that they're seeing in France with corrosion on the rods, so there's a lot of other benefits I think from the international perspective, so I hope we get to learn more about that, too.

MEMBER ARMIJO: Charlie.

MEMBER BROWN: Pass. I have nothing else.

MEMBER ARMIJO: Dr. Ballinger.

MEMBER BALLINGER: Well, it's a very good presentation. I'd like to get the other presentations, but I think we do need to be -- I'm sort of heretic when it comes to this stuff. I think it's a probabilistic problem. I think we have a problem with fidelity of the models versus the fidelity of the measurements that we can actually use on irradiated rods. And it's very expensive to do these as kind of experiments, so we had to make a pretty good -- somehow strike a balance between spending a ton of money looking at rods that have been ramped and things like that, and what kind of -- how accurate the information we get is compared to what we can actually model. I mean, you could see some of the trends in the data. It's not a black and white failure/no failure.

MEMBER ARMIJO: There's various levels of quality in that --

(Simultaneous speech.)

MEMBER BALLINGER: Increase in probability of failure with certain types of -- and that sort of lends -- that sort of screams to me that we've got some uncontrolled variables. Either that, or variables that we think we know that we don't, so -- but this has been going on since like -- you know, the first time Main Yankee had a massive amount of failures, everybody went up the imaginary axis and wanted to model fuel performance.

MEMBER ARMIJO: Well, I think more analysis of the SCIP data, critical analysis, because some of the data are not so good. In fact, I pointed out in the White Paper a lot of testing was done on rods were just cut out of full length PWR rods commercial stuff.

Well, when you cut a rod out all the fission gases go away, you mechanically change it, and we started to see some differences in earlier failures with refabricated rods. And that's the first time I'd ever seen that effect. I never liked that approach, but there's different qualities of test data that are suitable for validating your calibrating models.

MEMBER BALLINGER: We don't operate PWRs like the transients that they run.

MEMBER ARMIJO: Well, that's clear.

MEMBER BALLINGER: Okay.

MEMBER ARMIJO: Anyway, Mike.

MEMBER RYAN: Nothing else, Sam. Thanks.

MEMBER ARMIJO: Dennis.

MEMBER BLEY: I really appreciated this. I learned a lot from this and, you know, one can't with good conscience say don't follow the data. You know, of course, we want to follow that. The modeling side of it I kind of agree with Ron, I'm not -- it would be nice to have a good model for this, but that's a long-term research effort I think.

On the other hand, if we're worried about anticipated operational occurrences, we've got not really envelope couple of the 3,000 years of operating experience and we aren't getting them. So, if they're working there in some unusual transients they're postulated accidents under the design. And there are postulated accidents that do a hell of a lot worse than this, so I'm not in a panic here.

MEMBER BALLINGER: I think understanding that what appears to be a sudden drop in failure probability at 50,000 megawatts --

MEMBER BLEY: That would be pretty neat to understand.

MEMBER BALLINGER: That's a different story there.

MEMBER BLEY: We might learn something from that that would be very helpful. Yes.

MEMBER ARMIJO: Okay.

CHAIRMAN STETKAR: I don't have anything more.

MEMBER ARMIJO: Harold.

MEMBER RAY: AP1000 advertises a low cooling capability uniquely. Is there anything about that that you want to comment on? Is this just some expectation they have?

MR. CLIFFORD: In the latest version of the DCD they did change out and they put in these gray rods to support load following. Not my understanding that the Staff has approved the load -- because it was never a load -- there was never a envelope, a power time envelope presented to the Staff that says this is the type of load follow we want you to do. Is this okay? They just -- all of the -- if you -- one of the things the IAEA was concerned about is that all of the advanced reactors are just making these blanket statements. We're good for load follow, we're good for load follow. And some of them have physical changes, but most don't.

MEMBER RAY: Well, Vogtle will find out one of these days, I guess. That's all I have.

MEMBER ARMIJO: Dr. Powers.

MEMBER POWERS: I was intrigued by your discussion of changes in the way plants are operated in response to moves toward wind and solar sources that are forced upon the utilities. I didn't hear anything that suggested there was a risk to the public health and safety. It strikes me as that's an issue to stay alert to as you indicate this becomes more pandemic, and we're spending resources to the point that we do have to operate nuclear units in an unfamiliar way.

MR. CLIFFORD: It's no longer load follow, it's supply follow.

MEMBER SCHULTZ: I agree with Dana. I

really appreciate both the presentation and I -- I see that you -- and agree that you've drawn the right conclusions from the evaluation that you have done. I don't think it's just fortunate that this is not a problem for PWRs. There's been a lot of thinking that's gone into PCI as a result of what's happened at BWR, and even the -- what was, in fact, a very small issue associated with missing pellet surface. A lot of thought went into what that meant in terms of overall fuel performance for PWRs. And the problem was resolved, but it's an interesting problem to bring to bear on this because very small deviation associated with pellet surface caused fuel failure.

MR. CLIFFORD: Yes, and I would just like to add something. I mean, this may have been more of an issue with PWRS except they've been very aggressive to try to get ahead of the curve. And, for instance, if you look at the manufacturing of the pellets they chamfer and have dishes in the pellets which reduces the amount of ridging, which reduces the local stress concentrations at the pellet-pellet interface. You don't see that in all BWRs, so the PWRs have design features just in the pellet stamping phase.

MEMBER SCHULTZ: Which goes back to as Dick was saying the experience that was gained in the '70s.

MEMBER ARMIJO: Dick.

MEMBER SKILLMAN: Yes, sir. On page 52, what it takes to actually drive the failure, the newer reactor protection systems are so dependable, they are so precise. The new instrumentation is so good it'll be a long time before we let a P go up into that range without some preemptive action to bring the power back whether it's automatic rod insertion through an integrated control system or a trip.

The second thing has just been mentioned. It's on slides your 13, 14, and 15. I think there ought to be some explanation of why that fuel did not fail above 50 megawatts days per kilogram. I still hold out that there may be fabrication of the pin, fabrication of the pellet, or just that these are the strongest soldiers that statistically were able to survive. But there's something in that group that seems to me to be compelling for more information. Those blue circles, why did that fuel not fail when the fuel that was exposed to lower burnups did?

MR. CLIFFORD: I'll take an action item to talk to Research, and as part of the SCIP program to really try to drive that home and find out what's causing that. I can't imagine, you know, after years, and years, and years of evaluating this they haven't identified that and questioned it. I just don't know the answer.

MEMBER ARMIJO: You'll have a little bit of a debate but there's lots of good explanations.

(Simultaneous speech.)

MEMBER SKILLMAN: Paul, great presentation. Thank you.

MEMBER ARMIJO: Pete.

MEMBER RICCARDELLA: Yes, I, too, think it was a great presentation. I appreciate it, and I agree with your conclusion that in the current operating mode of PWRs that it's not a problem. I think we need to try to better understand the French experience into why they haven't had failures in that load following mode because I believe it's coming. I think that, you know, the nuclear plants are going to have to operate in a more flexible load following mode or they're not going to operate, they're going to shut down.

MEMBER ARMIJO: Sanjoy.

MEMBER BANERJEE: At last. Last but not least, whatever. But it's a great presentation. I was puzzled by a lot of the data because you've got a lot of red dots where there were blue dots, as well. And whether this is just random sort of behavior because small problems can lead to problems, or there was something more deep in that in terms of some history effect or whatever that lead to those red dots, or most of them, where the blue ones were operated in some other way. That would be interesting to understand. Is there some cumulative effect which is there? That's just a question.

Also, I noticed that at the high burnups you had a lot of these blue dots and very few red dots, actually, so I don't know if that was just an optical illusion, or it was for real, you know. And then what that was due to. Maybe you explained it, but I missed it.

MR. CLIFFORD: Maybe we have to look at it some more, but just fundamentally it's tougher to push a high burnup fuel to higher kilowatts a foot.

MEMBER BANERJEE: Right. But you knew the ramp rate there sort of, you see, so I was assuming those are sort of like equivalent ramp rates or whatever.

MR. CLIFFORD: I can't go back to it right now.

MEMBER BANERJEE: No, no, but it's -- you don't have to -- but if you look at it, you'll see that many of the indicators are somewhat similar, at least the indicators you were looking at. Maybe they're a little bit lower, but they're not actually materially lower, so it's sort of interesting to understand that.

And the third thing, I echo what Pete said. You know, it's interesting to try to understand what the French have done and where their data falls on those curves that you showed because we can plot it and see. And they would be blue dots. Right? Because they're not getting failures. So that would be very interesting to know where they come in that failure data.

And, finally, I think we should try to follow this as closely as possible because I agree with Pete that we are going to go to load following. I mean, if you're going to make money out of these nukes probably in 10 years, yes, we'll be doing load following. Because whatever you say the political reality is they're going to be renewables, and they're going to have to be found.

MEMBER BLEY: Sam, could I sneak in a last thing? I forgot to ask. And when we look at all those curves it seems kind of clear we aren't looking for the right parameter. Now, you guys have mostly talked, you think it's rate, you think it's extent of power increase and the time at power. Is it possible from the data from those tests to plot these against some combination of ramp rate and time at power to see if -- if you get the right parameter we ought to see the good ones here and the bad ones over here. And we haven't found the right parameter yet.

MEMBER RICCARDELLA: Has anyone tried to do a statistical analysis, generate Y-able curves or some kind of curves to see --

MEMBER BANERJEE: That's more --

MEMBER ARMIJO: In that little White Paper I turned out, the BWR one, that's exactly what we did back in the '70s. And you have curves at 1 percent probability, 50 percent probability failure, 99 percent. But that was BWR.

MEMBER BANERJEE: You had 800 data points?

MEMBER ARMIJO: We had a lot of data points. And we were very consistent in how we fabricated it, but was still probabilistic. It wasn't -- it has to be.

MEMBER BLEY: That's just the way material failure is.

MEMBER ARMIJO: Yes, and see similar things with this. You know, there was a lot of different sets of data. When you have one big set of data all made the same way it's much easier to analyze. But I'd like to, first of all, I can't help but to point out that that high burnup effect thing, it's been also seen in BWRs. And I'll tell you an experiment we did many years ago as a remedy for PCI was to change the oxygen to uranium ratio. We made fresh pellets with a very high ODU, irradiate them in the reactor, then in ramp testing they worked pretty damned well. They didn't all survive but they were much better than the standard, so it has something to do with chemistry. We never really could understand it. It had negatives for manufacturing and thermal connectivity, had all sorts of other problems, so there's lot of ponies out there, and there may be better explanations on that, but the trouble is you don't have those properties at 20,000 megawatts per ton in 30, you have to -- that's where the power -- you have ability to get to high power, if at all.

But I'd like to, first of all -- first, I was laboring under burden that we -- at some point we'd have to rely on an operator putting off one of these very fast PCI events, and what I've learned here is that you really are -- that you're really covered by the reactor protection systems. They're fast enough and they're covering all of them, and if the worst one is that one that lasts what, what was it, six minutes, or three --

MR. CLIFFORD: It was three minutes.

MEMBER ARMIJO: Three minutes, something like that, and if that's the worst one and you have an RP that's protecting you and you're not relying on operator action, I'm very, very happy.

The other thing that I felt was -- that the Staff was taking comfort with the 1 percent PCMI SAFDL. And, obviously, that's not what -- that wouldn't protect you because if that was the only thing was protecting you, you would have a lot of failures because the system -- if the system wasn't tripping or protecting you. So, anyway, that -- but all in all I think a lot of progress has been made, and a good presentation. There's a -- I think the Staff would benefit by really getting FRAPCON up to better capabilities in this area of analyzing the fuel and the pellet for these kind of things, whether it's a load following problem or something else that comes up. I think the code is capable, but it's going to take some effort. There's no crisis, but to improve it.

MR. CLIFFORD: I mean, this is an area where you guys need to help us to do that, too, because you review the research plan.

MEMBER ARMIJO: Yes. Well, that's very timely.

MEMBER BALLINGER: Does FRAPTRAN have anything -- what about FRAPTRAN? Doesn't that do strain calculations?

MR. CLIFFORD: Yes, we -- let me see if I remember this. Maybe, Harold, you remember. I remember they used both FRAPTRAN and FRAPCON to evaluate the subject ramp tests and I don't remember off the top of my head why they felt that FRAPCON did a better job.

MEMBER BALLINGER: Because FRAPTRAN, they were using that for the reactivity insertion stuff. Right?

MR. CLIFFORD: Right, right.

MEMBER CORRADINI: What are they using for --

MEMBER BALLINGER: FRAPTRAN. Transient means transient.

MEMBER CORRADINI: But can I turn this around since you brought up research. So, are you telling me that there's no user need for an improved FRAPCON?

MR. CLIFFORD: Every year --

MEMBER CORRADINI: Put you on the spot a bit.

MR. CLIFFORD: Office of Research -- well, I'll let the Office of Research --

MR. SCOTT: This is Harold Scott from Research. Patrick does have a plan for FRAPCON and FRAPTRAN for the next few years, but right now there's not a particular PCI effort in there. But let me bring up another point that hadn't come up yet. This CASL program that Department of Energy is sponsoring, a consortium for advanced simulation light water reactors, they have a big effort on PCI modeling. And they're going to probably spend $5 million, and Patrick might spend $500,000, so -- and they have a schedule for 14 asymmetric worldwide stress calculations, local stress calculations, integrated methodology by the end of this calendar year, so I would suggest to Patrick that we wait and see what happens in the DOE CASL program and then move forward with something with FRAPCON. We'll also have another -- the SCIP-3 program is going to do improv tests, manual tests, slow ramp rates. There'll be workshops. As mentioned, the French have these more sophisticated 3D codes, that may not be applicable since they run for hours, but there might -- I'm just saying I think if we wait a little bit, enough other people are moving ahead rather quickly that we can piggyback off of their efforts and maybe not have to spend a lot of our time doing the same things.

MEMBER CORRADINI: So, can I just make sure I understand what you're saying? So, you're saying because the -- just be real careful because whatever they call the animal that they're using in CASL, I think it's Peregrine.

MR. SCOTT: Yes.

MEMBER CORRADINI: Right? The only calculation I've seen so far have been to 2D asymmetric calculations. They have nothing to validate it with as far as I can tell. They have integral tests which you're using yourselves, so for all intents and purposes they're basically comparing Peregrine to FRAPCON.

MR. SCOTT: Yes, that's what they started with but eventually they could use the SCIP data and PCI data itself that we have available that's been mentioned.

MEMBER CORRADINI: So, let me just -- okay. So, I agree with you there, but let me ask you a different question. So, this is a question maybe you guys don't want to answer it. So, is NRC going to default and essentially use the DOE product as their base tool?

MR. SCOTT: Oh, I'm not saying that.

MEMBER CORRADINI: Okay.

MR. SCOTT: I'm saying --

MEMBER CORRADINI: Okay, so because -- what I guess I'm also asking is from the standpoint of a user need, it strikes me that -- I'm sure Sam is going to show some version of a research report recommendation that will say something like thou shalt go forth and do good things in this area. But my only thought is we have historically gotten the response back that unless there's a user need from NRR that's a potentially less than optimal way to do things. So, I see Dr. Lee is up.

MR. LEE: Well, there are certain so called infrastructure code that don't need to have the user need from the other offices to do development or maintaining. FRAP codes is one of it, MELCOR and the TRACE code, for example, these are absolute we need to have for the Agency, so we don't need to have the user office keep writing us user need on specific things.

MEMBER BANERJEE: Could I ask a question? Sorry, go ahead.

MEMBER POWERS: The fundamental trouble is I suppose -- suppose you break fuels, so what?

MEMBER ARMIJO: Well, it's your first

barrier, and we're not supposed to break a lot of fuel. Fundamentally, that's a poor way to run a reactor. It never happens --

MEMBER POWERS: That's kind of the licensee's business, if he wants to run crappy -- run his reactor crappy, as he long as he doesn't threaten the public health and safety, so what?

MEMBER ARMIJO: But, Dana, why do we spend so much time on DNB?

MEMBER POWERS: Good question.

MEMBER ARMIJO: How much have we failed as a result of DNB?

MEMBER CORRADINI: But that's different. That's the --

(Simultaneous speech.)

MEMBER CORRADINI: If you want to wait for that answer, I can give you the answer.

MEMBER ARMIJO: I think the purpose of this knowledge or these codes is to keep things from happening that we can prevent, to spot where there's a problem.

MEMBER POWERS: I mean, we're getting into the licensee's -- how he wants to run his plant. He can do it any way he wants to as long as it doesn't threaten the public health and safety. I mean, you've got to be able to tie this back in a fairly transparent fashion to the mandate of the Agency before you spend huge resources trying to -- I mean, making a finite element three-dimension fuel response code that covers the entire core strikes me as a pretty ambitious undertaking.

MEMBER CORRADINI: But I wasn't -- I guess, Dana, just to kind of join on Sam's side on this one. I'm not saying that this is what the Agency should do, but I'm asking given the fact that I sense DOE is supporting the industry which is going this way, eventually NRC is going to have to have some tool to say yes, we have done our evaluation model, whatever the right word is, calculation. We agree or we don't agree, and we have the database to do it. And my sense of it is, at least with this one, unless Paul was sending me the wrong path, it seems a bit muddled as to if you started going down to -- if you started ramping up and down the reactor and you start having fuel failures, I don't think NRC is going to stand for that, whether or not it's dealing with the health and safety or not. So, that then they will get involved, and they will have to make some decision on if the licensee is allowed to go on some percent change of power per unit time. And it's got to be some model that you guys have to have confidence in. And I sense that at least in this area you don't have confidence.

MR. CLIFFORD: Correct. But, I mean, we haven't done a load follow license amendment request, but I would hope that one would include maneuvering requirements or restrictions, and that we would approve those.

MEMBER BALLINGER: But don't current fuel have warranty -- there are warranty limits?

MEMBER ARMIJO: Those are commercial.

MEMBER BANERJEE: Can I ask about CASL? Because it is DOE --

MEMBER ARMIJO: Who is doing CASL?

(Simultaneous speech.)

MEMBER BANERJEE: Can I ask you about CASL? Is the information generated in CASL available to NRC, because by and large it is proprietary. You know, we have to sign NDAs and all sorts of things.

MEMBER BALLINGER: There's a lot of universities involved.

MEMBER BANERJEE: But not all have signed NDAs. And who is doing this? Is it Westinghouse?

(Simultaneous speech.)

MEMBER POWERS: -- and their advisory board.

MEMBER BANERJEE: Who is doing it, and is it available? Can you answer that?

MEMBER POWERS: Who is doing it?

MEMBER BANERJEE: Like who in the CASL group? Is it Westinghouse doing the modeling?

MEMBER POWERS: Westinghouse, GE, AREVA all have representatives on their applications board. The center of it is at Oak Ridge. Let's see. University of North Carolina, or North Carolina State.

MEMBER CORRADINI: But I think his question is for Peregrine that is very limited distribution because there specific proprietary correlations that are horn swaggled, or that are fit into it that EPRI controls, as far as I understand. The base tool which is the -- as Dana was saying, is the finite element tool which has a different name. I can't remember what that name is. It is essentially open literature correlations that FRAPCON uses and others use. But the one that they're using for their calculations for any customer, such as Westinghouse, has proprietary correlations in it for a lot of these details.

MEMBER BANERJEE: So --

MEMBER CORRADINI: Fission gas --

MEMBER BANERJEE: But what you're saying -- well, we should have the Staff answer this, but what you're saying is really that it's partly available the developments on the CASL.

MEMBER CORRADINI: Yes, on the last review Steve Bajorek was the NRC representative at the review.

MEMBER BANERJEE: They have access to some of this.

MR. CLIFFORD: There was a presentation last week on the status of CASL, and there's two days worth of slide presentations that are in ADAMS right now.

MR. JACKSON: Right. I was at the briefing. It was led by Steve Bajorek. DOE led the briefing to us, but they had all the members. So, you know, at the moment they're focused on things that the industry is concerned with, things that they can make a lot of money on or save money, so CRUD. They want to have very cool predictive tools on things that affect operation, and PCI has a huge impact on their finances, so this is one of the things they're looking at. There's no regulatory submittal to us at this point, not to say that there couldn't be in the future, but there's nothing now. If they wanted to push the envelope farther and operate the plants much different, I guess hypothetically you could --

MEMBER BANERJEE: So, could we do confirmatory analysis? Just take their results?

MEMBER CORRADINI: This kind of goes back my original question. I think now I'll take Dana's side, is that if we think FRAPCON is enough for the regulatory agency, then there's got to be a set amount of experimentation that both sides have got to be pointed to and validate against so that we're comfortable with the tool that the Agency has versus DOE or whoever EPRI is providing.

