Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Tuesday, February 18, 2014

Work Order No.:NRC-597 Pages 1-323

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

TUESDAY

FEBRUARY 18, 2014

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Subcommittee Chairman

DENNIS C. BLEY, Member

STEPHEN P. SCHULTZ, Member

JOHN W. STETKAR, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

LARRY AARON, Westinghouse

ROSSNYEV ALVARADO, NRR

STEVEN ARNDT, NRR

ERIC T. BERNARD, MPR Associates, Inc.*

MARK BURZYNSKI, Rolls-Royce*

GORDON CLEFTON, NEI

SAMIR DARBALI, NRR

BERNIE DITTMAN, RES

BILL GALEYEAN, NuScale Power*

DAN HEAD, Invensys

JOHN HEFLER, PG&E

SHIATTIN MAKOR, Region IV*

JOHN MCKAY, Invensys

JONATHAN NAY, MPR Associates, Inc.

WARREN ODESS-GILLETT, Westinghouse

JODI RAPPE, NuScale Power*

KENNETH SCHRADER, PG&E

RICHARD STATTEL, NRR

JOHN THORP, NRR

JERRY VOSS, EXCEL Services Corporation*

STEVE WYMAN, NRR

*Present via telephone

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

Opening Remarks
Charles Brown.....5
Diablo Canyon Process Protection System (PPS)
System Overview
John Thorp.....7
Rich Stattel.....20
Diversity Defense-in-Depth
Rich Stattel 61
Review of Advanced Logic System (ALS) System
Diversity Approach
Rich Stattel.....81
Communications
Rossnyev Alavardo.....110
Secure Development Environment Evaluation
Samir Darbali.....169
Deterministic Performance Characteristics of PPS
Richard Stattel.....183
Additional Discussion.....208
Closing Remarks
Charles Brown.....210

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

1:02 p.m.

CHAIRMAN BROWN: This is a meeting of the Digital Instrumentation Control Systems Subcommittee. I'm Charles Brown, Chairman of the Subcommittee. Advisory Committee members in attendance are John Stetkar, Steve Schultz, Dennis Bley. Our consultant, Myron Hecht. And Ms. Christina Antonescu of the staff is our designated federal official for this meeting.

The purpose of this briefing is for the staff to provide a preliminary review of the safety evaluation with the Diablo Canyon Power Plant, Unit 1 and 2 digital replacement to the process protection system of the reactor trip system and engineering safety features actuation system.

The final safety evaluation report is not yet complete. I think that's correct, isn't it?

MR. STATTEL: That is correct.

CHAIRMAN BROWN: Okay. The Subcommittee will gather information, analyze relevant issues and facts and formulate proposed positions and actions as appropriate for deliberation by the Full Committee. The rules for participation in today's meeting have been announced as part of the notice for this meeting previously published in the *Federal Register* on February 12th, 2014.

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

Also we have some folks on the bridge phone line listening to the discussions. Jodi Rappe and Bill Galeyean, NuScale; Mark Burzynski, Rolls Royce; Jerry Voss, EXCEL; Eric Bernard and Jonathan Nay from MPR; and Shiattin Makor and others from Region VI.

To preclude interruption of the meeting the phone line will be placed on listen-in mode during the discussions, presentations and Committee discussions. Also the bridge line will be open at the end of the meeting to see if anyone listening would like to make any comments. You should identify yourself at that time, by the way, when you make comments as to who you are. I will remind you at that time, I hope.

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

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

We will now proceed with the meeting. Mr. John Thorp, the INC branch chief at NRR who will provide some opening comments.

MR. THORP: Good afternoon. Thank you, Charlie.

CHAIRMAN BROWN: All right.

MR. THORP: It's a pleasure for me and my staff to be here. As you pointed out in your remarks the staff's been requested to provide an informational briefing to the ACRS Subcommittee on several topics related to the Diablo Canyon Process Protection System upgrade license amendment request.

I'll be briefly describing the regulatory history of the Tricon and ALS platforms; i.e, the Tricon and ALS topical reports and the Diablo Canyon license amendment request. I'll also describe just a very high-level overview of the system architecture and communications architecture for the Diablo Canyon Digital Process Protection System.

We have a number of folks here with us. Pat Hiland, my division director, is here seated at the side table along with our senior level advisor Dr. Steven Arndt. Rich Stattel and Rossnyev Alvarado are our principal technical reviewers for this evaluation, and they'll describe the regulations, the relevant regulatory guidance and the status of the evaluation for the topics shown as we move along through the slides. Samir Darbali is also assigned as a reviewer for this evaluation and he'll be describing the secure development and operational environment evaluation that's being performed for this system.

I'd like to introduce some of the Pacific Gas and Electric and industry members present and allow them to address the Committee if they would like. So from PG&E we have Mr. Kenneth Schrader over on my right hand at the side table there. From Invensys I believe we have Dan Head and John McKay, all right, seated in the back behind there. From Westinghouse we have Larry Aaron and Mr. Warren Odess-Gillett. They've been raising their hands. I don't know if you spotted them. They've been pretty quick.

CHAIRMAN BROWN: I figured somebody was behind me and I don't have eyes on the back of my head.

MR. THORP: Right, right. And from the Nuclear Energy Institute we have Mr. Gordon Clefton.

So here's our presentation outline and introduction that I'll provide. And then you'll see an overview of the Diablo Canyon license amendment request; discussion of diversity and defense-in-depth; communications; SDOE, as I had mentioned earlier; current platform status. And by the way, the members of my staff who conducted the reviews of these platforms are also here. Bernie Dittman. And Steve Wyman is back over on my left side. And then some discussion of the PPS project schedule for Diablo Canyon.

Go to the next slide. So in October of 2011 Pacific Gas and Electric Company submitted a license amendment request to replace the existing Eagle 21 Digital Process Protection System at Diablo Canyon at their nuclear power plant's units 1 and 2 with an improved Digital Plant Protection System. Hereafter I'll call that PPS.

The new PPS system will be comprised of two PPS subsystems, one of which is based on the Invensys Tricon platform and the other based on the Westinghouse Advanced Logic System, ALS. The Tricon system is a computer-based programmable logic control system, a PLC system. The NRC issued a safety evaluation report for the Tricon Version 10 platform topical report in May of 2012. With respect to the Advanced Logic System, ALS, it is a field-programmable data ray FPGA-based system, which includes diverse features to address the NRC guidance for diversity and digital protection systems. The NRC issued a safety evaluation report for the ALS topical report in October of 2013.

We accepted the license amendment request for evaluation in January of 2011 and we identified a number of issues that could present challenges at the time to approving the LAR, and these were deterministic performance of software, software planning documentation, equipment qualification testing plans and set point methodologies. So those are some of the areas of focus that we've engaged in. And in the process thus far we've done a number of things, as well as PG&E. PG&E has since provided several license amendment request supplements and they've responded to all of our RAI questions, our requests for additional information questions. There were 67 of them.

Staff has conducted two audits at the vender facilities of Westinghouse and Invensys and the results for those audits are publicly available.

Next slide. So our review process. We're conducting the review in accordance with the Standard Review Plan, chapter 7. That's NUREG-0800, chapter 7. With our administrative office instruction LIC-101 and Interim Staff Guidance, the ISGs applicable to digital systems. Interim Staff Guidance has already been reviewed I think previously by ACRS.

These documents clarify the licensing criteria for digital safety systems. Compliance with the ISGs represents more or less the fast track, the HOV lane, as it's been called before, for review and approval. Specifically the staff used the following ISGs for the Diablo Canyon PPS review: We've used ISG-04 to guide the review of communications aspects of the LAR, and we're using in fact piloting with this Diablo effort ISG-06, which establishes the process used by NRC for licensing digital I&C systems, the what-do-you-need-to-bring-to-the-table-and-when-do-you-need-to-bring-it-types of information.

CHAIRMAN BROWN: Can I ask a question?

MR. THORP: Yes, go ahead.

CHAIRMAN BROWN: We reviewed ISG-06 and wrote a letter on it I guess probably four or five years ago, if I remember the time frame, and it was a multi-phase including a set of preliminary discussions. And since this is a pilot program, have you come to any conclusions as to whether this has improved your ability to get ahead of the game relative to the information you need to make your - -

MR. THORP: Yes, I'll give you a general answer and then I'll let Rich give you something more specific. We've had some lessons that we have learned and are learning as a result of the process. We do think it's a more organized approach and has made it more clear, and you can probably ask the folks that are here from industry as well their opinions on this. We've conducted a couple of presentations on how things have gone thus far with ISG-06, and I think that some of the lessons that are learned from those have been expressed to industry and to all of the various stakeholders. But overall we feel like this has been a very worthy effort and is continuing to be so in terms of the organization of what we need to get and types of information we need to have and when we need to get that to effect the best review possible.

Now there are other reasons that things can slow down or not fulfill the sort of timely aspects of business, and that can be addressed further, if you like.

MR. STATTEL: Sure. Well, obviously the review is still in progress, but there were several aspects of ISG-06 that we found very helpful. If you might recall, there was an annex in IC-6 that identified by phase exactly what documents and what information we required at the time of receiving the license amendment request and then subsequent phases of the design, because the design is still in progress. Those were very useful.

During the acceptance review we were able to really pinpoint what material was there, what material was missing. We identified that and we subsequently received the follow-up information from the licensee. So we've used those both for phase 0 and phase 1, or phase 1 and phase 2 of the project. We still haven't received all of the phase 2 documents, but we have a schedule for the licensee to get that later on this year. It was very useful even identifying what material was missing so that we could point them right to that section in IC-6 and we could basically be on the same page with regard to what information we needed to complete the review.

CHAIRMAN BROWN: Okay.

MR. STATTEL: We've also identified there's a lot of duplicate information that's in the ISG, and we're kind of marking that up. There was a lot of material that was pulled from the various branch technical positions and chapter 7. And personally, I don't like having the same material in two different places because it can be taken out of context, so we're marking that up as we go and we hope to use that down the line to incorporate --

CHAIRMAN BROWN: But you're looking at a revision possibly to the ISG, or are you just --

MR. STATTEL: We'd rather not to that.

CHAIRMAN BROWN: Yes. No. No.

MR. THORP: Preferably I guess, you know, our goal in all these Interim Staff Guidance documents is to eventually fold those into more permanent guidance, into our SRP or other guidance, reg guides, etcetera. And so my preference would be that we take these lessons learned from the pilot effort and then get that folding done so that we don't have to do a revision to the ISG.

MEMBER BLEY: Do you have a plan for that or a schedule? I've just seen some ISGs last for years and years and years and years.

MR. THORP: Yes.

MEMBER BLEY: And this is already been quite a few years.

MR. THORP: We've had quite a few that we actually have folded into the reg guides and things.

MEMBER BLEY: Yes, I know. We've seen a couple.

MR. THORP: And so the schedule, we depended upon the completion of the pilot effort.

MR. STATTEL: I'll say my personal preference is to roll it into the update of the Standard Review Plan. I think it belongs in chapter 7. After having worked with this for awhile, I think it's useful information.

MEMBER BLEY: Yes.

MR. STATTEL: I think it can be rolled right into a Standard Review Plan.

I'll point out one shortcoming of the ISG-06. That is it's really geared towards an entire reactor protection system upgrade and it's not very scalable. So if we have an amendment request that's only affecting one safety function or it's only digitizing one card of a reactor protection system, it really doesn't account for that. So we're hoping to work with the licensee and kind of discuss those prospects and kind of come up with some better guidance on how to handle that, how to scale it.

MEMBER SCHULTZ: Rich, you mentioned that the ISG helped you to identify those areas and point the licensee to areas where they had not provided all the information that you required for your review.

MR. STATTEL: Yes.

MEMBER SCHULTZ: Do you understand why you didn't get the information in the first place given that it was already in the ISG? Was it not identified clearly, or --

MR. STATTEL: Right.

MEMBER SCHULTZ: -- enough detail to provide you what you would like?

MR. SCHRADER: I can answer.

MR. STATTEL: Actually, yes, go ahead, Ken. Thank you.

MR. SCHRADER: Hi, I'm Ken Schrader, and I'm responsible for the license amendment request and prepared the LAR.

A couple of the issues: One of them was the set point. Okay? And there we were actually and are doing a separate license amendment request for industry, Tech Spec Task Force, TSTF-493. And so we were going to include the set point information in that LAR. Okay? But that caused the staff a problem because the set point information, you know, wasn't in the LAR we submitted. So we corrected that. We submitted the set point information as, you know, part of the LAR. So that really was -- we totally understood what ISG-06 required. We just were going to provide it in a separate licensing action. So we corrected that.

As far as the equipment qualification, that really was a vendor scheduling issue as far as when the equipment qualification tests were being performed. Some of the tests that the vendors did for the equipment qualification, they were very conservative in terms of, you know, the criteria, the loads or spectra, whatever, that they used in the tests, and there were some issues in some of those tests. So some of those are being redone to take out some of the conservatism in order to get better results. So it's really a scheduler thing as opposed to a deficiency with ISG-06. I'll just say preparing the LAR having ISG-06 was just excellent to be able to prepare the LAR.

MEMBER SCHULTZ: Thank you. That's very helpful.

CHAIRMAN BROWN: With the comment you said it was useful using the word "excellent," I guess one of my concerns with folding it into the SRP would morph the thing or spread it out depending on how it gets incorporated.

MR. THORP: Probably depends on the form that it would take because we've had some preliminary discussions.

CHAIRMAN BROWN: I'm just laying that thought process --

MR. THORP: Yes, understood.

CHAIRMAN BROWN: -- on the table, when you get around to that.

MR. STATTEL: Well, one of the aspects of the ISG is instead of identifying documents by title, it identifies documents and it has a descriptor of what information we expect to be in that document, because obviously not all vendors and not all licensees use the same titling and procedures for developing the documents. So I think, you know, when we performed our acceptance review, we went to the description of the information that we needed to have available to us to do the evaluation and we used that instead of just doing a check mark of the, you know, document titles. It was pretty good. It actually facilitated a lot of the discussions in the meetings we had, you know, trying to rectify, because we might have interpreted one piece of information. They might have had a different interpretation of what was expected. But, you know, in general we were able to get the information we needed. So far.

CHAIRMAN BROWN: Okay. Any other questions?

(No audible response.)

CHAIRMAN BROWN: You want to go on, John?

MR. THORP: Okay. So next we'll just do a very brief overview of the process protection system. So this figure and the next will show the Diablo Canyon Reactor Protective System and the Engineered Safety Features Actuation System combination RPS/ESFAS architecture and how the plant protection system fits within the plant design.

The digital PPS system consists of four protection sets to support reactor protection system and the engineered safety features functions with either two of four or two of three coincidence actuation logic. The integration of RPS and ESFAS, which we've, you know, historically seen as separate quote/unquote "systems" combines two of the four more or less echelons of defense layers that are described in NUREG/CR-6303 for protection against software common cause failures. We'll discuss that in a little bit more detail during our discussion of diversity.

But as you look at the figure, the work that this license amendment request, the scope of the LAR work that we're involved in is contained within that red box. The process racks. The other white boxes that you see, the rod control power cabinet, reactor trip, the solid state protection system, the NIS, the nuclear instrumentation system racks, etcetera, are actually not within the scope of this LAR.

With that said, I'd like to turn it over to Rich Stattel to give you more detail in this presentation. Thank you.

MR. STATTEL: Okay. Thank you. Before I leave this slide, just want to mention that even though the systems in the white boxes here are not being modified under this license amendment, we are evaluating them in terms of the interfaces between what is being modified and those systems. So you'll see during our discussion here we'll be talking quite a bit about what the solid state protection system is doing and what the NI system is doing.

Okay. I'll start out with -- this is an expanded view of the existing Eagle 21 system. There are a few points I'd like to make about this diagram. First of all, both the reactor trip system and ESFAS systems are -- those functions, those safety functions are being performed by the Eagle 21 processors now. They use discreet analog sensor inputs that are separated between safety divisions. And I'm going to use the term "divisions" and "protection sets" interchangeably. So basically the terminology that Diablo Canyon uses is "protection set." And what that means is the individual four redundant divisions performing the safety functions.

All the voting logic for the ESFAS and the reactor trip function is performed by the solid state protection system, which is shown in the gray box at the bottom of this figure. And that's again not being modified by this particular amendment. The actuation signals to the SSPS voters are hardwired connections. They do not use any communications technology or any digital technology at all. And I have a couple of diagrams I'll show later on in the presentation to show exactly how those interfaces take place. There are no inter-divisional communications being implemented in this design. So in other words, there's no communication between the protection steps.

Okay. This figure here shows the replacement digital process protection system. And I'll make the same points here: Both the reactor trip and ESFAS systems will continue to use discreet analog sensor inputs. The sensors are not being changed as part of this amendment. The voting logic will still be performed by the solid state protection system. And the actuation signals to the SSPS voters, as I mentioned, are hardwired connections. Okay?

CHAIRMAN BROWN: Can I ask you a question relative to that? You said the sensors are all the same. And I guess I understand that point. Got that out of looking at the LAR.

MR. STATTEL: Okay.

CHAIRMAN BROWN: And I don't know with the Eagle 21 how that worked, but I mean I noted that in some of the diagrams temperature information, particularly narrow range and a few things like that fed -- only inputted into the ALS parts of some of these systems. And then they fed into -- is that different? I would have imagined in the Eagle system they all went into the same processing chain in each division.

MR. STATTEL: That is correct. The temperatures are a bit unique as far as all the signal inputs to the system. And the reason is because the ALS is actually doing the signal conditioning for the RTD inputs and then it sends an analog signal over to the Tricon portion of the PPS.

CHAIRMAN BROWN: I got that.

MR. STATTEL: So both systems, both digital subsystems are relied upon to complete the safety functions associated with temperatures. So they're unique in that respect. All of the other signals are wired to either the Tricon or the ALS subsystems, or both in some cases. And the diagrams kind of show that relationship.

CHAIRMAN BROWN: Okay.

MR. STATTEL: I'll talk a little bit more about the temperature signals; and I think Rossnyev will cover some of that during the communications discussion, because they are a bit unique. And we're currently evaluating the operating procedures or the anticipated operating modes for the system. And the temperature signals really do play into that.

Okay.

CONSULTANT HECHT: Can I ask a question? In the presentation, as I have looked through it, there didn't seem to be much of a discussion of the internals of both the Triconics or the ALS. Now the Triconics is a processor system that relies on software. We understand that.

MR. STATTEL: Yes.

CONSULTANT HECHT: With respect to the ALS, of course there we're dealing with FPGAs, we're dealing with a different development paradigm, different design structures. We have VHTL, I assume. We have finite state machines and fixed logic. We have just a number of differences that don't get covered by the normal set of the IEEE Software Development Standards. Are you going to cover that in this talk, or is there an appropriate time to cover that?

MR. STATTEL: Well, we can discuss it a little bit. With regard --

CONSULTANT HECHT: There's only one page in the LAR that I could see that spoke about hardware product assurance.

MR. STATTEL: Well, both of these platforms were individually evaluated by the NRC prior to this. That's what John had mentioned earlier. So we have completed safety evaluations for both the Tricon platform and the ALS platform. So really the subject of our review, our current evaluation is the application development. So the internals of the box, those have already been evaluated.

CONSULTANT HECHT: Well, that's true, but there's software which is unique to Diablo Canyon which is running on the Triconics and there's probably logic which is unique which is running on the ALS. And that would have to be part of this LAR, wouldn't it?

MR. STATTEL: The application, that is true, but for instance the operating system that's used in the Triconics, that would not be part of this evaluation that we're currently performing.

MS. ALVARADO: And I just want to add, regarding the ALS system, is not all the components that are being application-specific for Diablo Canyon. We're just talking about one. It's the ALS-102, which is the core logic. So that's the only module that is unique for this application. So that one we are definitely looking into more detail.

CHAIRMAN BROWN: Well that goes to the point about if you've already approved in some previous SER the ALS --

MR. STATTEL: Straw building blocks.

CHAIRMAN BROWN: -- building blocks --

MR. STATTEL: Yes. Okay.

CHAIRMAN BROWN: -- whatever it is --

MR. STATTEL: Yes.

CHAIRMAN BROWN: -- and yet this -- and I remember seeing this about the 102 in there. That was the core logic block was different for this application, or was new, or what -- I don't --

MR. STATTEL: Well, it's unique to each application.

CHAIRMAN BROWN: Yes. And so is there an additional evaluation done of that core logic block, or is it assumed to have been taken care of under your previous SER?

MS. ALVARADO: I just want to clarify, because I'm also responsible for reviewing the software plans and tests that they are doing for the applications.

CHAIRMAN BROWN: For Triconics?

MS. ALVARADO: For both. Besides doing communication, I'm also responsible for the software plans. But the ALS-102, even though I'm saying it's customized, you can customize it for each application, you don't need to customize the whole board. It's certain functions that we're customizing. For example, the communication, the protocol that we use you have to customize it to fit what Diablo Canyon's requirement. So we are looking definitely at those customization of the ALS-102 by reviewing the requirements or how they're implemented, especially in the ALS, how they're implementing the diversity into these application-specific parts.

MR. STATTEL: So let me add: The way the hand-off takes place is we have a reviewer perform a separate evaluation of the platform, and that's application-independent. So they don't know if it's going to trip the reactor or safety injection or what it's going to do. And they spend a lot of time reviewing things like the deterministic performance characteristics of the system, the operating system, the building blocks.

The way the hand-off takes place, in those safety evaluations they identify a list of what we call application-specific action items or plant-specific action items, and those are things that need to followed up by the subsequent reviewer of the application. So for example, each one of the platforms has a list of approved boards by part number. So for the ALS application what we, the application reviewers, would be looking at, we would confirm that the boards that are being used in this Diablo Canyon application are the same model number, the same version boards that had been previously approved during the platform review.

And then there are several action items that we're required to perform to verify that the applications are meeting the requirements, like the single-failure criteria requirements of IEEE-603 or the communications aspect requirements of IC-2. So it's kind of a two-part evaluation.

CONSULTANT HECHT: Well, let me try to be as specific as I can. I said hardware, and I guess that was kind of ambiguous. The two first letters of FPGA are for field-programmable, and particularly programmable. So there is a program that's running inside that FPGA that consists of finite state machines to handle I guess the ship registers and the RS-422 and 485 ports, and then there's some static logic ad handle the eight signals coming in from the reactor. Those are unique. And those are the equivalent of programs written in SEER or ATA in the Triconics platform.

MR. STATTEL: Yes.

CONSULTANT HECHT: But they're very different in the sense of the technology that's used, the tools that are used, the way that the FPGA is made. And, you know, the FPGA you're actually making links. This appeared to be a board where you actually create the links rather than break them. And that is a development process that's a complex development process, and that's --

MR. STATTEL: Yes, we agree, and we apply the same criteria to the FPGA as we do a programmable logic device as far as the development process is concerned. So in other words, we have review guidance in our Standard Review Plan and BTP-7-14 identifies all of the planning aspects of the development plan. So for example, configuration management control, quality assurance control, testing planning. All of those aspects are evaluated by the staff for any digital system regardless of whether it's an FPGA-based system or a computer-based system, PLC system. And that's in both of the reviews.

So to the extent that we're able to we evaluate the BTP-14 criteria during the platform review, all of the planning aspects of the system design. And the later phases where we confirm that the plans have been implemented, those activities are performed by the staff during the application review.

CONSULTANT HECHT: Well and I guess I'll end the questioning here and maybe you can follow it up later with the ACRS, if they feel it's appropriate. For software you have eight IEEE standards that talk about how you go through all the processes that you mention.

MR. STATTEL: Yes.

CONSULTANT HECHT: For VHTL and FPGAs I don't think you have the same industry standard guidance.

MS. ALVARADO: No, I want to point out we do recognize that we don't have guidance specific to or target to VHTL, right? So what we're trying to do is use the guidance that we have and try to see how we can use it to perform the review of the VHTL code. And then to answer your question regarding like the specific of the finite state configuration, what we are doing -- and we had done thread audits where we pick a requirement, right, like for example, communication between the ALS and the maintenance work station and we track that requirement and see how it has been implemented in the finite state machine, right, like it has been implemented and the tools being used. And here we have two cores, right, so how is that diversity being implemented and followed throughout the process?

So that's how we are reviewing I think what you are asking about, like are we looking at the code and the difference between with the Triconics? That's what we are doing for the application-specific part in the ALS.

CONSULTANT HECHT: I would just observe that the LAR, which was a very welcome --

MS. ALVARADO: Well --

CONSULTANT HECHT: -- document, had very little information on it.

MS. ALVARADO: And this is one of the things with ISG-06, is that a lot is rely upon the information that was provided for the platform. So because we already look into how that development was done, I don't think the licensee; and you can contradict me, felt a need to go into that level of detail.

CHAIRMAN BROWN: So let me make one observation. I don't know whether you're familiar with ISG-06 or not --

CONSULTANT HECHT: Yes.

CHAIRMAN BROWN: -- and even my memory is somewhat fuzzy, but there was three different methodologies to be used if there were already approved platforms.

MS. ALVARADO: Right.

CONSULTANT HECHT: Right.

CHAIRMAN BROWN: Then there was an -- I don't want to call it abbreviated, but it was a --

CONSULTANT HECHT: Modified.

CHAIRMAN BROWN: -- modified approach.

CONSULTANT HECHT: Right.

CHAIRMAN BROWN: You didn't have to go look at this. You still had to look at the application --

CONSULTANT HECHT: Right.

CHAIRMAN BROWN: -- programming that was going to be done to make sure that was going to be okay, but the fundamental platform operation, you know, know it performed its functions and its housekeeping and all, that was all looked at, theoretically. Okay?

CONSULTANT HECHT: Well, they --

CHAIRMAN BROWN: Well, let me finish. And then so there's a next phase where there is an intermediate stage and then there's a third phase or a third stage or methodology where everything is brand new and nothing has been seen. So this effectively, in my understanding from looking at the LAR, took -- we've already got topical reports that have been approved by the staff, and therefore those pieces, the generic pieces have been looked at and we only have to look at the touch points, the interfaces and the fundamental application to make sure we meet the requirements.

CONSULTANT HECHT: They did say that the ALS portion was going to be level 3, or 2 or 3 I guess is the word that was used.

CHAIRMAN BROWN: Yes, that's the one that's new, I think.

CONSULTANT HECHT: Okay.

CHAIRMAN BROWN: I've forgotten. Was it two or one is the one where everything is --

MS. ALVARADO: Right. In an ideal situation we review the platform. You know, we spend our time performing a safety evaluation of the platform. And then that platform unaltered gets used. So we know what the building blocks for the application are and all we really have to do is make sure that they put those blocks together correctly to meet the regulations.

It's very rare to get that ideal situation because time passes, improvements are made, corrections are made to the platform over time. So in previous applications, you know, several years had passed between when we preformed the platform evaluation and when the application was developed and they had new versions of the platform at that time. So we're not only reviewing the application development, we're reviewing the deltas or the changes that have been made to the platform.

This is pretty close to the ideal situation because the Tricon, the V-10 safety evaluation was completed very recently, well, within the last year or two. And so they're really not deviating from what was evaluated by the staff at that time. The ALS is even more recent, because you know, just late last year we issued that safety evaluation. So very few actual changes have been made to those platforms. So most of our review is concentrating on the application development.

Now there are some changes to both of those platforms, but we have a separate evaluation section in our safety evaluation that we cover that under.

MR. THORP: This kind of goes to the fundamental concept of what is the benefit of having a topical report for a platform which we've reviewed in the greatest detail that we can review and satisfied ourselves that for the generic aspects of it we understand what it does, how it's come together and what it's intended to do. And then we've identified those things that when this platform is taken to a specific application have to be looked at. So the application-specific action items are then taken into account to look at that melding of the platform to its particular utilities application.

MR. SCHRADER: Can I --

MS. ALVARADO: I think --

CHAIRMAN BROWN: Hold it. I'm sorry.

MR. SCHRADER: This is Ken Schrader. We've got two points we want to add here. One is is that this is to address Myron's comment about the LAR and the content, you know, on the software development. So each vendor for this application has their own software development plan for this project, which is its own document. You know, and it's based on the requirements of their topical, but then, you know, essentially the project-specific requirements. And so those documents, you know, have been developed by the vendors and have been submitted kind of like separately from the LAR, but they're tied to the LAR, to the staff and the staff is reviewing those.

So the information is not contained in the LAR itself. It's contained in the vendor document that we've submitted.

CHAIRMAN BROWN: I agree, there were a number of references to vendor documents.

MR. STATTEL: That's correct. If we did everything in one, the LAR would be --

CHAIRMAN BROWN: Yes. No, I understand that.

MR. STATTEL: -- about this thick.

(Laughter.)

CONSULTANT HECHT: Yes, references 15 and 61, which I guess were FPGA development procedure in the ALS topical report --

MR. STATTEL: That's correct.

CONSULTANT HECHT: -- but you didn't mention them when you were up here, so I didn't know if you were using them or not.

MR. STATTEL: Okay. We refer to them frequently during our evaluation.

CHAIRMAN BROWN: We're going to have to move along.

CONSULTANT HECHT: I'm sorry.

CHAIRMAN BROWN: No, no. That's fine. The FPGA thing we did not have a number of discussions on that in any great depth, so this is a useful discussion.

MR. STATTEL: Honestly, it's a very daunting review because the volume of material that we have in front of us, it's pretty daunting, I'll say. It's a fairly simple application. They're not really doing a lot of fancy things. For the most part it's signal input, comparator and signal output to the SSPS voters. But the documentation that goes with that is fairly significant. So we have requirements documents that we're using for our thread audits. We're pulling those threads into the actual implementation. So we have view of all of the design documentation here. So there's a lot of detail there. It's not an easy review task, I'll say that.