MEMBER BANERJEE: Yes, but I think if you look at thermal hydraulics as an example, the industry is pushing the boundaries because they want to get closer to the limits. Right? Now, obviously, they're trying to do that. And we have to be able to at least follow them. Right? I mean, they have more sophisticated models already than TRACE, and they're putting that forward. And if we have no way to confirm it, what do we do?

MEMBER BALLINGER: The CASL -- you can have the mesh size of a nanometer in CASL and make great 3D pictures which is exactly what they do, but you don't have fidelity on the data for the ramp test.

MEMBER BANERJEE: But imagine 10 years, 5 years from now they come in with submissions which say you know we can do this now, and our codes do it, and we don't have a confirmatory tool.

MR. JACKSON: I think that's why Paul recommended that we continue to improve the FRAP code, that there's an opportunity for --

MEMBER BANERJEE: I mean, to me that answers your question.

MEMBER ARMIJO: Mr. Chairman, sorry for --

CHAIRMAN STETKAR: No, that's fine. I was going to give you two more minutes because my role here is on average to keep everything average. I was an hour under, Charlie was right on time. You're an hour over, so I figured, you know, you've got two minutes.

MEMBER ARMIJO: I think a lot of progress has been made even though -- particularly in this area, on the PWRs, so, I'm much more relaxed about this thing than I used to be. I don't think you're going to have a PWR AOO that gets you up to the high powers for enough length of time, assuming that these trip systems actually work, that you have to ever worry about some operator having to say oops, or failing a lot of fuel. And unlike Dana, I have an aversion to failing a lot of fuel in a transient. It's a licensee's problem and the fuel supplier's problem if they fail a lot of fuel during normal operation, that's the big commercial mess. But in a transient I think it's a regulatory issue. So, anyway, Paul, good presentation. Thanks to the Staff for doing a lot of work, appreciate it. And, Mr. Chairman, the meeting is your's.

CHAIRMAN STETKAR: Thank you.

MEMBER ARMIJO: Right on schedule.

CHAIRMAN STETKAR: Fine. We will take a break and we are going to be off the record when we return. Come back at 4:30, please, and we can talk about the Research report.

(Whereupon, the proceedings went off the record at 4:13 p.m.)

LUMINANT GENERATION COMPANY

Comanche Peak Nuclear Power Plant, Units 3 and 4

612th ACRS Meeting

FSAR Chapters

3 (less 3.7, 3.8), 9, and 14

March 6, 2014

Agenda

- Introduction
- Topics of Discussion with ACRS Subcommittee
  - Chapter 3 (less 3.7 and 3.8)
  - Chapter 9
  - Chapter 14

Introduction

- COLA uses “Incorporated by Reference” methodology
- FSAR Chapters 3, 9, and 14 take no departures from US-APWR DCD
- No contentions pending before ASLB
- All confirmatory items were incorporated in FSAR Rev 4 (Nov 2013)
- Luminant has responded to all Open Items
- No outstanding issues identified in SERs

Luminant

US-APWR

MNES
MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC.

Topics of Discussion with ACRS Subcommittee

- Chapter 3
  - Military air crash probability
  - Turbine missile probability calculation
- Chapter 9
  - Wet bulb temperature; calcs for UHS evaporative losses
  - Duct heaters in electrical HVAC equipment rooms
  - Sharing Fire Brigade between Units 3 and 4
  - Incident Commander
  - Fire Brigade Leader
  - Flooding in the ESW Pipe Tunnel

Topics of Discussion with Subcommittee (cont'd)

- Chapter 14

Acronyms

ASLB	Atomic Safety and Licensing Board
COLA	Combined License Application
DCD	Design Control Document
FSAR	Final Safety Analysis Report
HVAC	Heating, air conditioning, and ventilation
SER	Safety Evaluation Report
UHS	Ultimate heat sink
US-APWR	United States Advanced Pressurized Water Reactor

US-APWR
Design Certification Application

Chapter 3 (except 3.7 and 3.8) and
Chapter 14 (except 14.3.2 and 14.3.9)

ACRS Full Committee Presentation

March 6, 2014

Mitsubishi Heavy Industries, Ltd.

Presenters

- **Ryan Sprengel**
  - ✓ DCD Licensing Manager
- **Masatoshi Nagai**
  - ✓ DCD Licensing Engineer, Ch 3
- **Rebecca Steinman**
  - ✓ DCD Licensing Engineer, Ch 14

Introduction

- **Previous ACRS Full Committee meetings**
  - ✓ September 9, 2011 – Chapters covered: 2, 5, 8, 10, 11, 12, 13, 16
  - ✓ September 6, 2012 – Chapter 9 covered
  - ✓ April 11, 2013 – Chapters 4, 15, 17, 19; Topical Reports supporting Chapters 4 and 15, respectively
  - ✓ December 5, 2013 – Chapters 6 and 7; Topical Reports supporting Chapters 6 and 7, respectively
- **Significant upcoming submittals**
  - ✓ Chapter Status Reports 3/31/2014
- **Adjustment of ongoing US-APWR DC Activities**
  - ✓ Letter (UAP-HF-13256) submitted to NRC 11/5/2013
  - ✓ Coordinated slowdown of DCD Licensing Activities, while maintaining a commitment to US-APWR

Chapter 3 – Design of Structures, Systems, Components, and Equipment

- **ACRS Subcommittee meeting held November 20 and 21, 2013**
  - ✓ All sections except 3.7 and 3.8 presented
- **Remaining Review Areas**
  - ✓ Areas that require further review and interactions include:
    - 3.9.2 - Dynamic Testing and Analysis of Systems, Components, and Equipment
    - 3.9.4 - Control Rod Drive Systems
    - 3.10 - Seismic and Dynamic Qualification of Mechanical and Electrical Equipment
    - 3.11 - Environmental Qualification
  - ✓ NRC audit of Design and Procurement Specifications conducted February 2014
- **Written responses to ACRS SC questions to be submitted, March 2014**

Chapter 14 – Verification Programs

- **ACRS Subcommittee meeting held March 4, 2014**
  - ✓ All sections except 14.3.2 and 14.3.9 presented
- **Remaining Review Areas**
  - ✓ MHI response to RAI 1076-7368 Q 07-09-27 (follow-up to RAI 992-6999 Q 07.09-26) was submitted on February 25, 2014 to address the only SE Open Item
  - ✓ No additional Ch 14 RAIs requiring MHI response
- **Written responses to ACRS SC questions to be submitted, March 2014**

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

Presentation to the ACRS Full Committee – 612th Meeting

Comanche Peak Nuclear Power Plant, Units 3 and 4
COL Application Review

Safety Evaluation Report with Open Items

Chapter 3: Design of Structures, Systems, Components, and Equipment
Chapter 9: Auxiliary Systems
Chapter 14: Verification Programs

Perry Buckberg
US-APWR Design Certification Lead Project Manager

March 6, 2014

CPNPP COLA
Review Schedule

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

	COMPLETION DATE
Phase 1 – Preliminary Safety Evaluation Report (SER)	10/09/2009
Phase 2 – SER with Open Items	TBD
Phase 3 – ACRS Review of SER with OIs	TBD
Phase 4 – Advanced SER with No OIs	TBD
Phase 5 – ACRS Review Adv. SER with No OIs	TBD
Phase 6 – Final SER with No OIs	TBD
Rulemaking	TBD

Summary of the CPNPP COLA Safety Evaluation Reports

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

- The staff has issued Safety Evaluation Reports (SERs) with Open Items for Chapters 2, 3 (partial), 4, 5, 6, 7, 8, 9, 10, 11 ,12 13, 14, 15, 16, 17 and 19 (partial).
- Of the issued chapters, by CoB today all will have been presented to the ACRS Full Committee.

CPNPP Chapter 3
Design of Structures, Systems, Components and Equipment

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

- The following Chapter 3 Open Items were discussed during the November 2013 SC Meeting:

  - **RAI 244-6222, Question 03.09.06-21**: Audit of a sample of applicable design and procurement specifications for functional design, qualification, and inservice testing programs
    - **Status**: Open - Audit conducted February of 2014, will remain open pending the issuance of the audit report

  - **RAI 239-6159, Question 03.11-18**: Audit of a sample of applicable design and procurement specifications for the environmental qualification of mechanical equipment..
    - **Status**: Open - Audit conducted February of 2014, will remain open pending the issuance of the audit report

  - **RAI 239-6159, Question 03.11-19**: COL environment qualification operational program review is dependent on the completion of the review of MHI's MUAP-08015, "US-APWR Equipment Environmental Qualification Program"
    - **Status**: Open – Review after shutdown

CPNPP Chapter 9
Auxiliary Systems

- The SE for Chapter 9 addresses:
  - Fuel storage and handling
  - Water systems
  - Process auxiliaries
  - HVAC
  - Other auxiliary systems.
- The following Chapter 9 Open Item was discussed during the November 2013 SC Meeting
  - **Open Item 09.02.05-01:** The “governing” heat load for UHS basin cooling capacity.
    Status: Now a CI

CPNPP Chapter 14 Verification Programs

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

- The SE for Chapter 14 addresses:
  - Specific Information to Be Included in Preliminary/Final Safety Analysis Reports
  - Initial Plant Test Program
  - ITAAC
- There were no technical Open Items discussed during the March 4, 2014 SC Meeting

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Presentation to the ACRS Full Committee – 612th Meeting

United States – Advanced Pressurized Water Reactor (US-APWR) Design Certification

Safety Evaluation Report with Open Items

Chapter 3: Design of Structures, Systems, Components, and Equipment
Chapter 14: Verification Programs

Perry Buckberg
US-APWR Design Certification Lead Project Manager

March 6, 2014

US-APWR DC
Review Schedule

United States Nuclear Regulatory Commission
Protecting People and the Environment

	COMPLETION DATE
Phase 1 – Preliminary Safety Evaluation Report (SER)	June 2009
Phase 2 – SER with Open Items	TBD
Phase 3 – ACRS Review of SER with OIs	TBD
Phase 4 – Advanced SER with No OIs	TBD
Phase 5 – ACRS Review Adv. SER with No OIs	TBD
Phase 6 – Final SER with No OIs	TBD
Rulemaking	TBD

Summary of the US-APWR Safety Evaluation Reports

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

- The staff has issued Safety Evaluation Reports (SERs) with Open Items for Chapters 2, 3 (partial), 4, 5, 6, 7, 8, 9, 10, 11 ,12 13, 14, 15, 16, 17 and 19 (partial).
- Of the issued chapters, by CoB today all will have been presented to the ACRS Full Committee.

US-APWR Chapter 3
Design of Structures, Systems, Components and Equipment

- The following Chapter 3 Open Items were discussed during the November 2013 SC Meeting
  - **RAI 1015-7054, Question 03.09.03-31**: Design/procurement specification audit
    - **Status**: Open - Audit conducted February of 2014, will remain open pending the issuance of the audit report
  - **RAI 841-6055, Question 03.04.01-29**: Flooding analysis audit .
    - **Status**: Resolved
  - **RAI 841-6055, Question 03.04.01-30**: Changes to the building layout, flood barriers, and water-tight doors resulting from seismic design changes.
    - **Status**: Resolved
  - **RAI 546-4345, Question 03.04.02-6**: The use of 0.7 as the coefficient of friction at the soil-concrete interface.
    - **Status**: Resolved
  - **RAI 782-5910, Question 14.03.07-58**: MHI modified the ITAAC for turbine generator arrangement and turbine missile probability
    - **Status**: Resolved
  - **RAI 758-5680, Question 03.05.03-10**: Automobile missile on all seismic Category I structures not covered by RG 1.76.
    - **Status**: Resolved
  - **RAI 1013-7031, Question 03.09.02-103**: Postulated steam generator failure mechanisms associated with the San Onofre.
    - **Status**: Open - Under review.

US-APWR Chapter 3
Design of Structures, Systems, Components and Equipment

- Chapter 3 Open Items cont.
  - **RAI 1013-7031, Question 03.09.02-104**: Preliminary design of the steam generator tube bundle and the design criteria for the steam generator tubes and retainer bars against flow-induced excitations, including random turbulence, fluid elastic instability (out-of-plane and in-plane), and vortex shedding.
    - **Status**: Open - Under review.
  - **RAI 209-1803, Question 03.09.03-21**: Seismic analysis changes.
    - **Status**: Resolved
  - **RAI 107-1293, Question 03.09.04-1**, Subquestions 1293-01, 1293-06, and 1293-07, and RAI 848-6093, Question 03.09.04-14: Margin between the calculated maximum control rod drive mechanism deflection and the design limit prior to seismic analysis changes.
    - **Status**: Open – Review after slowdown
  - **RAI 288-2274, Question 03.09.06-1**: Design/procurement specification audit
    - **Status**: Open – Under Review
  - **RAI 486-3861, Question 03.10**-17: Gas turbine generator system qualification and methods, criteria, and procedures. TeR MUAP-10023.
    - **Status**: Open – Review after slowdown
  - **RAI 650-5093, Question 03.11-39**: Addressing all environmental qual.n requirements in 10 CFR 50.49 and ASME QME-1-2007, App QR-B
    - **Status**: Open – Review after slowdown

US-APWR Chapter 3
Design of Structures, Systems, Components and Equipment

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

- Chapter 3 Open Items cont.
  - **RAI 589-4536, Question 03.11-36**: Calculational methods/results for total integrated dose to equipment in containment following a LOCA.
    - **Status**: Open – Review after slowdown
  - **RAI 589-4536, Question 03.11-37**: Calculational methods/results for the beta ray source term for equipment inside containment following a LOCA.
    - **Status**: Open – Review after slowdown
  - **RAI 589-4536, Question 03.11-38**: Inconsistencies in the operability times of post accident equipment inside containment.
    - **Status**: Open – Review after slowdown
  - **RAI 880-6142, Question 03.11-42**: MHI to provide a equipment qualification data package template.
    - **Status**: Open – Review after slowdown
  - **RAI 805-5915, Question 03.11-41** and **RAI 880-6142, Question 03.11-43**: MHI demonstrate US-APWR satisfying the environmental qual for electrical equipment (10 CFR 50.49) (1)
    - **Status**: Open – Review after slowdown
  - **RAI 901-6257, Question 03.11-55**: The ITAAC do not include demonstration of environmental qualification of nonmetallic parts of mechanical equipment.
    - **Status**: Open – Review after slowdown (supplemental RAI response needs to be reviewed)
  - **RAI 804-5938, Question 03.12-26**: The design loads for piping were updated and the seismic analysis methods of steam generator supports unclear.
    - **Status**: Resolved

US-APWR Chapter 14
Verification Programs

- The SE for Chapter 14 addresses:
  - Specific Information to Be Included in Preliminary/Final Safety Analysis Reports
  - Initial Plant Test Program
  - ITAAC
- The following Chapter 14 Open Item was discussed during the March 4, 2014 SC Meeting
  - **RAI 1076-7368, Question 07.09-27** (Follow-up to RAI 992-6999, Question 07.09-26): Provide ITAAC to verify that the as-built protection and control systems are separate such that failure of any control system or component would not impact the performance of safety functions to satisfy the GDC 24 requirements. The Open Item applies to Section 14.3.5.

    Status: Still and Open Item

United States Nuclear Regulatory Commission

Protecting People and the Environment

Presentation to the ACRS Full Committee – 612th Meeting

Comanche Peak Nuclear Power Plant, Units 3 and 4
COL Application Review

Safety Evaluation Report with Open Items

Chapter 3: Design of Structures, Systems, Components, and Equipment
Chapter 9: Auxiliary Systems
Chapter 14: Verification Programs

Perry Buckberg
US-APWR Design Certification Lead Project Manager

March 6, 2014

CPNPP COLA
Review Schedule

	COMPLETION DATE
Phase 1 – Preliminary Safety Evaluation Report (SER)	10/09/2009
Phase 2 – SER with Open Items	TBD
Phase 3 – ACRS Review of SER with OIs	TBD
Phase 4 – Advanced SER with No OIs	TBD
Phase 5 – ACRS Review Adv. SER with No OIs	TBD
Phase 6 – Final SER with No OIs	TBD
Rulemaking	TBD

Summary of the CPNPP COLA Safety Evaluation Reports

- The staff has issued Safety Evaluation Reports (SERs) with Open Items for Chapters 2, 3 (partial), 4, 5, 6, 7, 8, 9, 10, 11 ,12 13, 14, 15, 16, 17 and 19 (partial).
- Of the issued chapters, by CoB today all will have been presented to the ACRS Full Committee.

CPNPP Chapter 3
Design of Structures, Systems, Components and Equipment

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

- The following Chapter 3 Open Items were discussed during the November 2013 SC Meeting:

  - **RAI 244-6222, Question 03.09.06-21**: Audit of a sample of applicable design and procurement specifications for functional design, qualification, and inservice testing programs
    - **Status**: Open - Audit conducted February of 2014, will remain open pending the issuance of the audit report

  - **RAI 239-6159, Question 03.11-18**: Audit of a sample of applicable design and procurement specifications for the environmental qualification of mechanical equipment..
    - **Status**: Open - Audit conducted February of 2014, will remain open pending the issuance of the audit report

  - **RAI 239-6159, Question 03.11-19**: COL environment qualification operational program review is dependent on the completion of the review of MHI's MUAP-08015, "US-APWR Equipment Environmental Qualification Program"
    - **Status**: Open – Review after shutdown

CPNPP Chapter 9 Auxiliary Systems

- The SE for Chapter 9 addresses:
  - Fuel storage and handling
  - Water systems
  - Process auxiliaries
  - HVAC
  - Other auxiliary systems.
- The following Chapter 9 Open Item was discussed during the November 2013 SC Meeting
  - **Open Item 09.02.05-01:** The “governing” heat load for UHS basin cooling capacity.
    Status: Now a CI

CPNPP Chapter 14 Verification Programs

- The SE for Chapter 14 addresses:
  - Specific Information to Be Included in Preliminary/Final Safety Analysis Reports
  - Initial Plant Test Program
  - ITAAC
- There were no technical Open Items discussed during the March 4, 2014 SC Meeting

Presentation to the ACRS Full Committee – 612th Meeting

United States – Advanced Pressurized Water Reactor (US-APWR) Design Certification

Safety Evaluation Report with Open Items

Chapter 3: Design of Structures, Systems, Components, and Equipment
Chapter 14: Verification Programs

Perry Buckberg
US-APWR Design Certification Lead Project Manager

March 6, 2014

US-APWR DC
Review Schedule

	COMPLETION DATE
Phase 1 – Preliminary Safety Evaluation Report (SER)	June 2009
Phase 2 – SER with Open Items	TBD
Phase 3 – ACRS Review of SER with OIs	TBD
Phase 4 – Advanced SER with No OIs	TBD
Phase 5 – ACRS Review Adv. SER with No OIs	TBD
Phase 6 – Final SER with No OIs	TBD
Rulemaking	TBD

Summary of the US-APWR Safety Evaluation Reports

- The staff has issued Safety Evaluation Reports (SERs) with Open Items for Chapters 2, 3 (partial), 4, 5, 6, 7, 8, 9, 10, 11 ,12 13, 14, 15, 16, 17 and 19 (partial).
- Of the issued chapters, by CoB today all will have been presented to the ACRS Full Committee.

US-APWR Chapter 3
Design of Structures, Systems, Components and Equipment

- The following Chapter 3 Open Items were discussed during the November 2013 SC Meeting
  - **RAI 1015-7054, Question 03.09.03-31**: Design/procurement specification audit
    - **Status**: Open - Audit conducted February of 2014, will remain open pending the issuance of the audit report
  - **RAI 841-6055, Question 03.04.01-29**: Flooding analysis audit .
    - **Status**: Resolved
  - **RAI 841-6055, Question 03.04.01-30**: Changes to the building layout, flood barriers, and water-tight doors resulting from seismic design changes.
    - **Status**: Resolved
  - **RAI 546-4345, Question 03.04.02-6**: The use of 0.7 as the coefficient of friction at the soil-concrete interface.
    - **Status**: Resolved
  - **RAI 782-5910, Question 14.03.07-58**: MHI modified the ITAAC for turbine generator arrangement and turbine missile probability
    - **Status**: Resolved
  - **RAI 758-5680, Question 03.05.03-10**: Automobile missile on all seismic Category I structures not covered by RG 1.76.
    - **Status**: Resolved
  - **RAI 1013-7031, Question 03.09.02-103**: Postulated steam generator failure mechanisms associated with the San Onofre.
    - **Status**: Open - Under review.

US-APWR Chapter 3
Design of Structures, Systems, Components and Equipment

- Chapter 3 Open Items cont.
  - **RAI 1013-7031, Question 03.09.02-104**: Preliminary design of the steam generator tube bundle and the design criteria for the steam generator tubes and retainer bars against flow-induced excitations, including random turbulence, fluid elastic instability (out-of-plane and in-plane), and vortex shedding.
    - **Status**: Open - Under review.
  - **RAI 209-1803, Question 03.09.03-21**: Seismic analysis changes.
    - **Status**: Resolved
  - **RAI 107-1293, Question 03.09.04-1**, Subquestions 1293-01, 1293-06, and 1293-07, and RAI 848-6093, Question 03.09.04-14: Margin between the calculated maximum control rod drive mechanism deflection and the design limit prior to seismic analysis changes.
    - **Status**: Open – Review after slowdown
  - **RAI 288-2274, Question 03.09.06-1**: Design/procurement specification audit
    - **Status**: Open – Under Review
  - **RAI 486-3861, Question 03.10**-17: Gas turbine generator system qualification and methods, criteria, and procedures. TeR MUAP-10023.
    - **Status**: Open – Review after slowdown
  - **RAI 650-5093, Question 03.11-39**: Addressing all environmental qual.n requirements in 10 CFR 50.49 and ASME QME-1-2007, App QR-B
    - **Status**: Open – Review after slowdown

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

- Chapter 3 Open Items cont.
  - **RAI 589-4536, Question 03.11-36**: Calculational methods/results for total integrated dose to equipment in containment following a LOCA.
    - **Status**: Open – Review after slowdown
  - **RAI 589-4536, Question 03.11-37**: Calculational methods/results for the beta ray source term for equipment inside containment following a LOCA.
    - **Status**: Open – Review after slowdown
  - **RAI 589-4536, Question 03.11-38**: Inconsistencies in the operability times of post accident equipment inside containment.
    - **Status**: Open – Review after slowdown
  - **RAI 880-6142, Question 03.11-42**: MHI to provide a equipment qualification data package template.
    - **Status**: Open – Review after slowdown
  - **RAI 805-5915, Question 03.11-41** and **RAI 880-6142, Question 03.11-43**: MHI demonstrate US-APWR satisfying the environmental qual for electrical equipment (10 CFR 50.49) (1)
    - **Status**: Open – Review after slowdown
  - **RAI 901-6257, Question 03.11-55**: The ITAAC do not include demonstration of environmental qualification of nonmetallic parts of mechanical equipment.
    - **Status**: Open – Review after slowdown (supplemental RAI response needs to be reviewed)
  - **RAI 804-5938, Question 03.12-26**: The design loads for piping were updated and the seismic analysis methods of steam generator supports unclear.
    - **Status**: Resolved

US-APWR Chapter 14
Verification Programs

- The SE for Chapter 14 addresses:
  - Specific Information to Be Included in Preliminary/Final Safety Analysis Reports
  - Initial Plant Test Program
  - ITAAC
- The following Chapter 14 Open Item was discussed during the March 4, 2014 SC Meeting
  - **RAI 1076-7368, Question 07.09-27** (Follow-up to RAI 992-6999, Question 07.09-26): Provide ITAAC to verify that the as-built protection and control systems are separate such that failure of any control system or component would not impact the performance of safety functions to satisfy the GDC 24 requirements. The Open Item applies to Section 14.3.5.

    Status: Still and Open Item

Diablo Canyon Process Protection System LAR

Presented by: NRR / EICB

John Thorp Branch Chief EICB
Rich Stattel Technical Reviewer EICB
Rossnyev Alvarado EICB
Samir Darbali EICB

Thursday March 6, 2014

Presentation Outline / Agenda

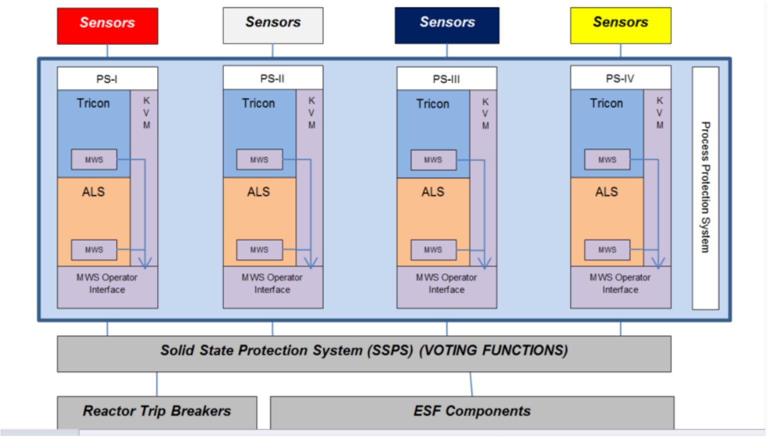
- Introduction
- Platform Evaluation Background
  - Tricon
  - ALS
- Overview of Diablo Canyon License Amendment Request
- Safety Evaluation Topics
  - Communication
  - Diversity and Defense in Depth
  - Secure Development and Operations Environment (SDOE)
  - Deterministic Performance

Introduction
Diablo Canyon PPS Replacement LAR

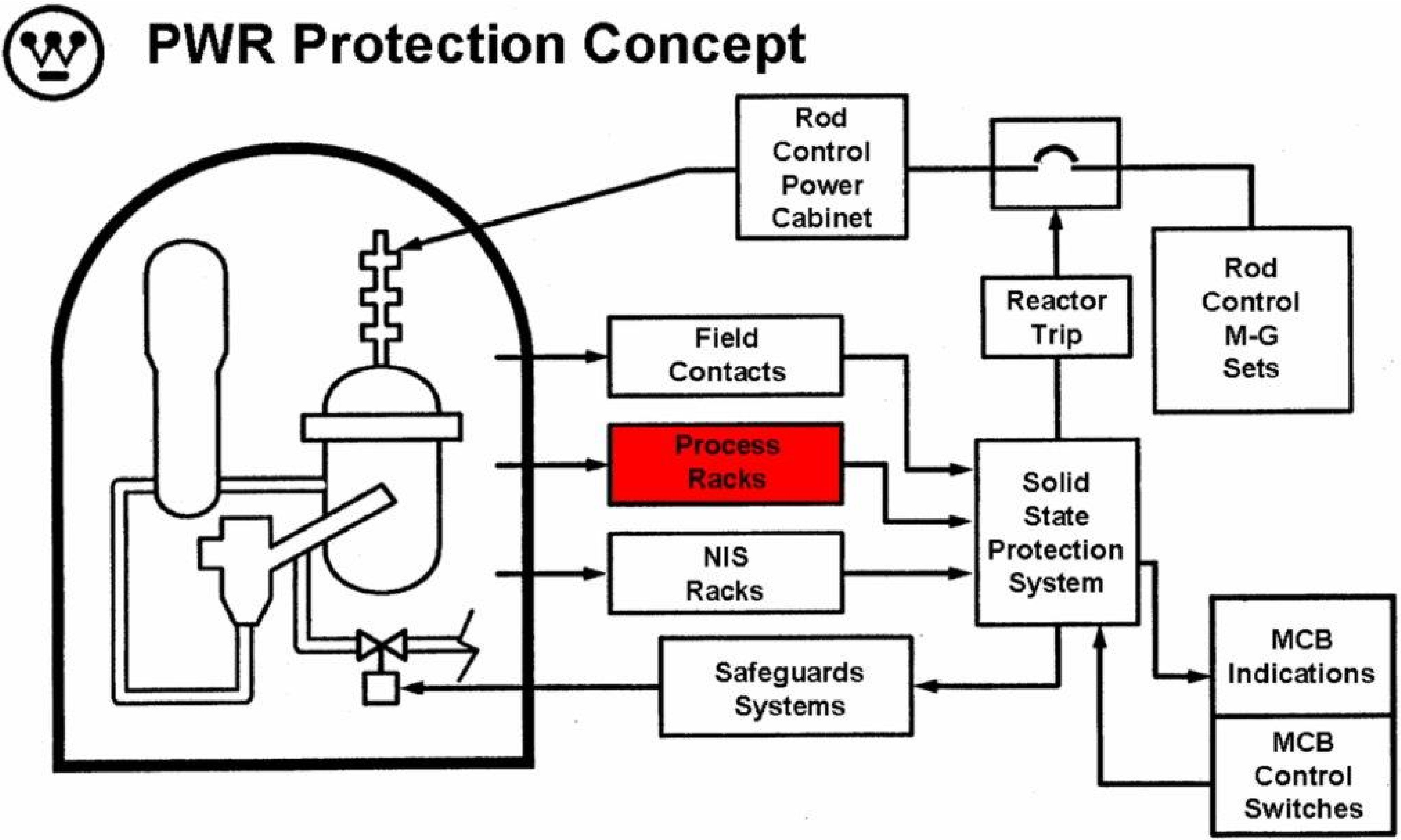
- **Diablo Canyon License Amendment Request Submitted on October 26, 2011**
  - LAR is to replace the existing Eagle 21 Process Protection System with a new more modern digital system.
  - The Diablo Canyon Digital Process Protection System (PPS) is based on both the Microprocessor based Invensys Tricon and the FPGA based Westinghouse ALS Platforms.

- **The NRC accepted the LAR (January 13 2012) for review and documented several review areas which would require particular attention prior to approving the LAR. These are:**
  - Deterministic Performance of Software
  - Equipment Qualification Testing Plans
  - Software Planning Documentation
  - Setpoint Methodologies

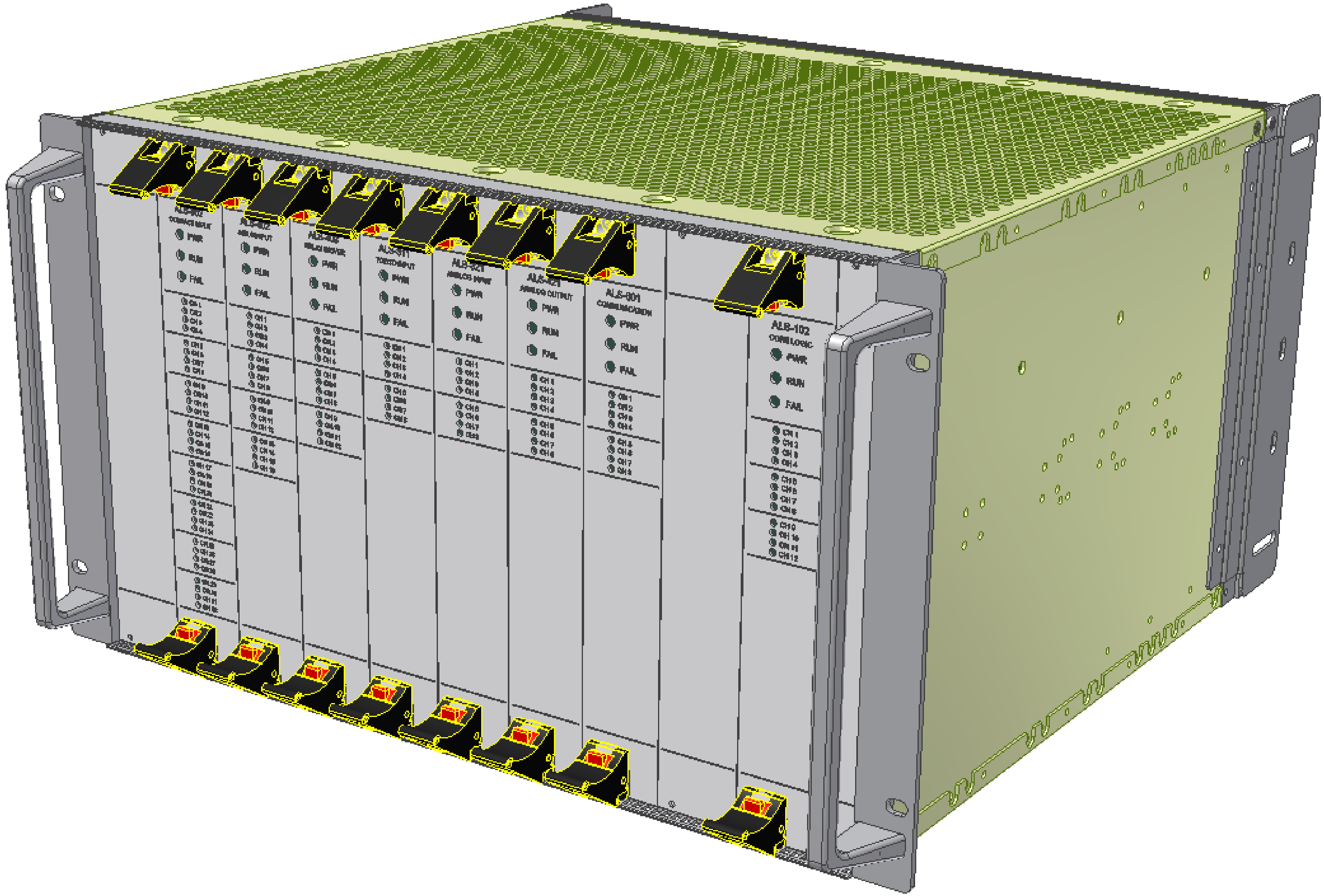
Process Protection System Overview



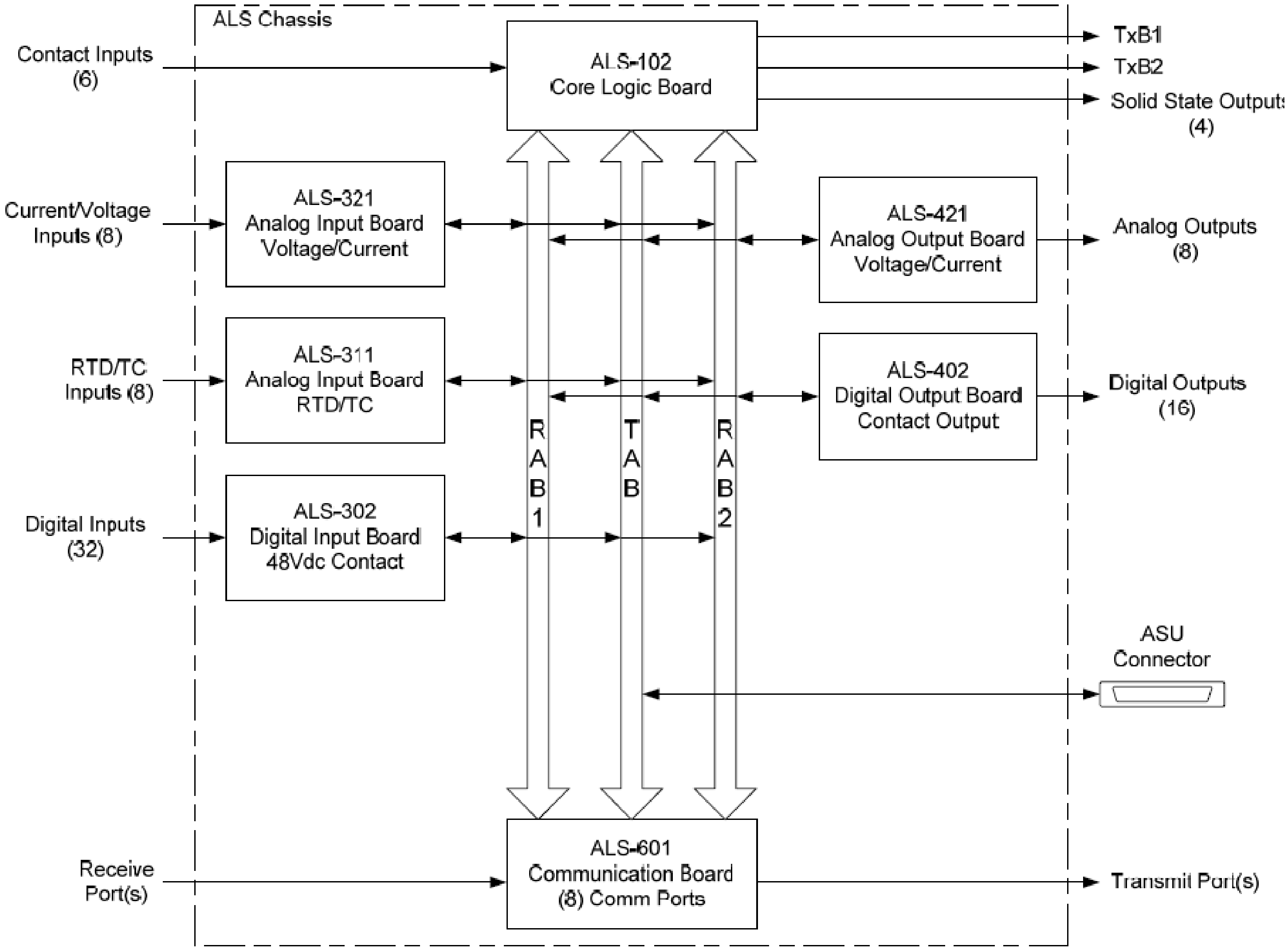
Overview of Diablo Canyon Application
PPS System Architecture