So the next slide. Okay. I want to first point out a couple of the abbreviations that are used here. MWS is the abbreviation for maintenance work station. And even on the Eagle 21 system there was an operator interface maintenance work station within each cabinet, within each Eagle 21 cabinet. And this is a non-safety-related PC basically that interfaces with the protection system.

In the replacement system there are actually two maintenance work stations in each protection set, one for the Tricon system and one for the ALS system. The line goes over to a KVM abbreviation. That's simply an abbreviation for keyboard, video and mouse. So these are collocated with the safety system. And those cabinets have very limited space, so there wasn't any point in adding two video displays, two mouses, two keyboards. So they simply run that through a switch so there's only one operator interface.

CHAIRMAN BROWN: That's the cabinet interface where somebody can look it at and it handles both the Tricon and the ALS?

MR. STATTEL: Only one at a time.

CHAIRMAN BROWN: I understand.

MR. STATTEL: Right.

CHAIRMAN BROWN: Okay. Thank you.

MR. STATTEL: Now just to be clear, you know, both the ALS and the Tricon within each protection set are in the same protection set. So there isn't a regulatory boundary that needs to exist between those systems, but in this design PG&E chose to keep those systems independent of each other. Okay?

So these red walls here, these vertical walls I'm showing here are basically reemphasizing the fact that there is no communications between protection set. So there's no communications A to B, B to C, C to D. And the line that go down to the solid state protection system voters are simply hardwired connections going to relays that are inside the solid state --

CHAIRMAN BROWN: But those were referred to as bistable outputs in a number of places.

MR. STATTEL: Right.

CHAIRMAN BROWN: After our discussion I was able to --

MR. STATTEL: Okay.

CHAIRMAN BROWN: -- finally find some. But in terms of the bistable output from the PPS --

MR. STATTEL: Yes.

CHAIRMAN BROWN: -- is that a solid state on/off high/low or is it a --

MR. STATTEL: It's basically a solid state relay. Correct me if I'm wrong.

MR. HEFLER: John Hefler representing PG&E. Yes, that's correct.

CHAIRMAN BROWN: The Tricon or the ALS initiates a driver, which is a solid state relay of some kind and you get a high or a low and it goes off to the SSPS?

MR. HEFLER: That's correct.

CHAIRMAN BROWN: That's fine.

MR. STATTEL: And I have a figure later on that represents that as well.

So then this next slide shows the horizontal lines which is basically a choice. This is not a regulatory requirement, but there's a choice made by the licensee to keep the Tricon and ALS systems separate. So there are no communications between the Tricon and the ALS, so there's no dependency.

MEMBER BLEY: That switch you talked about, it's a hardwired switch. You're either looking at one or the other.

MR. STATTEL: The KVM switch is only for the maintenance work station.

MEMBER BLEY: Right.

MR. STATTEL: Right? So it's basically just --

MEMBER BLEY: But you can't get any communication through that because you're either hooked to one or the other --

MR. STATTEL: That's correct.

MEMBER BLEY: -- period?

MR. STATTEL: That is correct, yes.

CHAIRMAN BROWN: The ALS does communicate with the Tricon because it creates an analog temperature output and feeds it back into the Tricon system.

MR. STATTEL: Right, but that is --

CHAIRMAN BROWN: So that line is really --

MR. STATTEL: -- an analog signal. There's no digital communication.

CHAIRMAN BROWN: No digital communication.

MR. STATTEL: That's correct.

CHAIRMAN BROWN: No serial coms or anything like that?

MR. STATTEL: That's correct.

CHAIRMAN BROWN: Okay. That's what you meant?

MR. STATTEL: Yes.

CHAIRMAN BROWN: Okay.

(Laughter.)

MR. STATTEL: That's right.

CHAIRMAN BROWN: Thank you.

MR. STATTEL: Okay. The figures in the next set of slides represent in varying levels of detail how safety functions are accomplished by the PPS in terms of inputs, which are shown on the left. The processes in the center, those are the processes that will be performed by the PPS system. And the outputs are shown on the right side.

On the left of this figure are the monitored plant parameters, or inputs to the PPS system. The blue boxes represent the parameters that are used to perform reactor trip functions. The pink boxes represent parameters that are used to perform ESFAS or engineered safety feature-related functions. And the purple boxes represent parameters that are used to perform both reactor trip and ESF functions.

In the center is the existing Eagle 21 processor. Note that there's a single processor for each protection set. No redundancy is provided within each protection set. So as you'll see when we get into our diversity discussion, when the software failure is postulated, basically all of the PPS functions on the right side of this diagram would be compromised. So each processor performs all of the safety functions within a single protection set.

And on the right side are the functions supported by the PPS system. The top red box is the reactor trip function, and all the others are ESF functions.

CHAIRMAN BROWN: Before you go on, back up to your PWR protection concept, the big, big, big block diagram.

MR. STATTEL: That one?

CHAIRMAN BROWN: Yes. And I'm just trying to clarify something that's a little bit inconsistent on the figures that are in the LAR --

MR. STATTEL: Okay.

CHAIRMAN BROWN: -- and in your discussions. Here it says the NIS functions or protectors come out to the NIS, go to the solid state protection system. If you look at the rest of these figures, it shows an NIS input into the Tricon neutron flux. You know, like figure 4.5, figure blah, blah. There's a couple other ones. So am I missing something here?

MR. STATTEL: No. No, that's true. The nuclear instrumentation signals actually provide input. This diagram is a little bit overly simplified. They provide input directly to the solid state protection system as shown on this figure.

CHAIRMAN BROWN: Yes, I understand that.

MR. STATTEL: But they also provide an input to a certain safety function in the process racks, and that is the overpower DT, delta T protection function. And that's exactly the same configuration as in the Eagle 21.

CHAIRMAN BROWN: Okay. All right.

MR. STATTEL: So it's both.

CHAIRMAN BROWN: So it's just an oversimplification?

MR. STATTEL: That's correct. Yes.

MR. THORP: Could have a thin little arrow, NIS racks into that red box, but we left that out.

CHAIRMAN BROWN: That's fine. Just a difference.

MR. STATTEL: Okay.

CHAIRMAN BROWN: All it means is I read it, right?

(Laughter.)

MR. STATTEL: Okay. And this figure represents the replacement system. In the dark blue box is the microprocessor-based Tricon subsystem. Each protection set will have three Tricon processors. So that's part of the Tricon system. So the second in the orange box is the Westinghouse FPGA-based ALS subsystem. Each protection set will have two redundant ALS cores. Okay? So instead of having a single processor to perform all safety functions, the replacement system includes multiple layers of redundancy within each protection set. This is being done primarily to increase system reliability and fault tolerance. It is not being done to meet any specific regulatory requirement.

Okay. The next set of figures --

CHAIRMAN BROWN: Well, let me ask you a question about that then. Later in the LAR and in your SE on the D3 --

MR. STATTEL: Yes.

CHAIRMAN BROWN: -- which you all issued I think three years ago, or two years ago, whatever it was --

MR. STATTEL: Correct.

CHAIRMAN BROWN: -- there were some comments about the diversity in the ALS system, and you used that as a -- when PG&E or you all pointed out that they did not meet some position precisely that -- and then you go on and say you've finished up with SAMBOLT (phonetic), but the diversity, the modifications made and the diversity that is in the ALS system, we conclude that everything is satisfactory and acceptable. So you say there's two cores in the ALS system. Are those two cores programmed differently or something? Is that the diversity you're referring to in your SE?

MR. STATTEL: Yes. Yes, they are. We're kind of jumping ahead to the diversity --

CHAIRMAN BROWN: If you're going to talk about that later, we can wait.

MR. STATTEL: Yes. If you don't mind -

-

CHAIRMAN BROWN: That's fine. Let's just go on.

MR. STATTEL: -- I'd like to defer a little bit of that discussion until later.

CHAIRMAN BROWN: That's fine. Let's just go on.

MR. STATTEL: Okay.

CHAIRMAN BROWN: I was afraid I was going to forget it.

MR. STATTEL: Okay. No, we'll definitely cover that.

So basically this is just showing a little bit more detail on the Tricon portion of the PPS. You can see which process signals are being provided and which functions are being performed by the Tricon system. The determinations of function allocation to the PPS subsystems were made based on the results of the D3 analysis. Okay?

So the way that was done is all functions for which there was already an automatic diverse backup actuation signal, and it could be credited in the analysis, those were assigned to the Tricon subsystem because the Tricon would be -- the functions that are performed by Tricon would be subject to the common cause failure. Those functions would be postulated lost on the common cause failure in the Tricon affecting multiple protection sets.

All of the remaining functions; and those are the functions associated with the three you see here, reactor coolant flow, pressurizer pressure and containment pressure, those function were allocated to the ALS system.

MR. THORP: Or a combination.

MR. STATTEL: Right. Okay? As the next slides will show, all the remaining signals are allocated to ALS so that the built-in diversity features of that platform could be used. Okay?

Okay. The next figure, I didn't plan on spending a lot of time on this unless you had questions regarding this, but basically this shows what functions are being performed. This is just simply showing bistables and the relationship between the system inputs and the outputs, the safety functions being performed.

An example is -- I just kind of broke this one out. This is really just showing the steam generator level signal going to a high bistable. And when the level exceeds a high-level set point, it initiates a partial turbine trip and feedwater isolation, partial actuation. And that would be a signal input to the voters in the SSPS.

CHAIRMAN BROWN: Will you watch your paper on your microphone there, Rich?

MR. STATTEL: Oh, I'm sorry.

CHAIRMAN BROWN: Move the microphone back some.

MR. STATTEL: Okay.

CHAIRMAN BROWN: Very good. Thank you.

MR. STATTEL: And just a reminder, this is only showing one protection set. So the partial actuation signal is sent to the voters. And in this case there's a two out of three coincidence logic that would be required to actually initiate the safety function. Okay?

The next slide shows the ALS functions, the relationships between the inputs and outputs. For the functions associated with these signals for the Eagle 21 manual operator actions were needed to be credited in the D3 analysis. So this goes back to your question earlier. So in the Eagle 21 in 1993 when that was installed a D3 analysis was performed and basically the common cause failure or loss of all safety functions was postulated coincident with each accident in the plant safety analysis.

And the result of that analysis was there was a subset of functions for which there was no automatic diverse action. And they credited manual operator actions. So there were switches, basically hard wire inputs to the solid state protection system that would have to be actuated on a common cause failure in order to accomplish those functions and mitigate the effects of a common cause failure. Those are the functions that are being allocated to the ALS system in the new design. So the effect is they're eliminating the necessity to rely on manual operator actions for those cases.

CHAIRMAN BROWN: But as stated in the reports, the manual capability has been retained fully.

MR. STATTEL: That's correct.

CHAIRMAN BROWN: I think you said completely, that none of those were eliminated or changed.

MR. STATTEL: That's correct. Those are all being accomplished by hard wire inputs directly

to --

CHAIRMAN BROWN: Still available --

MR. STATTEL: -- the SSPS system. They're still available to the operator.

MEMBER BLEY: So for something we haven't thought about that --

MR. STATTEL: Right.

MEMBER BLEY: -- somehow takes out the whole system, we can still override it?

MR. STATTEL: Well, not software. Right. So the manual operator actions were not dependent on software --

MEMBER BLEY: Right.

MR. STATTEL: -- on the Eagle 21 and they are still independent from the software or logic implementation on the replacement system.

CHAIRMAN BROWN: I think that's what you meant by overriding.

MR. THORP: Or if there's something we haven't found or thought of relative to core A, core B within the ALS and we end up with a belly up on both of those, there's still the manual backup.

MR. STATTEL: So in a sense this figure, what you're looking at right now, this figure is showing what the PPS system functionally becomes or falls back to when a total common cause failure of the Tricon system occurs. Okay? As you can see, there are two functions on the right side that are disabled during such a failure. And I'll talk a little bit about those, because these are analyzed in the plant's D3 analysis. And I'll talk about the coping strategies that are employed for those functions.

CHAIRMAN BROWN: You say three. You said two, rather.

MR. STATTEL: There are three input signals, right, that I mentioned before; reactor coolant flow, pressurizer pressure and containment pressure. And the functions that I'm talking about now, those are signals that had no diverse functionality, no automatic diverse functionality --

CHAIRMAN BROWN: In the old system?

MR. STATTEL: -- existing. The safety functions I'm talking about now are functions that are only performed by the Tricon. So in this figure you can see; it's the blue boxes on the right side, the safety functions, turbine trip feedwater isolation and auxiliary feedwater initiation. So think about it this way: If the Tricon fails, everything that has a blue box next to it goes away. So we still have a reactor trip, we still have safety injection actuation, we still have containment spray, but we don't have the turbine trip feedwater isolation. Okay?

So for the turbine trip and feedwater isolation function this function is designed to address excessive heat removal due to a feedwater system malfunction event. This safety function has an existing backup mitigating function which is the power range high-flux reactor trip, which is a direct input to the solid state protection system and doesn't rely on any of the PPS software or logic.

This backup safety function does not rely on the PPS system, and thus will not be affected by the CCF of the PPS.

MEMBER STETKAR: Rich?

MR. STATTEL: Yes.

MEMBER STETKAR: I'm going to wait until you get past all of this stuff to ask the real meaty things, but since you've stopped here --

MR. STATTEL: Okay.

MEMBER STETKAR: -- what trips the main turbine?

MR. STATTEL: What trips the main turbine? Well, a number of things.

MEMBER STETKAR: You just know because you've reviewed this. So what trips the main turbine? I don't care about tripping the reactor. In fact I'd actually like to have the reactor running if the main turbine isn't tripped. What trips the main turbine?

MR. STATTEL: Well, there are several trips of the main turbine.

MEMBER STETKAR: No, no, no. On this particular event what trips the main turbine? How do I prevent a really rapid cool down is what I'm trying to get at? I can trip the reactor and if I'm delivering 100 percent steam flow to the secondary side, step on the primary side, ain't going to be happy. So I'd like to know what trips the main turbine.

MR. STATTEL: In terms of protecting the turbine?

MEMBER STETKAR: No. No, in terms of protecting the plant. This is very severe overcooling transient equivalent to a steam line break.

MR. STATTEL: Okay. So we're going to initiate a high-flux reactor trip.

MEMBER STETKAR: Good.

MR. STATTEL: Right?

MEMBER STETKAR: That makes the power low, so that exacerbates the effects of this now large steam line flow.

MR. STATTEL: Okay. I'm looking for some help from the PG&E --

MEMBER STETKAR: I'm keeping the secondary side delivering 100 percent steam line flow until I get a main steam isolation signal, which, oh, by the way, comes through Tricon.

MR. STATTEL: Yes, I'm thinking it's going to be the steam isolation.

MEMBER STETKAR: Which comes through Tricon for these events. You don't have a containment high-pressure signal here. This is all outside.

MR. STATTEL: But there's an ALS function for isolating main steam.

MEMBER STETKAR: On high-containment pressure.

MR. HEFLER: If I could interject, this is John Hefler, there is a turbine trip on reactor trip.

MEMBER STETKAR: That's what I wanted to hear. Where does it come out of though? Does it come out of the --

MR. HEFLER: That's hardwired.

MEMBER STETKAR: That's hardwired?

MR. STATTEL: Off of the trip --

MEMBER STETKAR: Thank you. Thank you.

MR. HEFLER: Yes, it's the old -- like it used to be.

MEMBER STETKAR: Enough said. Thank you.

MR. SCHRADER: It's a tech spec requirement.

MEMBER STETKAR: Thank you.

MR. STATTEL: One of our random trips.

MEMBER STETKAR: Thank you.

MR. STATTEL: Okay. The second function that I'll talk about is the auxiliary feedwater initiation function. The low, low steam generator level is the primary AFW initiator. This function is designed to address major secondary pipe rupture, major rupture of a main feedwater pipe, loss of non-emergency AC power to the station auxiliaries and loss of normal feedwater event. This safety function has two existing backup mitigation functions which are pressurizer pressure reactor trip and high containment pressure safety injection and reactor trip. Again, neither of these backup safety functions rely on the Tricon subsystem and thus would not be affected by the CCF of the PPS system.

Additionally, the auxiliary feedwater system is actuated by the independent AMSAC system on low steam generator level. The non-safety-related AMSAC is independent and diverse from the PPS system as we'll see later.

MEMBER STETKAR: Yes, let me ask you to stop here, because we're getting there. What starts auxiliary feedwater on a plain vanilla loss of all main feedwater event? The diverse signal.

MR. STATTEL: For a diverse signal? So we're saying the CCF is present so we don't have a Tricon safety function? I believe it would be --

MR. HEFLER: Rich? John Hefler again. That's AMSAC.

MR. STATTEL: AMSAC. I was going to say --

MEMBER STETKAR: Is AMSAC conditioned on the fact that you still have to have high first-stage impulse pressure from your main turbine?

MR. HEFLER: Yes.

MEMBER STETKAR: Okay. I'm asking you on a plain vanilla loss of all main feedwater. The reactor trips. The turbine does trip. What starts the auxiliary feedwater? I didn't say the reactor failed to trip. What starts the auxiliary feedwater?

MR. HEFLER: The auxiliary feedwater will be started on the AMSAC initiation.

MEMBER STETKAR: No, no, no. Does it start it regardless of first-stage impulse pressure or only if first-stage impulse pressure is still high?

MR. HEFLER: Well, the AMSAC actuation is dependent on being over the C-20 interlock, which is high first-stage turbine pressure.

MEMBER STETKAR: Okay. So but if I trip the main turbine will AMSAC initiate main auxiliary feedwater, is what I'm asking. If I successfully trip the main turbine at T-0?

MR. HEFLER: If you've tripped the main turbine as a result of AMSAC, which the AMSAC --

MEMBER STETKAR: No. No, no, no. No. It came through.

MR. HEFLER: The reactor pressure is still high.

MEMBER STETKAR: The reactor tripped. You told me that the reactor tripped. Breakers and the single to trip the turbine. All of that works fine. All of that works perfectly fine. What starts the auxiliary feedwater?

MR. STATTEL: It would probably be a manual initiation.

MEMBER STETKAR: Manual initiation is the answer if that's what's left? Those are the answers I'm looking for here.

MR. STATTEL: But the other thing I'd like to point out, neither of these functions are being impacted by this modification at all. We're postulating the loss of the safety function, and the identified mitigating action here is the same for Eagle 21 as it will be for the new system.

MEMBER STETKAR: My questions will eventually get to the point of what are we doing with this modification and how effective is it at preventing a need for operator actions?

MR. STATTEL: Okay.

MEMBER STETKAR: Okay? So auxiliary feedwater. I now have a tick mark over here that says operators will probably have to start that. Okay.

Suppose I have a LOCA in the plant and ALS doesn't work. How do I mitigate a LOCA?

MR. STATTEL: Well, when you start with ALS doesn't work --

MEMBER STETKAR: ALS doesn't work.

MR. STATTEL: Right?

MEMBER STETKAR: I can say that.

MR. STATTEL: So we're saying both of the cores?

MEMBER STETKAR: That's right.

MR. STATTEL: Both ALS cores?

MEMBER STETKAR: Well, I can have --

MR. STATTEL: Even though they're diverse, they don't perform --

MEMBER STETKAR: You know, I've got three processors in each protection set from Tricon, and yet your magic, very special software common cause failure can kill all of those. So ALS doesn't work.

MR. STATTEL: Basically you put the plant in the exact same situation as Eagle 21 is operating under.

MEMBER STETKAR: Okay. So that's another operator has to manually start stuff for any LOCA?

MR. STATTEL: That's correct.

MEMBER STETKAR: Okay? And we already talked about a steam line break outside containment, not inside containment. Does the operator have to manually close the MSIVs to mitigate that event?

MR. STATTEL: I believe so. I would have to look at the D3.

MEMBER STETKAR: It does, unless there are other signals. I'm waiting for --

MR. STATTEL: Yes.

MEMBER STETKAR: -- people from Diablo to chime in and say, yes, but there are these other signals.

(Laughter.)

MR. STATTEL: Right.

MEMBER STETKAR: Not hearing that, I'm assuming there aren't any.

Now, if that's the case, you have postulated a clean software failure of Tricon. And when I say "clean software failure," I mean the kind of death I'd like to have. I'd like to die painlessly and I would like to not thrash about in the death throes. So you're not postulating any kind of spurious operation. You're saying it doesn't do what you thought it was supposed to do and it doesn't do that cleanly? You've not postulated any types of failures of the ALS, is that correct? Common cause failures.

MR. STATTEL: We did not eliminate common cause failure from the ALS, but the effects of the common cause failure on the ALS would not affect the safety functions being performed by the ALS.

MEMBER STETKAR: High-pressure injection from a LOCA it wouldn't affect?

MR. STATTEL: No, it would not because the common cause failure would affect one core or the other. It would not affect both cores.

CONSULTANT HECHT: Of the ALS?

MR. STATTEL: That's correct.

MEMBER STETKAR: Okay. I guess you're going to explain why that's true later.

MR. STATTEL: Yes. I'm getting to that, yes. And again, keep in mind that we're addressing a software or a logic implementation error that's common to multiple divisions or multiple protection sets. Okay?

CONSULTANT HECHT: But not necessarily a design flaw.

MEMBER BLEY: Or specifically excluding a design flaw perhaps.

MEMBER STETKAR: Or people going and noodling set points through your maintenance work stations on both of those cores.

CONSULTANT HECHT: That's true, too. I was thinking specifically about that, but I was out of order. I apologize. I'll wait until the --

MR. STATTEL: Okay. For the D3 analysis, we'll start by reviewing the current requirements for diversity. There are three primary documents that provide guidance for addressing and evaluating diversity. They're all based on the direction provided by the Commission in SRM to SECY-93-087. NUREG-6303 describes a methods for analyzing a CCF of a computer-based nuclear safety system and its potential effects on the overall plant safety analysis.

Okay. The BTP-7-19, which was recently revised, provides guidance for evaluating an applicant's D3 analysis and the design of automatic and manual controls and displays for use as diverse actuation systems. Okay?

ISG-02 was developed as one of the Steering Committee efforts to provide clarity and establish expectations for the D3 analysis. This ISG has been incorporated into BTP-7-19, however, I'm still listing it here because it is relevant to Diablo Canyon in that the safety evaluation that was done on the D3 analysis was performed before the recent update to BTP-19. So ISG-02 was used at that time.

Okay. As I mentioned before, BTP-7-19 requires a coping strategy to be developed for a digital safety system to address the effects of a software or common cause failure when the potential for a CCF cannot be eliminated. Okay? A D3 analysis was initially performed for the existing Eagle 21 system in 1993. This analysis postulated a software CCF resulting in a failure of all PPS functions, failure to actuate.

For functions associated with containment pressure, reactor system coolant flow and pressurizer pressure the analysis credited manual operator actions as a means of coping with such a failure. This modification will eliminate the reliance on manual operator actions to cope with software or logic implementation CCF.

Okay. The licensee performed the D3 analysis and updated D3 analysis, and the staff completed a safety evaluation of that analysis in 2011. The D3 analysis does not make a case that software CCF of the ALS subsystem is not possible. Instead, it determined that the effect of the postulated CCF of the ALS subsystem does not cause a loss of the safety functions. And I'll discuss the effects of the postulated software for loss of logic

-- or common failure of the logic implementation next.

Okay. This slide, I'm not going to spend time on this because I'd like to advance, but basically I'm showing the Tricon system. Even though there are three processors and redundancy is built into this system, there are elements of the software that are running in this system that are common on all protection sets. Therefore, no credit is given as far as eliminating the possibility of common cause failure on the Tricon.

MEMBER STETKAR: And I think, if I remember, Rich, the arrows that you show kind of running around in circles or whatever is some sort of algorithm that it uses to determine the middle value of each parameter that's input, right, so that all three of the processors use that -- I'll call it the middle value?

MR. STATTEL: There's a voting that takes place --

MEMBER STETKAR: Yes. Yes.

MR. STATTEL: -- in the Tricon processes, yes.

MEMBER STETKAR: So in some sense --

MR. STATTEL: So the signals are validated. Essentially the added layers of redundancy certainly provide an improvement in system reliability. And that really plays out because one of the documents we're reviewing is the reliability analysis. And we're seeing that the numbers do show because of the added redundancy here there's increased -- we expect there to be an increase in reliability of the system.

MEMBER STETKAR: Tell me if you're going to talk about this, but one of the questions that I had was when I read through the LAR I think it told me that while the system is operating, if I have a detected fault on one of the main processors here, I can remove that processor and the system, you know, adjusts appropriately because --

MR. STATTEL: That is correct.

MEMBER STETKAR: -- it's not there.

MR. STATTEL: That is correct.

MEMBER STETKAR: And that when I plug it back in, it essentially does what I'd call a hot reboot. In other words, it starts operating by itself without my needing to test anything. Is that true?

MR. STATTEL: That is true. And that's kind of unique to the Tricon system. When we looked at other platforms, they don't normally have that level of redundancy built into them. It's not required by regulation. I guess it would keep them out of LCOs.

MEMBER STETKAR: Well, what I was going to ask is is there any -- I mean I understand the upside to that.

MR. STATTEL: Yes.

MEMBER STETKAR: You don't have to declare that protection set inoperable and do whatever you need to do to restore it to operability after things are replaced.

Is there any downside to it?

MR. STATTEL: It does increase the level of complexity as far as the handling of those failures and the shift of control between processors, but those are all aspects that we evaluated during the safety evaluation. So there is an increase in the level of complexity as far as handling the flow of the --

MEMBER STETKAR: I was thinking more about when you install the good -- so, you know, probably good processor in the slot.

MR. STATTEL: Right.

MEMBER STETKAR: And everything else then automatically makes it happy. Let me put it that way. I don't want to try to prejudice you or --

MR. STATTEL: But as far as the outside --

CHAIRMAN BROWN: That would -- comes out the way it's supposed to after you do that.

MR. STATTEL: From a control -- because understand, these systems are much more widely used in control system applications, for instance, paper mill or process control. And from those standpoints, yes, you're concerned about bumpless transfers of control, you're concerned about failing over to pre-failure conditions, things like that. But from a protection system perspective we don't really have as much concern about that, because generally when the maintenance is being performed we're not crediting those functions anyway, right, because we have the three other redundancies that are already performing that. So we have a lot more layers of redundancy here.

MEMBER STETKAR: Well, but what you just said is a little bit different than what I thought I said.

MR. STATTEL: Okay.

MEMBER STETKAR: You said when maintenance is performed you're not crediting those other redundancies, which to me says something is de-energized and tagged out of service and therefore my system is now only three protection sets. It's not three and two-thirds. What I thought I read is that the system is fine with three and two-thirds --

MR. STATTEL: It's still --

MEMBER STETKAR: -- protection sets --

MR. STATTEL: It maintains the safety function, yes.

MEMBER STETKAR: And when I plug this new module in at power, system operating, not removed from service or anything, then --

MR. STATTEL: Well, I guess my point is when they plug it in, well, what can go wrong? We're really talking about a bistable output, a digital output here. So it could cause an actuation, right, or it could fail to cause an actuation. In either case any time maintenance performed on the system some kind of operability determination would need to be performed to confirm that the system is still functioning, operable.

MEMBER STETKAR: Okay. I like to hear those words. I don't think I was reading them anywhere.

MR. STATTEL: Okay.

CHAIRMAN BROWN: John, like you, the detail I saw when I was reading that was that if you didn't do -- if one had a fault, it would remove itself. Somehow you've got --

MEMBER STETKAR: Yes, I mean, you'd get an alarm --

CHAIRMAN BROWN: -- and the other two continue operating and everybody's happy.

MEMBER STETKAR: It's fine. You know, it's inputs. Yes, it signals when you lose --

CHAIRMAN BROWN: Yes, and so you've still got four divisions at that point. It's the point at when somebody goes and does something to remove the one that's inoperable, you --

MEMBER STETKAR: I think --

CHAIRMAN BROWN: -- you plug it back in. It wasn't real clear.

MR. SCHRADER: This is Ken Schrader. So we would not, you know, operate for a long period of time with one or two of these Tricon modules out. In fact we committed in the LAR there's on module out, we would replace it within 30 days. And if there was two --

CHAIRMAN BROWN: That's not a long time?

(Laughter.)

MEMBER STETKAR: Ken, let me follow on that. I don't care about the time window. Is the system alive and processing signals when you do that replacement?

MS. ALVARADO: Yes, it is.

MR. STATTEL: It's processing signals, but I think the real question is is it operable? Is it considered operable?

MEMBER STETKAR: I'm not an attorney. I'm never going to go get a law degree. I don't care about attorneys. I care about hardware.

MS. ALVARADO: Well, when you say --

MEMBER STETKAR: Hold it. Stop. Declaring something legally inoperable is an attorney's problem. It's not a technical problem. I'm worried about technical problems. If it is plugged in and processing signals, even though you might declare it legally inoperable, what needs to be done to it to declare it legally operable when I plug that new module in there? And if the answer is nothing because it takes care of itself, that's one answer. If some sort of functional testing has to be done on it, that's another answer. So that's the information I'm looking for. I don't care about 30 days or legally.

MR. McKAY: Excuse me. John McKay from Invensys. What happens -- and the word that you were -- that were used is reeducating the MP when you plug in a brand new one.

MEMBER STETKAR: I read that word. I didn't want to use it.

MR. McKAY: It will reeducate, which means it will download the control program running in the other two MPs. It will perform self-diagnostics and then it will come back up and become a TMR system again. Until that time that MP has no input into the process.

MS. ALVARADO: So just let me point out the figures work model. Assuming you're losing one of these processors, so you're going to go from three voting to two voting. Until you connect this processor again and it does checking and confirms that it is okay, you're not going to go backwards to three voting. So that's what is happening.

MEMBER STETKAR: If everything works as the designers believe it out to should kind of work, that might sort of kind of happen. In our experience the world doesn't always sort of kind of work the way designers think it should have might have kind of worked according to their design philosophy. Sometimes funny things happen. And what I'm trying to probe is how carefully you've all thought about the funny things that might happen if I'm plugging a new module into an operating system that's producing signals. That new module then must become; we'll use the term, because we heard it, reeducated.

MS. ALVARADO: Again, if that were to happen, this new processor that I'm plugging in right into the Tricon system, when it check itself and the system realize there is something wrong, it will be mark as a fail component, right?

MEMBER STETKAR: If the system realizes there's something wrong.

MS. ALVARADO: Okay. That's one item. The second item, if the input from that processor is different than the other two, that output is not going to be considering the voting, because they all have to agree.

CHAIRMAN BROWN: Well, hold it. There were words about selecting a median value as opposed to them all agreeing so that they're never going to all agree exactly because they get different -- they're going to process inputs from the quote "input legs," and with whatever errors -- one might read, you know, 10.56 and another one might be 10.03 and another one will be something else and it will be --

MEMBER STETKAR: Okay. Pick the 10.3 because it's --

CHAIRMAN BROWN: They won't read the same.

MEMBER STETKAR: -- on the 10.3

MR. STATTEL: Well, going back to our review, our safety evaluation, we look at the changes they're making to their technical specifications.

MEMBER STETKAR: Right.

MR. STATTEL: So there are still surveillance requirements that would have to be met. So there are functional requirements that would have to be met. And I would expect that those would be applied before -- you know, if they replaced a card, before they declared that system operable --

CHAIRMAN BROWN: You mean that division operable?

MEMBER STETKAR: Correct. They would have to complete the functional surveillance --

CHAIRMAN BROWN: By a human?

MEMBER STETKAR: -- requirement for that division.

CHAIRMAN BROWN: By a human?

MEMBER STETKAR: Yes.

MR. SCHRADER: That's correct. We don't have a fully automated surveillance as part of this. It would require a person at the maintenance work station to verify that.

CHAIRMAN BROWN: So let me phrase it this way: When the new processor is put in and it's being reeducated, that division does not become -- that's effectively out of service in my mind -- let me -- John, I see you're shaking your head. I agree with your shaking your head. Based on what you're saying, it almost says we're making that out of service in some form until a human says that new one is working right. Now whether the other two are still crunching along and putting stuff out or whether they're momentarily ignored from that division because of something the human intervention does when he plugs the new card, it's not clear at all and I don't know whether it's --

MR. STATTEL: Quite honestly, I don't see it as being a lot different than replacing a circuit board in an analog system. Because when I put the new circuit board in, yes, it's going to energize, it's going to function, it's going to perform the safety function, but until I do a functional test, a surveillance test on that, an operability determination, then I'm not crediting that.

MEMBER BLEY: Well, in older systems --

MR. STATTEL: Yes.

MEMBER BLEY: -- if -- call it channel 3 out of 1, 2 or 3 -- if 3 is not working right, you could actually take it out of service and it would have no output. And then I'd work on it and I'd test it. And then when I knew it was working right, I'd put it back in service. So in-service and out-of- service to me means it's really not putting any signals out. This sounds like it's still putting something out that could be anything for a little while until it all gets worked out.

And, you know, whether we call that operable or inoperable, I'm kind of like John, I don't care. What could it be doing? What might it make the plant during this interim time? When it's not working right is it really out of service or does it still have outputs that are getting fed into this system? Sounds likes it does. And what can those do? You kind of hit early on some things it might do, but I haven't seen what tells me you've really thought through could this get us in any trouble in these interim times?

MEMBER STETKAR: In the old days you have the infamous bypass inoperable switches.

MR. STATTEL: Well, they still have those switches.

MEMBER STETKAR: But, well, the key is would they play -- if they had a single main processor in one protection set --

MR. STATTEL: Yes.

MEMBER STETKAR: -- fail; I'll use that term, would they place that protection set in a bypass inoperable state? And I don't know how they do that. I don't know the philosophy at Diablo because it's different from plant to plant. For the reactor trip you either put it into trip mode and you go to one out of the remaining three, or whatever, or you can to go to a two out of three logic. It's plant-specific.

MR. STATTEL: With those surveillances those LCO requirements are not being modified by this --

CHAIRMAN BROWN: Yes, but, John, let me phrase it slightly -- I can understand if you're going to leave it in service. One fails and we've got 30 days to do something with it and the other ones are working fine, the division, the protection set is in service, it's doing its job. Now after 15 days, hey, we're going to go replace one of them. But my question would be do you put that protection set, bypass it while you insert the new processor in and let it run through its -- is there a -- what did you call it, an LC -- is there a requirement? I mean if I was an operator, if I was owning this thing, I sure as heck wouldn't just put it back in. I don't think I would anyway.

I mean I've faced this issue because I had an automatic control system for a large turbine generator set where we needed it to stay on line and we had a voltage regulator and a governor, both of which were designed with two hot running redundant systems and you had to transfer from one to the other in less than five milliseconds in order to not dump something like 20 megawatts worth of load at the wrong time. And so we had to have a transfer.

But now we got that part working fine, but now the question is what do you do with the one that was not operating right that you left? Because you could go take the card out, put a new card it, computer, whatever it is. And we struggled like crazy trying to figure out what do you -- now, that's a little bit more dynamic situation. Well, this is, but I mean that's -- I guess if -- left to my own desserts. I don't know.

MR. STATTEL: Your points are well taken. I'll be honest with you, we're reviewing a license amendment, therefore --

CHAIRMAN BROWN: No, I understand that.

MR. STATTEL: -- we are evaluating what is changing. And the tech specs that are associated with the determining operability are not changing.

CHAIRMAN BROWN: But this is different.

MR. STATTEL: They're the same as before. My expectation would be when the shift supervisor issues a key to an I&C technician, here, go replace that circuit board, that main processor, safety processor, that the operators would have entered the required LCO for that prior to issuing that key.

MEMBER STETKAR: That's your expectation.

MR. STATTEL: That's correct.

MEMBER STETKAR: Having played games with tech specs 30 years ago, I'd ask Diablo Canyon officially on the record what their interpretation would be, because many people can interpret the requirements of tech specs differently. So the question is would Diablo Canyon declare that protection set inoperable with whatever the requirements of the tech specs are if one and only one main processor -- I'll say fails, because eventually it has to be replaced. I don't want to split hairs over --

CHAIRMAN BROWN: Well, but they could leave it operating and it's when they go to replace it is when, you know, the problem --

MEMBER STETKAR: Well, if you want to split hairs down to that.

MEMBER STETKAR: Yes, it's a nuance.

MR. THORP: Because I think they're going to try to take advantage of the technology that allows the system to continue to operate so that they

don't --

CHAIRMAN BROWN: Yes, absolutely.

MEMBER STETKAR: That's fine. So let's focus on --

MR. STATTEL: I think Charlie's --

MEMBER STETKAR: -- the replacement.

MR. SCHRADER: This is Ken Schrader.

CHAIRMAN BROWN: Before you say anything, this isn't -- but see this is different than now than Eagle 21. There the division was down if the processor failed. You had to go to -- you had to take it out service maybe, you know, for whatever it is. So this is different. Now you're leaving it running. It's running hot. Now you're putting something in while it's running hot. What can happen when you reintroduce that into the system? How does it get reeducated? Can it bullocks up something else in the process?

So I'm sorry. Now I interrupted you, but I wanted ad make that somewhat a thought-valid important point, and maybe, maybe not.

MR. SCHRADER: This is Ken Schrader now. So we did address this on page 243 of the LAR supplement. So what we had said was for the Tricon if one leg goes out, we would allow it out for up to 30 days. We'll control that in what's called our Equipment Control Guidelines. So it's kind of a sub-tier of the tech specs. If there's two legs out, we would only allow seven days to get one back. And if all three are out, then we declare all the associated channels inoperable.

CHAIRMAN BROWN: Of that particular protection set? And that still doesn't address putting one back in service if you've got the other two running.

MR. SCHRADER: Right.

MEMBER STETKAR: There's nothing that I've read, and I studied the tech specs, I studied --

CHAIRMAN BROWN: I'm sure, John.

MEMBER STETKAR: -- some of the words, and there was nothing in there that satisfies the logical "and" and "or" in my mind that says they must declare it inoperable when you replace it and do anything to verify that it's operable after you replace it. And I'm not hearing Diablo say anything to the contrary. So this sounds like it can be performed. It's a totally hot swappable during power operation with no need for administrative declaration of inoperability and no need for human being intervention to verify and let's say assert operability. Which as Charlie noted is different than Eagle 21 because Eagle 21 was the equivalent of all three of those processors going belly up.

CHAIRMAN BROWN: That's correct.

MEMBER STETKAR: And there they say obviously within a seven-day, or whatever time period it is, you know, that you do enter LCOs.

MR. STATTEL: One of the pieces of information we don't have at the time is the actual surveillance procedures, the modified surveillance procedures. With past applications we, in absence of that -- because normally our safety evaluations are performed prior to the development of those. In absence of that, what we normally do is we include in our safety evaluation recommended inspection items. And those are things that after the safety evaluation is issued our inspectors would basically go to the plant, inspect and make sure that those procedural requirements are met. There are procedural requirements that are established in the safety evaluation that we write. And this seems like it would be in that area. And those haven't been developed yet.

CHAIRMAN BROWN: Okay. Let's roll on.

MR. STATTEL: Okay.

CHAIRMAN BROWN: We've beat this one. It's an open question, I guess.

MR. STATTEL: Okay. Now onto the ALS. So the next couples slides are going to be discussing the diversity features that are part of the ALS subsystem. It's designed with two important redundancy features that are considered in the NRC safety evaluation. The are core diversity and imbedded design diversity.

So core diversity as implemented in the Diablo Canyon application generates two redundant logic implementations for placement within each FPGA for a standardized circuit board. This is the ALS-102 board. The two redundant logic implementations represented in relation between core A1 and core A2 on this figure and between core B1 and core B2 use the same hardware descriptive language or HTL files per standardized circuit board. However, each logic implementation is produced using different synthesis directives. Therefore, the synthesis tool is used as a means of making the core logic in the number one implementations different than the core logic in the number two implementations.

CONSULTANT HECHT: So the diversity comes in the synthesis step?

MR. STATTEL: This is for core diversity. This is one of the two means of diversity that are implemented in the system.

So it's in the synthesis step. So they have procedures that have the teams -- when they're performing the synthesis, they set the directives to a certain configuration and then they implement the logic. And they do that for the number one and the number two logic. And the results are different implementations of the same HTL code.

CONSULTANT HECHT: Okay. And you also said that there was another level of diversity? Is that --

MR. STATTEL: That's correct. The second level of diversity is what we call imbedded design diversity. This provides an additional level of diversity to that provided by the core diversity. The imbedded design diversity requires the production of two versions of hardware descriptive language files for each standardized circuit board. This is represented on this figure as the difference between the A cores and the B cores in the figure. So the imbedded diversity is at the top of the figure.

Okay. The Diablo Canyon application defines the configuration and arrangement of the PPS system and creates two different sets of FPGA design variance. So what you see on the figure, they have basically two different teams that are creating the HTL code to implement the system requirements. So you have an A team that will basically develop a set of HTL code to implement requirements. And then there's a complete other team that develops a separate set of HTL code that's independently developed to develop the code for B, the HTL code for the B logic. Okay? And that's the imbedded diversity.

And within each of those teams they both implement the synthesis process using different sets of HTL logic.

MEMBER BLEY: I've read some stuff about this idea in other applications than here, and you often run into the fact that either people who have had the same training -- lots of different things lead them to the same solution so that you come up with the same thing. Has anybody ever looked into this, at what the two teams do and see if there is any diversity in approach?

MR. THORP: The end?

MEMBER BLEY: Yes.

MR. THORP: As a result of their process are they actually different?

MEMBER BLEY: Yes. Because the stuff I've read says there's so much imbedded dependency among people trained to do this either through their organizational or through where they went ad school that often you find they're the same.

MR. STATTEL: Yes, and this is a question we've been asking Westinghouse --

MEMBER BLEY: Yes.

MR. STATTEL: We understand that you have a team A and a team B. What's to tell me that they don't -- you know, great minds think alike. They don't come up with the exact same solution and therefore you compromise the diversity that you're trying to establish.

MEMBER BLEY: Yes.

MR. STATTEL: And so what we asked was what type of V&V activity -- who is looking at the end product, the resulting HTL code or the resulting binary files to make sure they're different and make a determination that they're different enough so that we don't have to consider the common failure between those two. Right? And, you know, we haven't completed our evaluation, but in the process of performing our thread audits, we are pulling various requirements and we're pulling them down to that level and we're looking at those actual files that are created, the completed files.

And we have looked at them in a couple of instances already. We have another audit that's coming up in the summer and we'll be pulling those threads further to basically provide some kind of assurance that the end results are in fact diverse as they're designed to be. So basically you're going to end up with four different implementations, two pairs basically forced by the synthesis process to be diverse and then diverse from the other set of cores by the implementation of different HTL code.

Now what we have before us today is we have the procedures that the developers are using for the development of that HTL code. And they are different. They have a different set of implementation procedures for the core A team and the core B team. So it's really unlikely that they would come up with the same solutions because basically their coding instructions are based -- how would you word that? They're based on different --

MS. ALVARADO: Different approach. They're taking a different approach.

MR. STATTEL: Different approaches. Different design approaches, right?

MS. ALVARADO: Yes.

MR. STATTEL: Now the other thing -- a part of our evaluation, one of the things we have yet to do is to identify the actual V&V activities that are being performed by their people. Because we're only doing thread audits. We're only pulling, you know, one or two requirements out of thousands.

MEMBER BLEY: Is this something you guys dreamed up or is this a common term nowadays?

MR. THORP: It's just pulling a thread, you know?

MEMBER BLEY: Okay.

MR. THORP: A vertical slice, you know, that goes all the way down.

MEMBER BLEY: Same as a vertical slice? Okay.

MR. STATTEL: So we're only doing a spot check. So we're only checking a really statistical insignificant set of the requirements. But, so that in and of itself we don't consider adequate to ensure necessary diversity. We also want to see that in their processes they have V&V activities that they're performing and they have people, independent V&V people that are looking at the end products and making sure that they are in fact diverse as they are designed to be.

MEMBER BLEY: I suspect it would be a great temptation for even those people to say team A has done a lot better job than team B. We ought really encourage them to do the same thing.

(Laughter.)

CHAIRMAN BROWN: Actually back in the '80s we not only used the software or the program -- which this isn't software. The microprocessor days, not FPGAs. But we actually had two cabinets with two sets of hardware like this, another two with another set of hardware plus two different teams designing the software. And after we went through that drill we threw it out as being cost-prohibitive and not very reliable in terms of improving anything because a number of studies were -- and this is on the software side, not on the FPGA programming-type stuff. That if you used the same language then as people program using the same language they get to certain things they have to solve, but it was amazing how few solutions you could get to. There were limited choices and some were better than others. And so you didn't have the true diversity. Now if you used a different language in each one, then your support costs just skyrocketed, particularly when you do everything customized the way we did it.

MEMBER STETKAR: I was going to say it was too expensive for --

CHAIRMAN BROWN: No, I mean --

MEMBER STETKAR: I was going to say, too expensive for the Navy is a perspective.

CHAIRMAN BROWN: And we really had to look at, you know, where was the value-added coming from. So I mean it's --

MR. STATTEL: Now, I'll mention one of our previous reviews that we performed was on the Wolf Creek MSFIS system. They used the same system -- well, the same FPG.

MR. THORP: For folks on the phone, the Wolf Creek Main Steam and Feedwater Isolation System.

MR. STATTEL: Thank you. So they used the same ALS system, but they only used core diversity. So they were only implementing differences in the code by giving different synthesis directives. Okay? And we approved that, but in that safety evaluation we identified -- that was a very simple function which could be fairly comprehensively tested. So we approved it for that application, but we identified the fact that a more complex application, like what we're looking at today with Diablo Canyon, would require an additional level of diversity. And that's where the imbedded diversity is implemented.

MEMBER BLEY: Well, this would be interesting to see how it all turns out.

CONSULTANT HECHT: Yes, I just wanted to ask a couple of things.

MR. STATTEL: Yes.

CONSULTANT HECHT: I guess number one question is, does this not introduce a problem where you would have mismatches and thereby cause the ALS system to become less reliable because of those mismatches?

And then associated with that is can't you take some credit for diversity in the Tricon? And why do you need to have, you know, redundancy within -- diversity within diversity here?

MR. STATTEL: Well, I'll answer the second first. In a way they do take credit for diversity of the Tricon in that in the D3 analysis there are several cases where a function of the ALS is -- in the backup column they've identified a diverse function in the Tricon. So they have taken credit for the diversity between ALS and Tricon.

MEMBER STETKAR: Right.

MR. STATTEL: So that's part of the equation.

Now, the first part of your question, let me think about this a second.

MS. ALVARADO: If I can jump in, first of all, both cores have to meet the requirements as specified, right?

MR. STATTEL: Right. Okay.

MS. ALVARADO: So the V&V team is definitely looking into that both core perform per the requirements to where define for the cores to perform. Even though your synthesis process is different and your design is different and your different teams, you still have to meet the same requirements.

CHAIRMAN BROWN: You mean get the same end result so there's not a mismatch?

MS. ALVARADO: Correct.

MR. STATTEL: That's correct. Well, it's a little more complicated than it.

CONSULTANT HECHT: Yes, actually it is.

MR. STATTEL: So core 1 and core 2 are implemented basically on the same circuit board. The results of those cores and intermediate signals of those logic implementations are compared and that comparator is actually part of the design of the system. So if there is a mismatch -- and this is a question I have asked to the vendor, right? If there is a mismatch how is the system going to respond to that? What are the failure modes of that? That's one of the RAIs that I asked to the vendor and they provided me with that information, right, because it is defined in the system requirements.

As far as the core A and core B, basically the outputs of those are or'ed, basically. And actually this next figure kind of shows that. So each protection set has a core logic A and core logic B implementation. The outputs are or'ed before they go down to the SSPS coincidence.

CONSULTANT HECHT: Well, I guess or it depends on whether that's to trip or not to trip, right? So and the other thing is is that is the only output that you're getting from the ALS logical or is there actually some numerical output as well?

MR. STATTEL: The safety functions are all logical outputs.

CONSULTANT HECHT: What about diagnostics or what about things that people would make decisions on?

MR. STATTEL: I'm trying to think. I don't think there are any analog output signals from the ALS portion of the subsystem. Those are handled either by analog devices -- they have analog isolator devices that are on the signal inputs and they provide a signal over to meters, right, that are on a control board.

CONSULTANT HECHT: Yes.

MR. STATTEL: Or there are cases where the Tricon is actually sending a signal over to a meter on the control board to indicate like trip set points.

MS. ALVARADO: Right.

MR. STATTEL: Right? So the operator would have that information. Now that would go away on a common cause failure, right, but it's a trip set point that's calculated within the Tricon system. So it has to be reliant on the computer system to develop that signal.

CONSULTANT HECHT: So I guess --

MR. STATTEL: But for ALS I don't believe -- I'm trying to -- I'm wracking my brain right now. I don't believe there are any signal outputs for operator indications.

MS. ALVARADO: No, I have all these great signals.

CONSULTANT HECHT: So basically you're relying on the completeness of the requirements and if those requirements are complete -- and by the way, I guess there's also timing associated with that --

MS. ALVARADO: Correct.

CONSULTANT HECHT: -- so that there's this, I guess -- I don't know that or gate, I don't know exactly how that works. Does it sample --

MR. STATTEL: I'll show you that.

CONSULTANT HECHT: -- at the light times. So if there's one vote to trip, you trip?

MR. STATTEL: That's correct.

CONSULTANT HECHT: If it's energized or de-energized?

MR. STATTEL: Right. So let me jump ahead a couple slides and I'll show you that.

CHAIRMAN BROWN: There is one analog output and that's the temperatures that come through, because those are fed into --

MR. STATTEL: That's an analog output, but it's to an operator indication necessarily.

CHAIRMAN BROWN: No, that just goes ad Tricon, wherever it goes from there.

MR. STATTEL: That's right.

CONSULTANT HECHT: But that's I assume before it comes to this board though, right?

CHAIRMAN BROWN: This is just a box on the diagram.

(Laughter.)

MR. STATTEL: This diagram is showing the logic output, the trip determination, the partial trip determination coming from the ALS. So this is the safety function. This is not showing analog signals. The only analog signal outputs that I'm aware of on the ALS would be the temperature signals that are input into the Tricon system.

CHAIRMAN BROWN: And reactor coolant flows.

MR. HEFLER: Excuse me, Rich. There's also the reactor coolant pump flows.

MR. STATTEL: Oh, the indicators?

MR. HEFLER: There's indicators for the RCS flows.

MR. STATTEL: From ALS?

MR. HEFLER: Yes. Because RCS flows and is processed by ALS.

MR. STATTEL: Okay. All right. I didn't know of another way to represent how the outputs are or'ed, right, so I put an or gate in this figure. The way it's actually accomplished is this schematic diagram. So this shows the digital output cards. And this is a de-energize to trip configuration. And then the next slide will be the energize to trip configuration. So these are digital output cards. And since this is de-energize to trip, think of the DO card as being a closed contact. So in this case 120 volts is being provided through the two closed contacts through the manual trip switch and it energizes the SSPS train A and train B relays. Those are actually relays in the SSPS system.

So you can see if either one of those card contacts opens, it will cut the power to those relays, it will drop out and that initiates the trip. That's a de-energize to trip.

CHAIRMAN BROWN: The circle with the 120 is just the voltage? It's not a relay?

MR. STATTEL: That's just a voltage, that's correct.

CHAIRMAN BROWN: That's a voltage? Okay.

MR. STATTEL: I didn't draw it. They drew it, so --

(Laughter.)

CONSULTANT HECHT: For trips the switch is basically the operator of the or gate.

MR. STATTEL: That's exactly right. And you can see here -- I mean this is a schematic drawing. So that if you open manual trip switch, it doesn't matter what happens on the computer system, it's going to de-energize those relays. It's just a direct in-line contact with the relays. So you can see that the manual trip function is not impacted by the digital system at all.

CONSULTANT HECHT: Wait a second. There's a manual function. I get that. And then there's the operator of the or gate. I thought you just said that the output of the or gate is kind of the metaphorical manual trip switch here. Is that not true, or is this a real manual trip switch?

MR. STATTEL: Well, I guess the or gate should have a third input, and that would be the manual trip switch. So it would be either ALS A, or ALS B, or the manual trip.

CONSULTANT HECHT: I see. Got it. Okay.

MR. STATTEL: That would be more accurate.

CONSULTANT HECHT: Yes, that would be better. I did not understand this figure.

MR. STATTEL: Right. And then the next figure basically shows the same configuration, but on an energize to trip situation. So here you can see the contacts of the digital output card are in parallel. So here it's 48 volt DC and in order to energize you have to close the DO contact of ALS A or ALS B. And if either one of those closes, it's going to put 48 volt DC over to the relays that are in the SSPS system.

Now here the manual trip switch is also in parallel, right? So here closing the manual trip switch energizes those relays regardless of the state of the digital system. Okay?

CHAIRMAN BROWN: You're going backwards in your slides. That's messing up my time frame here.

MR. STATTEL: That's okay. I'm going to go through the next couple pretty quickly.

CHAIRMAN BROWN: Before we get moving, you've got five minutes, because we're going to take our break at 3:00 as opposed to 2:45.

MR. STATTEL: Okay. So this figure here is really just showing here's what a software or logical implementation CCF malfunction of the B cores might look like. So here we have the common error on all four protection sets. All four B cores use the same logic, so all four would be affected. Though the fault affects all four redundant protection sets, each set retains its ability to perform its safety functions via the diverse core A logic. And again, the or gates would not be affected by the CCF.

Okay. And the next figure is basically just the opposite. So if we have a common cause failure of the core logic A, this is basically the functionality of the system would be maintained.

MEMBER STETKAR: And you're basically saying that there's no conceivable way that I can have both a core A and core B common cause failure?

MR. STATTEL: Well, I haven't said that yet --

(Laughter.)

MR. STATTEL: -- because we're performing our safety evaluation.

MEMBER STETKAR: Okay.

MR. STATTEL: But the object is to have reasonable assurance that that would not occur.

MEMBER STETKAR: We're probably close to a good stopping point. Let me ask you a --

MR. STATTEL: Yes, it's probably fine.

MEMBER STETKAR: -- 30-second question, unless you want -- where's a good stopping point, Rich?

MR. STATTEL: Let me look real quick. I have three more slides, and these are really just talking about the ATWS and the manual operator actions, which we've already mentioned. So I could probably go through these pretty quick.

MEMBER STETKAR: Go through them then, because I --

MR. STATTEL: This slide is pretty busy, but it's really just showing that, you know, part of our evaluation is establishing that the replacement digital system remains diverse from the ATWS system, right? So these are basically the different attributes of the system that we're comparing between the two systems. We're comparing the differences between the existing AMSAC and the replacement PPS system. This really shows the results of what we've seen so far.

Though the ALS and AMSAC systems are currently supplied by Westinghouse, they are the same vendor technically, the ALS platform was originally developed by an independent vendor CSI, which was later purchased by Westinghouse. So it's in fact a different vendor as far as the development of that.

The ATWS system is implemented via the existing Diablo Canyon ATWS Mitigation System, which trips the main turbine and it starts auxiliary feedwater and isolates the steam generator blow-down on coincidence of low, low steam generator water level in three out of four steam generators.

This figures shows the functional relationships between the PPS and the AMSAC systems. As you can see, the only interface between these systems is the steam generator level signal. Actually and turbine impulse pressure as well. That does feed over the AMSAC system.

The steam generator level systems that are used for AMSAC actuation are derived from the same sensors that provide input to the Tricon subsystem, however, these signals are provided to AMSAC through qualified analog isolation devices. Again, no reliance on software or logic implementation there.

Okay. We confirmed through our review of the interface requirement specification for the PPS system that the steam generator level input signals used for AMSAC are independent and isolated from the PPS system.

Okay. Finally on manual operator actions, I kind of show on the schematics where the trip functions -- how they're independent from the digital system. One of the objectives of this modification is to eliminate the need to perform certain manual actions as a means of coping with software common cause failure.

The modification does not affect the ability of the operators to perform the manual operator actions of the safety functions. Again, we talk about this early on. Those are direct hardwired inputs into the SSPS system, so they still retain the ability for channel level or functional actuation of the various safety functions. So the previously credited manual operator actions will still be available to the operators, so both the component and division level actuation capability at the control boards is retained.

And that's it for diversity.

MEMBER STETKAR: This slide, that first bullet, I'll come back my earlier ranting. If I can have a software common cause failure only in the Tricon system, I still don't understand how it eliminates the need to perform manual operator actions as a means of coping with software common cause failure within the PPS, because I still don't understand how you get the main steam line isolated for a steam line break outside the containment and I don't really understand how you can get aux feedwater started for a reactor -- a loss of main feedwater that results in a successful trip of the reactor and a trip of the main turbine without manual action.

MR. STATTEL: I mean I guess more accurately what I'm saying is; and I guess this is a poor choice of wording on this slide, the modification is eliminating those manual actions that were being credited for the three input signals that I had mentioned before.

MEMBER STETKAR: That is a logically correct statement.

MR. STATTEL: It is not eliminated credited manual operator actions that had previously been credited in the original D3 analysis.

MEMBER STETKAR: Okay.

MR. SCHRADER: This is Ken Schrader. I agree with that statement.

MEMBER STETKAR: Okay. You have to be very, very careful when you use words like "eliminate," "all," "no."

MR. STATTEL: Right.

MEMBER STETKAR: Because one could be left with the impression that that first bullet can be taken at face value, which it can't.

MR. HEFLER: Mr. Stetkar?

MEMBER STETKAR: Yes?

MR. HEFLER: This is John Helfer. I had a question for you, sir. When you just mentioned on starting aux feedwater --

MEMBER STETKAR: Yes?

MR. HEFLER: -- you said that was after a successful trip.

MEMBER STETKAR: After a successful reactor and turbine trip, yes.

MR. HEFLER: And what was the reactor trip based on?

MEMBER STETKAR: Low-level steam generator level coming into the Tricon system.

MR. HEFLER: Okay. in that case the low, low steam generator level, if it trips the reactor through the Tricon will also initiate aux feedwater.

MEMBER STETKAR: Regardless of the status of turbine first stage impulse pressure?

MR. HEFLER: That is correct, sir.

MEMBER STETKAR: Ah, thank you. Good. We solved that one. People design the AMSAC systems -- you know, I've seen a bunch of different designs
and --

MR. HEFLER: Well, that particular scenario that you described does not go through AMSAC. But I'm doing some checking on AMSAC because there may be a feature in AMSAC that addresses your concern there, too.

MEMBER STETKAR: Just simply the low, low -- let me see if I can understand what you're telling me.

MR. STATTEL: Just a simple loss of feedwater?

MEMBER STETKAR: Yes, and I don't want to get into -- the problem is you can lose feedwater many different ways. I've seen people stylistically say that, well, the only way I can really lose feedwater is tripping the main feedwater pump, so signals are taken off of main feedwater pump output breakers.

MR. STATTEL: Right.