ALS Platform – Physical Representation



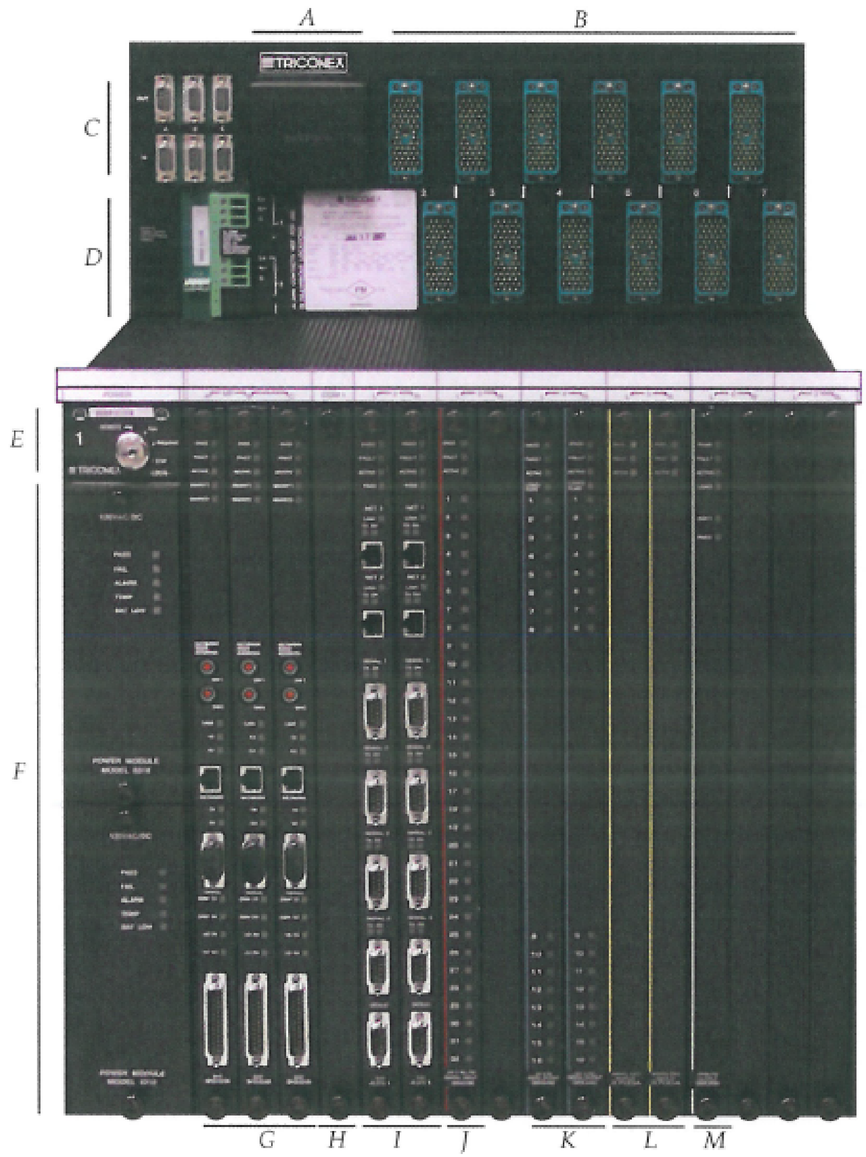
ALS Platform – Block Diagram



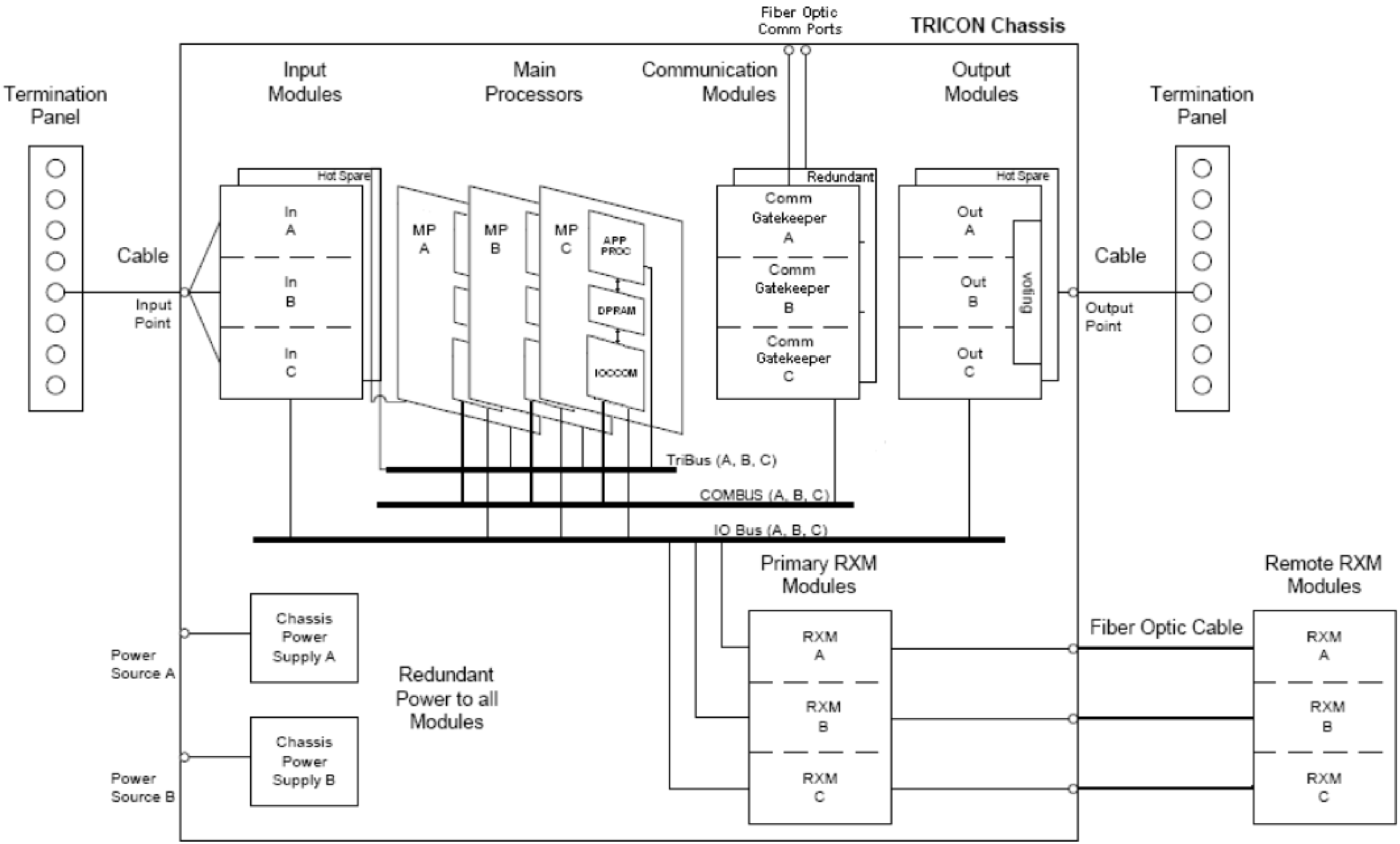
ALS Platform – Scope

- **The Approved ALS Platform**
  - Defines the architecture and internal communications approach upon which to build an I&C system
  - Specifies seven boards
  - Specifies all board functionality and functional allocation to programming (with the exception of the application-specific logic of the "Core Logic Board," ALS-102)
  - Uses diversity attributes to create two-design variants of each board
  - Establishes the development process for the boards, their programming, and verification and validation
  - Establishes qualification boundaries for the platform and design features to support implementation of safety functions for a plant's application-specific system

Populated Tricon V10 Chassis



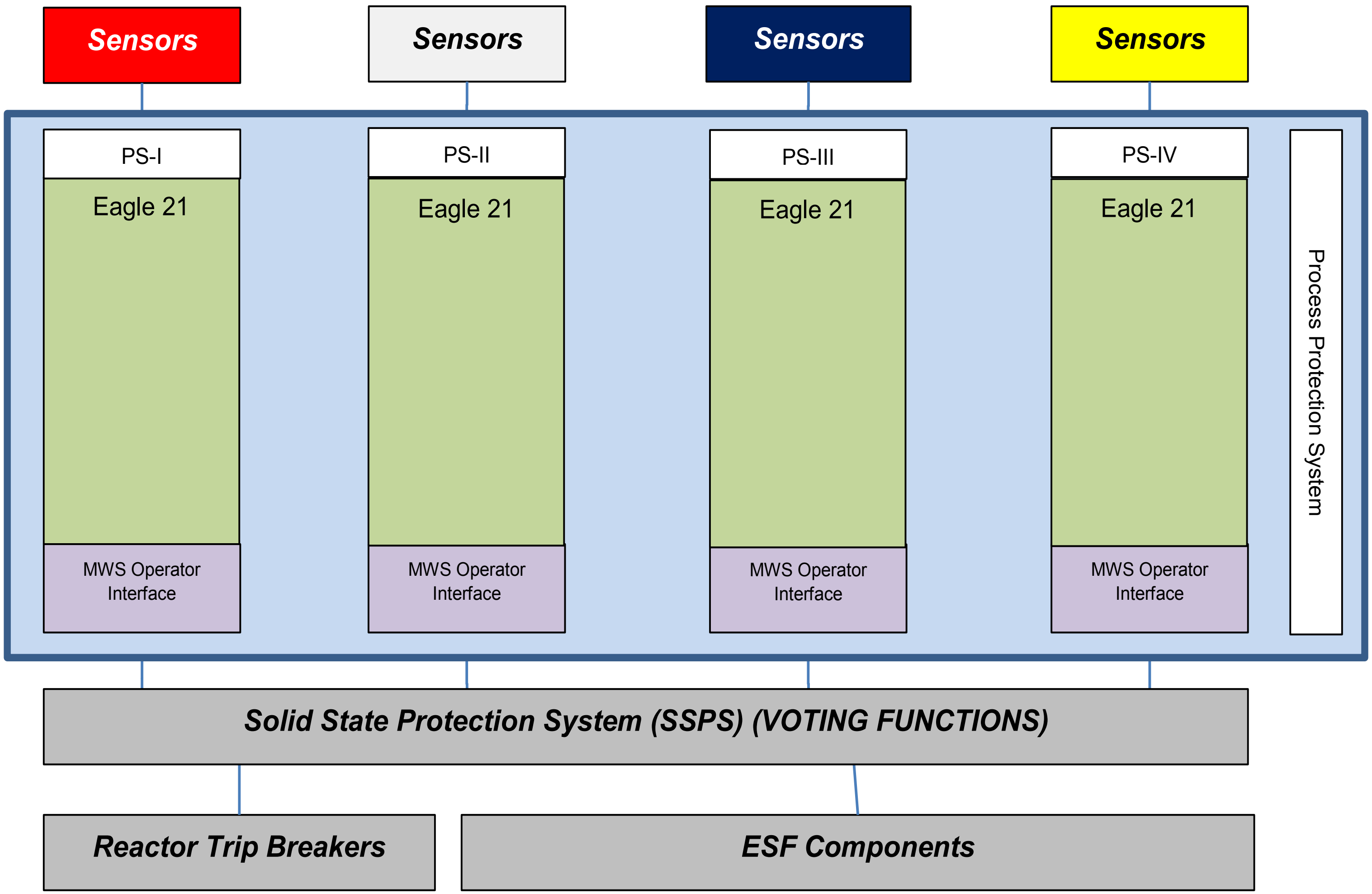
TRICON V10 Block Diagram



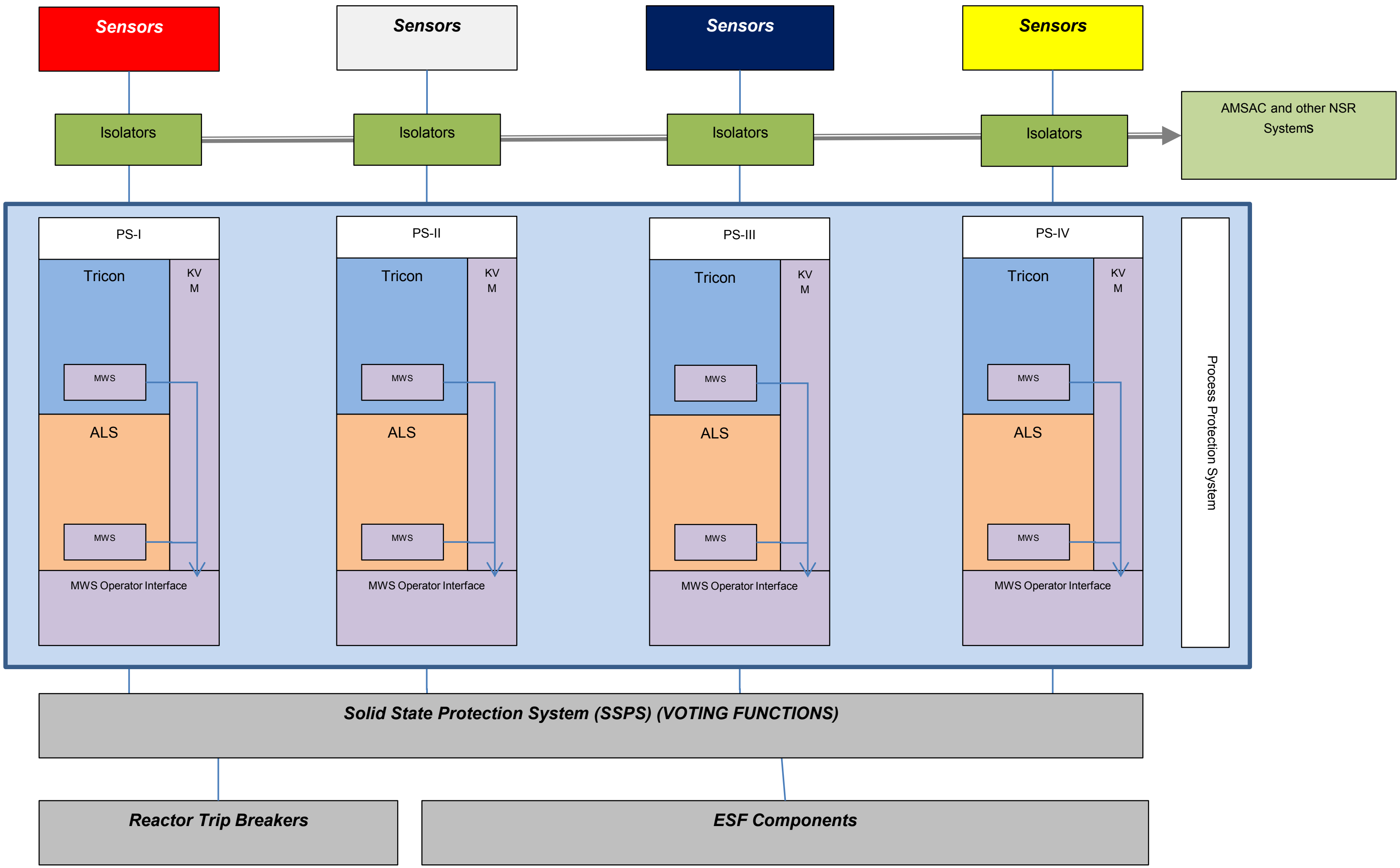
TRICON Platform – Scope

- **The Approved Tricon V10 Platform**
  - Reviewed against the SRP with emphasis on areas of change
  - New MP3008 main processor and TCM communications module
  - Establishes guidance on communications and compliance with ISG 4
  - Establishes the development process for the boards, their programming, and verification and validation
  - Establishes qualification boundaries for the platform and design features to support implementation of safety functions for a plant's application-specific system

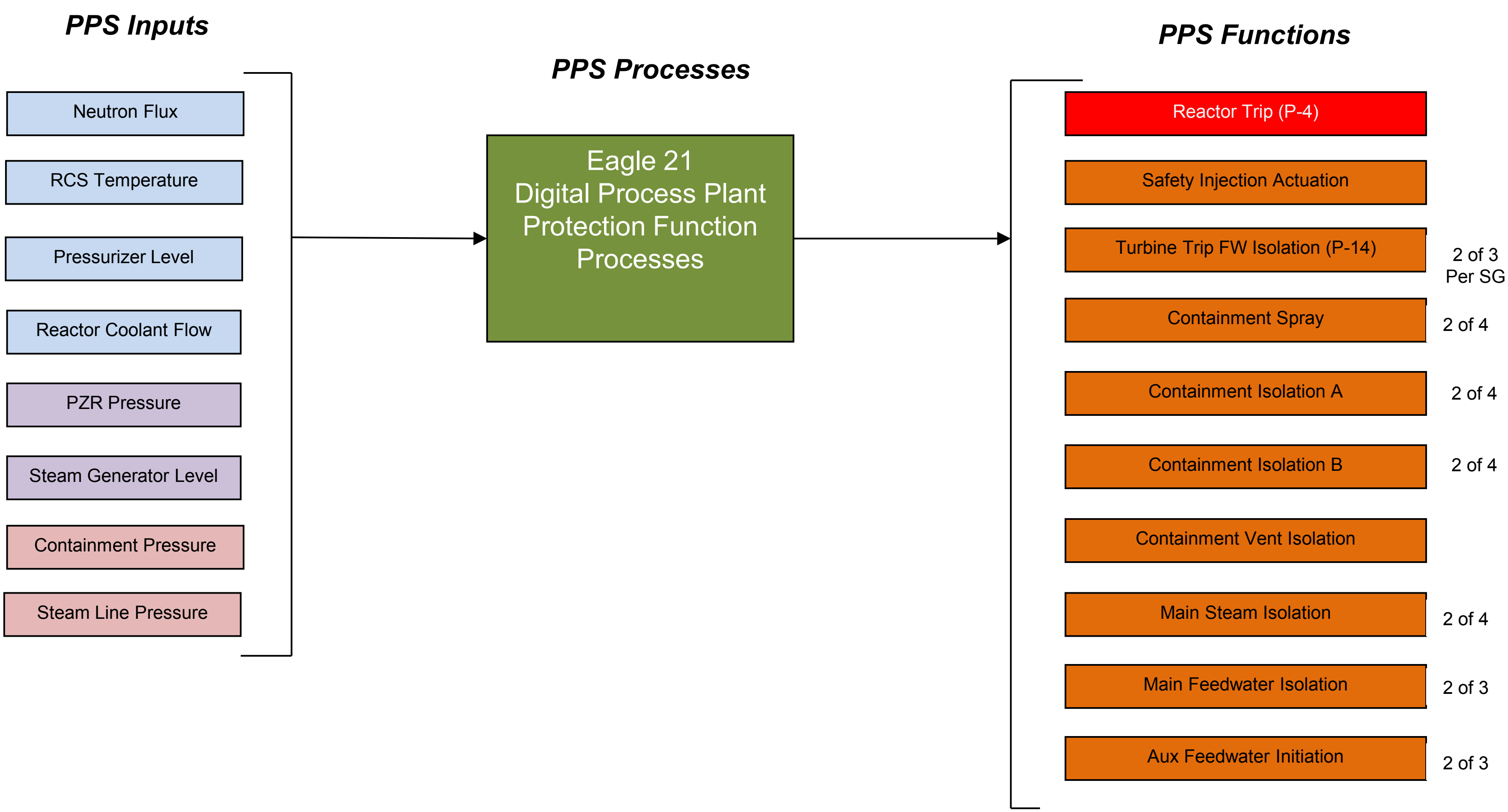
Overview of Diablo Canyon Application
PPS System Architecture



Overview of Diablo Canyon Application
PPS System Architecture



Overview of Diablo Canyon Application
Current PPS System Functions



Overview of Diablo Canyon Application

New PPS System Functions

PPS Inputs

- Neutron Flux
- RCS Temperature
- Pressurizer Level
- Reactor Coolant Flow
- PZR Pressure
- Steam Generator Level
- Containment Pressure
- Steam Line Pressure

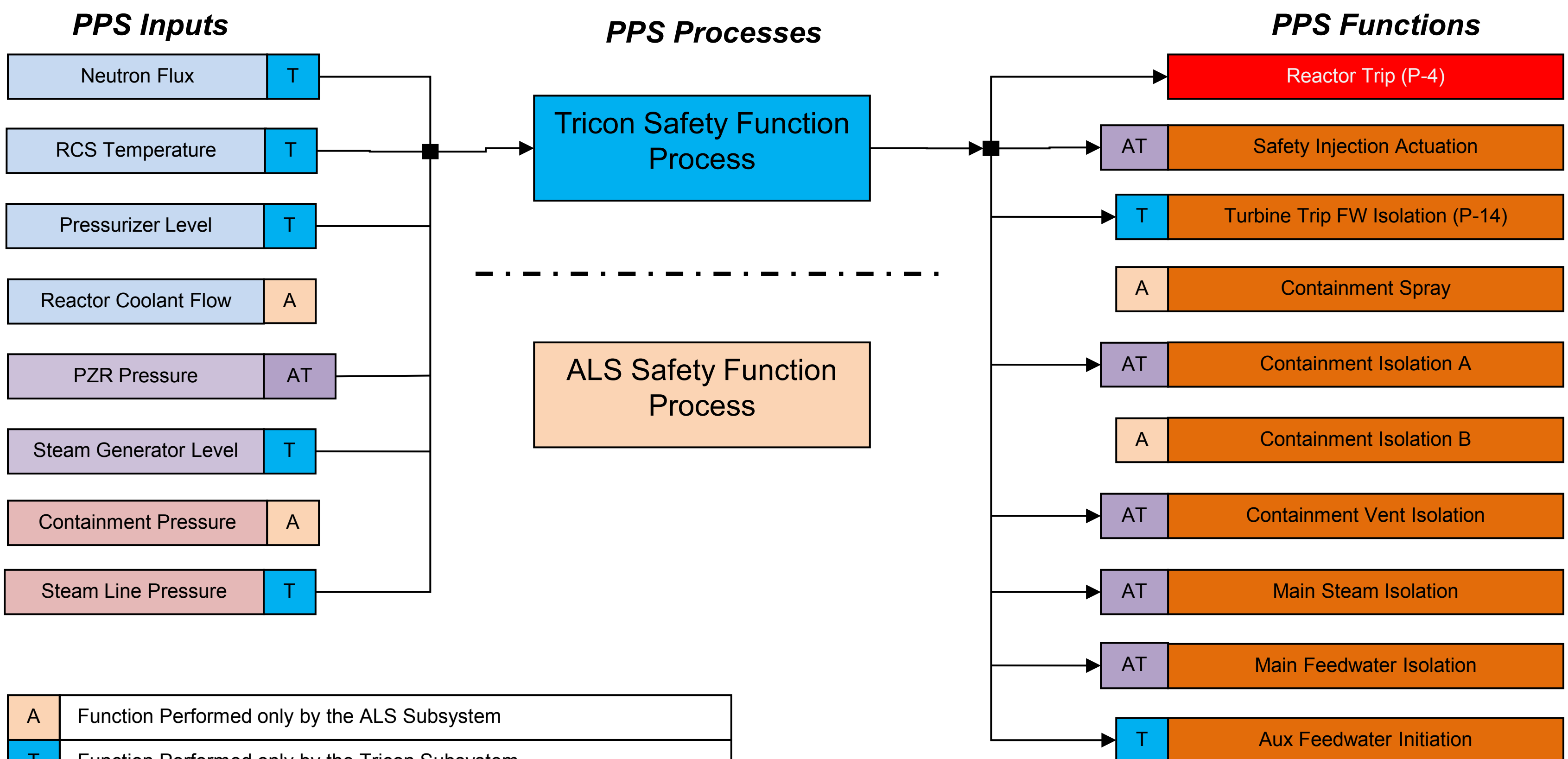
PPS Processes

- Tricon Safety Function Process
- ALS Safety Function Process

PPS Functions

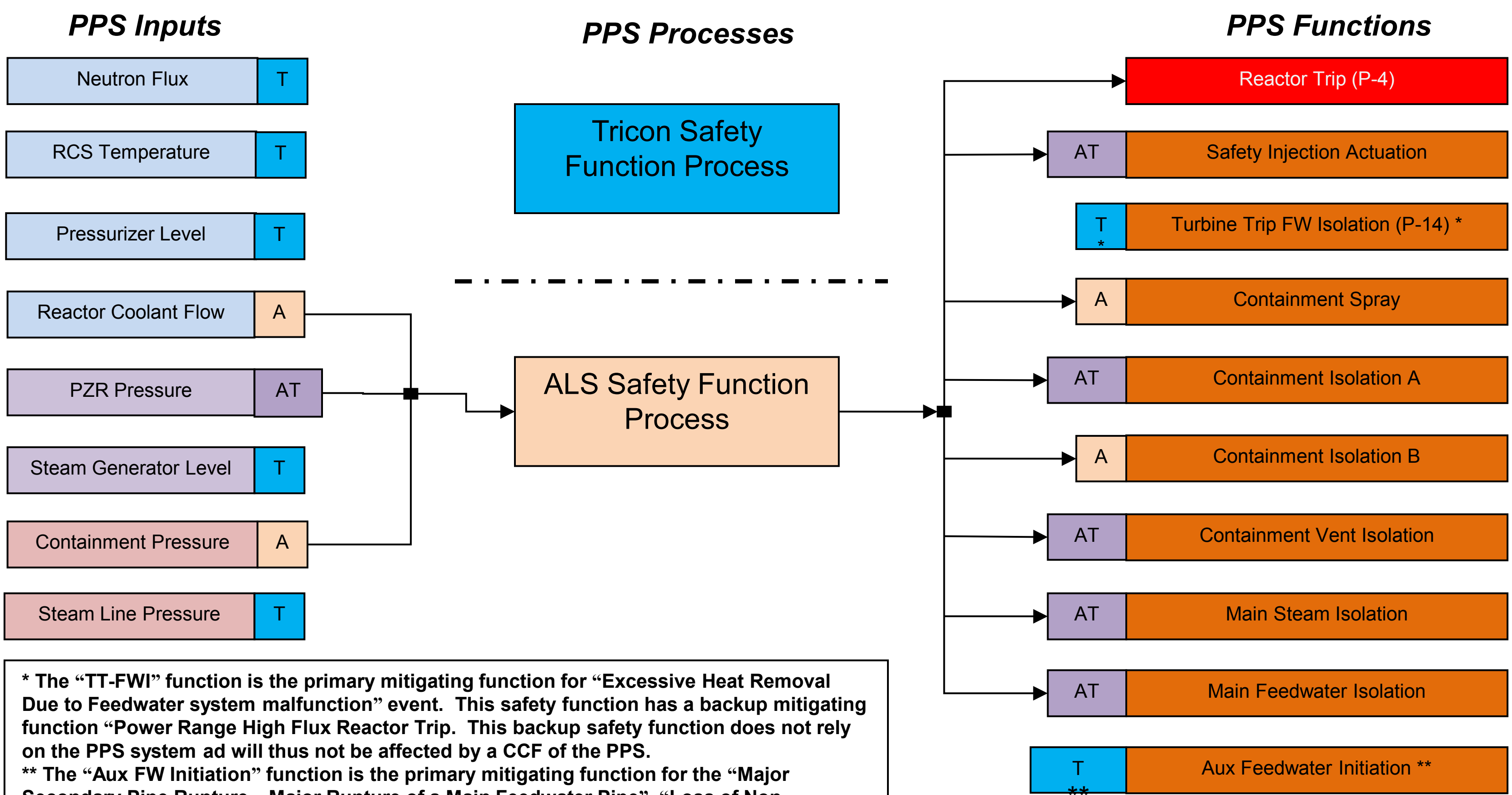
- Reactor Trip (P-4)
- Safety Injection Actuation
- Turbine Trip FW Isolation (P-14) — 2 of 3 Per SG
- Containment Spray — 2 of 4
- Containment Isolation A — 2 of 4
- Containment Isolation B — 2 of 4
- Containment Vent Isolation
- Main Steam Isolation — 2 of 4
- Main Feedwater Isolation — 2 of 3
- Aux Feedwater Initiation — 2 of 3

Overview of Diablo Canyon Application
PPS System Tricon Function Allocation



A	Function Performed only by the ALS Subsystem
T	Function Performed only by the Tricon Subsystem
AT	Function Performed by both Tricon and ALS Subsystems

Overview of Diablo Canyon Application
PPS System ALS Function Allocation



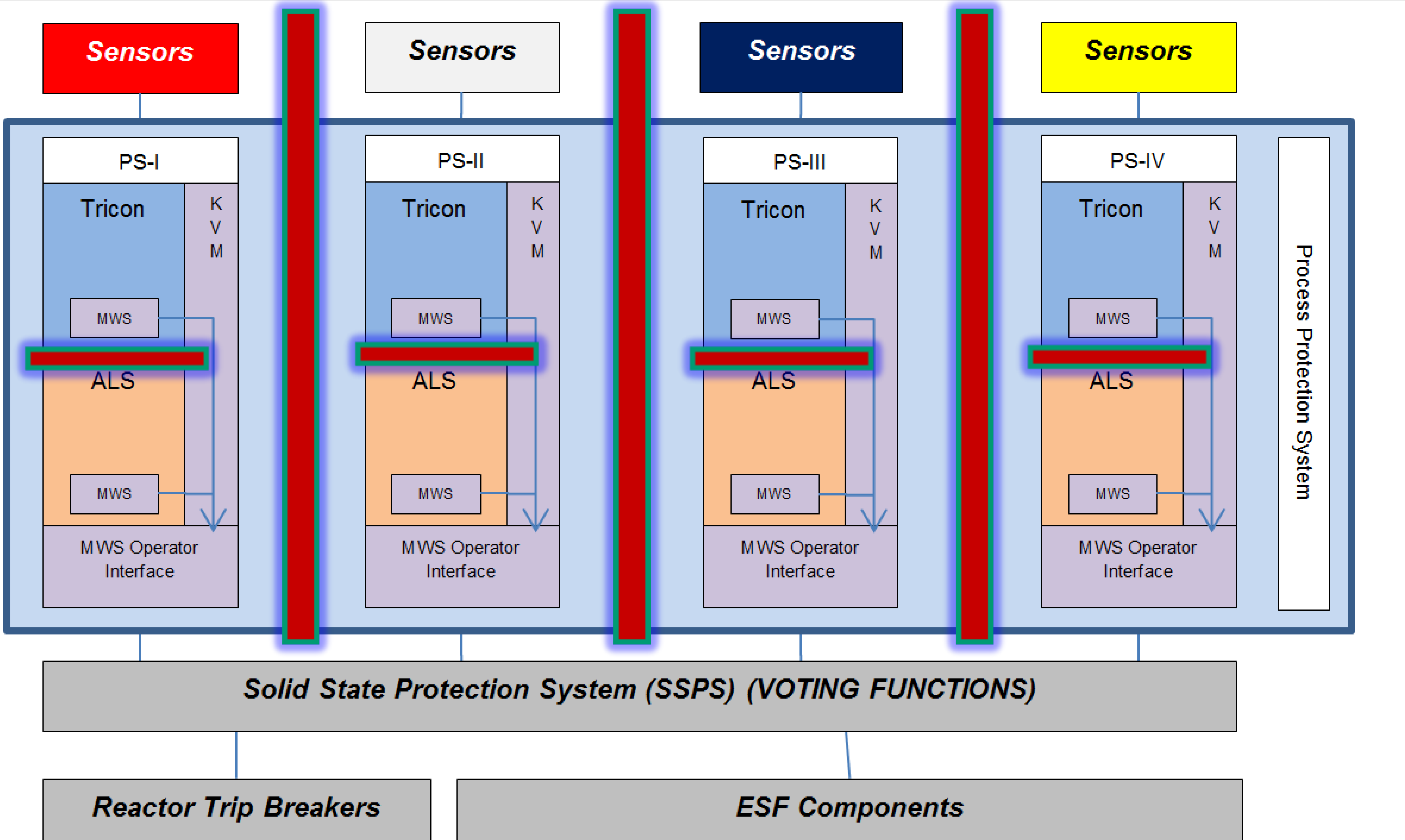
*** The "TT-FWI" function is the primary mitigating function for "Excessive Heat Removal Due to Feedwater system malfunction" event. This safety function has a backup mitigating function "Power Range High Flux Reactor Trip. This backup safety function does not rely on the PPS system ad will thus not be affected by a CCF of the PPS.**
**** The "Aux FW Initiation" function is the primary mitigating function for the "Major Secondary Pipe Rupture – Major Rupture of a Main Feedwater Pipe", "Loss of Non-Emergency AC power to station auxiliaries", "Loss of Normal Feedwater " events. This safety function has backup mitigating functions of Pressurizer High Pressure reactor trip, Safety Injection and Reactor Trip on High Containment Pressure. Both of these backup mitigating safety functions do not rely upon the PPS and will thus not be affected by a CCF of the PPS.**

Communications

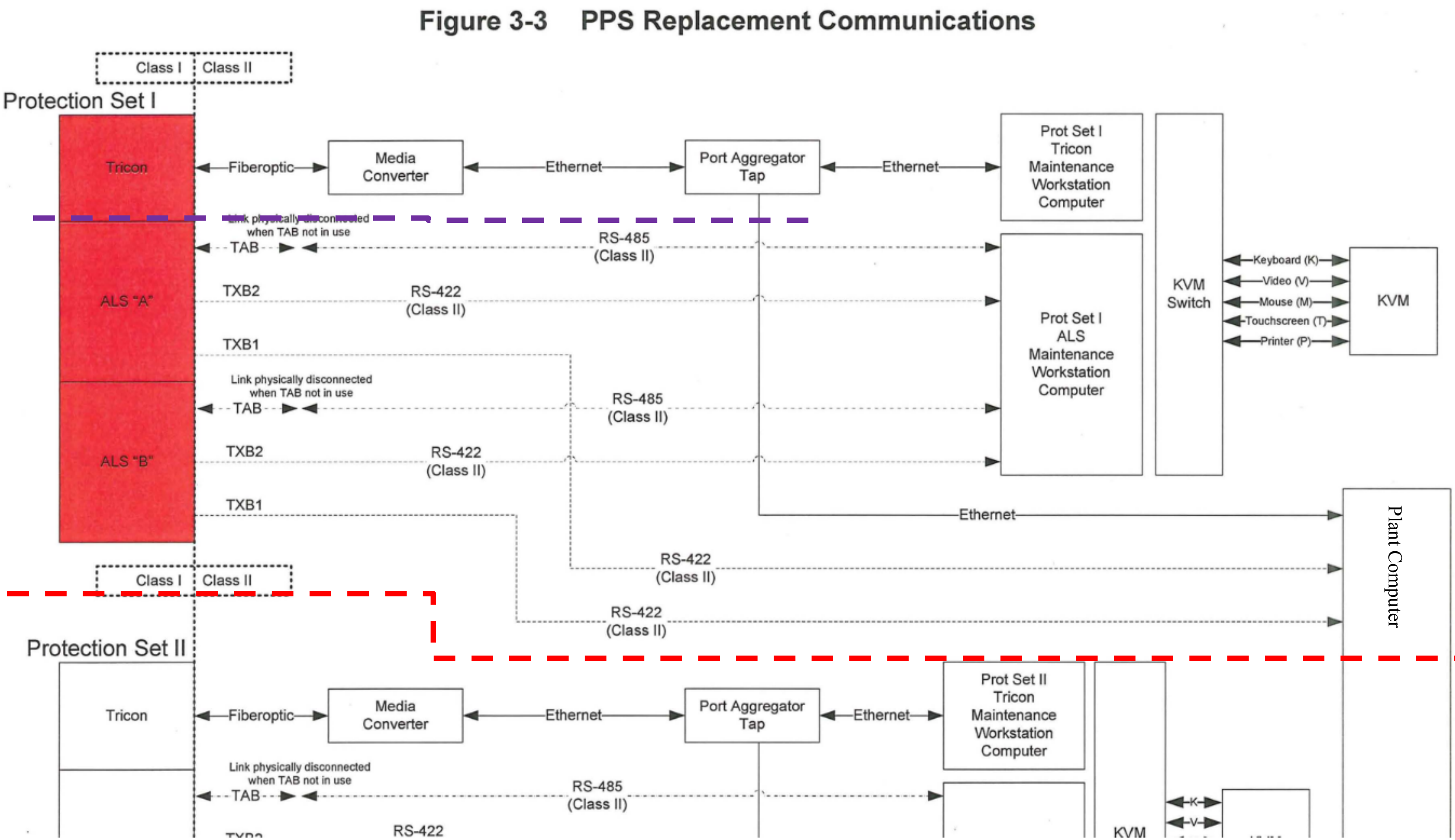
Communication
Guidance

- **Guidance for Communication**
  - IEEE 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”
  - IEEE 7-4.3.2, “Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Station”
  - DI&C-ISG-04, “Highly Integrated Control Rooms-communication Issues”

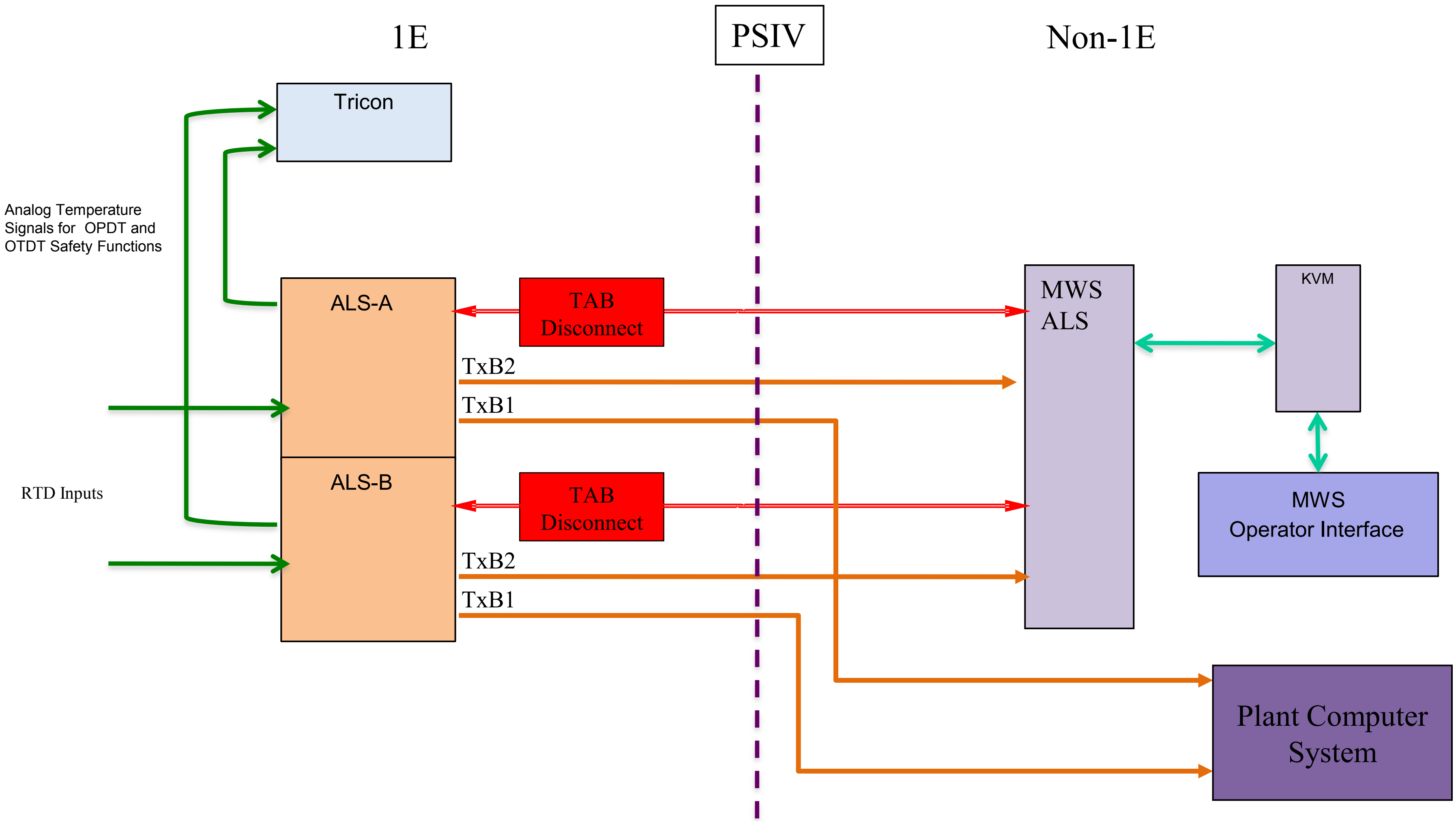
Overview of Diablo Canyon Application
PPS System Architecture



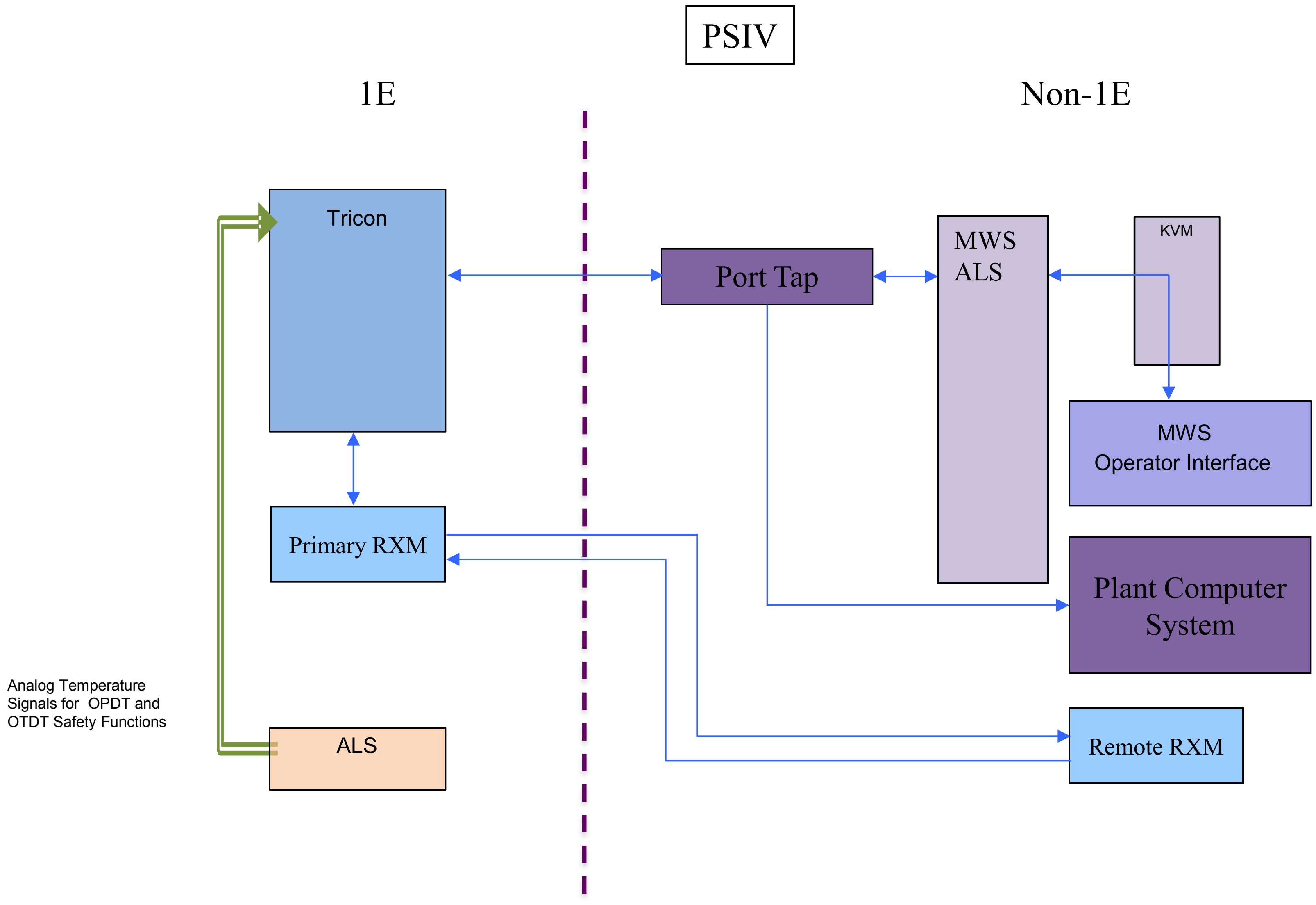
Communications Architecture



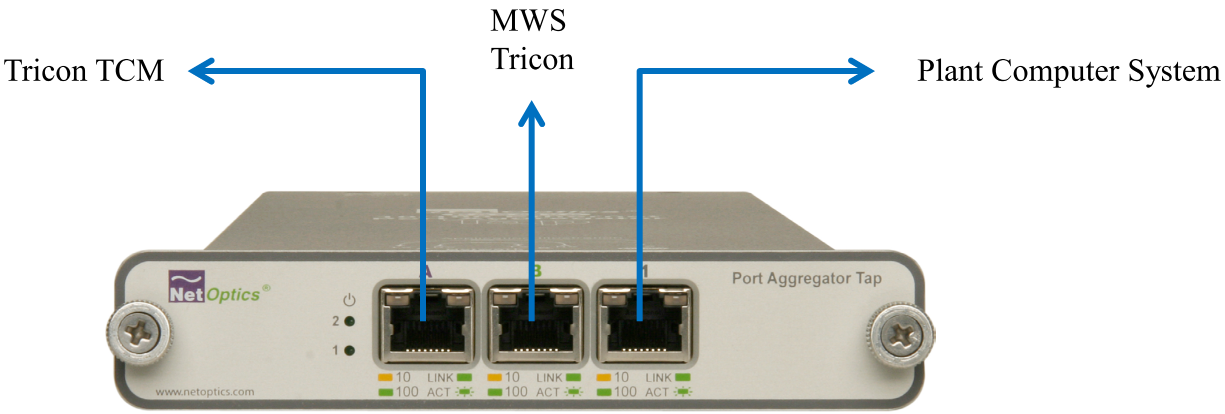
Overview of Diablo Canyon PPS Application
ALS Communication Architecture