MEMBER STETKAR: I've seen people say the only way you can lose it is loss of power, so signals are taken off of loss of power. I also need to careful about low steam generator levels, but I think that's pretty much the way --

MEMBER BLEY: Well, that comes through Tricon, so that wouldn't have tripped yet.

MEMBER STETKAR: No, Tricon --

MR. STATTEL: That's the CCF --

MEMBER STETKAR: It's the CCF. I believe in things that I was looking at --

MR. STATTEL: The steam generator level is the Tricon --

MEMBER STETKAR: -- the Tricon system is aux feedwater. ALS does not initiate aux feedwater.

MR. STATTEL: That's correct.

MEMBER BLEY: Are you saying if you anchored this with a low, low steam generator level you wouldn't have even gotten it because it failed in Tricon? That's a Tricon signal.

MR. HEFLER: But in that case if you've lost the Tricon, then you haven't had your successful reactor trip. You haven't had your turbine trip --

MEMBER STETKAR: Yes, you have, because you have the --

MR. HEFLER: -- initiated aux feedwater through the armed Tricon system.

MEMBER STETKAR: Yes, except for the fact that the redundancy for the reactor trip indeed you get is pressurizer high reactor trip, which comes through ALS. I couldn't find any reactor trip signals, at least in kind of my thought process, that didn't have redundancy between Tricon and ALS. I couldn't get an ATWS, but some of these other functions I think I could get. So I think that you would get the reactor trip through the high pressurizer pressure from the ALS.

MR. STATTEL: I'll say this: When this application came in, I was a little bit surprised, because I knew they were using two different platforms and I assumed that they would duplicate functionality between Tricon and ALS. So basically ALS would be the diverse actuation system for the Tricon. But that wasn't the design philosophy that was used. So I was very surprised when I initially saw this particular application. However, when you get into it, you really find that there is some reliance on the diversity between those two subsystems when we actually got into the review.

MEMBER STETKAR: When you say diversity --

MR. STATTEL: And it comes out in the D3 analysis.

MEMBER STETKAR: When you diversity in the subsystems, you mean Tricon versus ALS?

MR. STATTEL: Correct.

MEMBER STETKAR: Not the cores within ALS?

MR. STATTEL: Yes, and they are diverse, so there's no reason not to take credit for that.

MEMBER STETKAR: You know, the only things I found were the ones that I've mentioned, the steam line isolation on a steam line break outside containment, downstream of the MSIDs --

CHAIRMAN BROWN: We're losing control here a little bit, John.

MEMBER STETKAR: -- aux feedwater and LOCA response.

MR. STATTEL: Correct.

MEMBER STETKAR: Fine.

MR. STATTEL: Okay?

MEMBER STETKAR: One last question to the applicant: I thought that I read that the Diablo has three DC power divisions. Is that correct? Do you have three or four safety-related DC power, 125-volt DC power?

(No audible response.)

MEMBER STETKAR: Okay. We'll take a break.

CHAIRMAN BROWN: Okay. We will now recess for 15 minutes and we will return at 3:20, and we'll catch up.

(Whereupon, the above-entitled matter went off the record at 3:05 p.m. and resumed at 3:26 p.m.)

CHAIRMAN BROWN: The meeting is back in order. During the break --

MEMBER STETKAR: Just for the record, Charlie, we got a little more information about how the Diablo Canyon AMSAC system performs, and that I believe alleviates my concern, at least about automatically initiating auxiliary feedwater with a common cause failure in the Tricon.

So if Diablo would like to for the record put --

CHAIRMAN BROWN: Make a statement?

MEMBER STETKAR: -- make a statement---

CHAIRMAN BROWN: Have at it. Take charge.

MEMBER STETKAR: -- because I don't want to risk too much misinterpretation of their system.

CHAIRMAN BROWN: Have him go ahead and make a statement for the record on answering your question.

MR. HEFLER: Thank you, Mr. Stetkar.

CHAIRMAN BROWN: Can you hear okay?

MR. HEFLER: This is John Hefler with PG&E. And what I just wanted to clarify on the way that AMSAC works, it monitors the forced steam generator levels and also monitors turbine impulse pressure or turbine first stage pressure.

And it arms itself when the two impulse pressures have been over their setpoint. The important thing to remember, though, is that it remains armed for four minutes or 240 seconds after the turbine trips. There's a time delay there.

So in the scenario that we were describing here where you had a reactor trip due to something, not necessarily low steam generator level, and let's say that it was high pressurizer pressure, which could happen through the ALS rather than through the Tricon, in that case as soon as the heat input to the steam generator stops due to the reactor trip, the levels will collapse, and that's a very fast collapse.

The AMSAC is monitoring the levels, the steam generator water levels. And because it remains armed for 240 seconds afterwards, it will start aux feedwater. And so that alleviates I believe that concern.

The other thing that's important is that the turbine impulse pressures and the steam generator levels come off the front end of the instrument loops prior to any digital processing. So they are independently isolated and independent from any digital processing.

MR. STATTEL: Right. And that's an important feature, and that's something that I didn't mention earlier. But in the existing Eagle 21 system, that is a weakness of that system because currently the Eagle 21 provides an analog signal over to AMSAC, I believe, for the aux feed actuation.

MR. HEFLER: No. It -- right now it provides signals to digital feedwater.

MR. STATTEL: It was aux feed actuation as well, I'm pretty sure. But, anyway, those dependencies are -- there are dependencies where the Eagle 21 provides analog signals to other external systems, and those have been eliminated in this design. So there is no longer the reliance on the software or digital system in order to provide those signals to the independent system.

I believe it's aux feedwater. There was an issue at another plant with similar design, Eagle 21 design.

MR. HEFLER: This is John Hefler again. That is an important point -- that the design of the replacement system for those important signals that would be -- are dependent on digital processing right now. Those will be taken off the front end of the instrument loops for the critical control systems like digital feedwater, pressurizer pressure, and so on, so that you don't have the possibility of a malfunction in the Tricon causing an undue influence in those control signal systems. It sort of decouples them.

MR. STATTEL: Thank you.

CHAIRMAN BROWN: All right. Rich, are you ready to go?

MR. STATTEL: Our next area of discussion will be communications, and I'll have Rossnyev Alvarado lead that discussion.

MS. ALVARADO: Thanks. This is my first time presenting in the ACRS. I am going to do 10 seconds of bio, so this is really quick.

I'm Rossnyev Alvarado. I work for NRR/DE, Division of Instrumentation and Control -- I'm sorry, the Branch of Instrumentation and Control. I have been with NRC since 2010, and before coming to the NRC I worked for almost 10 years with MPR Associates, which is a consulting firm down in Alexandria. And prior to my graduate work I worked in Venezuela. I'm from Venezuela, and I worked for the oil and gas company. So it has always been in the instrumentation and control area. So that's a little bit about me.

Next slide?

This slide summarizes the guidance that we have available for communication. And 603, which is referenced in 10 CFR 50.58(hh), provides the criteria for independence between redundant portions of our safety system and between safety systems and other non-safety-related systems.

7-4.3.2 adds to the requirements of the IEEE 603 that data communication between safety channels or between safety and non-safety systems should not inhibit the performance of safety functions. To clarify the guidance provided in 603 and 7-4.3.2, the Digital I&C Steering Committee created a Task Working Group Number 4, and this task working group prepared what we now have, ISG-04, which provided that there is points for evaluating digital systems communication and compliance with the NRC regulations.

The ACRS, as Rich mentioned before, has reviewed the ISG-04, and that is the guidance that I am currently using for evaluating the communications for Diablo Canyon PPS system.

Next slide?

Stealing this slide from Rich, two of Rich's slides actually, I just want to reemphasize that there is no communication between the protection sets, which are the vertical lines that we can see here, and there is no communication between the Tricon system -- digital communication between the Tricon system and the ALS system. So, in this manner, the licensee agreed to maintain divisional independence between these protection systems.

In addition, there is no communication -- and Rich went into detail providing this -- between the protection system and the solid state protection system. As he mentioned before, these are trip sessions that are sent from the PPS to the solid protection system as discrete electrical signals through the interposing relays.

Next slide?

Again, sorry for repeating this, but I just want to show this is the figure that was provided in the license amendment for Diablo Canyon. This figure shows one protection set, and it is exactly the same communication architecture for all protection sets.

Here we can see the separation between the independence between protection set with the red line, which is exactly the same that we saw in the previous slide on the vertical lines, and then the separation of communication between the Tricon and the ALS for the digital communication, which is the horizontal lines that we saw in the previous slide.

The same level of communication separation is used for all four protection systems.

Next slide?

So taking one of those, what I am going to do is walk through the different communications data links provided in our protection system. In this case, we are doing protection set IV, and I'm going to explain each one of these components.

So here is like the previous figure loaded into the different components to show more detail. So there is a link between the ALS and the Tricon, as we have talked about before, but this is an analog temperature signal that is processed in the ALS, and the Tricon uses to perform the overpower differential temperature and overtemperature differential temperature reactor trip safety function.

This is an analog signal, and there is not any kind of digital communication.

Within each protection set we can see several components that are non-safety-related, and there is communication between the Tricon and the ALS to these non-safety-related elements. So I am going to talk about them, and I am going to describe how the Tricon and the ALS performed these communications.

But before we go there, I want to just point out some of the elements that we can see here. The MWS is what Rich described before as the maintenance workstation. The KVM is the keyboard/video/mouse switch. So what we have in this slide --

CHAIRMAN BROWN: Can I ask a question? I'm transitioning from two slides earlier over to this one, and this is supposed to illustrate safety to non-safety communications, and --

MS. ALVARADO: That's correct.

CHAIRMAN BROWN: -- where -- by "non-safety," in this circumstance do you mean information that goes to the operators, or what---

MS. ALVARADO: Yes.

CHAIRMAN BROWN: -- type of -- because I don't -- this all looks like safety stuff, if I look at this picture.

MS. ALVARADO: Right. And I should have like provided a line to separate what is safety from non-safety here. I just wanted to show all the components that are related. The maintenance workstation, the stations that are---

CHAIRMAN BROWN: That's a non-safety system.

MS. ALVARADO: Right.

CHAIRMAN BROWN: So that's the way --

MS. ALVARADO: Correct. Yes. So the maintenance workstations are non-safety-related, and the plant computer system is non-safety-related. So those are the non-safety-related that are shown in this slide.

MR. STATTEL: If you look at the previous slide, this slide here, the boundaries -- so the maintenance workstations are shown. The maintenance workstations are shown here. This is the Tricon maintenance workstation, and this is the ALS maintenance workstation, through the keyboard/video/mouse display to those components. And then the plant computer is shown on the right side here. That's the interface to the plant computer.

And these directional arrows are meaningful in that this is a one-way communication path. Okay? So those are the equivalent paths to what we see here. So, again, the communication to the maintenance workstation, Tricon, and ALS, operator interface, and then the plant computing system.

So everything, really, outside of the Tricon and ALS boxes here is a non-safety-related component.

CHAIRMAN BROWN: Okay.

MS. ALVARADO: Did I answer the question?

CHAIRMAN BROWN: Yes. I have one other semi-related question. In an earlier discussion, we had talked about this port tap.

MS. ALVARADO: Yes. I will go into details to talk about it later.

CHAIRMAN BROWN: Okay. Then I'll wait.

MS. ALVARADO: Like I was saying, we have two maintenance workstations, one provided for the ALS and one is provided for the Tricon. Two maintenance workstations are provided per protection set.

The maintenance workstations do not communicate with other maintenance workstations in other protection sets or with other controllers, except for the ones in their division. In addition to that, both the Tricon and the ALS portion of the PPS communicate data to the plant computer system. The plant computer system is part of the existing system and is not part of the scope of this license amendment. So we are not changing anything for that.

I will talk into details about how the communication is done, but, in summary, the Tricon transfers the data to the port tap, which I will present later, and the ALS does it through the transmit TXFB communication ports, which I will talk about when I go into details.

CHAIRMAN BROWN: What did you assess? It communicates -- are you talking about just the TAB to the MWS?

MS. ALVARADO: No. The TAB is used actually --

CHAIRMAN BROWN: Okay. Are you talking about the bottom red line?

MS. ALVARADO: Yes.

MR. STATTEL: Well, the orange lines.

MS. ALVARADO: These two lines are the ones that are used for communication, and it's one-way communication. Let's just go into the ALS description, and I will explain that in more detail, because the TAB -- the one that I have -- the TAB here is a two-way communication.

CHAIRMAN BROWN: Yes. I got that part. I'm looking at the other one. Okay. Skip the next one.

MS. ALVARADO: No. Hold on. The KVM switch, which Rich talked about it, is keyboard, video display, and mouse. It is just a switching device that -- what it does is provide access to the peripheral devices for the operators to monitor the PPS subsystem. So it will be either the ALS or the Tricon per division.

MR. STATTEL: Now, I'll mention these -- these displays are mounted inside the cabinets that are in the cable spreading room, which is a level below the control room. So these are not displays that the operators would be standing at or operating. That's not our expected use of those displays. They are really used for initiating surveillance tests and performing diagnostic functions.

MS. ALVARADO: Okay. I just want to point out, the last thing in this is like near the maintenance workstation or the KVMs which has any sort of access to the plant network or the internet.

MEMBER STETKAR: Rich, something you just said just struck a chord here. When you use the term "operator," do you really mean human being, or do you mean a licensed operator?

MR. THORP: Maintenance or ops.

MEMBER STETKAR: Okay.

MR. THORP: Really --

MEMBER STETKAR: Because the qualification you inserted about the displays at the cabinets are not things typically that I would think that licensed operations personnel would be --

MR. STATTEL: I was really talking about the licensed operators. Right. So basically these displays are inside of cabinets with opaque doors that are closed and locked during normal operations. So it's not something operators would typically be relying on to make any operating decisions. That's my point.

MEMBER STETKAR: Okay. Thanks.

MS. ALVARADO: Okay. Next slide?

This is just -- Rich, I guess we didn't get into the --

MR. STATTEL: Did you want this one?

MS. ALVARADO: Yes. this slide is just to show how the signals from -- the analog temperature signals are used by the ALS and the Tricon to perform the protection functions. This is just for information, to see that these signals, how they are processed by -- and used by both systems.

And the orange or pink is the ALS that is processing the signal, and then in the blue is how the Tricon performs the function. So this is just for information.

Next slide?

Okay. Now let's talk about the ALS communication. First of all, there is no communication path between the Redundant Safety Division or the protection sets in the ALS portion of the PPS replacement. The ALS subsystem doesn't require a port tap device to enforce one-way communication.

Instead, the ALS has two custom ports called TXB ports, which are in this case the orange lines that you can see there and are one way. These ports are configured such that it is only possible to transmit data through these connections. This is one-way communication and doesn't require the use of handshaking signal.

I'm going to skip to the next slide, please.

CHAIRMAN BROWN: Say that again.

MS. ALVARADO: Next slide?

So this is the --

CHAIRMAN BROWN: No, no, no, no, no. Go back. You're way ahead of my question.

MS. ALVARADO: I'm explaining the orange lines.

CHAIRMAN BROWN: No. I'm -- you said "handshaking."

MS. ALVARADO: There is no handshaking.

CHAIRMAN BROWN: Oh, I thought you -- I missed the "no." I'm sorry about that.

MS. ALVARADO: No, that's okay.

CHAIRMAN BROWN: I missed that.

MEMBER BLEY: And now she is going to show you why they can't.

MS. ALVARADO: Yes. I was going to tell you again there was --

CHAIRMAN BROWN: I was just going to tell you, if you want to say what you're going to say, your Slide 36 is a lot better than this one.

MS. ALVARADO: My Slide 36?

CHAIRMAN BROWN: That's your next one.

MS. ALVARADO: Okay.

CHAIRMAN BROWN: No. Slide 36 is the one that shows TXB-1 and TXB-2 coming from these and going over to the plant computer with the RS-422 lines on them.

MS. ALVARADO: Oh, no, no. What I'm trying to -- okay.

CHAIRMAN BROWN: That's what those lines are.

MS. ALVARADO: Right. Correct. What I'm trying to show with the next slide is just how the ALS has configured these ports to enforce one-way communication that is hardwire-enforced. So this is the circuit that they're using, and the way this works is that the TXB that you can see there on the top is the one that drives the transmit channel circuit, and the receiver, which is the TXFB, is configured in such a way that the transmit data is looped back for channel integrity.

So the data will -- it will never -- you will never get data from the outside into the --

CHAIRMAN BROWN: NSR? Non-safety-related.

MS. ALVARADO: Non-safety-related.

CHAIRMAN BROWN: Plant computer? Yes.

MS. ALVARADO: Yes. In this case, it will be the plant computer system or the maintenance workstation.

CHAIRMAN BROWN: Correct.

MS. ALVARADO: Through the TSX. I still have the TAB bus, which is a different -- we will talk about it --

MR. STATTEL: That's why there's two links here. One -- these are both TXB ports, the two orange lines. One is communicating to the maintenance workstation; the other is to the plant computer system.

CONSULTANT HECHT: Can I ask a question?

MS. ALVARADO: Sure.

CONSULTANT HECHT: You don't have the handshaking, so the receiver has got to get what it can. But the plant system is depending on signals coming from the ALS. Isn't there a problem about, you know, loss of signal integrity, loss of corruption, loss of synchronization, that might result in the plant computer system not getting the signals from the ALS?

MR. STATTEL: Well, these are not safety-related systems. So they are not relied upon for performing any safety functions. Even the operators would not use indications from the plant computer to make their safety determinations.

CONSULTANT HECHT: But they are still being used by the plant computer. I mean --

MR. STATTEL: They are inputs to the plant computer. That's correct.

CONSULTANT HECHT: Right. So what happens if the plant computer doesn't get them?

MR. SCHRADER: This is Ken Schrader. You know, the plant computer does not -- it is just for information. It doesn't perform any safety function whatsoever.

CONSULTANT HECHT: Well, are those computers saying like the ALS has tripped something or that -- I forgot exactly what the signal --

MR. SCHRADER: Those indications would be provided on the control board.

MS. ALVARADO: Yes. They will provide -- if there is any problem or failure with the ALS system, it will be annunciated in the main annunciator system.

CONSULTANT HECHT: Well, then, why have any links?

MR. SCHRADER: Just so that you -- you have a way to get information on the performance of the system online without going down to the cabinets in the cable spreading room.

CONSULTANT HECHT: So they're only status signals for the ALS?

MR. HEFLER: Excuse me. Its information signals go to the plant computer, but they're not relied on to make safety decisions. In one case that you had mentioned, if the ALS tripped something, or if the Tricon tripped something, there is hardwired -- well, they're multiplex, but there's indicator lights coming out of the solid state protection system.

It's a hardwire multiplexing, but there are postage stamp indicators on the main control board that will tell you what the trip status is of the SSPS for whatever initiates the trip. Those don't depend at all on these data links.

CONSULTANT HECHT: I'm still trying to figure out if there is any impact at all on plant operations, normal operations, if you don't have those indications. And if you don't have those indications, why are they there?

MR. SCHRADER: The answer is no, because the plant computer does not perform any, you know, relied upon functions. It's just for information.

MR. THORP: I might offer just an observation that as SRO on a nuclear plant for about eight and a half years, our typical use of the plant computer was to provide just sort of ongoing point trending. In fact, we would as individual operators select groups of points that we found most interesting to us or that would help us as we were trying to perhaps analyze some way that a system was not operating as efficiently as it could or wanted to see what was going on. And so we would observe those points.

So typically the way the computer was set up -- and I'm not a computer expert, but I was a computer user, and we would -- we would identify -- see that the points that were coming in, if there was something that went wrong upstream, that began to feed bad data to those points, there were means by which the computer could identify that the point was now bad and would indicate so, and then that would give us pause to reflect on what is the source of that, and we would call for help if we needed it.

But it was -- it was always more informational and just sort of that extra degree of cognizance of what's going on in the plant, allowing us to stay more well informed.

CONSULTANT HECHT: So the only thing that is happening is that these signals would be displayed? They were not used in any control algorithms or anything like that?

MS. ALVARADO: No.

MR. SCHRADER: That's correct.

CHAIRMAN BROWN: Okay. Let me go back to my question, because I had -- before she started talking, I was pretty much sold.

(Laughter.)

MS. ALVARADO: Wow.

CHAIRMAN BROWN: I didn't mean that in a negative --

(Laughter.)

MS. ALVARADO: Don't worry. I can take it.

(Laughter.)

CHAIRMAN BROWN: You know, I have looked back and forth at so many of these pictures, and I thought I was pretty much convinced that everything was happy, and I was going to be happy, but then I look at that picture and that's an ALS/TXB communications port.

And then I go look at the LAR, where it talks about the receive capabilities with TXB channels and the -- this is an ALS-102 line, are physically disabled by hardware on the ALS board, and I don't see any physical disabling at all. I just see a continuous back and forth. One set of data goes out, and another set of data comes back in from the --

MS. ALVARADO: This is the one driving, right?

CHAIRMAN BROWN: That's the transmit.

MS. ALVARADO: Okay. Well, this one is coming back here.

MEMBER STETKAR: It's easier -- stay close to the mic and use a mouse or something, so we pick up --

CHAIRMAN BROWN: I see what you're doing, but you've also got a direct feed from the NSR that comes back in and goes in that way also. So your diagram just shows --

MS. ALVARADO: Look, this is --

CHAIRMAN BROWN: Go up. I have no idea what a little round circle means.

MS. ALVARADO: It's a knot. It's not coming back. It's a knot.

CHAIRMAN BROWN: On that line, but you're feeding something back the other way back to the FPGA.

MS. ALVARADO: No, I'm not. This is the line that is transmitting data, and it's -- this is the loop back that I'm sending to check for integrity check between the data that you send, to compare there is -- that it is the same data that you are receiving. This is not connected. I'm sorry. This is not connected.

CHAIRMAN BROWN: That's a solid line, and I'm --

MR. STATTEL: Even if you were to transmit data on this lower line here --

MS. ALVARADO: It will not come back here. It will not come back here.

MR. STATTEL: It wouldn't go anywhere. It's not connected.

MS. ALVARADO: It's not connected.

CHAIRMAN BROWN: It's transmitting on the upper line. Does that little circle mean it's disconnected?

MS. ALVARADO: Yes.

CHAIRMAN BROWN: The wire is separated, is that what that means?

MR. THORP: You should see a little hump there.

CHAIRMAN BROWN: That's all you had to say. That's not obvious. I see little lines. It's just a connector going in. That's all.

MR. STATTEL: Would someone from Westinghouse care to chime in?

CHAIRMAN BROWN: This is their diagram, is that right?

MR. STATTEL: Yes. This is from the topical report, the ALS topical report.

CHAIRMAN BROWN: I got it. You don't have to --

MR. STATTEL: Okay.

CHAIRMAN BROWN: I'm just trying to make it correspond to the LAR, which said very clearly that it was physically disconnected. That means the wire -- it's also what I was told earlier in a verbal discussion.

MR. STATTEL: What's not shown on here is the actual logic implementation that would be needed for the receive. It's not implemented within the core logic.

CHAIRMAN BROWN: Well, that's okay. That's just a design error. All of a sudden it gets implemented and somehow it's there and that's -- so having a wire broken makes it very difficult to transmit information on it, so I'm happy with that.

MS. ALVARADO: Can you go back? Okay. So let's go back, and then I'm going to talk about the TAB bus, which TAB stands for Test ALS Bus. This is the line that is shown in red. Okay?

The TAB bus can be connected to the ALS maintenance workstation to provide direct two-way communication for maintenance activities. Normally, the two-way connection between the ALS maintenance workstation and the ALS PPS is physically disconnected from the ALS subsystem. When online testing of the ALS subsystem is required, the TAB is physically connected, allowing two-way communication between the ALS maintenance workstation and the ALS subsystem. I want to point out there is no software associated with disconnecting or connecting this data link.

CHAIRMAN BROWN: There's no what?

MS. ALVARADO: Software.

CHAIRMAN BROWN: Is it a switch?

MS. ALVARADO: It's a cable. It's a cable that you have to --

CHAIRMAN BROWN: So the guy has got to hook up a cable from both sides.

MS. ALVARADO: Yes. So for this connection to be available, the TAB has to be physically connected to the maintenance workstation by qualified personnel under administrative controls; and, two, only one ALS -- core A or core B -- can be connected to the TAB at a time in a protection set. So I can just connect to core A or core B.

CHAIRMAN BROWN: Because there is only one cable.

MS. ALVARADO: The restrictions that we are imposing is --

CHAIRMAN BROWN: It's a procedural restriction.

MR. THORP: And just to clarify, I think Charlie had asked, does it have to be connected at both ends of the cable, or is it just one connection that has to be made? And that's --

MR. SCHRADER: I can respond to that. We disconnect at the maintenance -- back at the maintenance workstation.

MR. THORP: So there's just a single connection that you need to --

CHAIRMAN BROWN: All right. That's fine. I just --

MR. SCHRADER: Each ALS core, Alpha and Bravo, have a separate cable.

MR. HEFLER: Actually, we're more likely to disconnect it at the ALS chassis. It's easier to get to.

CHAIRMAN BROWN: All right. All right. Keep going. Keep going. We've got to make up some time here.

MS. ALVARADO: Okay. The diverse ALS subsystem connected to the TAB bus will be taken out of service with a section of the ALS added to the signal processing function, the temperature signals that we were talking about, which will remain operating during a specific surveillance test performed on the ALS functions.

The diverse ALS system that is not connected -- that the TAB is not connected to will continue to perform its safety function without being affected. Whenever the TAB is physically connected to one of the cores, an alarm will be annunciated in the main annunciator system.

Next slide?

Now I'm going to talk about the Tricon. The Tricon is slightly different, because the Tricon uses the port tap aggregator. And the Tricon communicates with the non-safety system to this port tap, and also the port tap provides two-way communications to the Tricon maintenance workstation.

So in the next slide, which Rich pointed out, it is -- we're showing the port tap aggregator. This is how it is devised. It does not rely on computer software to perform its function. It has three ports, and I added the color -- the blue arrows to show into which one of them they are connected.

Port A is for communication with the Tricon module, TCM. Port-B is for communication with the maintenance workstation. And Port 1 is for communication with the PCS, the plant computer system. So Ports A and B are two-way communications, and Port 1 is for one-way communication.

The port tap was previously evaluated and has been approved as an acceptable means of isolating safety systems. This evaluation was performed when we did a Tricon platform evaluation.

As part of this evaluation, the NRC performed a circuit analysis of this device to identify internal data signal flow paths using the device schematic, which is the schematic shown in the corner.

For these tests, the signal flow -- for the signal to flow from -- by the directional communication, in this case from the TCM towards the receiving instrument, in this case the plant computer system, electrical signals has to pass through a buffer amplifier integrated circuit component.

The buffer amplifier was further analyzed for the potential of electrical signals to flow in the opposite direction during failure or overload conditions. The result of this analysis shows that the amplifiers were not capable of passing electrical signals in the reverse direction under any condition.

So, in other words, data cannot flow from Port 1 to Port A, which is from the plant computer system to the Tricon.

To confirm this analysis, and the conclusions that the staff reached, the Office of Research contracted a lab to conduct data tests on an actual port tap device. During these tests, several attempts were made to force data signals to flow in the reverse direction. The test involved using several techniques to challenge the device integrity.

And I will ask Rich if he wants to add anything else, because I know he was involved on this testing.

MR. STATTEL: Well, I'll leave it up to you. I mean, I can describe the testing that we performed. It was pretty intrusive testing, and they basically challenged the device in many different ways. And they were able to cause communications to fail, right, through -- like large electromagnetic fields and things like that. But they were not able to force communications in the incorrect direction, the wrong direction, which is really the purpose, the function of the device.

CONSULTANT HECHT: That's true I guess between Port 1 and Port A or Port B, right?

MR. STATTEL: Correct.

MS. ALVARADO: Yes.

CONSULTANT HECHT: Okay. And I would have -- I assume that, once again, there is no information upon which the plant computer would make a decision coming out of the Tricon, is that correct?

MS. ALVARADO: That is correct.

MR. SCHRADER: That's correct. The plant computer does not perform any accredited functions.

CONSULTANT HECHT: All right. So, and from the MWS to the Tricon, obviously there has got to be bi-directional communications.

MS. ALVARADO: Correct.

CONSULTANT HECHT: And that only happens when Tricon is offline.

MR. STATTEL: No.

MS. ALVARADO: No. I will go there in the next slide. I will explain that.

MR. STATTEL: There is two-way communications to that -- the Tricon maintenance workstation during normal operation.

MS. ALVARADO: Yes.

MEMBER STETKAR: And can I ask one quick one before you get to the other thing? In the license amendment request, when they discuss the port aggregator, they talk about setting dip switches in the aggregator, and that those dip switches are set administratively and controlled under administrative practices.

Can those dip switches allow reverse communication from Port 1 to A or B? In other words, you said if the dip --

MR. STATTEL: We evaluated that, and the answer is no.

MEMBER STETKAR: It cannot.

MR. STATTEL: Those switches are used to basically set the parity mode and the modes of communication that are going through the device. So if the switches were set incorrectly, it could affect the ability to communicate through the device, but it would not impact the --

MEMBER STETKAR: The direction and flow.

MR. STATTEL: Right. So we evaluated that specifically.

MEMBER STETKAR: Thank you.

MS. ALVARADO: It doesn't set the direction of the communication. Okay.

MR. STATTEL: Actually, that question came up. One licensee was implementing the device, and they had the dip switches out of position, and the -- well, the inspectors called me and asked me about that, and we had evaluated that, and I told them, "Well, we really don't care what position they put those dip switches in."

MEMBER STETKAR: That's fine. Thank you.

MR. STATTEL: Okay.

MS. ALVARADO: Okay. The next slide?