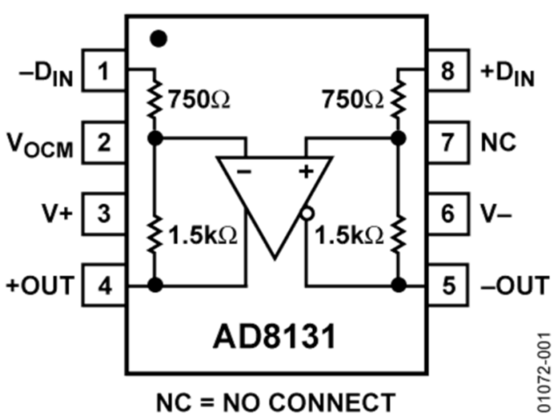


Overview of Diablo Canyon PPS Application
Tricon Communication Architecture



Port Aggregator Tap

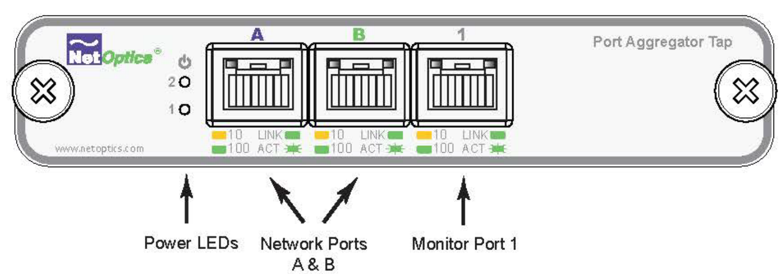




NetOptics®

10/100 Port Aggregator Tap

Product Diagrams



Overview of Diablo Canyon PPS Application
Tricon Input/Output Signals

Remote RXM Chassis
I/O Signals

INPUT:

- OTDT / OPDT Interlock Manual Trip Switches
- Power Supply Failure Relays

OUTPUT:

- Delta T Indicator
- Over Power Setpoint Indicator
- Over Temperature Setpoint Indicator
- T average Indicator
- OTDT and OPDT Interlock Signals
- Various System Alarms to Main Annunciator System (MAS)

Diversity & Defense-In-Depth

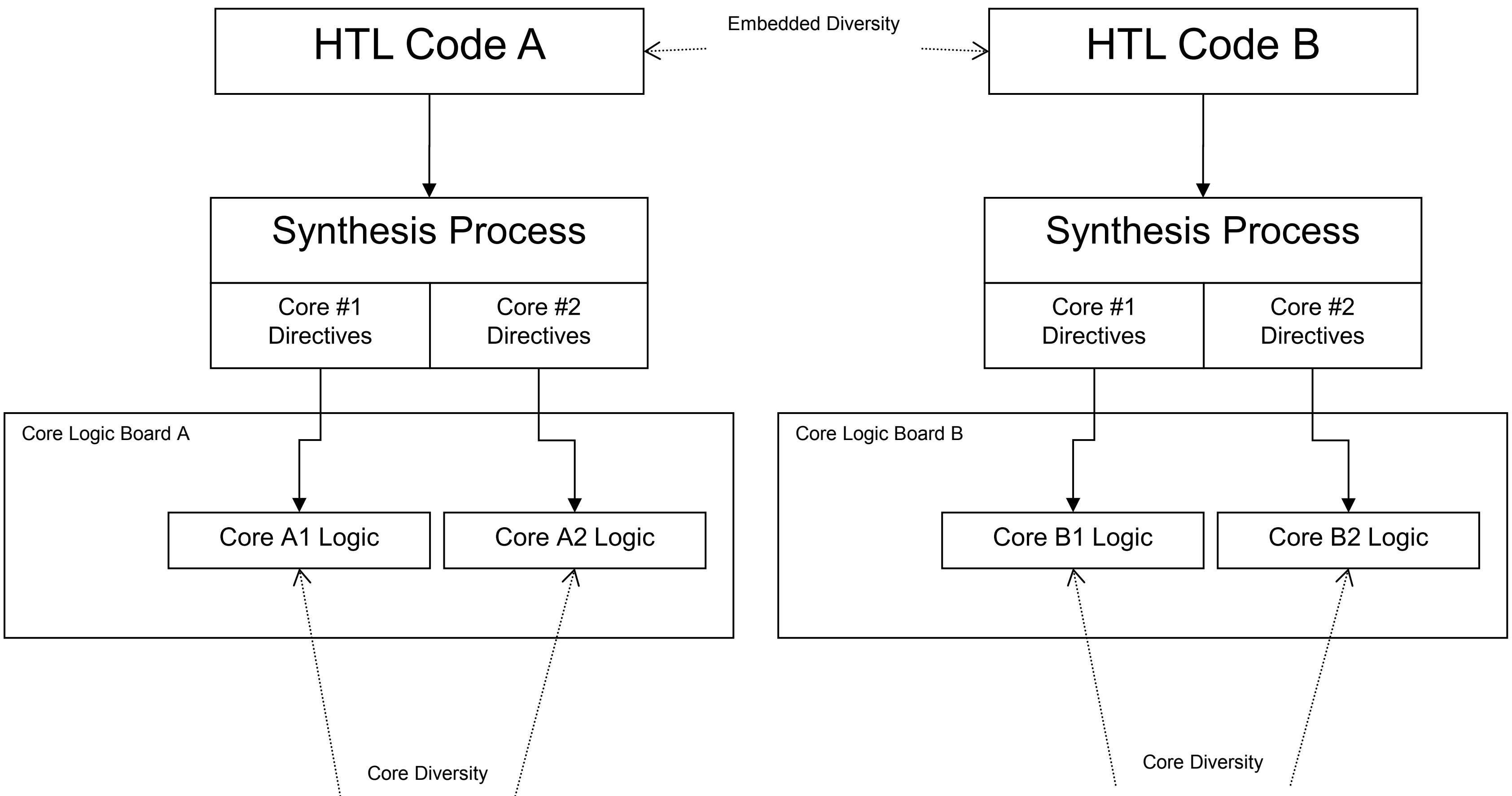
Diversity and Defense in Depth (D3)
Guidance

- **Guidance for Diversity Assessment**
  - **SRM to SECY-93-087 Item II.Q**
    Establishes NRC policy for Diversity and Defense in Depth
    - **NUREG/CR-6303**
      Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems
    - **Branch Technical Position (BTP) 7-19**
      Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems
    - **Interim Staff Guide (DI&C-ISG-02)**
      Diversity and Defense-in-Depth Issues

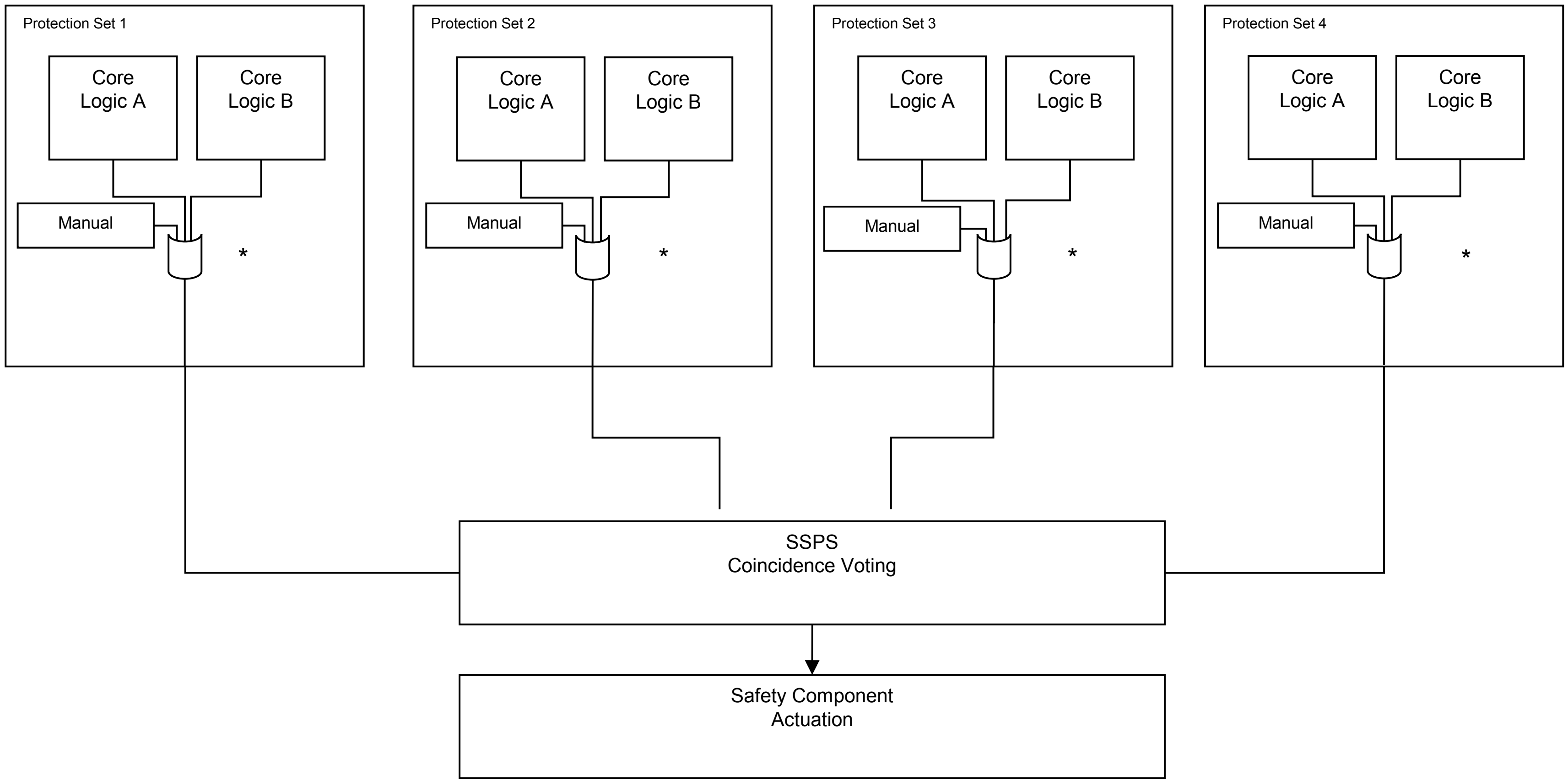
Diversity and Defense in Depth (D3)
Analysis Preformed by Licensee

- **Diversity and Defense-In-Depth Analysis Performed**
  - **Eagle 21 (1993)**
    Assumed CCF of PPS resulting in loss of all PPS safety functions
  - **Replacement PPS System (2011)**
    Assumed loss of all Functions performed by the Tricon Subsystem.
    - Update to Previous Analysis Tables
    - All plant Accidents and AOO's are included in the analysis
    - Three Parameters identified for which there is no existing Automatic Diverse Backup function.
      - Pressurizer Pressure
      - Containment Pressure
      - RCS Flow
    - Describes ALS Diversity and postulates CCF of ALS. This CCF does not result in loss of ALS assigned Safety functions

Diversity and Defense in Depth
Diablo Canyon Diversity Solution

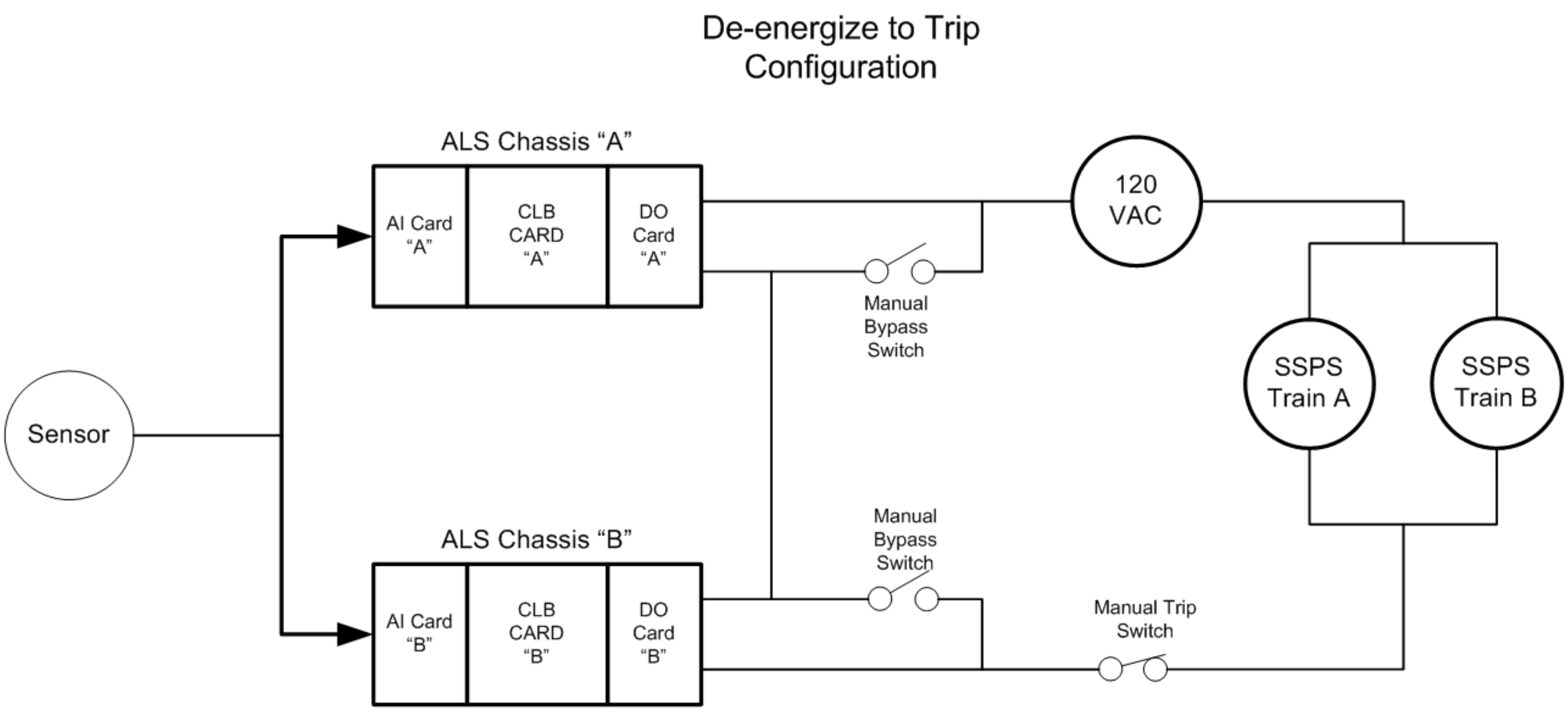


Diversity and Defense in Depth
Diablo Canyon Diversity Solution

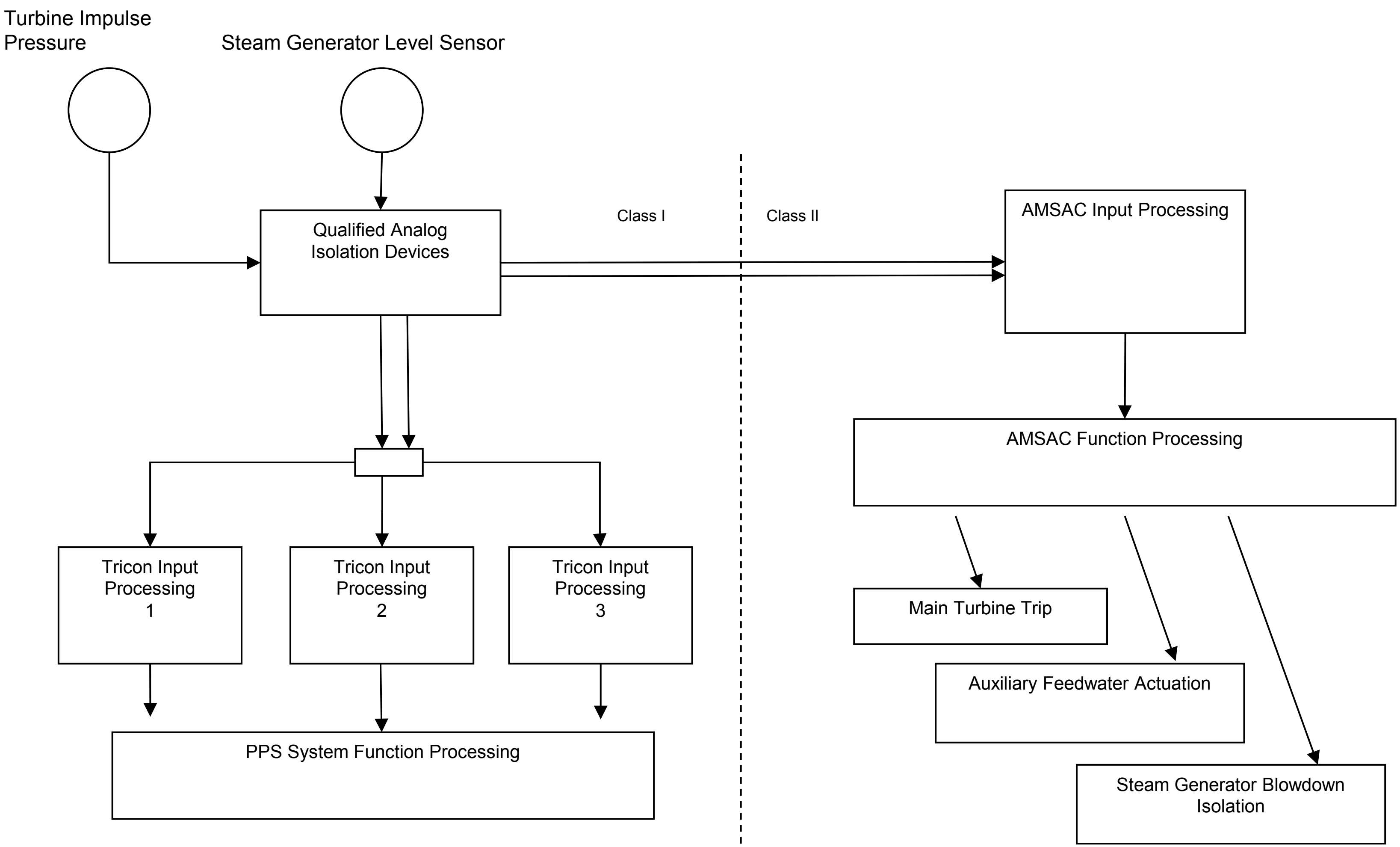


* OR function is accomplished by DO contacts in series for De-energize To Trip (DTT) or in parallel for Energize To Trip (ETT) function.

Diversity and Defense in Depth
Diablo Canyon Diversity Solution



Diversity and Defense in Depth
Anticipated Transient Without Scram (ATWS)



Diversity and Defense in Depth
Anticipated Transient Without Scram (ATWS)

- **Diverse Attributes**
  - Different architectures
  - Different vendors
  - Different microprocessors produced by different manufacturers
  - Different Electrical Power source
  - Initiation path is separate and independent from the PPS

- **Interface Features of AMSAC and PPS**
  - Shared Sensors are not digital devices and are not subject to the effects of a software CCF.
  - Input signals are isolated using qualified isolation devices
  - The AMSAC output actuation signals are transmitted through relays that provide isolation between the safety-related control circuits actuated by AMSAC and the non-safety related AMSAC system.

Diversity and Defense in Depth
Manual Operator Action

- The new Diablo Canyon Digital Process Protection System reduces reliance on Manual Operator Actions as a means of coping with a software CCF within the PPS.
- The modification does not however affect the ability of operators to perform manual actuations of safety functions.
  - Manual Initiation signals are provided directly to the SSPS system which is not being modified.
  - Previously credited MOA's will still be available to the operators.
  - Existing component and division level actuation capability at the main control boards will be retained

Secure Development and Operational Environment

Secure Development and Operational Environment (SDOE)

- **Guidance for SDOE**
  - **RG 1.152, Rev. 3, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”**

- A secure development environment must be established to ensure unwanted, unneeded, and undocumented functionality is not introduced into a digital safety system

- A secure operational environment must be established to ensure predictable, non-malicious events will not degrade the reliable performance of the safety system

Secure Development Environment

- The secure development environments for the ALS and Tricon platforms were reviewed as part of their respective Topical Report reviews and were found to be acceptable

- The same development environments are being maintained for the DCPP PPS replacement application

- These development environments include:
  - Vulnerability assessments
  - Physical and logical access control of the development infrastructure
  - Control of portable media
  - Configuration Management of documentation and source code files

- Code reviews to detect and prevent the use of unintended code or functions

- The licensee will not develop or modify the software

Secure Operational Environment (Control of Access)

- Once the PPS replacement project is completed and the PPS is in the Operations and Maintenance phases, software modifications to the Tricon and ALS platforms will be controlled by the PPS Replacement Software Configuration Management Plan

- Modifications to the PPS replacement components produced by the vendors will be performed by the vendors, not the licensee

- The PPS replacement system will be located in a plant vital area
  - In the cable spreading room
  - In the same cabinets that currently house the Eagle-21 PPS
  - These cabinets are locked and the keys are administratively controlled by operations personnel
  - Access to the MWSs is password protected

Deterministic Performance of PPS

PPS Deterministic Performance Characteristics

- Deterministic performance characteristics for each platform were evaluated and accepted by the NRC as part of the associated platform safety evaluation.
  - Each SE considered the following system characteristics;
    - Input and Output Signal Processing
    - Data Transfer Methods / Techniques
    - Software or Logic Implementation Structure
    - System Diagnostic functions
  - The NRC is also evaluating Application Specific Characteristics of the PPS such as;
    - System loading
    - Application architecture

ALS Deterministic Performance Characteristics

- No Embedded Microprocessor Cores
- FPGA Design Does not use Interrupts
- Deterministic sequence of performing logic operations:
    1. Acquire Inputs
    2. Perform Logic Operations
    3. Generate Outputs

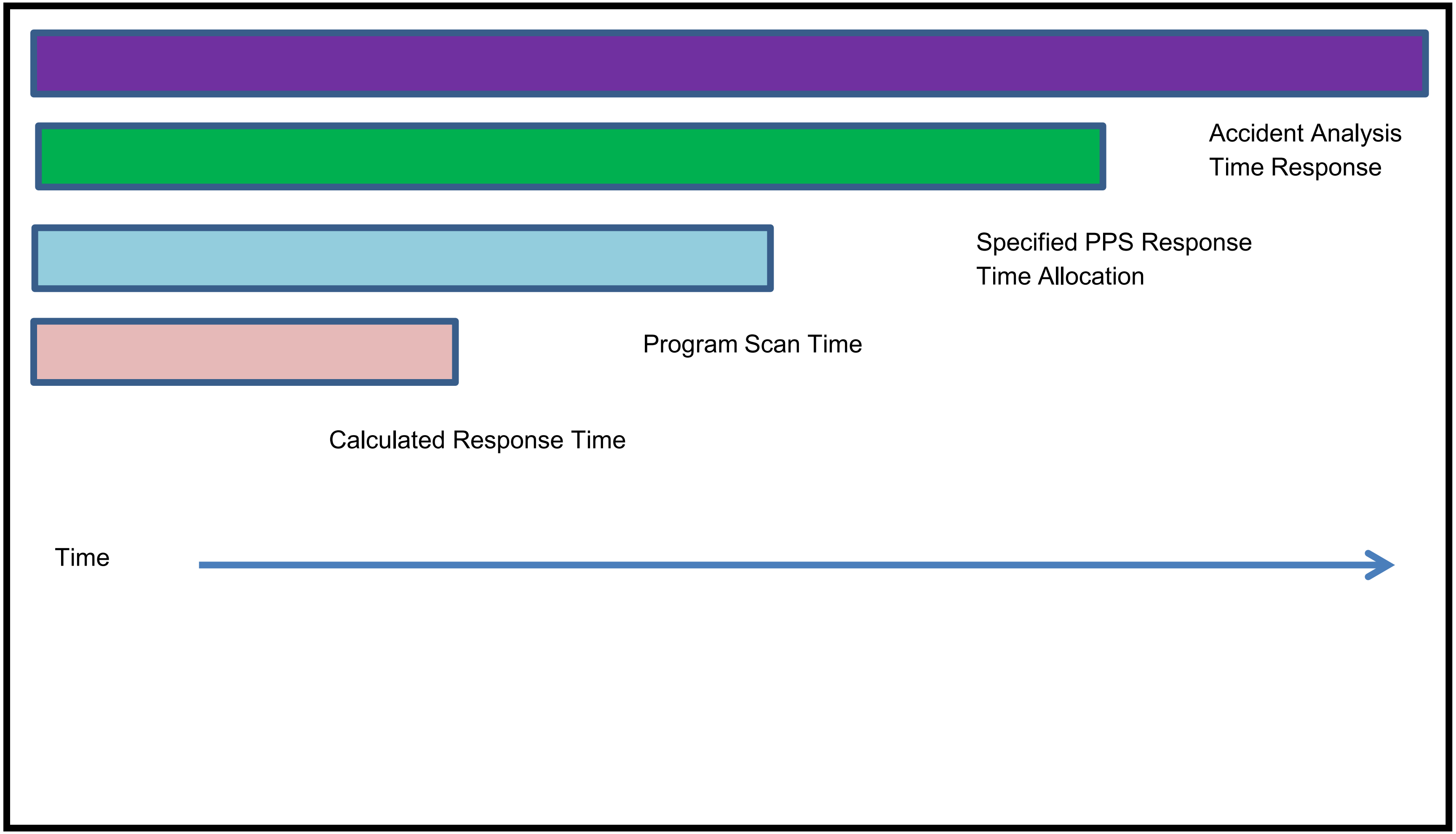
Tricon
Deterministic Performance Characteristics

- The Tricon application program (calculational cycle) cannot be interrupted by any of the lower priority tasks during the program execution cycle.

- Actual processing time is established during program development.

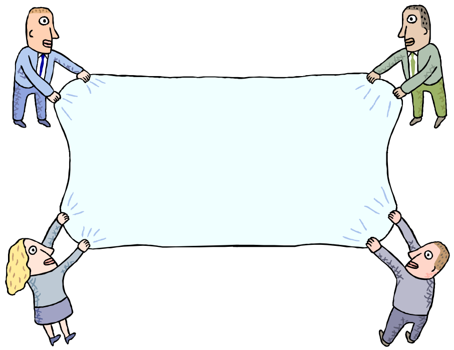
- Once application program development is complete, the cycle time does not vary as a function of calculational loading of the system.

Tricon
Deterministic Performance Characteristics



Summary

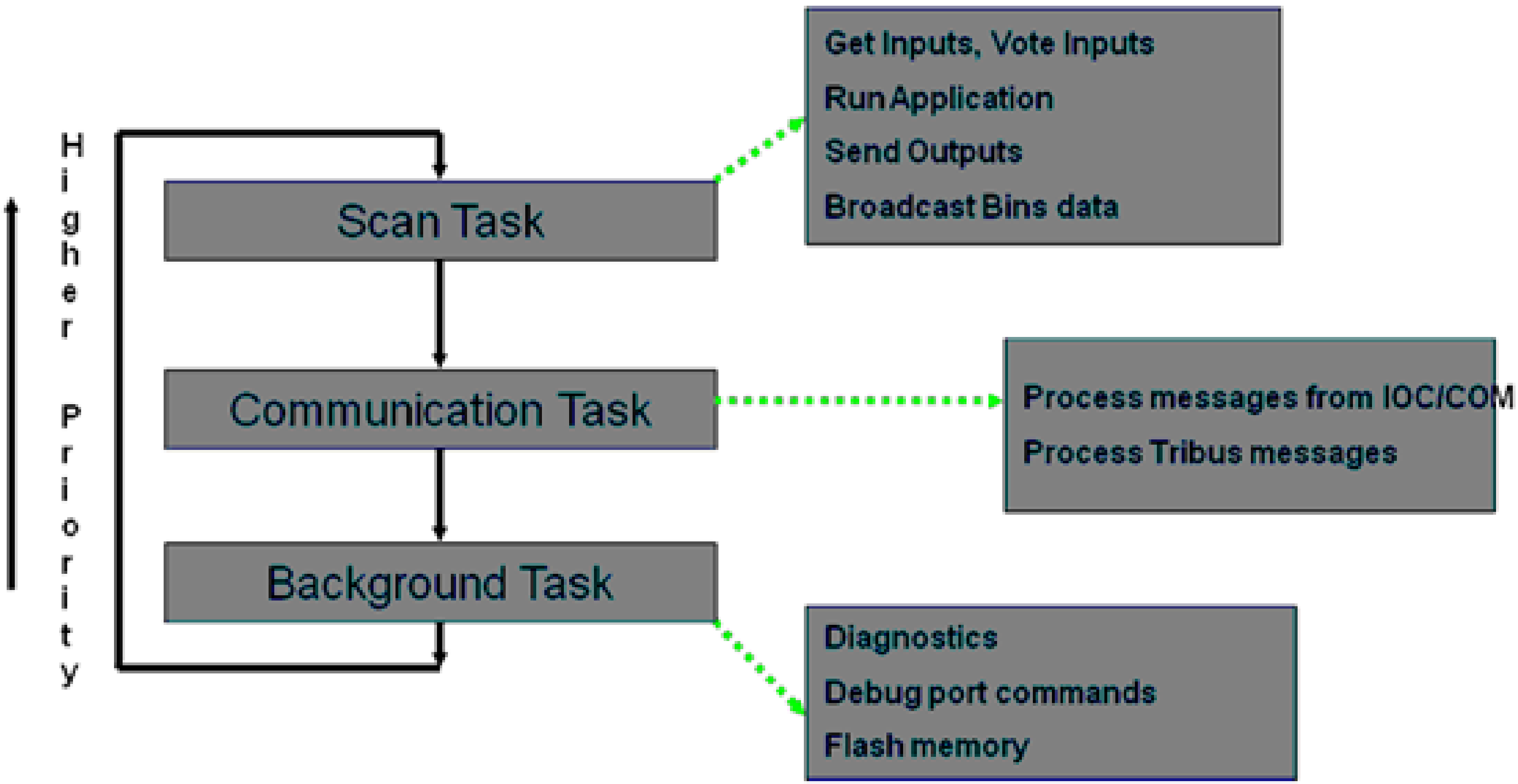
Backup Slides



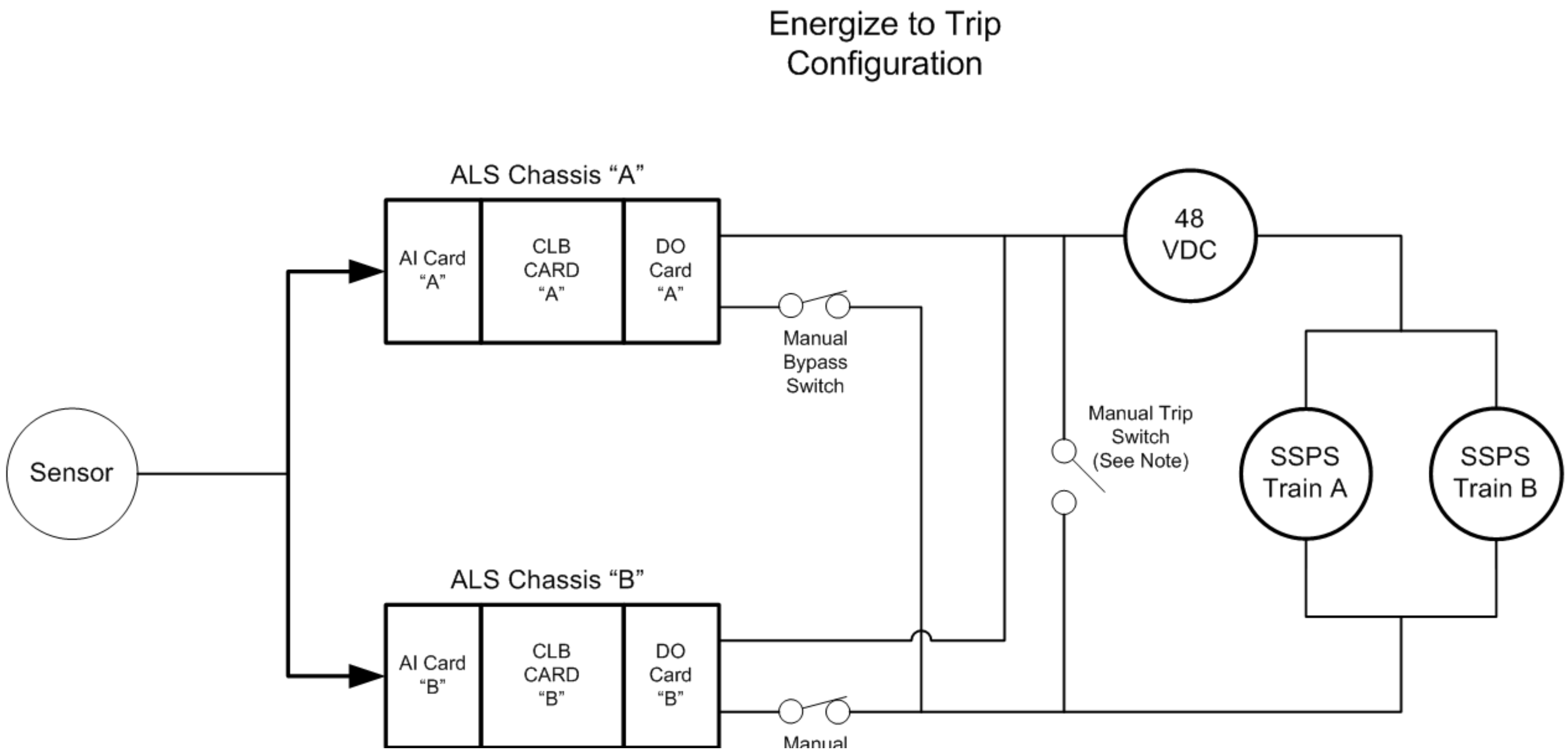
Tricon
Deterministic Performance Characteristics