In this slide I'm going to describe the communications for the Tricon system. So as I mentioned before, the Tricon system used the port tap to communicate the non-safety-related. There is also a non-safety-related communication that is happening with the remote RXM, which is a module that Tricon provides to acquire IO signals.

But before we go there, let's focus in the Tricon communication module, TCM, which is to the right of the system.

The TCM communicates with the port tap, right? But the communication that is acquired to the TCM doesn't go directly into the main processor. Instead, the Tricon uses the IOCCOM, which is the one here in the middle, which is an independent processor with dedicated memory location for communications with the TCM.

The IOCCOM processor is scan-based and does not use interrupts.

CHAIRMAN BROWN: What?

MS. ALVARADO: Scan. Scan.

CHAIRMAN BROWN: Oh, Scan. Okay. Excuse me.

MS. ALVARADO: No, that's okay.

It doesn't use interrupts. All communications between the main processor and the IOCCOM processor are via dual port RAM, DPRAM, which I'm showing in this slide. The dual port RAM provides separated, fixed, and dedicated memory locations and cues for communication messages and IO data.

The IOCCOM processor verifies the data before processing it and forwards it to the DPRAM. And from the DPRAM, the main processor can retrieve these data.

The DPRAM and the IOCCOM processor provides the primary protection for the safety processor, in this case the main processor in the Tricon. The Tricon subsystem also incorporates, as I've mentioned, the safety-related/non-safety-related communications to remote RXM chassis. The purpose of the remote RXM is to process non-safety-related IO signal to support non-safety functions in the PPS, such as the main annunciator system inputs and analog output signals to various main control board indicators.

The communications with the remote RXM, the Tricon uses the IO bus, which is showing here in the lines with the IOCCOM, to the primary RXM. And this communication is a master and a slave with the IOCCOM as the master. So the IOCCOM will send a request to the primary RXM, and this will process that request and send it to the non-safety-related RXMs to request the information provided.

The second --

CHAIRMAN BROWN: Okay. You've got me confused.

MS. ALVARADO: Okay.

CHAIRMAN BROWN: Let me tell you why I'm confused before you try to answer it. If you look at -- in your Figure 4-5, in the LAR it shows a primary RXM chassis, which you show there, and it shows a remote RXM chassis, which is --

MS. ALVARADO: The secondary.

CHAIRMAN BROWN: Okay. That's fine. But the primary RXM chassis is the one that issues trips to the SSPS, at least as shown on Figure 4-5. It says "discrete trips to SSPS."

MS. ALVARADO: Yes. Because that part is safety-related.

CHAIRMAN BROWN: So the main -- well, I guess what I'm getting to, there is a main chassis, which is TCM.

MS. ALVARADO: Right.

CHAIRMAN BROWN: And TCM --

MS. ALVARADO: No, no, no. No.

CHAIRMAN BROWN: I don't know. What's TCM?

MS. ALVARADO: TCM is for communication. TCM is only used for communication.

CHAIRMAN BROWN: Okay. All right. So it's the IO out of the main processor, IOCCOM.

MS. ALVARADO: Yes.

CHAIRMAN BROWN: I guess my question is, we have been talking about failures in the main processor or stuff like that. But is the primary -- I have no idea -- there was no real discussion of the primary RXM in terms of its functionality. I mean, is it another set of microprocessors?

MS. ALVARADO: Yes. It has its own microprocessor.

CHAIRMAN BROWN: Is it a TRICON platform?

MS. ALVARADO: It is a Tricon. It's a module of the Tricon. So it has --

CHAIRMAN BROWN: Okay. Let me go backwards. There is a data processing that you go through. There is a cycle time that the main processor goes through to calculate whatever -- throwing all of the variables together and come up with a trip. And then -- but now something goes over to the primary RXM, does it get operated on again? Is there a synchronization between? I'm trying to understand how that chain works in the normal processing cycle?

MR. STATTEL: Response here from Invensys.

MR. McKAY: John McKay from Invensys. The primary RXM will have three RXM modules in it, and they are going to kind of look like the MPs in the main chassis. But what they are is they are IO bus extenders, which allow us to have that non-safety connection to the remote RXM by a fiber optic connection.

CHAIRMAN BROWN: So it's for electrical isolation?

MR. McKAY: The fiber optics between the primary and the remote RXM are for electrical isolation between the safety and non-safety systems. But the RXM modules themselves are basically IO bus extenders.

CONSULTANT HECHT: But the diagram has the -- has an arrow indicating trips to SSPS. Figure 4-5.

MR. McKAY: That primary RXM still is a safety module.

MS. ALVARADO: It's a safety module. They are still within the safety --

MR. McKAY: The IO bus connection between the main chassis and the primary RXM are normal IO bus copper cables, but those are both safety chassis.

CONSULTANT HECHT: So is there voting in that remote chassis?

MR. McKAY: In the remote chassis, no. That is all taken care of in the main processors.

CONSULTANT HECHT: But there are three outputs out of the remote chassis. What's --

MR. McKAY: Those -- all that voting and all of the IO signals are taken -- are put forth through the IO bus, and that IO bus connection between the main and the primary RXM chassis is our copper IO bus cables. So in an up to 15 chassis Tricon system that we could have, you could have -- if they were all relegated as safety chassis, you could have safety signals going in and out of any of those other chassis. The primary RXM is still a safety chassis.

CONSULTANT HECHT: So if one channel of the Tricon says trip and the other two don't, what happens?

MR. McKAY: Do you mean one of the three?

CONSULTANT HECHT: One of the three going to the RXM or --

MR. STATTEL: It won't. That will be voted out.

CONSULTANT HECHT: That will be voted -- so then why do we need three RXM chassis there? Or is that three separate RXM chassis?

MR. McKAY: No, not three separate chassis, but three separate RXM cards, because the IOCCOM -- the main processors have also three separate IOCCOM processors, too. So each one is independent of the others.

MS. ALVARADO: These are the IOCCOM. These are the IO communication busses.

CHAIRMAN BROWN: Okay. I'm going to springboard from him. Okay? If you go back and look at the little picture they showed earlier of the three legs, each processor feeds out to an output leg, A, B, and C. It's way back there. Way back.

Now, those say -- where is the output? Is that the RXM? Or is that -- are those RXMs on the right-hand side? It says voter on that one.

MR. McKAY: No, they're not. But those are voted and then the output leg, A, B, and C, those are the independent IOCCOM processors. They will go out on each of the individual IO busses, which in the case of the remote RXM chassis are through those fiber cables.

CONSULTANT HECHT: So does that mean that there is a chassis after the voter? Where it says "output termination," that's where the chassis goes?

MR. McKAY: No, I don't believe so.

CONSULTANT HECHT: Because it looks like the voter is the last step before output.

MR. McKAY: No. The voter is -- the voting is done in the MPs.

CONSULTANT HECHT: The voting is done in the MP, and then you are fanning out the three lines to the chassis? That means that the -- is that what's happening?

MR. STATTEL: It's an extension of the IO bus.

MEMBER BLEY: What's confusing some of us is if it is an extension of the bus, it almost sounds like why do you need a processor there? You're just making that --

MR. McKAY: Well, it's a way of transferring the copper IO buses from the main chassis and the remote RXM into the fiber for the electrical isolation of a non-safety system.

CONSULTANT HECHT: Well, that would mean that the voting -- that means that there is nothing coming out of the IO chassis. But it says that there is a signal from the IO chassis going to the SS -- I mean, to the --

MR. McKAY: That's where those particular IO modules are. The voting of those IO signals is done in the IOCCOM, and then it goes out on the three IO buses to the primary RXM chassis, which then on all three channels will set that out.

MS. ALVARADO: I'm going to ask Steve if he has anything to add when he did the safety evaluation for the Tricon.

MR. WYMAN: Sure. Steve Wyman, DE I&C. Yes, I'll take a shot. I think of the RXM, the primary RXM, just like an input, IO module. So if you look up there you see three separate legs. You plug in an RXM module, and it's got three separate channels, just like an IO -- an input card or even an output card.

And the reason that it needs a microprocessor is because as it sits on the bus it is identified as a single address. Okay? But out here you have a whole other module that has got 10 more IO cards in it. So there is a whole bunch of addresses.

So when the main processor wants to talk out the IOCCOM processor, it says, "Hey, okay, we want to talk to that guy." So it's going to go and it's going to talk to that primary RXM module, and that primary RXM module is going to take that request and it is going to break it down and it's going to look at it. And it's going to say, "All right. Who am I talking to?"

Now, normally it would just be talking to a single IO card, but in this case it can potentially be talking to any one of, you know, a dozen or more IO cards. So there is extra information in there that it's not actually a processor.

They use an FPGA, and it strips the information off, it decodes it, and then it sends the information across the fiber optic cable and it now says, okay, on the other side, I'm talking to which of the 10 cards? And those -- that card will answer, and it will come back, and it needs to again take that return message and rewrap it, so that it looks like it's the answer coming from that single point. Does that make sense? No?

CONSULTANT HECHT: What's confusing in all of this is that if you look at Figure 4-5 there is a line saying directly to the solid state -- what is it, SSPS, and that is the problem. Figure 4-5, if we --

CHAIRMAN BROWN: Yes. And I'd like to get one other thing. This picture you showed, Slide 44, if you want to go to 44, is this one division?

MS. ALVARADO: Yes.

CHAIRMAN BROWN: So that's the three processors we see in one protection set.

MS. ALVARADO: Correct.

CHAIRMAN BROWN: And I come out to three primary RXMs.

MS. ALVARADO: Yes.

CHAIRMAN BROWN: And you say the voting is done within the circle of the main processors.

MS. ALVARADO: Correct.

CHAIRMAN BROWN: But they still go out on three legs. Is it the same -- so when we go out to output leg A, B, and C, is that an identical signal? Because supposedly if it's the median, or whatever it is, I mean, there was some --

MS. ALVARADO: Yes.

MR. McKAY: There is voting on each IO card also. There are three independent processors on each IO card as well.

MR. STATTEL: I think what part of the confusion is, this is not a functional diagram. This is really more or less showing the communications architecture. The RXM, the primary and secondary RXM, are just a means of extending the IO bus. So like the primary RXM is located in the same cabinet as your main chassis. So if you want to install input cards or output cards you can install them into that primary RXM chassis.

The fiber optic link over to the secondary RXM, that is our 1E barrier, right? So the communications that takes place between the primary RXM and the secondary RXM, that is something that we evaluated in the platform evaluation as being a qualified 1E to non-1E barrier.

So there are --

CHAIRMAN BROWN: Non-safety system communication.

MR. STATTEL: That's correct. This is non-safety-related system communication. So that was evaluated in the platform safety evaluation.

CHAIRMAN BROWN: Okay. Now let me ask one other question. The answer is either going to be yes or no.

MR. STATTEL: Okay.

CHAIRMAN BROWN: Maybe. If I look at this picture and each of those primary RXMs sends a discrete trip to the SSPS, I've got three other protection sets for any one function -- I just want to pick one of the functions -- does that mean I'm sending 12 trip signals to the SSPS?

MR. SCHRADER: This is Ken Schrader. I just want to point out this picture here is not showing the SSPS control --

CHAIRMAN BROWN: Yes, I've got that. I'm just thinking there is a little line going off of each of those off to the SSPS.

MR. STATTEL: No. What it is is you have -- so it's a digital output from the system. So we have a digital output circuit board that plugs into the primary RXM chassis. Right? It connects up to the Tri bus. It connects up to all three. The voting takes place in IOCCOM, and it tells that card to close your contact and initiate your safety function.

MS. ALVARADO: You're going to get only one signal out of these three to the SSPS.

CHAIRMAN BROWN: This is one of the reasons I asked the question earlier, to have a little bit more functionality-type picture that illustrates how this information flows. I agree that these are high level, but they are so -- they're a step level higher. I still want to understand, because I keep looking at one talking about these discrete signals leaving the primary RXM.

So some place it's got to go from -- and that's a digital signal in there is what you're telling me. That's just a data extender, which is digital data, serial-type data flowing through it, and you want to convert it to fibers to send it somewhere else. I've got to have a discrete signal coming out somewhere.

MR. STATTEL: So here is my dilemma, right? I have like 72 diagrams that are function block diagrams that show the functional level details that you are referring to. And I have the communication diagrams here, and I'm trying to, you know, come to the right degree of detail to get -- to answer your question. And I'm having a hard time doing that. Okay?

So, I mean, that was really the purpose of the earlier diagram that showed those functions, those bi-stable functions, the comparative functions are being performed within the Tricon. What paths they take and what communication busses they take, that's really part of the communications architecture. Data gets communicated from input cards to processor to output cards, and the IOCCOM is basically directing all of that traffic and performing voter functions on that data.

So it is a rather complex scheme, but that's the nature of that system. So, I'm sorry, but there is no simpler diagram that I could show.

MR. HEFLER: Rich, could we -- let me just give a try here. Could we go back to the Tricon conceptual? I think it was Slide 14.

MR. STATTEL: 14? Sure. Yes.

MR. HEFLER: It wasn't that one. It was the one that the Tricon concept.

MR. STATTEL: The three legs?

MR. HEFLER: Yes, the three legs.

MR. STATTEL: The one we were just at?

MR. HEFLER: Yes. The one we were at -- there. Okay. There we go. Okay. The way that this works -- and this is John Hefler again, by the way. What this is showing is there is three sections to this drawing. On the left you've got the input -- it says input, like A, B, and C. That's one input card that has three legs.

And so when you see the input termination the signal that comes in on that input termination goes to all three of those legs, A, B, and C, and then there is -- through the IO bus those signal -- each one of those goes through its corresponding main processor, A, B, and C. And those processors communicate with each other on the Tri bus.

And so the first level of voting takes place at the main processors, where they are processing the signals, comparing against setpoints, and so on, and through their communication on the Tri bus they will decide whether a trip condition exists or not.

MEMBER BLEY: So coming out of those main processors, those are identical signals, then, the three coming out of those and going to the output legs.

MR. HEFLER: Yes. But where it shows the IO bus, there's three signals now, and that's going to output leg A, output leg B, and output leg C. That's your IO bus, and what's going out on each one of those legs is what main processor A, B, and C have voted to do. But they have also -- they also vote among themselves. And so if one of them disagrees --

CHAIRMAN BROWN: Who? The second voter? You said they also vote -- you shifted from the main processors where you said they have decided that they are all going to have the same output.

MR. HEFLER: Right.

CHAIRMAN BROWN: And then you said then these other things vote also. Well, what -- they've only got one signal to vote on. How can they vote on it?

MR. HEFLER: One signal for each one. There's three of them. Output leg A gets a signal from main processor A. Output leg B gets a signal from main processor --

MEMBER BLEY: So those three signals aren't identical. Each main processor develops---

MR. HEFLER: Gets the signal from the corresponding main processor, and then on the output board that contains output leg A, output leg B, and output leg C, that votes again.

MR. THORP: So if there's a problem in one of those main processors, and it doesn't vote correctly, it doesn't vote or corresponds with reality, what you're saying is that's -- that's where it is detected is in those output legs because it does a comparison between the -- what it is receiving from A, B, and C.

MR. HEFLER: I think that's one of the layers of voting. But the main thing is -- and Mr. Hecht had mentioned it -- it sounded like you thought that there was a signal going -- each one of those boards sent three signals out to the SSPS so that you could -- you might have maybe 12 signals to the SSPS for one function. In reality, on the output board, the three legs are voted, and so each output board only sends one signal to the SSPS.

MR. THORP: For each function.

MR. HEFLER: For each safety function.

CHAIRMAN BROWN: Hold it, hold it, hold it. There's three RXM boards for each main -- for each division. And if each one of them is voting, there are still three signals, and I've got three more protection sets to go.

CONSULTANT HECHT: I want to give credit to Charlie for that.

MS. ALVARADO: This is the IO legs that's show in the processor for the RXM.

MR. HEFLER: Essentially, each one of those RXM -- what looked like an RXM card in the other figure is just that section of the IO bus.

MS. ALVARADO: Right.

MR. HEFLER: It is not really so much a card; it's a piece of the IO bus. It's the piece of the IO bus corresponding to that --

CONSULTANT HECHT: But the problem is is that the way it's depicted in Figure 4-5 is that that piece of the IO bus doesn't go through the voter; it goes back -- it goes straight to the SSPS.

MR. HEFLER: That's because in this case there is a whole -- there is a lot of detail -- the internal detail of what's happening on the output board that isn't shown. There are no output boards shown in that primary RXM chassis. In fact, the RXM chassis contains a number of input and output boards.

CONSULTANT HECHT: Okay. So what you're saying in that case is that there is one board that is sending out a signal -- single signal to the SSPS from the triple there, in the Tricon.

MR. HEFLER: Yes.

CONSULTANT HECHT: And that there are separate boards which are sending the safety to non-safety signals. So it's not --

MR. HEFLER: No. That's a completely -- in that case, the IO bus extension goes out to the remote RXM chassis, and that goes out via fiber. But it's still just an extension of the IO bus.

CONSULTANT HECHT: Okay. Well, I guess we're taking too much time up.

CHAIRMAN BROWN: We'll go on.

MS. ALVARADO: Okay. Just to continue, we were on Slide 44. The use of the RXM communication in this manner was described in the Tricon platform topical report and was evaluated by the NRC in its safety evaluation. In this safety evaluation, the staff concluded that this design provides adequate protection to the safety side of the IO bus and the overall safety functions.

This safety evaluation also states that all data received from a non-safety-related RXM must not be relied upon to perform the required safety function. For the PPS, the staff confirmed that signals acquired by the remote -- in this case the secondary RXM are not used to support mitigating functions for a common cause failure of the Tricon. And in the next slide we listed these signals that are acquired by the remote RXMs.

So these are the signals processed through the remote RXM chassis. As I stated before, none of these signals are associated with systems required to be diverse from the PPS.

Next slide is about communication and where we are currently now in our review. The NRC staff is currently reviewing the document provided, and we are evaluating this information based on ISG-04.

Next slide?

While evaluating ISG-04, the staff identified that it seems like they are in conformance with most of the guidance in ISG-04, with the exception of Staff Position 1, Point-10. And I'm briefly going to present the -- describe these deviations.

So for the Tricon the deviation is associated with the following statement. "Online changes to safety systems software should be prevented by hardwire interlocks or by physical disconnection of maintenance and monitoring equipment." In the case of the Tricon, the Tricon is using a key switch to prevent inadvertent changes to the application programs. There is a physical interlock that controls the mode of operation for the system.

Normally, the key switch is in the Run position, and the key is removed and stored in a secure location. And access to this key switch is administratively controlled. The key switch must be placed in the Load position to allow modifications to the application program. When this is done, the key switch relies on software to effect disconnection or connection of the maintenance equipment to modify the safety systems software.

PG&E has implemented the following administrative controls for the key switch. The maintenance for the station is located in the cable spreading room and has the similar access requirement as the main control room. The keys are administratively controlled, as I mentioned before.

Modification of the Tricon operation mode is alarmed in the control room, and any failure of the key switch to shift from the Load position to the Enable position is also alarmed in the control room.

Although this is an exception to the guidance in ISG-04, the staff is currently reviewing this feature to verify that it provides reasonable assurance against unauthorized changes to the system.

Then, regarding the deviation with the ALS, we found that this is related to the following sentence. "A workstation might alter addressable constant setpoints, parameters, and other settings associated with the safety function only by way of the dual-processor shared memory scheme described in this guidance of the ISG-04, or when the associated channel is inoperable.

The ALS allows the operator to modify certain data parameters during plant operation, with the subject channel in bypass mode. However, the design implemented allows the ALS to enable one sub-chassis to remain operable, meaning that one chassis will take -- be taken out of service to perform the changes required, with exception of the ITD signals where the ALS continues to operate.

So, in other words, the protection function can still be performed, and the channel remains operable. However, the redundancy and diversity of the ALS has been required by just keeping one --

CONSULTANT HECHT: Rossnyev, what can be changed during operation in the ALS?

MS. ALVARADO: We are talking about setpoints here. We are not talking about software. You cannot change software.

MR. STATTEL: Yes. You can't really implement or you can't modify the logic implementation. That requires the card removal.

MS. ALVARADO: In addition, to perform any modification, as we discussed before, the maintenance workstation requires that the top communication bus is connected. And to do so the TAB needs to be physically connected to the ALS maintenance workstation by qualified personnel under administrative controls, and only one ALS core A or core B can be taken out of service per division.

The diverse ALS subsystem connected to the TAB will be taken out of service with exception of the ALS RTD signal processing functions. The diverse ALS subsystem, whose TAB has not been enabled, will continue to perform its safety functions without impact.

Although this design is an exception to the guidance of ISG-04, the staff is reviewing this feature to verify that it provides reasonable assurance against unauthorized changes to the system. With this, I conclude my presentation about communications.

MEMBER STETKAR: Rossnyev, I have a question. I wanted to allow you to finish there. The key switch -- I read in the license amendment request the statement that says, "Tri Station 1131" -- that's maintenance workstation -- "is configured during development to prevent the application from halting when the key switch is turned to Stop."

Continuing on, "The default setting is used for the Diablo Canyon power plant PPS replacement, which means turning the Tricon key switch to Stop will not halt the application program." And I read those words. I'm not quite sure why that setting was implemented.

MS. ALVARADO: I understand, and I had the same question that you had, and this was formulated to PG&E in the last set of RAIs. So I will pass it to PG&E to see if they can provide an answer.

MR. HEFLER: This is John Hefler with PG&E. The requirement to disable the Stop is part of the SER, and the reason why the -- for maintenance purposes, it is actually written into the Version 10 SER, "The application program shall inhibit or disable Stop in the application." And the reason why was to prevent an inadvertent maintenance action from halting the processor.

The technician could accidentally turn the key switch to Stop and that would halt the controller. Now, that might not necessarily be a terrible problem because you've got three other divisions that are still performing the function, and that power -- Diablo Canyon restricts access or maintenance on the PSS to only one division at a time. So there wouldn't be a serious impact, but it could happen, and it's preventable. And so that was -- Steve might be able to amplify it a little bit more, but that actually is a requirement of the SER.

MEMBER STETKAR: Thank you.

MS. ALVARADO: I have to --

MEMBER STETKAR: Let me ask you this. I hear those words, regardless of where it came from. Is there any conceivable situation where I'm an operator in the main control room, and I'll use the technical term "Tricon goes nuts." And I, as an operator, would really like to go down and turn it off.

CHAIRMAN BROWN: A division or the whole --

MEMBER STETKAR: Well, it went nuts, so I want to turn it off. It's like my computer going nuts and me pushing the power go away switch. This tells me that I can't use the key switch to do that. Is that correct?

MS. ALVARADO: Yes.

MEMBER STETKAR: Is there any way that I, as an operator, can quickly make it go away and stop doing what it wasn't supposed to be doing?

MR. STATTEL: You can turn power off. There are breakers that feed the cabinets. That's about it.

MEMBER STETKAR: That's about it. Okay.

MR. HEFLER: The normal way of stopping the Tricon is to take the controller key switch to the Program position, and it actually continues to run in the program position. But then using the TS-1131 workstation, the processor can be halted from the workstation.

MEMBER STETKAR: That's not something I would expect an operator to do. I'm talking literally, I'm an operator and I know that I have key switches, and I know where those keys are, because I'm hoping that the Operations licensed people control those keys.

MR. SCHRADER: That's correct.

MEMBER STETKAR: Okay. Good. Thank you. And I want to make this stop -- stop doing what it's not supposed to be doing. I don't know how it got there, but I wanted to make it stop. And you're saying that in the current configuration the only way I can do that is to go basically unplug it.

MR. STATTEL: I really wouldn't say that. I mean, as far as actually stopping the processor from functioning, there are switches for manual trip, the forced trips, and there are switches for bypass that are included in the system. So if the system is going haywire and it's actuating, you know, at some crazy interval, clicking the bypass switch does bypass those functions.

So they can clear the trip, or they can---

MEMBER STETKAR: But is that bypass per channel?

MR. THORP: It's on a protection set basis.

MEMBER STETKAR: Protection set or per channel?

MR. STATTEL: No, no, no. It's per safety function. There are a series of switches in the cabinet --

MEMBER STETKAR: I want to use --

MR. STATTEL: -- one for each safety function.

MEMBER STETKAR: Okay. I want to use the terminology that I have become familiar with. I have become familiar with the terminology of protection sets, and I have become familiar with the terminology of channels within that protection set.

MR. STATTEL: Correct.

MEMBER STETKAR: And I interpret a channel as it might be a safety function or it might be an individual signal. Go start high pressure injection.

MR. STATTEL: There is a bypass switch for each channel within each protection set.

MEMBER STETKAR: So, again, as an operator, I have to go down and actuate a large number of bypass switches, more than one.

MR. STATTEL: Click, click, click, click, click. Yep.

MR. HEFLER: Or you could -- if it was something that was seriously wrong and you -- and as an operator you'd be governed by the -- by your procedures, you would actuate -- you would take the manual action, say trip the reactor, which is --

MR. STATTEL: Which would force the trip as well.

MR. HEFLER: And you'd use the high level trip, because to do anything other than open breakers, or, like you say, pull the plug, that would be something that would be done by Maintenance, not by Operations.

MR. STATTEL: But from an operator perspective, there is two states that he wants the signal to go to -- actuate or not actuate. And he has switches for both of those states for every channel. Correct?

MR. HEFLER: For the ALS -- the ALS has bypass and trip switches. For the Tricon, there are trip switches, but the bypass is normally -- I'll say that again. This is John Hefler. For the ALS portion of it, there are bypass and trip switches for most of the functions, very few exceptions. But in the Tricon, there are trip switches, but bypassing an individual channel is done on an individual channel basis.

You have to go through the maintenance workstation and go through a dialogue. It's not something that you could simply walk up to the panel and flip a switch.

MEMBER STETKAR: What I'm trying to probe here is not details of specific things. It's apparently a determination was made, and the applicant has said that determination was made by the SER.

So, therefore, that seems to be a determination made by the NRC staff that the stop function of the key switch shall be disabled. And what I'm trying to probe here is how far the collective wisdom NRC staff reviewers and the applicant has examined whether or not there are any downsides from that determination.

MR. STATTEL: Steve, care to chime in?

MR. WYMAN: Well, yes, I'm sorry I'm not prepared to answer that right now. I'm happy to take --

MEMBER STETKAR: That's all I was trying to probe is because, as I said, I used the technical term "it went nuts," okay? And I'm trying to determine at what level can the operator -- I understand the operators have manual trip the reactor capability. I understand the operators have some capability to actuate safeguards. But I didn't define what "went nuts" means.

MR. HEFLER: Okay. This is John Hefler. I just wanted to add one thing. One of the reasons for that -- and I think Steve would probably back me up -- since that's a mechanical switch that goes through software, the switch could fail --

MEMBER STETKAR: Yes. Sure.

MR. HEFLER: -- and halt the processor. And you don't want that to happen.

MEMBER STETKAR: I understand that perspective completely. I'm asking the other -- the flip side of the coin is by disabling that function, is there any downside? That's all I was asking. And whether or not anybody has thought about that.

CONSULTANT HECHT: Yes. When you have redundancy like that, yes, sure, for stop failures or hand crash failures, you certainly -- the redundancy gives you that. But for the other kinds of failures, which is basically -- in honor of John I'll call it the "goes nuts failure," you increase that by a factor of four. That probability goes up by a factor of four. It might be a small number, but it's still there. It's a tradeoff.

MR. WYMAN: This is Steve Wyman. Just, you know, one of the things to keep in mind is that the Tricon system was originally designed to be the kind of system that had long availability. It never stopped.

So I think that's just -- and it shows that they did a good job in their original design. It is actually hard to stop it.

CHAIRMAN BROWN: Okay. We're way behind. I thought you said you were finished a minute ago.

MS. ALVARADO: Yes. I was just going to introduce Samir Darbali.

(Laughter.)

CHAIRMAN BROWN: Then you weren't quite finished. No, I'm just teasing.

MS. ALVARADO: Finished is a relative term.

CHAIRMAN BROWN: So this is out of order from the schedule. We're going to go to Secure Development. And then before we talk about Deterministic Performance --

MR. DARBALI: Correct.

CHAIRMAN BROWN: -- and we have 30 minutes.

MR. DARBALI: I'll do it in that.

CHAIRMAN BROWN: No. For both of them. Not for you.

MR. DARBALI: Good afternoon. My name is Samir Darbali. I'm a technical reviewer in the Instrumentation and Controls Branch, Division of Engineering, Nuclear -- Office of Nuclear Reactor Regulation.

So let's talk briefly about secure development and operational environment. The staff is reviewing the SDOE to ensure reliable system functionality. So the applicable guidance is Reg Guide 1.152, Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, which endorses IEEE Standard 432.

I just want to make a clarification that Reg Guide 1.152 works in the Part 50 space. We are not talking about cyber security here. We are mostly talking about reliability.

Any questions?

CHAIRMAN BROWN: Just keep going.

MR. DARBALI: Okay.

CHAIRMAN BROWN: If you hadn't said that word --

(Laughter.)

MR. DARBALI: So secure development environment. The secure development environments for the ALS and the Tricon platforms were reviewed as part of their respective topical report reviews, and they were found to be acceptable. The staff is currently evaluating that these development environments are maintained for development of the Diablo Canyon application.

So far the staff has not found any deviation from the generic environment that was evaluated.

The vendors control access to their development environments by performing vulnerability assessments. These assessments identify both critical and life cycle vulnerabilities.

Control of access to development environment or that environment within their facilities is accomplished by the use of access security cards, control of development areas, including computers, workstations, network servers, and portable media.

The vendors have procedures for access, design, and material controls, as well as software development, configuration management, testing, and non-conformance reporting. Vendors use V&V activities, as well as code reviews, to detect and prevent unidentified functionality.

I want to make it clear that PG&E will not be developing or modifying their software.

The staff has also performed an audit at the vendor facilities to look at their secure environment -- development environment.

Next slide?

For secure operational environment, it is defined as a condition of having appropriate physical --

CHAIRMAN BROWN: When you did your review, was that an audit, a spot audit? Or did you just literally sit down and walk through their entire -- every area? I mean, you should have been able to go and have a meeting on this in a few days and walk through almost every one of these relative to how --

MR. DARBALI: Right.

CHAIRMAN BROWN: -- they actually do their control or --

MR. DARBALI: We did a review before we went to do the audit.

CHAIRMAN BROWN: Well, when you did your review, did they give you procedures? Did they -- what did --

MR. DARBALI: They looked at the vulnerability assessment documents. A lot of these are proprietary documents. And we went through the process of, for example, for identifying unidentified code functionality they would show us the V&V process, how they do testing and code reviews, and match that with the requirements, make sure there is no code that shouldn't be in there.

As far as their secure environment, we basically asked them, how do you get access to your procedures, to the code files? So they would show us, well, you know, the servers are---

CHAIRMAN BROWN: There at the plant.

MR. DARBALI: -- when we were there at the --

CHAIRMAN BROWN: Facility.

MR. DARBALI: -- at the vendor facilities.

CHAIRMAN BROWN: Yes. Okay.

MR. DARBALI: So we would see the -- every development workstation requires a password. The rooms are locked. You need a key access. Not every employee has access to that.

The network -- it's a separate network from the corporate network. So we looked at all of their procedures to make sure that the integrity of the product is maintained.

MEMBER SCHULTZ: So you did process -- what I'm hearing you say at this point is that you did process reviews to assure that the vendor had done all of those things --

MR. DARBALI: Correct.

MEMBER SCHULTZ: -- that you thought were appropriate.

MR. DARBALI: Correct.

MEMBER SCHULTZ: On the previous slide you had mentioned code reviews that were also performed. The code reviews, is that code reviews that are done by the vendor?

MR. DARBALI: Correct.

MEMBER SCHULTZ: And how did you review that part of their work?

MR. DARBALI: They would show us, for example, a non-conformance ticket or they would find -- they would -- an example, they would show us here is an example of how we identify the code that was not supposed to be there. And they showed us -- for example, in the case of Westinghouse, they showed us a presentation where they did some simulation -- they used a simulation tool to trace the code back to the requirements, and that way they could say, "Well, here is a piece of code that should not be there," and then they went through the process of showing how they address that.

MEMBER SCHULTZ: Okay. But you didn't go back and do independent review.

MR. DARBALI: No.

MEMBER SCHULTZ: You reviewed what they had done.

MR. DARBALI: No. We audited their process for doing that.

MEMBER SCHULTZ: Thank you.

MR. THORP: Walk us through it. Show us how you did it.

MEMBER SCHULTZ: Understood. Thank you.

MR. DARBALI: So going back to secure operational environment, once the equipment is installed at the plant, PG&E informed us that modification to the PPS replacement components that were produced by the vendors -- Westinghouse, Invensys -- will be performed by the vendors, not the licensee.

And we did mention where the cabinets or the PPS replacement system is going to be located, and it's going to be located in a vital plant area, in the cable spreading room, the same cabinet where the current Eagle 21 is located. And we did perform an audit last August at the plant, and we did ask the licensee, how do you gain access to the cabinet? So they walked us through the process.

We would go to the control room. It would ask the operators for the key, which is actually locking another cabinet. Then we would get access to the cable spreading room. You would go to the cabinet. You have to open it, and that's how you would get to the current Eagle 21, which is where the PPS replacement will be.

The maintenance workstations will require further access control, so they would have a password, for the ALS maintenance workstation and the Tricon maintenance workstation.

Any questions?

MEMBER SCHULTZ: Oh, one question. On the modifications, do you have some assurance that the same processes that you reviewed are going to be implemented associated with any modifications to the software? One of my concerns -- I understand you looked at processes, and they showed you, then, some things that they had found by implementing and using the process.

You know, the tough part is to figure, how robust is the investigation associated with that process implementation, which is now dependent upon what the vendor does and how invasive they are on their own to identify any issues. Any way that you could validate that, Westinghouse folks?

MR. ODESS-GILLETT: I can't speak for how the NRC would validate it, but from the Westinghouse point of view --

CHAIRMAN BROWN: Give your name, please.

MR. ODESS-GILLETT: I'm sorry. Thank you, Charlie. Warren Odess-Gillett from Westinghouse. And for the ALS platform we have certain commitments that we have made in our safety evaluation report for the platform. And we have to adhere to all of those commitments.

So regardless of the project that we do, whether it be this one or for some other safety-related project, we have to adhere to those commitments in that SER. So once we are done and there needs to be a change to the PPS, we would -- from the Westinghouse point of view anyway, we are committed to sticking with what the procedure said the NRC reviewed and approved and so were acceptable, and that's what we're going to have to follow.

CHAIRMAN BROWN: So you have to maintain those particular processes, follow procedures, whatever they are, independent of whatever you might do for another designer who wants something maybe a little bit different.

MR. ODESS-GILLETT: That's right. We're procedure-oriented. That's correct.

MEMBER SCHULTZ: I appreciate that explanation. Thank you.

MR. DARBALI: With that, I will --

MEMBER STETKAR: Charlie, I hate to do this because I don't know anything about operating systems software. But I did notice that both sets of workstations are supposedly using Microsoft XP Service Pack 3, both of them, ALS and Tricon.

CHAIRMAN BROWN: I didn't see that.

MEMBER STETKAR: Okay. Well, I did. I can show you the quotes. You have to look. Is there a vulnerability that's introduced by that, he asked?

CHAIRMAN BROWN: From what I've been reading.

MR. SCHRADER: This is Ken Schrader. I would just point out that that is on a non-safety maintenance workstation.

MEMBER STETKAR: Can you use those non-safety workstations to change safety-related setpoints and change programming -- in at least the Tricon you can change the programming. You can change setpoints everywhere. Can you do that? Yes or no.

MR. SCHRADER: The answer is yes.

MEMBER STETKAR: Thank you.

MR. SCHRADER: But let me add that after you do that you have to meet the tech spec requirements, including performing a channel operability test to verify that what was done during the maintenance meets the operability requirements.

CHAIRMAN BROWN: It's a good question, because I have been advised to throw my computer at home away, which is eight years old, and in which about two out of every six times I try to start it up it won't start and I have to punch the button and start over again.

MEMBER STETKAR: I'm worried about more sinister vulnerabilities.

CHAIRMAN BROWN: I understand that. But, I mean, the point being is it's not -- there is no -- there is no -- even though changes are still coming in, you know, to software, they will tell you there is no support for that anymore, although a little bit it's still -- you still get them.

CONSULTANT HECHT: I have another question on that same topic. It wasn't on the operating system, but it was of concern, and that is, is anybody worried about sustainability? And that's really on the ALS side. FPGA technologies are changing rapidly, and having -- I mean, is there going to be a lifetime buy of blanks? How do we assure that---

MR. STATTEL: I guess I could let the vendors respond to that. However, with regard to our safety evaluations, we essentially establish a snapshot when we issue the safety evaluation of the platform. That platform, SAE, identifies specific model number boards, specific versions of procedures and documents that we evaluate.

So any changes or improvements that are made to processes or changes to the hardware design would be subject to further evaluation, particularly if they had the ability to impact the safety conclusions that were drawn. So it is an issue with all platforms. It's an issue--- it was more prevalent with the earlier platforms, the AREVA platform, because a lot of time had passed between the safety evaluation and when the application was developed.

There are different ideas for how to handle this problem. One is to perform a 50.59-type evaluation. This would be a process that the vendors would implement, and so any time they made a change they would make -- they would do an internal evaluation and evaluate and make a determination of whether they felt that impacted the safety conclusions of the SE.

And if it reached that threshold, then it would require an update being submitted to the NRC and have the NRC update its evaluation. And, if not, if they could make a case where it doesn't impact it, they would document that evaluation, and on a subsequent application development we would have access to that documentation that they used for those evaluations.

MR. THORP: This is John Thorp. Let me just amplify that a little bit very briefly, because I know we are short on time. But this is an open question and a topic of our ongoing digital I&C meetings that we are having with industry. And it's a key topic for which industry and NEI have formed a task group to examine, what is the means by which we maintain configuration or they maintain configuration management and control of these various platforms, because -- recognizing that evolutions that will occur and improvements will be made, and we have evaluated a given version. So that exploration is ongoing. If you have further questions about it, Gordon Clefton can speak to that from NEI.

We'd like to see progress move on that a little bit faster than we've seen it, but nonetheless that is happening. And so what --which is described essentially as sort of the subject or the premise of that group's effort.

CONSULTANT HECHT: So it's an open question, basically. So do you think there will be any differences between FPGAs and, for example, software in that regard? Because FPGAs, if we have to change, you know, the packaging or the chip because of advances in technology, what we're doing, a whole new --

MR. STATTEL: What we've seen over the years seem to be -- seems to be pretty common among different technologies, and that is there is improvements made to the hardware, there is improvements made to the software, there is improvements made to the firmware, and there is improvements made to the processes that are used to develop that.

So we have seen changes in all of those areas for all types of technology. And it's nice -- these evaluations are fairly fresh. They haven't made a lot of deviations from what we evaluated. So we are not having to spend a lot of time evaluating changes, although there will be a change evaluation in this.

CONSULTANT HECHT: Well, it looks like you started in 2010, so it's getting to be five years until implementation.

MR. STATTEL: Yes. Yes. Well, so we do evaluate those changes, though. But, keep in mind, we don't see all digital upgrades in plants either, because some of them can be performed under 50.59 evaluations.

CHAIRMAN BROWN: Okay.

MR. STATTEL: And moving on to the deterministic performance, the final area of discussion we have today is for deterministic performance. Both the Tricon and ALS platforms are designed to process every piece of plant input data and every protection and safeguards function, including processing of all system outputs during predictable program cycles.

Okay. Each of the platform evaluations determined that there are application-specific parameters which could influence the system's ability to perform in a deterministic manner. Therefore, the staff -- we are currently evaluating deterministic behavior characteristics for each of the subsystems within the context of the Diablo Canyon application.

So as you can imagine, the more complex of an application you write, the more functions you are performing within that applications, the longer time it will take to execute. So those are characteristics of computer systems and FPGA systems alike. So, therefore, you can't really make a complete safety conclusion without knowing what the application-specific functions are.

Now, this slide talks about the standard review plan guidance. It advises the evaluation should confirm the system's real-time performance characteristics are deterministic and known, and we have Branch Technical Position-21, 7-21, which discusses design practices to be avoided for computer-based systems.

And some of these are really not -- we found are really not directly applicable to the FPGA-type designs. But we used this guidance as best we could, being it's all we have available right now. So these practices include a non-deterministic data communication, non-deterministic computations, interrupts, multi-tasking, dynamic scheduling, and event-driven design. So these are practices that our guidance say should be avoided in development processes.

So each of the platform evaluations concluded that there are application-specific parameters, as I mentioned. Therefore, we reevaluated deterministic behavior within the context of the Diablo Canyon application.

I'm going to skip to the next slide.

This is just a quick description here. Both of the platforms really have a similar architecture. In other words, there is a bus, there is input cards plugged into that bus, there is output cards plugged into that bus, and there is processing cards plugged into that bus.

And any determination or any evaluation of time response on a system like -- on a digital system like this really does rely heavily on how the communications is handled on that bus.

And in order to get from the input sensor shown on the left of this diagram to the output function as the triangle on the right side, basically data has to process -- be processed through the input cards, it has to be processed -- in other words, the functions performed using the processing, the microprocessor or the -- in the ALS it would be the core logic board, and then it goes over to the output card over that communication bus. Okay? And then the yellow box is just showing the communications capabilities that are connected in there.

So first I'll talk about ALS. The ALS platform is FPGA-based, and it is not embedded -- it does not embed microprocessor cores or use interrupts. It does not use interrupts.

The staff is in the process of confirming the Diablo Canyon application. It operates on fixed cycles where a deterministic sequence of acquiring inputs, perform logic operation, and process outputs, is followed without the use of a microprocessor core or interrupts. So we are basically confirming that it's meeting the guidance, the criteria.

This is consistent with the ALS -- ALS's platform's approved topical report. So that evaluation is in progress.

For the ALS system, there are two timing parameters that are used to establish deterministic performance of the subsystem. There are access time and frame time, and their definitions are on this slide here.

So although the ALS platform establishes fixed board access time, other aspects, including the number of times a board is accessed per frame, the number of boards accessed per frame, and the sequence of board accesses per frame, and the frame time itself, are determined using the application-specific design phase.

And, again, it goes back to the reason why we can't make the determination without knowing the specific design of the system. Okay? These are design aspects that are established and fixed during the development. Okay? So we are evaluating the application-specific attributes for the Diablo Canyon design.

Is there any question on ALS?

CONSULTANT HECHT: Yes. Access time is both input and output per board? Basically, if I understood what -- the message here it's that you can't determine frame time on the system level because you don't know how many IO boards there are.

MR. STATTEL: Correct.

CONSULTANT HECHT: But you can determine access time because you know what the time is between the central processor in each board --

MR. STATTEL: It's not both input and output. It is basically transferring data from the input board to the processor, or from the processor to the output board. So the number of times that that happens to complete a safety function is really part of the equation.

MR. ODESS-GILLETT: So, Myron, that's -- this is Warren Odess-Gillett from Westinghouse. That's two different access times.

MR. STATTEL: Correct.

CONSULTANT HECHT: Okay. Thank you.

MR. STATTEL: Okay. Now, under the Tricon system --

CHAIRMAN BROWN: Let me ask one other question just to make sure. Let's go back. You've got a functional plant that you know you -- what you have to do. I mean, the algorithms are set. The protection functions are set. The data that you've got to get in is set.

So saying the number of boards that you have to access to get data from is no different than -- it's similar to, not no different -- it is different -- but it's similar to even a software-based system where you have data coming in, you have to go hit every one of those, collect them all, whether they're buffer -- however you do that, and then you go into your processing. There's a number of algorithms or routines you have to process as you go through to develop all of your outputs, your trips, et-cetera, et cetera, et cetera. And then you've got to send it someplace when you finish that. When you finish that process --

MR. STATTEL: To the SSPS.

CHAIRMAN BROWN: Yes. It's got to be transmitted out. It's that last step. And so each of those, the more functions you have to process, the longer is your cycle time, which is affected by your accident analysis and all of that other kind of stuff, you've made determinations of what you can and can't do.

So there is really not a whole lot of difference, but in this case aren't they able to tell you the number -- what this information is? Have you all gotten that and you all are trying---

MR. STATTEL: Yes.

CHAIRMAN BROWN: Okay. You've gotten that and you're trying to use that to develop, because once you've got this you've got a -- you access, do all of them, and it's a matter of you get them all, you keep going through the calculational part, and then you toss the information out.

Once you've got that, you've got a fixed time, whether it's too long, to short, whatever it is.

MR. STATTEL: Right.

CHAIRMAN BROWN: But it should be repetitive, and it should be predictable, particularly given -- I'm presuming the FPGA -- I'm not an FPGA expert, by any means. But you don't stop that per se -- the question is, you don't want to stop that process. You don't want to have a state that says it -- to deviate from that process. You want it to walk right on through everything.

MR. STATTEL: That's what I would call an event-driven interrupt.

CHAIRMAN BROWN: Yes.

MR. STATTEL: You don't want something external that would --

CHAIRMAN BROWN: But can you do that with FPGAs? I mean, they've got a clock that is---

MR. STATTEL: If you wanted to, I suppose you could, but --

CHAIRMAN BROWN: I only did one of these in my past reincarnation, and we didn't have any of that. It was -- that was 25 years ago.

MR. STATTEL: So what the staff has to look at is we have been given some numbers, right? So we have -- we have access, of course, to the safety evaluation, which says the system needs to perform this safety function in this amount of time. And it's usually -- they are pretty long times, in order of seconds, right?

Now, that number includes the response time of the relays, the response time of the pumps starting up, the mechanical components, things like that, but it also includes the response time for the digital system that is one of the inputs to that.

We also have specs, the specifications for the systems, so we know the exact number of milliseconds that is being allocated for the ALS, and there is a different number being allocated for the Tricon system.

So in the case of signals that are temperature -- that are relying on temperature, those are kind of your worst-case conditions because both systems have to completely perform input process output in order for that safety function to occur, right? So we add up both of those times. We know what the allocations are. We know what the numbers -- what the specs are. Those are in the system specifications.

And we also have calculations that we have received from the vendors that basically tell us, based on the application, this is -- this is what the time, the cycle time for this is going to be when they build that board, right? Now understand that development is in progress right now, so it needs -- that still needs to be confirmed, and that will be one of the confirmation activities we perform this summer, right, to confirm that.

Now, with the ALS -- with the FPGAs, we are talking orders of magnitude. These are very fast. It is kind of akin to the old machine language coded programs or microcontrollers. The cycle times are much faster than what you would typically see in a microprocessor-based system.

There is a lot of margin. There is a lot of margin between the actual expected response time of an FPGA card, and the specified time that it needs to meet within the application. Right?

Now, for the Tricon system it is --

CHAIRMAN BROWN: Let me -- I guess what I'm trying to get to is there's two things we're trying to do. Will these things perform and meet the time response requirements that are necessary to give you -- is it going to perform the same as Eagle 21 did for the other system? That's one aspect. You've got to make sure that you understand that.

But the second part is that every cycle time is the same. It's not going to be stopped and be altered while you are trying to process and generate trips. I mean, there's a start time. You gather, you calculate, then you've got some spare time where diagnostics could be done, where housekeeping can be done, where extra buffers can be layered out, or a separate port can be accessed for whatever, or whatever you want to do.

But, I mean, you've got things you've got to time within that -- it ought to do all of those every time, and then you ought to just cycle back and start over again. But nothing alters that process. So it's not 10-milliseconds one time, 50 the next time, 75 the next time, and come back -- because it decided to do something else, okay, while it was doing -- in the middle of the processing cycle.

MR. STATTEL: This is something that varies between the technologies. Okay? So for the FPGAs, it is not like it is performing the functions and then it is switching over to another task, or it is doing diagnostic and then it switches back to functions.

CHAIRMAN BROWN: Yes, I've got that.

MR. STATTEL: It is really just a logic implementation. So it's just -- now it does go in a cycle, right? So it reperforms its functions periodically and -- but the answer to your question is, yes, it's independent of the loading or condition of the environment around it. It will perform those functions deterministically.

The Tricon is a bit different because it does -- it does use interrupts, but it doesn't use event-driven interrupts. There has to be interrupts in a computer system, because you have to tell that system when to start performing the function. Right? So you establish that cycle time for the application, right? And you want that to interrupt whatever is going on.

So if there is diagnostics -- so if it completes its application and is performing diagnostics in the spare time that it has, you need to be able to interrupt that and say, "Here, it's time to restart your application and" --

MR. STATTEL: I will grant you that there are what's known as good interrupts and bad interrupts. So our job, you know, the way we see it is to make sure that they are using the good type of interrupts to make sure that the deterministic performance is ensured without any reversion or any -- creating any back doors or anything that could affect -- or basically the use of the bad interrupts where we have an event or a condition external to the system that would affect its performance.

Now, there's a couple measures that are put into place. There is a calculation that Tricon uses. So basically they develop their application, so basically this is describing the scan task, and there is three -- there is three basic tasks that are performed on every cycle, and these are called the higher priority tasks.

And they are not event-driven. There is no -- now, they are initiated by interrupts, but they are not event-driven interrupts. Okay? They are basically initiated by the clock. Okay? The scan task, the communication task, and the background task, and every other task that is performed by that processor would be a lower priority task, and it basically would be performed as available.

CHAIRMAN BROWN: Does it come under the background? I mean, if you've got a cycle that you go through, that cycle should be repeated every time you finish the --

MR. STATTEL: That's correct.

CHAIRMAN BROWN: -- if that's the cycle you're going through, you start the scan, you do the communication, blah, blah, blah, and you go through it.

MR. STATTEL: That's correct. Now, I thought I had another figure, but I don't see it here. I guess I didn't put it in. But there was another figure basically that showed the way this works is it performs the scan task and then it cycles between the communication task and background task during the idle time until the next program cycle begins. Okay?

And those are the times where diagnostic functions are performed and self-checking, things like that.

CHAIRMAN BROWN: My point being is that although -- whether it's a 100-millisecond cycle or a 50 or a 200, whatever it is, they all get done to some extent during that time.

The primary tasks are done, the communications, the outputs are done, and then the background task takes care of whatever it can get done. It ends, it finishes the cycle, goes back and starts, but it knows where it left off on the diagnostics, and it will start there the next time it gets to that point. And that cycle is the same all the way through.

CHAIRMAN BROWN: As long as it's not altered, if you don't have event-driven things, it all of a sudden alters this stuff, which is out to lunch.

MR. STATTEL: That is correct. So deterministic behavior is assured through the synchronizing of application scan, which guarantees a new set of inputs and a new set of outputs for the IO modules are established during every application scan in each of the separate processors.

Now, the processors are running asynchronously.

CHAIRMAN BROWN: That's fine.

MR. STATTEL: Okay.

CHAIRMAN BROWN: That's good. Probably.

MR. STATTEL: So just a couple notes on that. The Tricon application program calculation cycle cannot be interrupted by any of the lower priority tasks during program execution cycle. The actual processing time is established during program development, and we are provided with calculations that determine what that -- what the expected cycle time is.

Once the application program development is complete, the cycle time does not vary the function of calculational loading of the system.

Okay. Next, this diagram basically shows what I was describing before, so we have a calculated response time, and this is basically what we expect the system to perform based on the number of functions in the application. The program scan time is set to a greater value, and this is basically a conservative number to ensure that we don't have any overruns based on normal performance of the system.

And, of course, that is less than what is specified as the specified requirement for time allocation of the system. And we are ensuring all of these numbers fall in.

And then, finally, it ties to the accident analysis required time response, which we are looking at that as well.

CHAIRMAN BROWN: What is the calculated response time? Calculated based on what?

MR. STATTEL: Actually, perhaps John you could answer that.

CHAIRMAN BROWN: Well, I was thinking, if you've got a calculated response time --

MR. STATTEL: Right.

CHAIRMAN BROWN: -- your program scan time and your -- all of the other ones ought to be shorter than the calculated.

MR. STATTEL: No. Calculated is actually the fastest theoretical time that we expect that program to run, right?

MR. McKAY: And that's exactly -- John McKay, Invensys again. We have to perform calculations based upon worst-case scenarios of like getting your input point right after the input processing has stopped for the scan, so you have to go all the way around again. And we have created a document that we have submitted to that effect, and then also just to go on what he said about the scan time itself is hard-coded into the program before it is delivered.

CHAIRMAN BROWN: The calculated response time is based on picking up every piece of data the instant you need it without having to go back through the cycle again.

MR. McKAY: No. The calculated -- we call it the maximum Tsat scan time, so it's the maximum response time that we will get, and we will get everything in this maximum time. Almost every scan we will get everything a lot faster than that.

CHAIRMAN BROWN: Then why is the program scan time longer than the calculated response time?

MR. STATTEL: It's conservative. We actually -- we know what the cycle time is going to be. If we just run it as fast as it can go, it is going to be on the pink line there. But what we do is we slow it down, we set a program scan time that is longer than that, basically gives us assurance that we are always going to be completing what we need to complete in the cycle with some conservatism. Okay?

The things that go into the calculation is like --

CHAIRMAN BROWN: That's fine. I mean, go on.

MR. STATTEL: It's an interesting calculation. I have reviewed it, and it assumes, you know, how long it takes to process the input and how long it takes to communicate that over to the processor, you know, how long it takes to perform all of the function blocks that are in the processor.

So it's a very comprehensive calculation, and it comes up with a number and then the actual scan time that is set, that is basically the interrupt. That is that clock interrupt that says start doing your safety functions now, no matter what.

CHAIRMAN BROWN: Where is your communications and your backgrounds? It's after that?

MR. STATTEL: It's basically the time between what actually -- you know, the time that is left between the calculated response time and the program scan time, that is your excess time. And that is where your background --

CHAIRMAN BROWN: Your program scan time then encompasses all three of those --

MR. STATTEL: Right.

CHAIRMAN BROWN: -- that you talked about. Not the scan tasks.

MR. STATTEL: Correct.

CHAIRMAN BROWN: That's different.

MR. STATTEL: That's correct.

CHAIRMAN BROWN: That's connecting the scan task to --

MR. STATTEL: I think Steve has the right diagram.

MR. WYMAN: Here is the scan task in green, and then toggling back and forth, this is background and communications. So the background is down here in the orange time, and the communication task is shown here in the blue time. So they toggle back and forth.

CHAIRMAN BROWN: And that's the program scan time. That's talking about --

MR. STATTEL: What you're seeing from the beginning of --

CHAIRMAN BROWN: Okay. All right. I got it.

MR. THORP: I think the reason, Charlie, that it's considered conservative is it eats up more time --

CHAIRMAN BROWN: We're okay, John. You can stop talking. Okay? My problem was connecting the previous viewgraph with scan task, communications, and background.

MR. THORP: Gotcha.

CHAIRMAN BROWN: And those are really all within the program scan time, not scan test. Scan test takes a part of that program scan time. Comm takes part of that scan time, and the background takes part of that, and as long as I understand that. The other thing is a nice piece of information.

MR. STATTEL: Okay. Now, we can spend as much time as you want on this slide. Really, all this is talking about is the use of watchdog timer functionality. Both of these platforms have watchdog timer-type functions, and all this is illustrating is basically we are just monitoring the performance of these scans using hardware components that are not dependent or not subject to common cause failure and they are not dependent on the application development.

CHAIRMAN BROWN: Is it a hardware timer?

MR. STATTEL: They are hardware, but they are not -- they are built into the platforms, and that's why you don't see them very --

CHAIRMAN BROWN: Is it hardware? Or is software controlling its performance?

MR. STATTEL: Well, in the case of the ALS, it is actually -- it is actually implemented within the logic, within the logic card. But it is a -- it is a watchdog timer function, type function.

So, for example -- for example, for the ALS, communications -- we talked about the importance of communications on the RAB bus, right? So this is where all of the IO is getting communicated to the processor. Okay. Each slave board can detect a communication failure and can isolate itself from further communication on the RAB until the communication failure is corrected.

Each RAB slave implements communication watchdog, timeout, and halt function for the RAB communications. So this is -- this is kind of a use of a watchdog timer-type function in order to ensure that that communication takes place in the designed time.

CHAIRMAN BROWN: If a watchdog timer is actuated because something didn't complete, that shows an alarm.

MR. STATTEL: That's correct.

CHAIRMAN BROWN: Does that go to the control room?

MR. STATTEL: Yes. In both cases. So basically it's a system failure.

CHAIRMAN BROWN: As you say for both---

MR. STATTEL: And then that's -- for both ALS and Tricon system. So basically the system -- it's system failure. If there is some -- something that would challenge the deterministic performance of that system, if the process is taking longer than expected, the watchdog timer is basically time out and they would alert the operators that there is something wrong. So they would question the operability of that channel.

CHAIRMAN BROWN: Is it on a card-by-card basis? Or is it --

MR. STATTEL: These are.

CHAIRMAN BROWN: Let me give -- okay. So it's not something that says, "Here is my program scan time. If I don't complete that, I get an alarm."

MR. STATTEL: Correct. It is independent of the application.

CHAIRMAN BROWN: But you still get an alarm. So you've got a lot of little processors that all have these watchdog timers on it.

MR. STATTEL: Yes. And those functions were evaluated -- I'm not evaluating --

CHAIRMAN BROWN: I'm not as worried about this on this by the way, because it's -- well, I'm not voting with these.

MR. STATTEL: Right. It's effectively an analog voting system if you look at it, and that's one way to look at the -- I think that's the way I look at the SSPS, right? I purposely didn't put a lot of details on this slide, because we're not -- this is not part of our evaluation. These are -- these features are features that are built into the platform.

CHAIRMAN BROWN: Does the Tricon topical report talk about these?

MR. STATTEL: Yes.

CHAIRMAN BROWN: Okay. I mean, I found V-10. It turns out that was nothing but deltas from an earlier report, so it was kind of --

MR. STATTEL: Version 9, right. Nothing but -- I mean, it's a 300-page SE. I mean --

CHAIRMAN BROWN: Well, not the SE. I'm talking about the -- not your all's SE but the actual topical report for the platform.

MR. STATTEL: It was an update. Yes.

CHAIRMAN BROWN: Yes. And it wasn't 300 pages. It was only 139-1/2. No, I'm just kidding. It was small.

MR. STATTEL: Actually, the V-10 SE was a fairly extensive safety evaluation.

CHAIRMAN BROWN: All it did was say the words and it had nothing about alarms going anywhere.

MR. STATTEL: Well, it did have --

CHAIRMAN BROWN: And neither did the LAR.

MR. STATTEL: Okay.

CHAIRMAN BROWN: And neither did the functional requirement spec.

MR. STATTEL: In the disc that I provided to you, I have provided you a document called Watchdog Timers. These are direct quotes.

CHAIRMAN BROWN: Oh, the disc?

MR. STATTEL: These are direct quotes from those safety evaluations.

CHAIRMAN BROWN: You said the disc you gave me?

MR. STATTEL: Yes. I provided --

CHAIRMAN BROWN: Did I get a disc?