ATTACHMENT 6

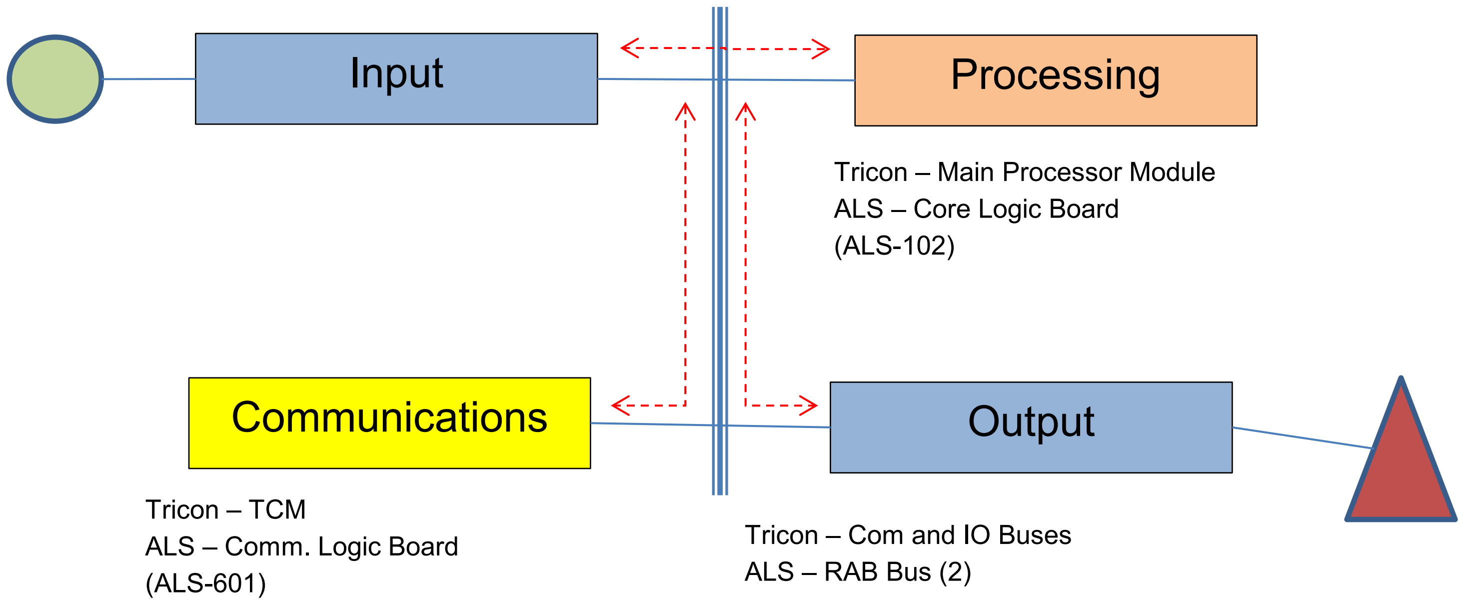
INVENSYS RESPONSE TO RAI No. 6



Diversity and Defense in Depth
Diablo Canyon Diversity Solution

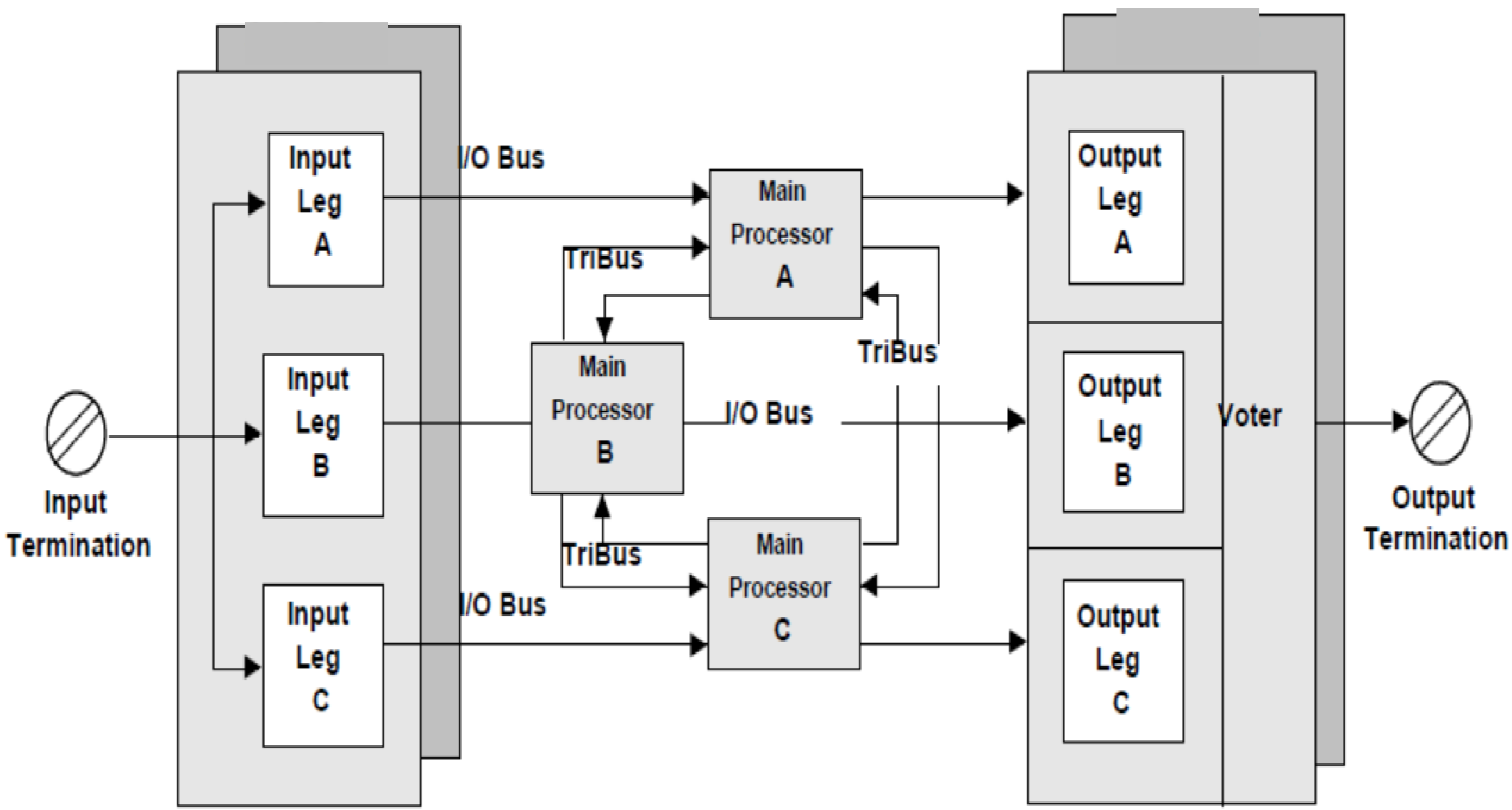


PPS Deterministic Performance Characteristics

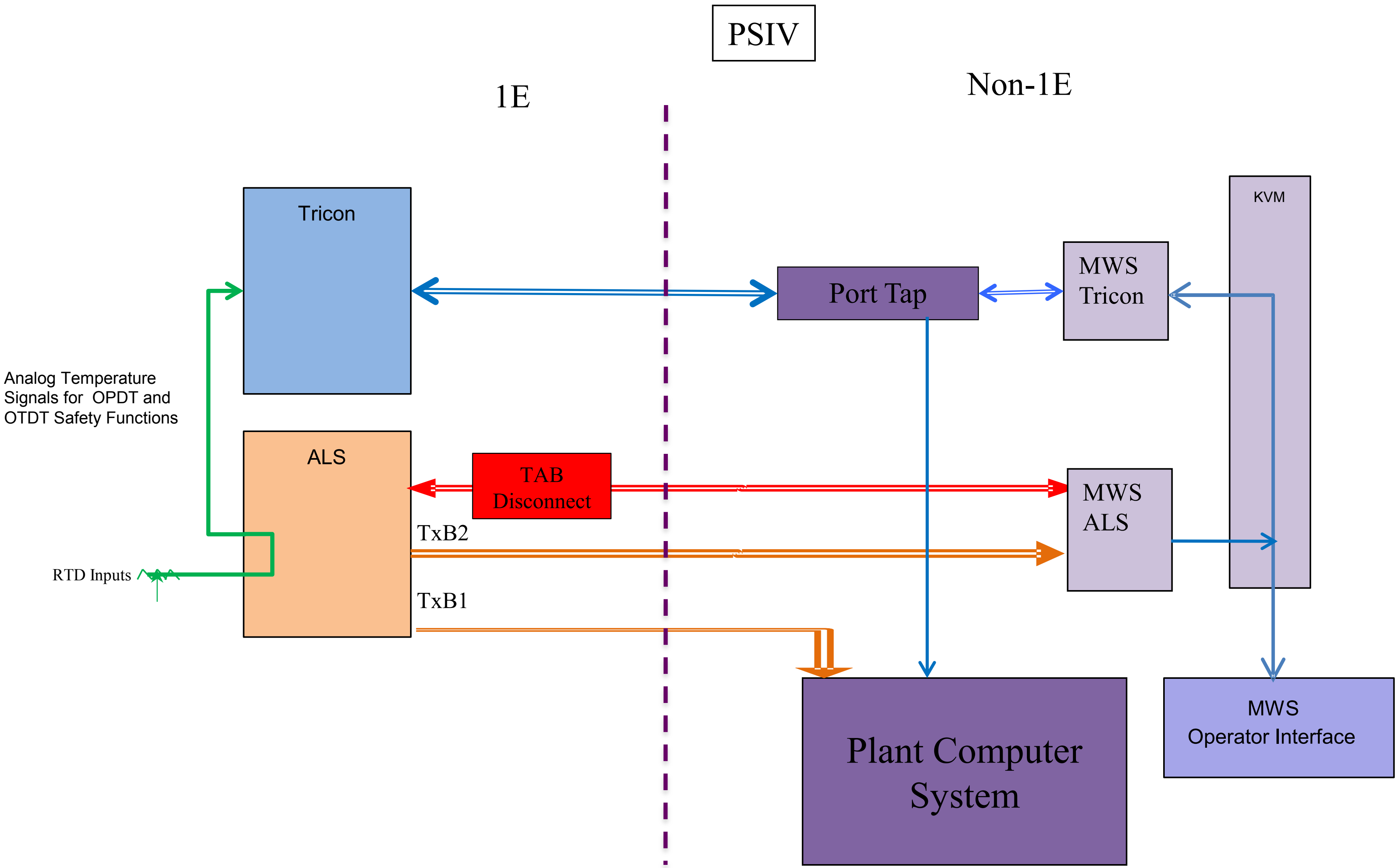


Diversity and Defense in Depth

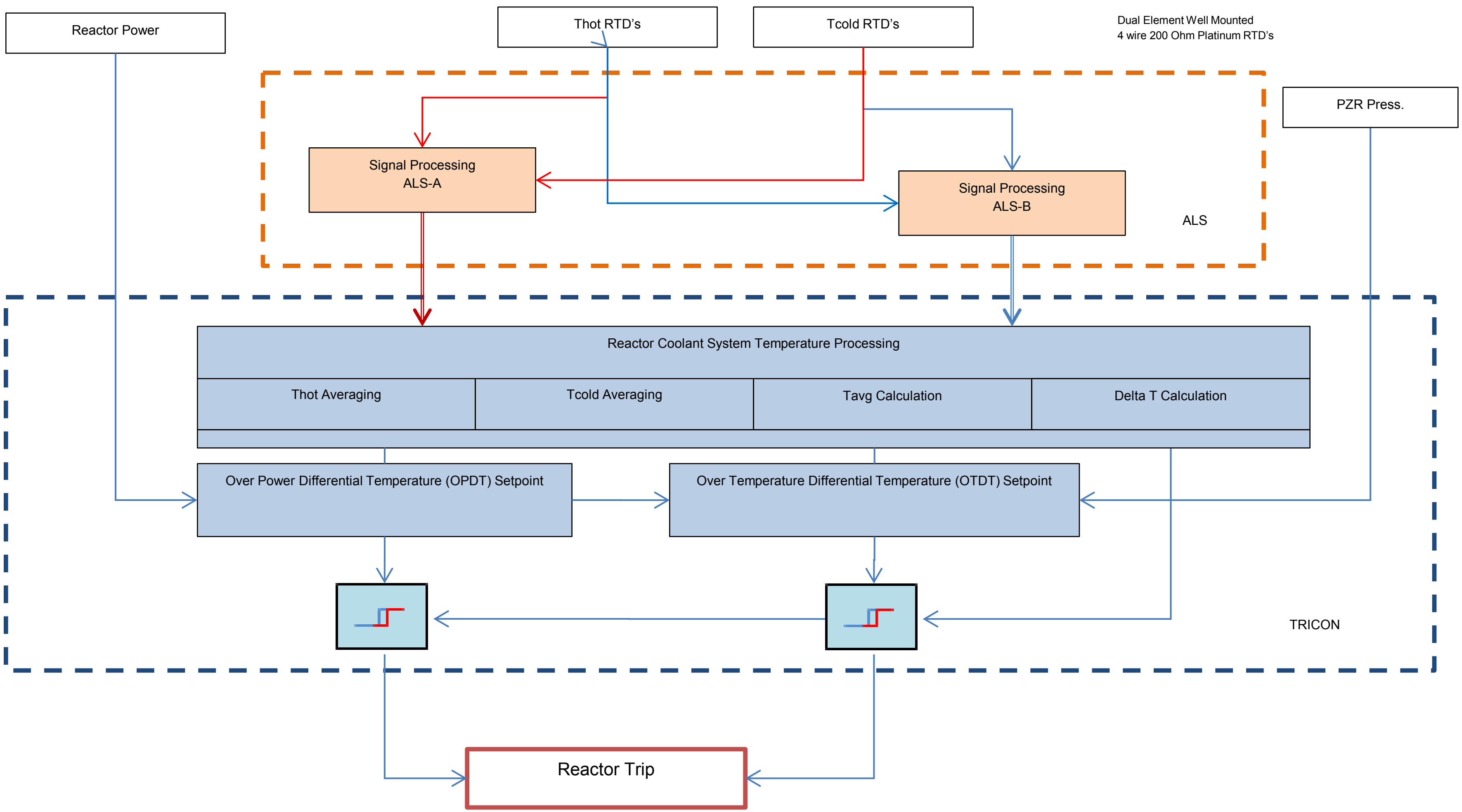
Diablo Canyon Diversity Solution



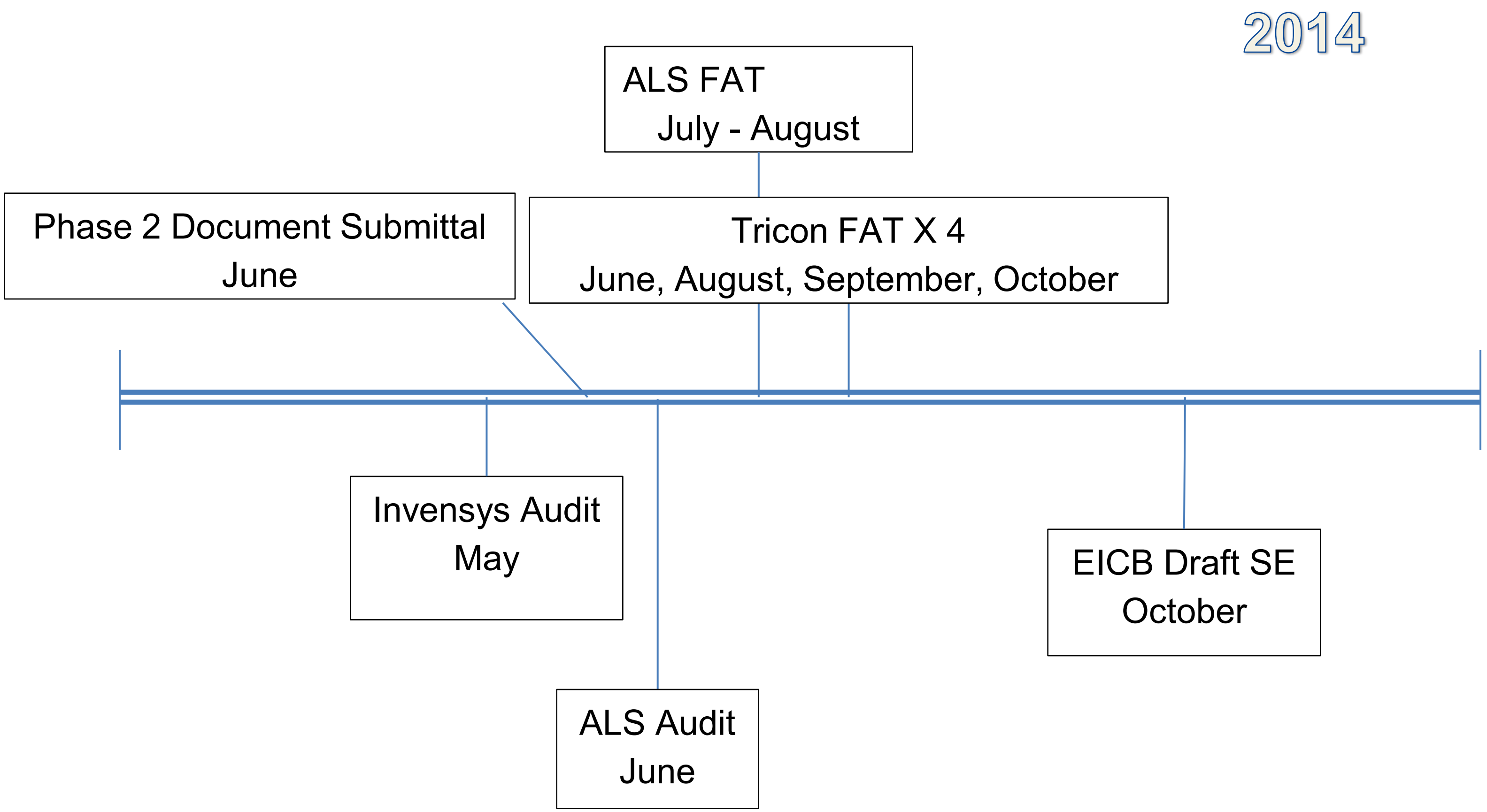
Overview of Diablo Canyon PPS Application
PPS Communication Architecture



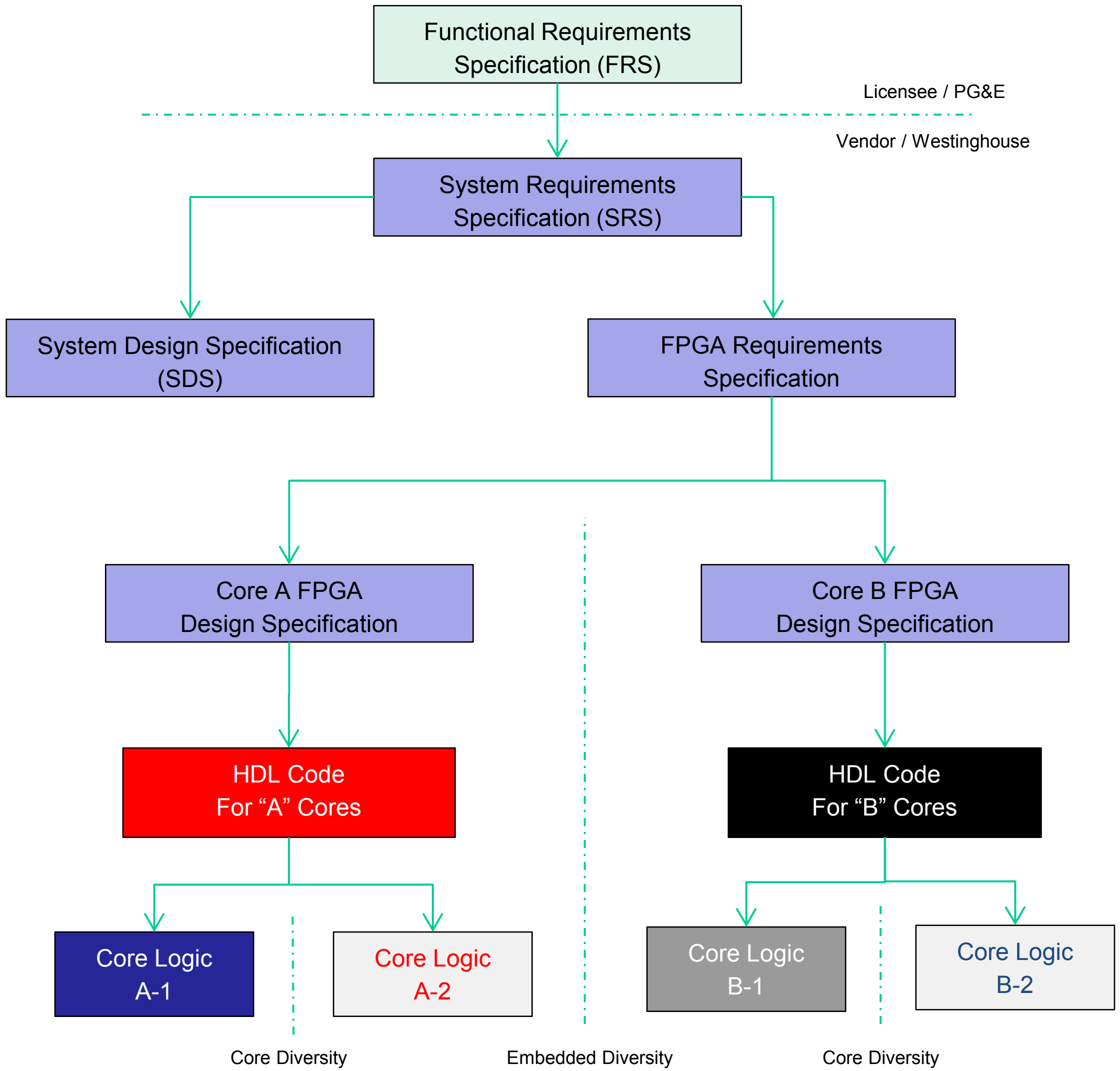
Overview of Diablo Canyon PPS Application
OPDT and OTDT Functions



Project Schedule

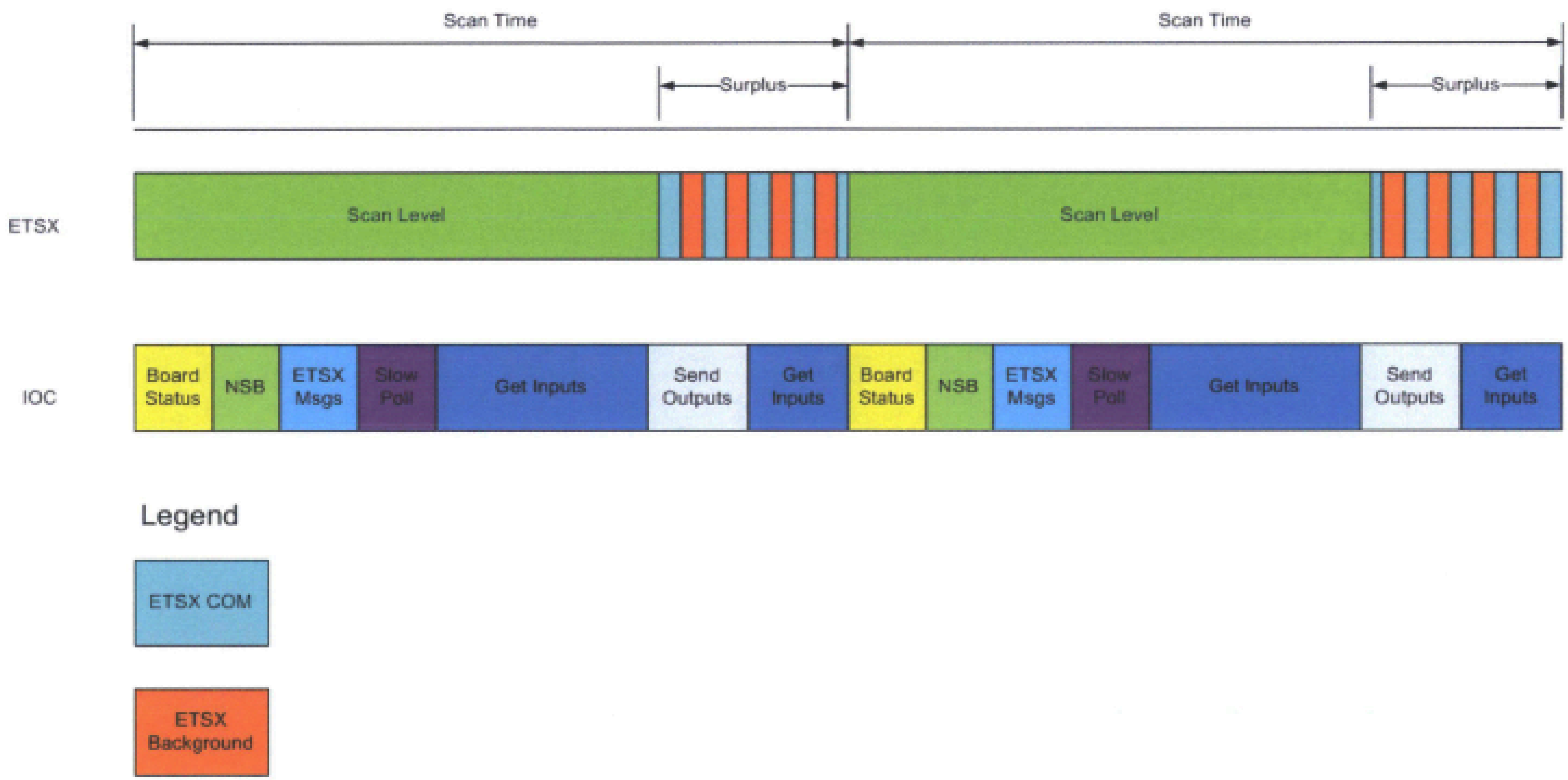


Diversity and Defense in Depth
Diablo Canyon Diversity Solution



ETSX & IOC Scan Loops

Tricon Scan



END