MS. ANTONESCU: Yes. You got --

MR. STATTEL: It was the supplemental one.

CHAIRMAN BROWN: Where did I put --

MS. ANTONESCU: Wait. I didn't send you the supplemental because I attached it in the status report, so it was easier that way.

CHAIRMAN BROWN: Oh, okay.

MS. ANTONESCU: So it's in the status report.

MR. STATTEL: I put a short document together. It's only two pages long, and it discusses the watchdog comments for both ALS and Tricon.

CHAIRMAN BROWN: Okay. Thank you.

MR. STATTEL: Sure.

CHAIRMAN BROWN: I'm finished on that, so you're -- keep moving.

MR. STATTEL: We kind of mentioned this before -- changes made to the platform. There haven't been too many, but we are evaluating the changes. The ALS platform safety evaluation was just issued in 2013, and there are no changes that we're aware of between that platform and what is being installed in Diablo Canyon.

The V-10 safety evaluation was issued in 2012, and some changes have been made to the platform. We have evaluated those. The majority of those changes we did not consider to be significant. We performed a review of these changes to ensure they are acceptable and ensure that the previous safety evaluation conclusions are not adversely impacted.

So we have that drafted now. It's not finalized.

MS. ANTONESCU: Could we get copies of the topical reports?

CHAIRMAN BROWN: I think I have one.

MEMBER BLEY: I don't know if it's the right one.

MR. STATTEL: I have the ADAMS numbers right here.

CHAIRMAN BROWN: How about just -- give them to Christina when we're done, and she can send them to us.

MR. STATTEL: Okay. I have both of them. That's these two books right here.

Schedule. So this is really the last item I'd like to mention. We are past the two-year point on this review. You might have noticed when John introduced that we started this evaluation in October of 2011.

I just want to mention -- so as of today, the licensee informed us that they had a delay in implementation. So basically we have several what we call Phase 2 documents that we require before we complete our safety evaluation. And those are dependent on completion of the design.

So right now this timeline here shows briefly what their current schedule is for the completion of the factory acceptance test. At those factory acceptance tests they will have the cabinets built and they will be doing functional testing of those. Prior to each of those tests, we intend to perform audits at each of the vendors' facilities. And these are mainly confirmatory audits. We are developing the plans for those audits right now.

And in June we should have the final document submittals of the completed designs. And right now we are planning to issue our draft safety evaluation. This is just from EICB to DORAL in October of this year.

And that's all we have.

CHAIRMAN BROWN: Okay. Yes?

MR. HEFLER: This is John Hefler, PG&E. I'd like to apologize and also correct the record if I might. I had said earlier that the SER said that the stop switch shall be disabled. I was incorrect. It is the Triconics application guide that is the appendix to the topical report. So with apologies to the staff---

MR. STATTEL: We still have an open RAI on that particular issue, so we haven't quite resolved that.

CHAIRMAN BROWN: Okay. Before we conclude, is there anyone in the audience that would like to add a comment?

(No response.)

Hearing none, I am putting the phone line -- for those of you who are on the phone lines, if you will hold on a second, I will confirm that it is open. Would somebody say something to let us know that the phone line is actually open?

MR. GALEYEAN: Yes, I can hear you.

CHAIRMAN BROWN: Okay. Is there anybody out there that would like to make a comment?

MR. GALEYEAN: Not here.

CHAIRMAN BROWN: All right. Not hearing any further responses, we will conclude this. Did I miss anything? Did you want to -- oh, yes, I forgot all about that. Yes. John, do you have any comments or --

MEMBER STETKAR: I do not. I would like to thank the staff for getting through a heck of a lot of material in four and a half hours or whatever it was, and I thought it was very, very useful dialogue. So thank you.

MEMBER SCHULTZ: I appreciate the staff's presentations today. They were very well done, and they really did give me an appreciation for the depth of the review that has been done and is ongoing.

Thank you.

MEMBER BLEY: I'd second that. Thank you, all. No other comments from me, Charlie.

CHAIRMAN BROWN: Okay. Yes. I'd like to go on and say that this was -- I think you've covered very, very thoroughly the -- what I call the topical areas that we have tried to, you know, put together to allow a good review by us, the committee, that we can then pass on when we have the full committee meeting to let them know where we stand on this as well.

But we will have to condense this obviously somewhat before the full committee meeting. And we will try to provide you some feedback, but largely along the lines of, how do we meet the four pillars of redundancy, deterministic, performance, and defense in depth and independence, and as well as the simplicity, which you could never convince anybody that this is simple. So you might not want to work on that one too hard in the full committee meeting.

MEMBER SCHULTZ: Charlie, are we going to meet again before -- in the midst of what is ongoing with the --

CHAIRMAN BROWN: Right now we've got a full committee meeting information briefing scheduled for the full committee meeting.

MEMBER SCHULTZ: Just information.

CHAIRMAN BROWN: That's -- well, that's the way it's listed right now, or at least it was--

-

MEMBER SCHULTZ: I just want to understand --

CHAIRMAN BROWN: And that's for the March full committee meeting. I think it would be useful to see them -- let them know what is being done in this area, because we haven't had any interface on -- what I call on the operating plant side with what has been going on in a while. So that's where we would intend to go with that.

So I'll try to give you some suggestions over the next couple of days. I'll pass them back to Christina to get them to you to where -- and if you guys have any suggestions, by the way, of stuff to cover --

MEMBER BLEY: I don't know quite how to say this. One of the reasons I think we had some trouble in going through this is we aren't -- at least I'm not fully informed about the two platforms and the review you did on those. So I think a lot of our questions were dealing with things that were addressed there.

I'm not sure how we can dodge that for the full committee, but -- and maybe it's by simplifying. You know, where we were getting into trouble was how these multiple channels within the protection sets talk to each other, and I think simplifying that and not quite showing as much for the full committee might --

MEMBER SCHULTZ: Yes. I think around a 10-minute presentation about what historical -- the review that has been done and what the results of those reviews has been --

CHAIRMAN BROWN: On the platforms.

MEMBER SCHULTZ: -- on the platforms would be very useful for the full committee. And then that puts what we heard today in a perspective for them in a shortened version that you indicated you would work with.

MR. THORP: Just along that line, I wanted to thank the two authors of the SEs for the two topical reports. Steve Wyman and Bernie Dittman have been here throughout the meeting, and we'll talk about how we might be able to get them involved in terms of giving that brief historical presentation on the review of those topical reports.

CHAIRMAN BROWN: The triplicate set of stuff in there and the interrelation to all of the communication paths and what happens because these RXMs are whatever, I mean, one of the key figures in this was one of the earlier ones in terms of showing the independence of this from the internet, from the -- you know, and the one-way communications and lack of connection to the outside world.

The control of access is of pretty high level of interest to us these days relative, even though you all don't look at -- theoretically at this stuff. This is really a control of access issue, in my own mind, that -- from a plant design standpoint. But some of those figures were -- just add confusion where they -- but they don't communicate any information that is useful. You know, the three-dimensional pictures of everything is -- was overwhelming, if there is a way to communicate that down to a simpler design, for instance, Slide 13 or 14 or whatever -- no, it's earlier than that -- was a pretty good one.

And a couple of the earlier ones with the red lines to show you that everything is separate and individual and independent and have that come after this -- what you all did for the platforms, after the 10-minute introduction on the platforms. So those are pretty key, since they have already been done and we are being asked to accept those as already completed, finished, and closed out.

Any other thoughts?

MR. THORP: Just a comment that I really appreciate some of the good probing questions and the scenarios that you put us through, especially John Stetkar. That was very helpful I think to us to kind of stimulate some thinking, and all of you had great questions for us.

So where we have fallen short on answering any of the questions, perhaps Christina will get back to us, if there is any other information that we need to provide.

CHAIRMAN BROWN: If somebody wants to feed me any questions or if they can send them to Christina, obviously, we'll feed them back to you.

MR. STATTEL: Some of the questions, John, you asked were in regard to the D3 analysis. And at some points I kind of wasn't sure we had the right people in the room to respond to that, because in actuality I&C doesn't perform evaluations of D3 analysis. That's not something that's done by the safety group. That's RXB.

So we did provide input to that, and we did -- we did generate the update to that, but it was more of -- does this system impact the existing analysis?

CHAIRMAN BROWN: Well, one way to approach that, to springboard from what John said during the meeting, and the key point was you in your slide said, "We eliminated the need for operator action," which was not correct. There are some. The point being is that Eagle-21 had some areas where they credited. There were other areas that were credited.

MR. STATTEL: Correct.

CHAIRMAN BROWN: You eliminated some of them by incorporating them, and so that's a simple approach. It's a better system because now we have reduced the number of operator actions needed to be credited for taking care of certain scenarios. Others, still there. Just like they were before. So that's a little bit more crisp way of phrasing it is a way to --

MR. STATTEL: Okay.

CHAIRMAN BROWN: -- get that -- does that help address -- if you get too complex on that, it's just going to explode.

MR. STATTEL: I mean, the D3 analysis covers dozens of scenarios. I only listed two as examples here. There are dozens of others where, you know, we could talk for hours about what the primary and what the backup mitigation and where manual operator actions come into play. But I kind of shy away from that level of meaning.

MEMBER BLEY: Well, there's a problem that we have. I mean, you partition things among yourselves. We kind of worry about who is looking at the integrated picture and picking up how these things all interact. A lot of John's questions were really of that sort.

MEMBER STETKAR: Yes. I mean, it's not our role to design a system. You know, we are ACRS. It is our role to try to keep this integrated -- some bit of high level perspective. And, you know, given a blank sheet of paper, would I have done things differently? Well, yes, I would. Would it be better? Would it be acceptable to the staff? You know, that remains to be seen.

But I think it is important for the full committee that you do provide that perspective of what was the purpose of this upgrade of the replacement, and not necessarily -- and be careful about not overselling things in clear black and white when they might not be.

CHAIRMAN BROWN: Okay. Okay. With that, if there's no other comments or observations, the meeting is closed. Adjourned.

(Whereupon, at 5:42 p.m., the proceedings in the foregoing matter were adjourned.)

Diablo Canyon Process Protection System LAR

Presented by: NRR / EICB

Pat Hiland Director DE
John Thorp Branch Chief EICB
Rich Stattel Technical Reviewer EICB
Rossnyev Alvarado EICB
Samir Darbali EICB

February 18, 2014

Presentation Outline / Agenda

- Introduction
- Overview of Diablo Canyon License Amendment Request
- Diversity and Defense in Depth
- Communication
- Secure Development and Operations Environment (SDOE)
- Platform Status
  - Tricon
  - ALS
- PPS Project Schedule

Introduction
Diablo Canyon PPS Replacement LAR

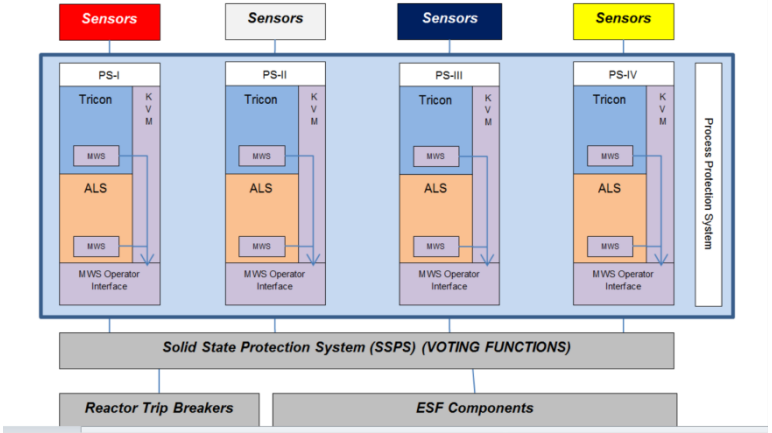
- **On October 26, 2011, PG&E submitted a LAR to replace the existing Eagle 21 Process Protection System with a new more modern digital system.**
- **The Safety Evaluation for the Tricon Platform Topical Report was Issued in 2012 and the Safety Evaluation for the ALS Platform TR was issued in 2013.**
- **The Diablo Canyon Digital Process Protection System (PPS) is based on both the Microprocessor based Invensys Tricon and the FPGA based Westinghouse ALS Platforms.**
- **As part of the NRR acceptance review process 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

Introduction
Review Process

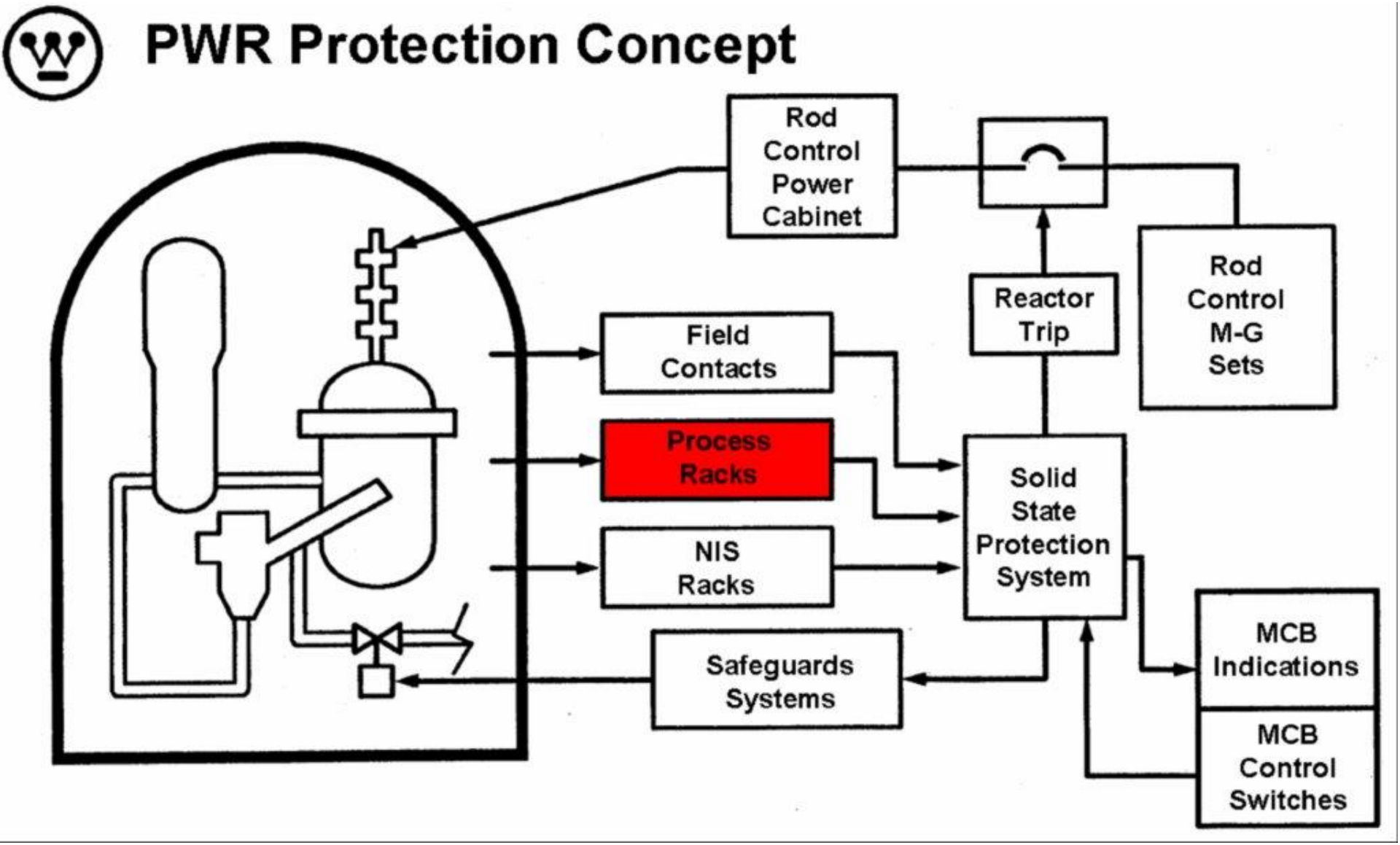
- **EICB is conducting the review in accordance with Standard Review Plan (SRP) Chapter 7 (NUREG-0800, Chapter 7) and LIC -101.**

- **Interim Staff Guide 06 “Licensing Process for Digital I&C Systems” is also being Piloted as part of this review effort.**

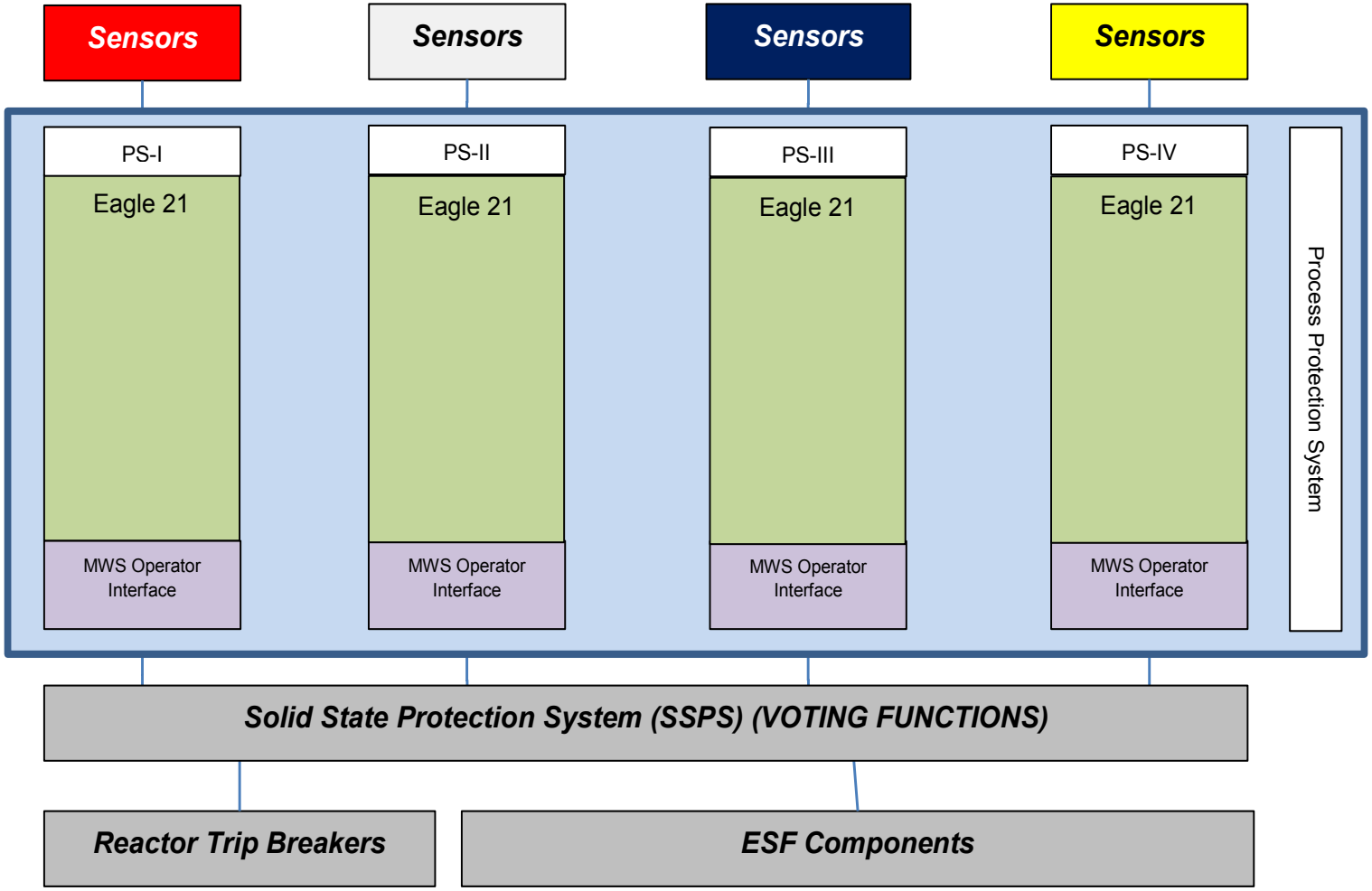
Process Protection System Overview



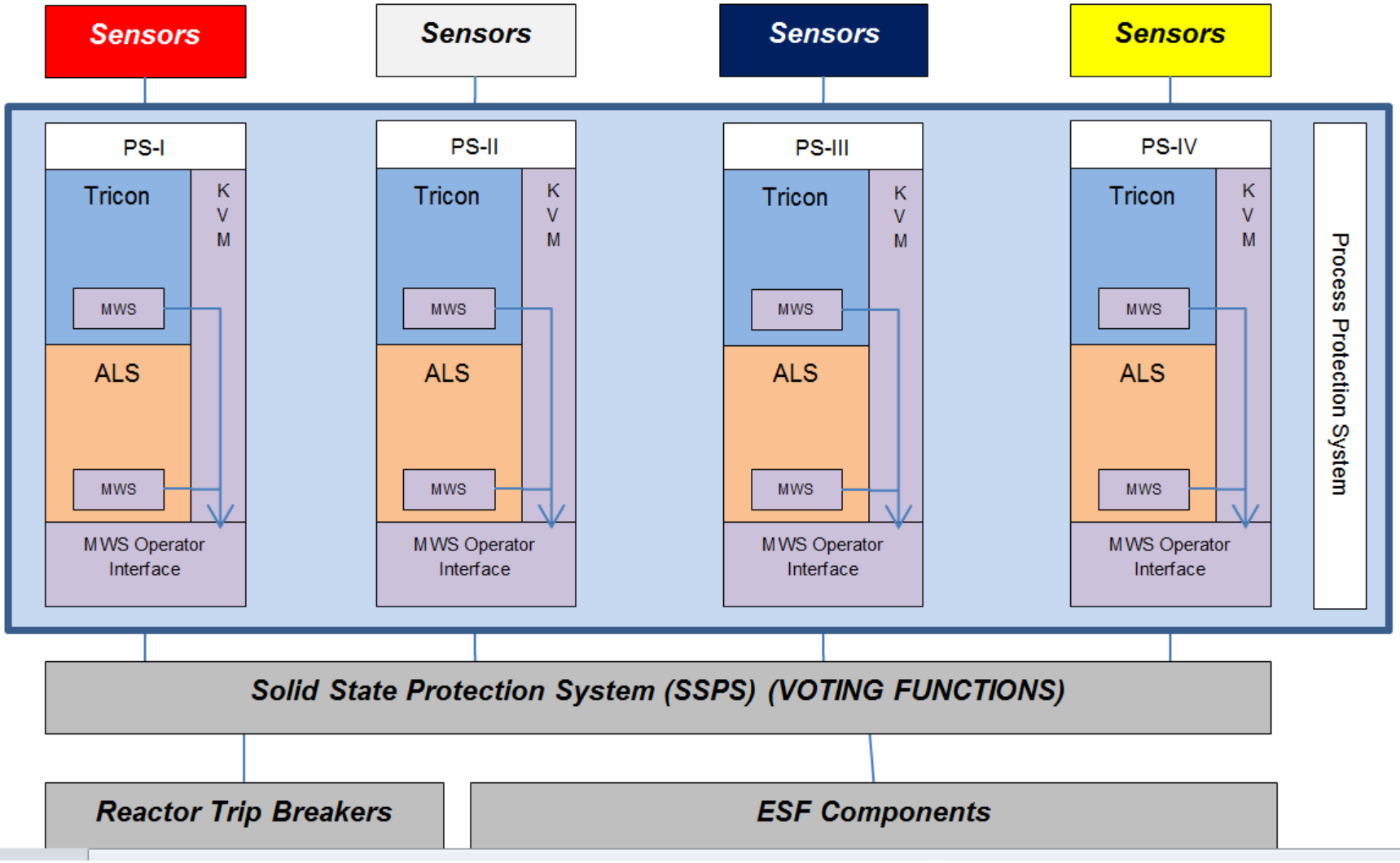
Overview of Diablo Canyon Application
PPS System Architecture



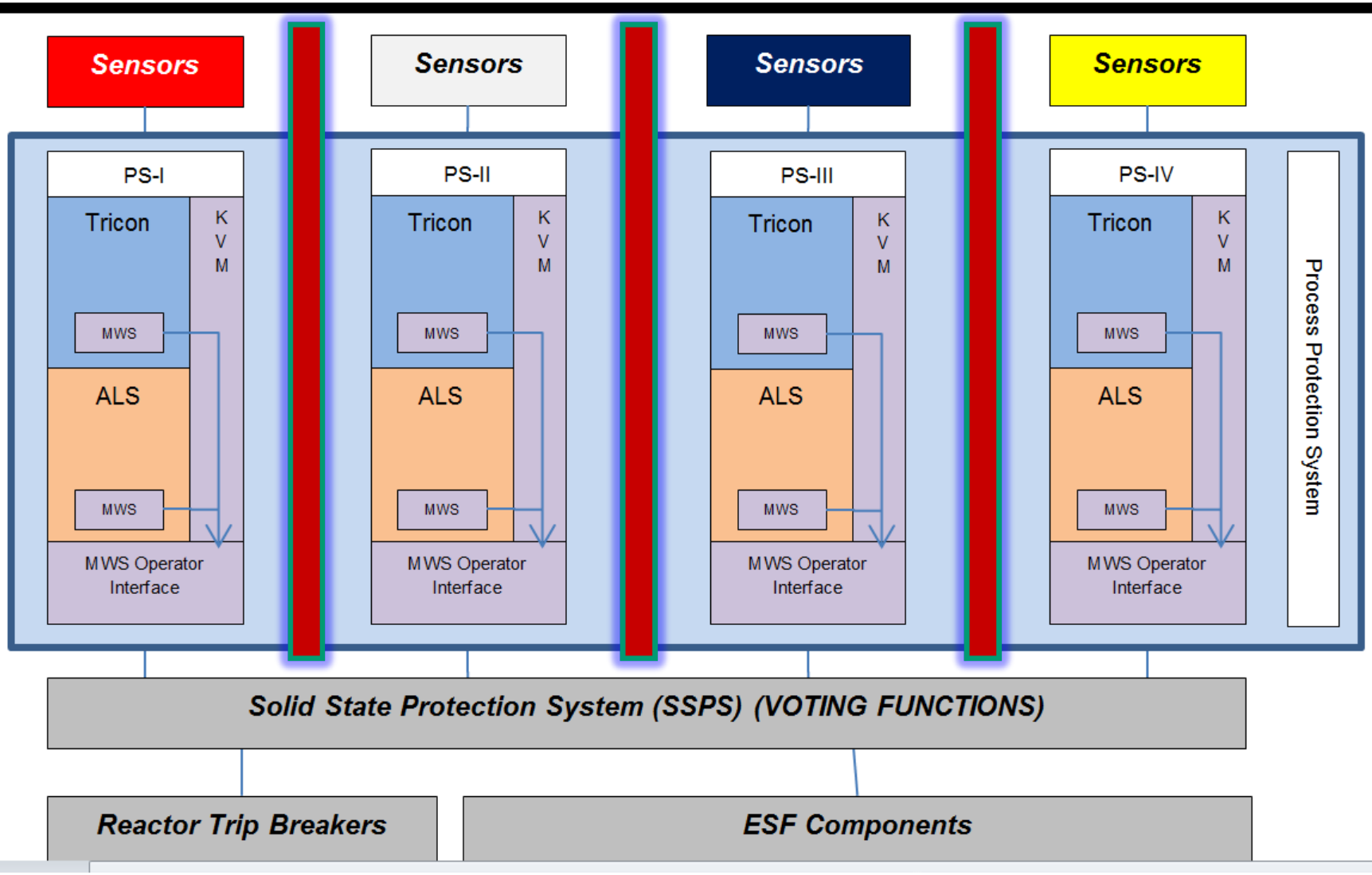
Overview of Diablo Canyon Application
PPS System Architecture



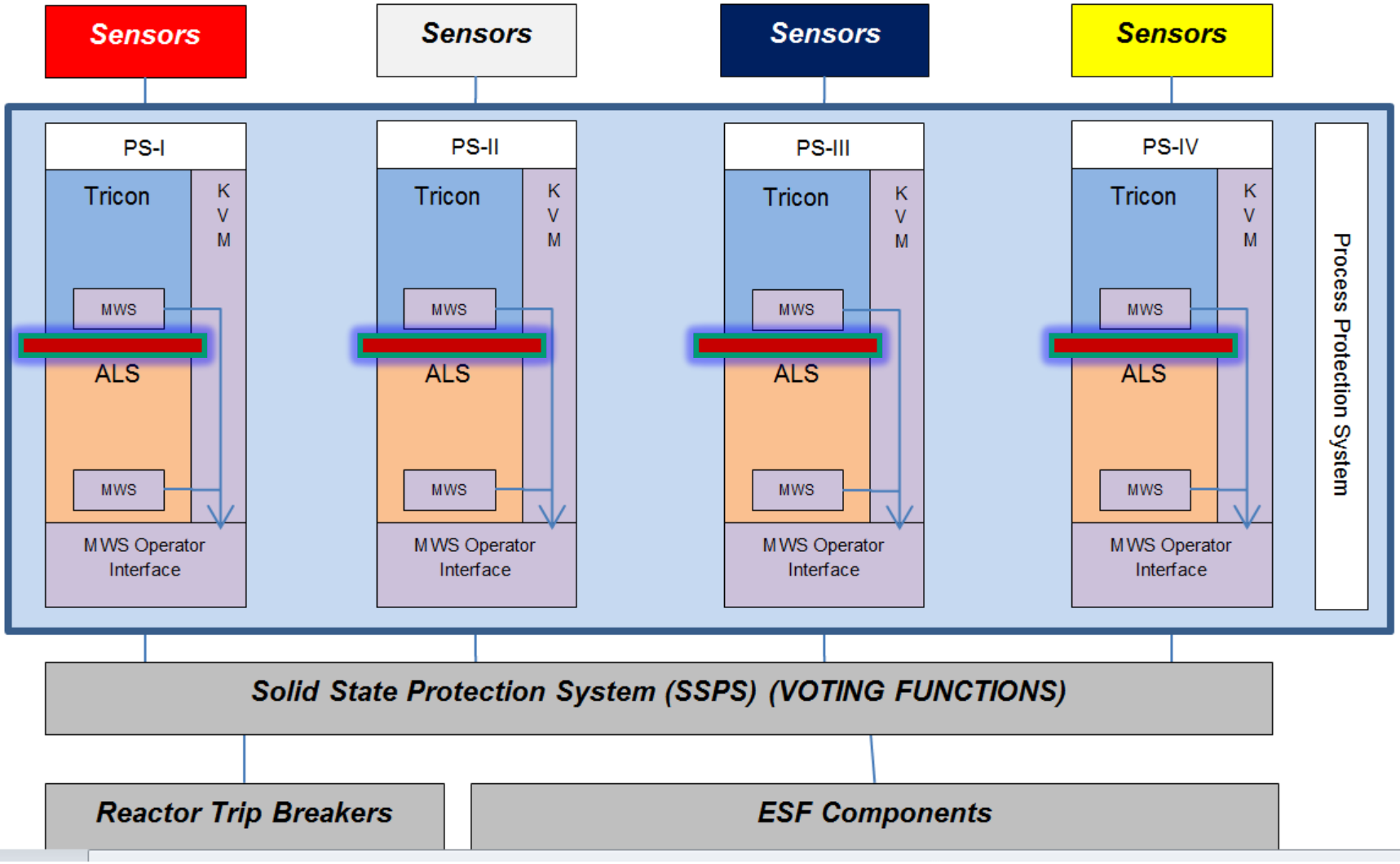
Overview of Diablo Canyon Application
PPS System Architecture



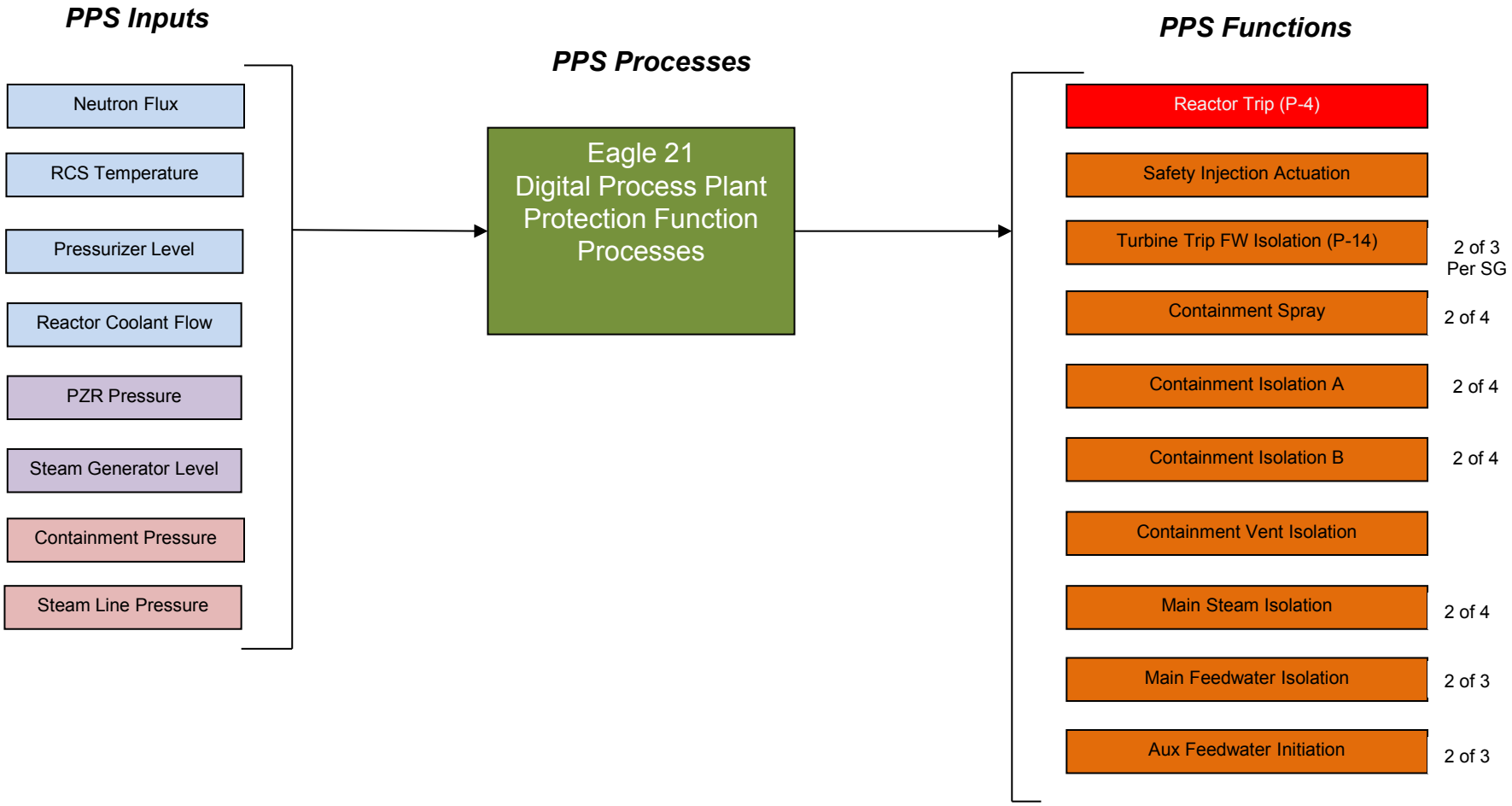
Overview of Diablo Canyon Application
PPS System Architecture



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

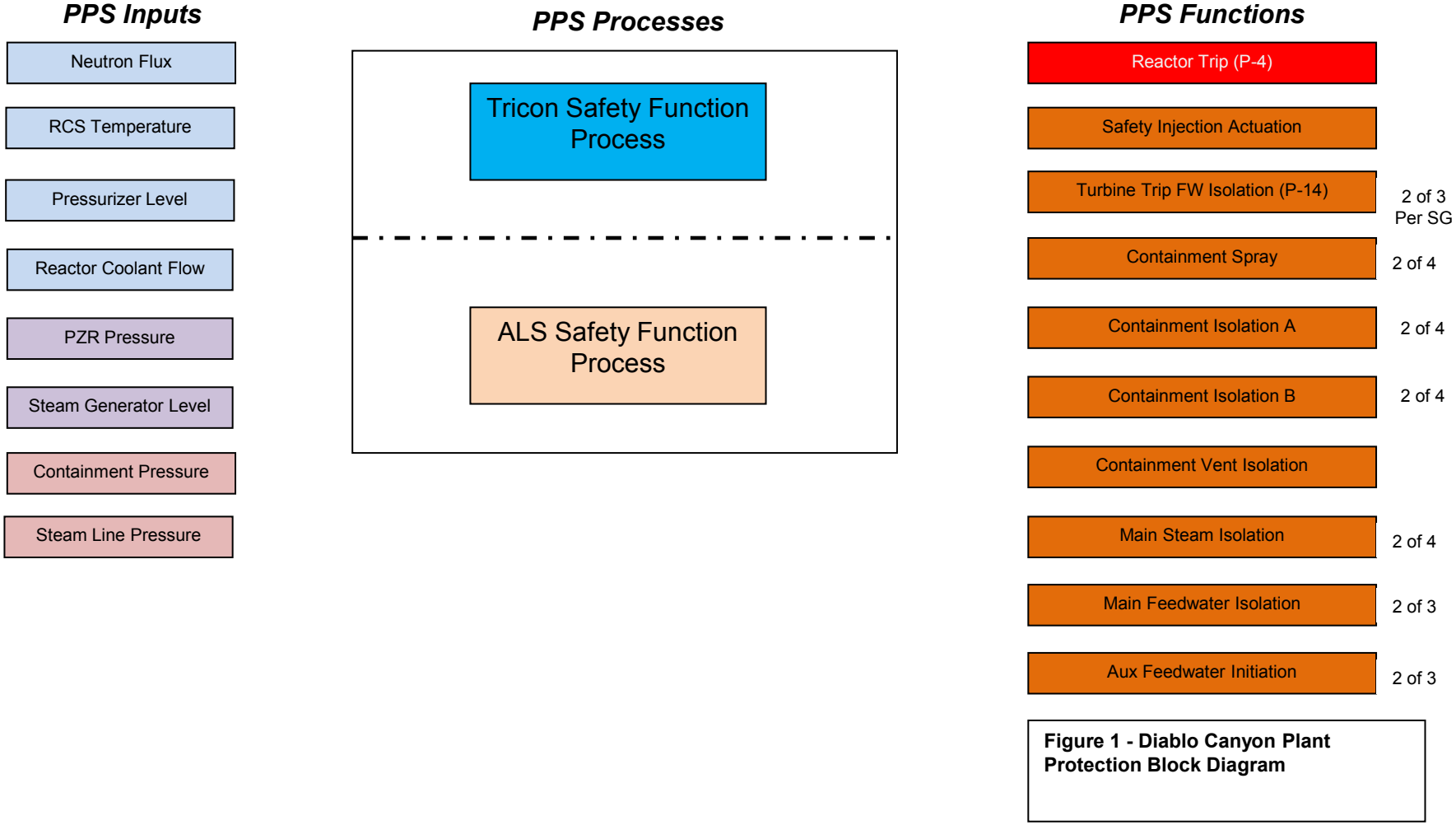


Figure 1 - Diablo Canyon Plant Protection Block Diagram

Overview of Diablo Canyon Application
PPS System Tricon Function Allocation

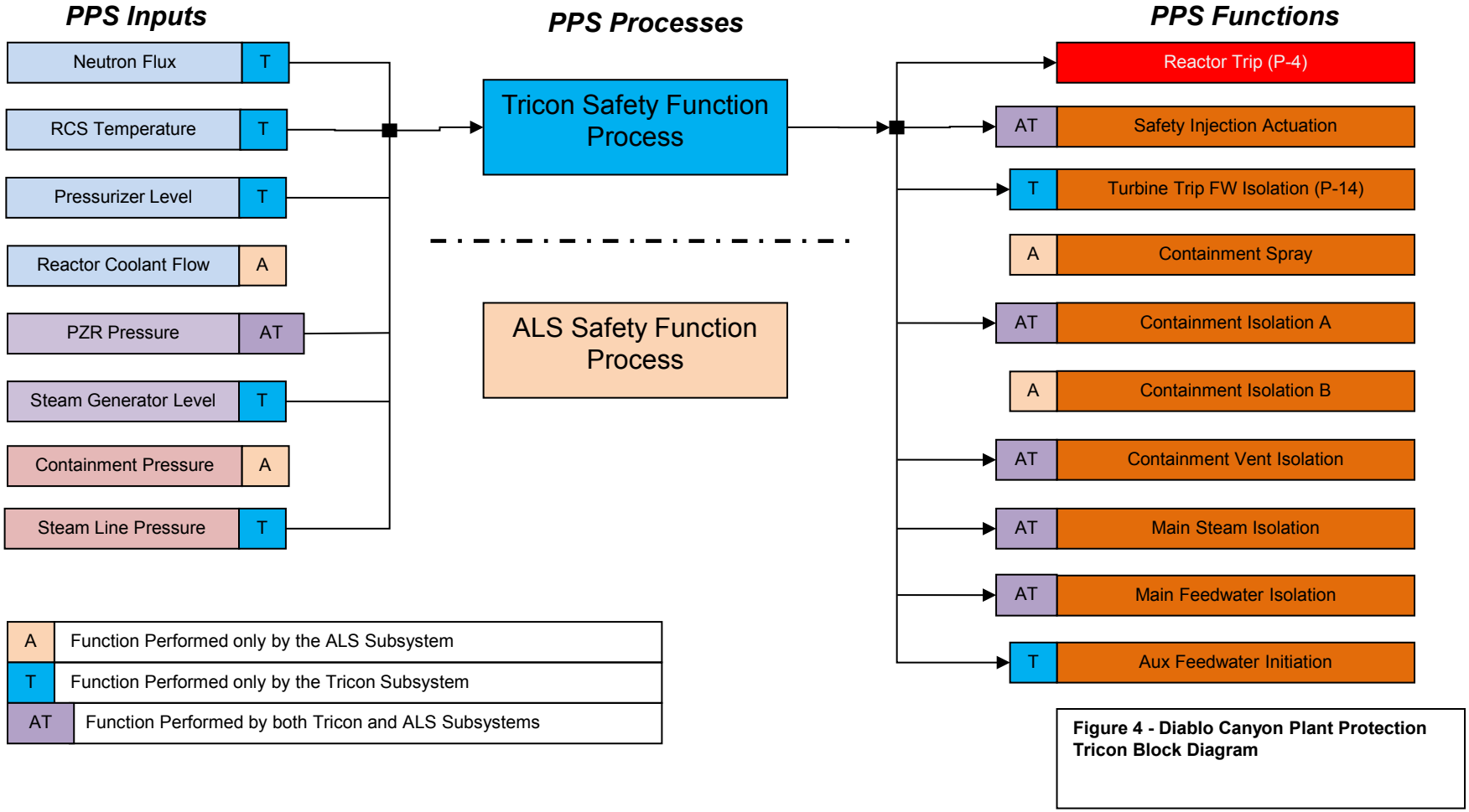


Figure 4 - Diablo Canyon Plant Protection Tricon Block Diagram

Overview of Diablo Canyon Application
PPS System Tricon Function Allocation

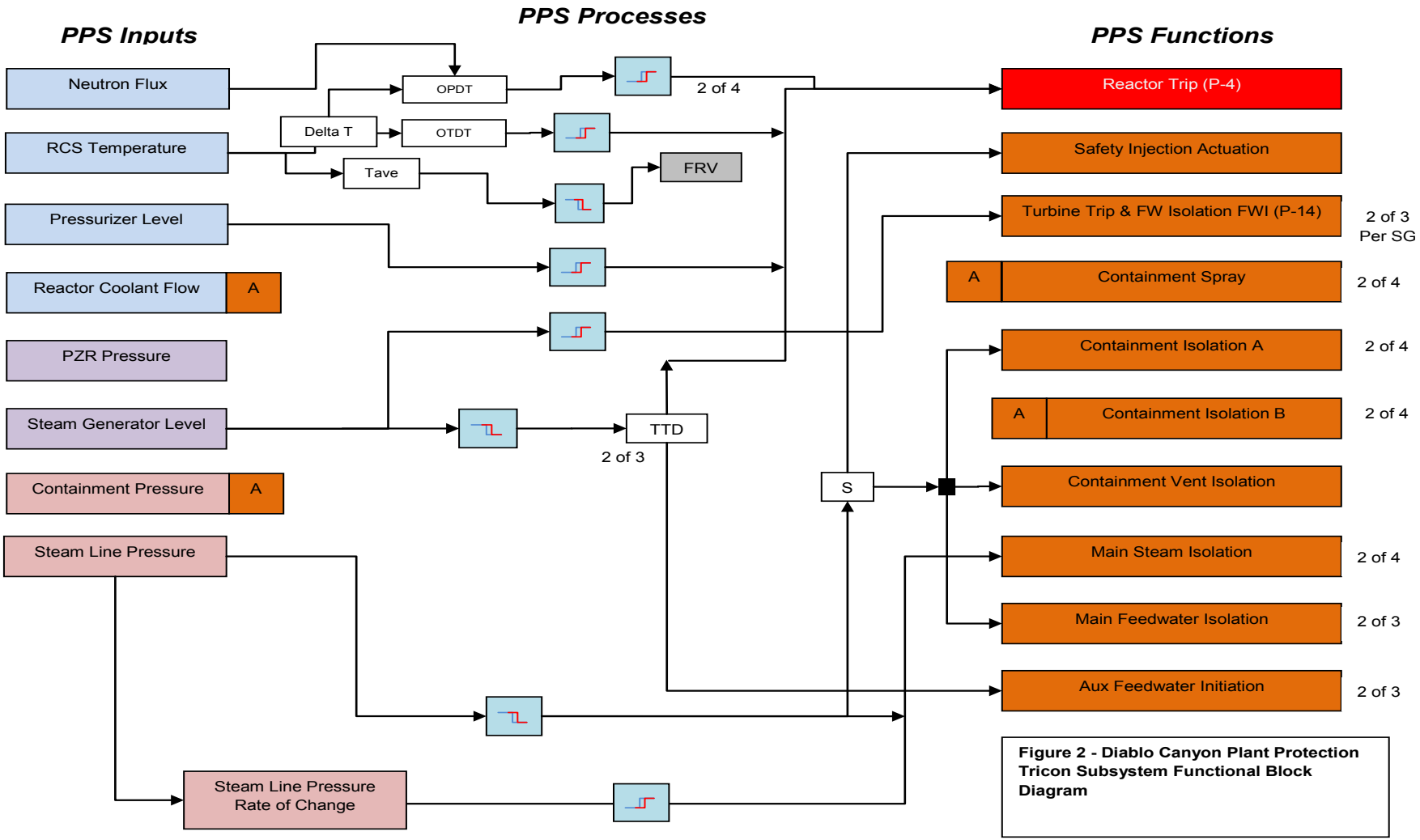


Figure 2 - Diablo Canyon Plant Protection Tricon Subsystem Functional Block Diagram

Overview of Diablo Canyon Application
PPS System Tricon Function Allocation

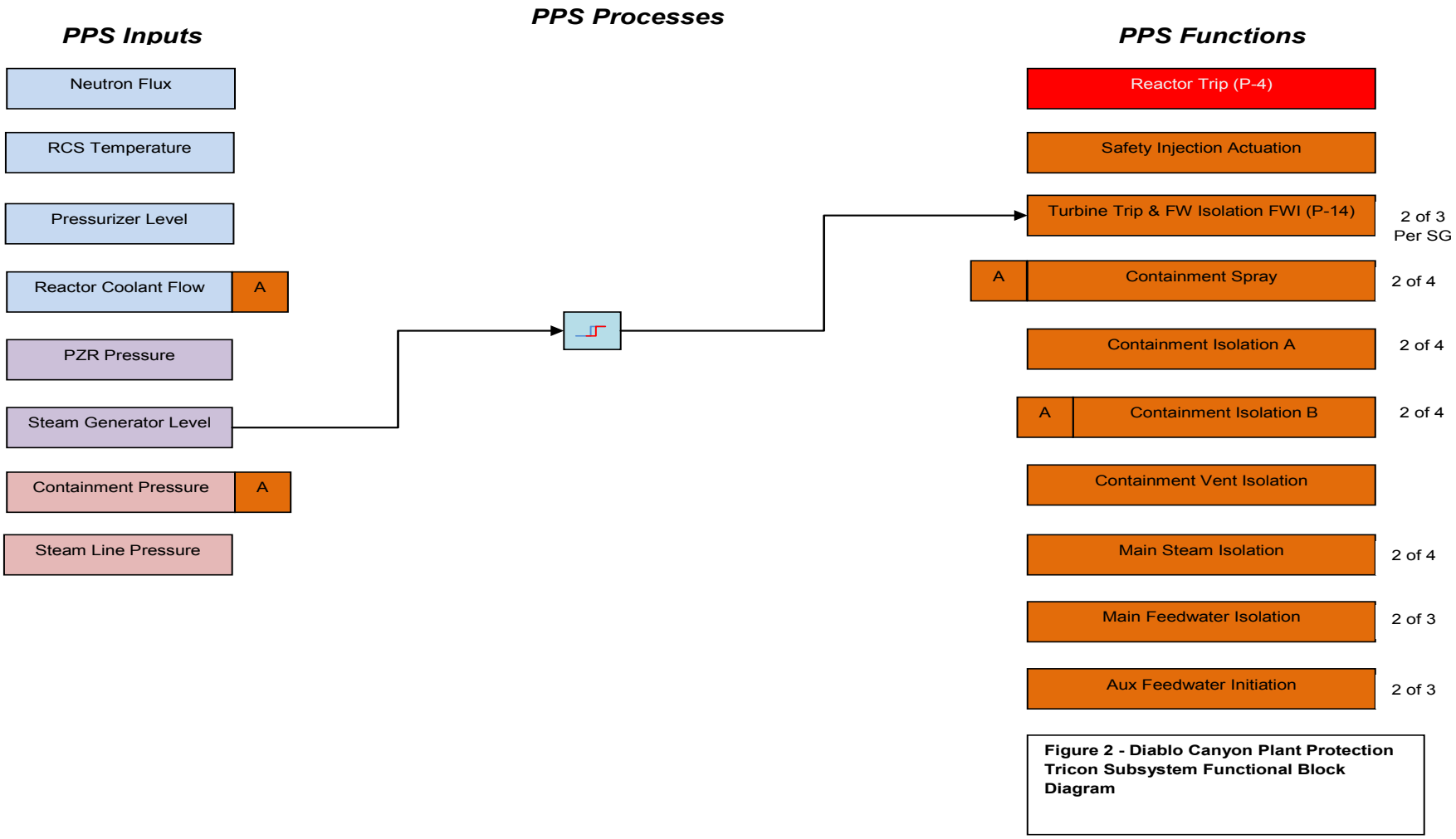
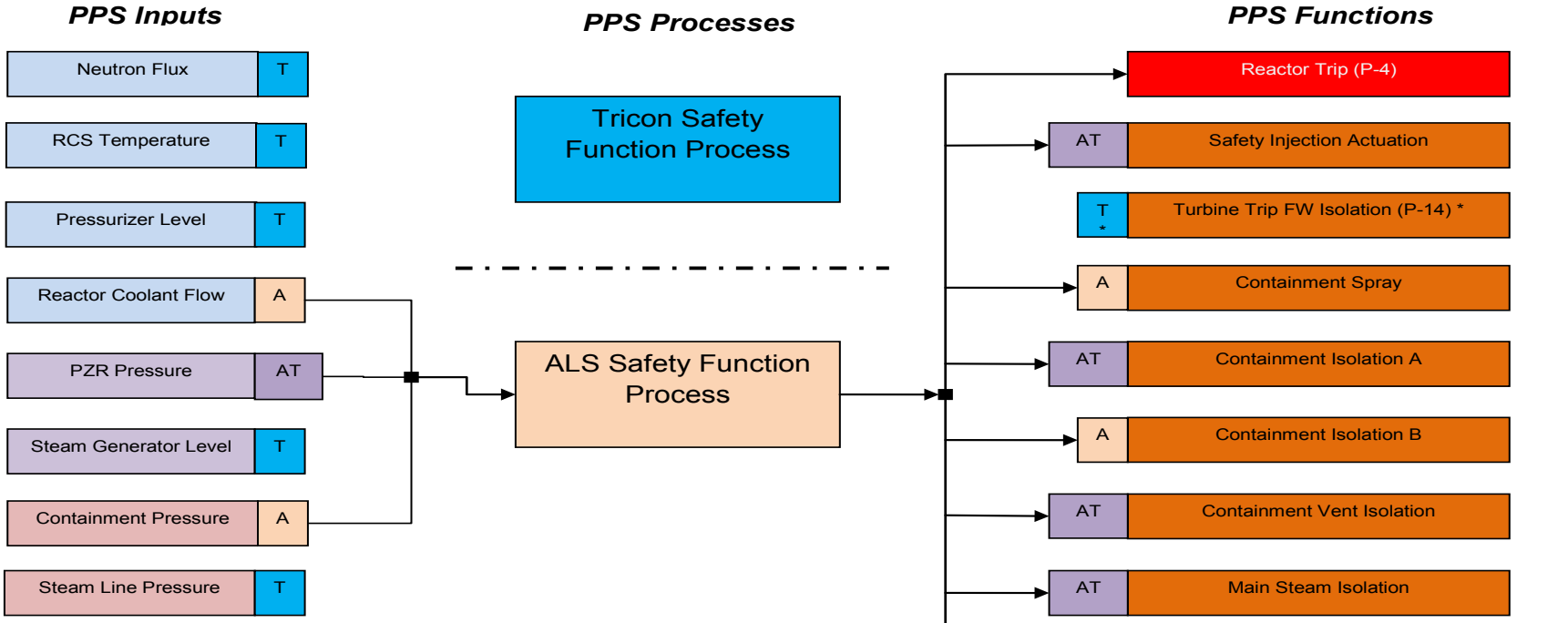


Figure 2 - Diablo Canyon Plant Protection Tricon Subsystem Functional Block Diagram

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.**

Figure 4 - Diablo Canyon Plant Protection ALS Block Diagram

Overview of Diablo Canyon Application
PPS System ALS Function Allocation

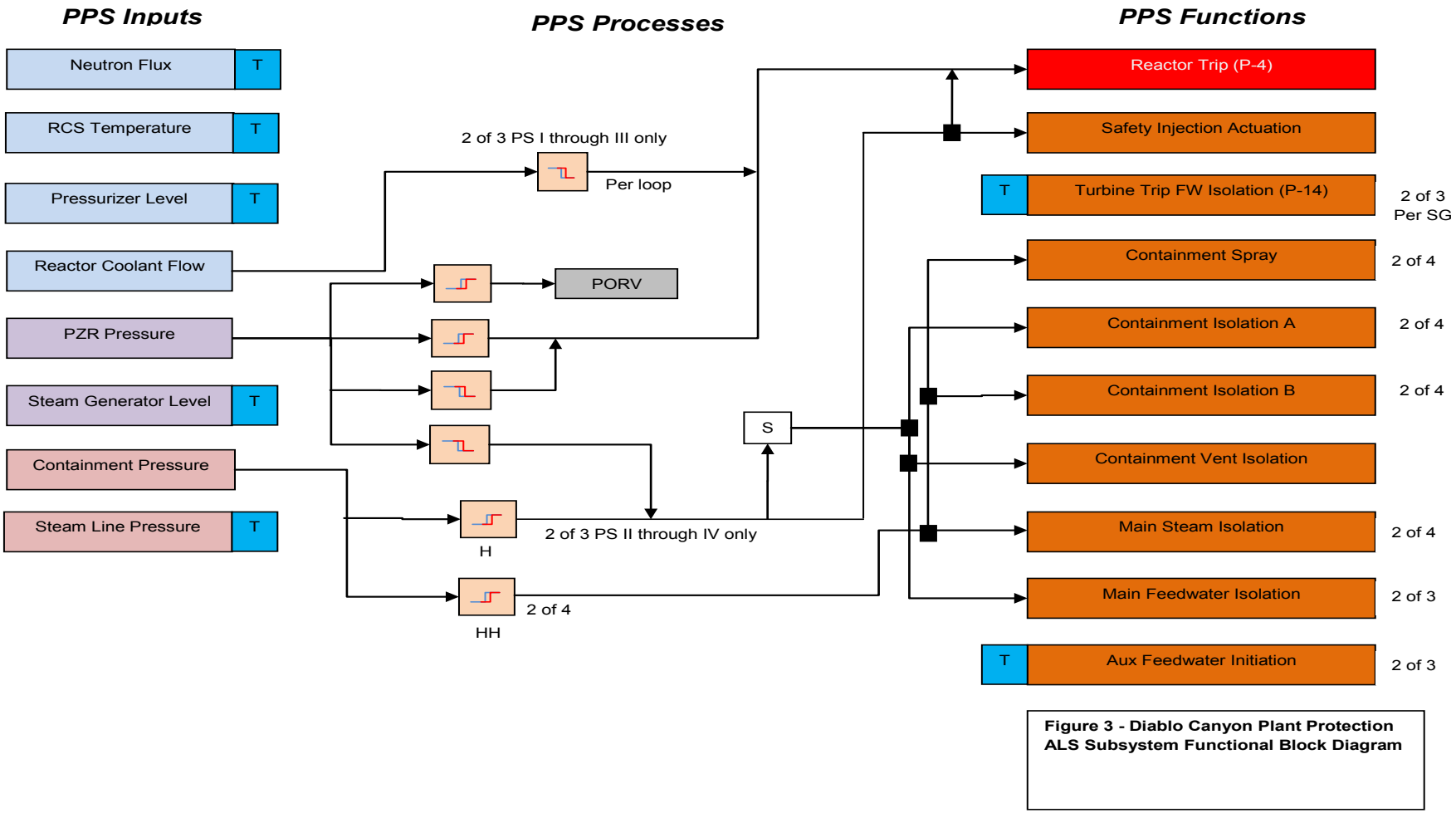


Figure 3 - Diablo Canyon Plant Protection ALS Subsystem Functional Block Diagram

Overview of Diablo Canyon Application
PPS System ALS Function Allocation

Turbine Trip and Feedwater Isolation function

This is the primary mitigating function for “Excessive Heat Removal Due to a Feedwater system malfunction” event.

- Backup mitigating function “Power Range High Flux Reactor Trip.”
- The High Flux Reactor Trip does not rely on the PPS system and will thus not be affected by a CCF of the PPS.

Overview of Diablo Canyon Application
PPS System ALS Function Allocation

Aux FW Initiation

This 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”, and “Loss of Normal Feedwater “ events.

- Backup mitigating functions are;
  1) Pressurizer High Pressure Reactor Trip,
  2) High Containment Pressure Safety Injection and Reactor Trip
- Both of these backup mitigating safety functions do not rely upon the Tricon subsystem and will thus not be affected by a CCF of the PPS.

In addition, the AFW system is actuated by the independent AMSAC system on Low SG level. AMSAC is independent and Diverse from the PPS system.

Diversity & Defense-In-Depth

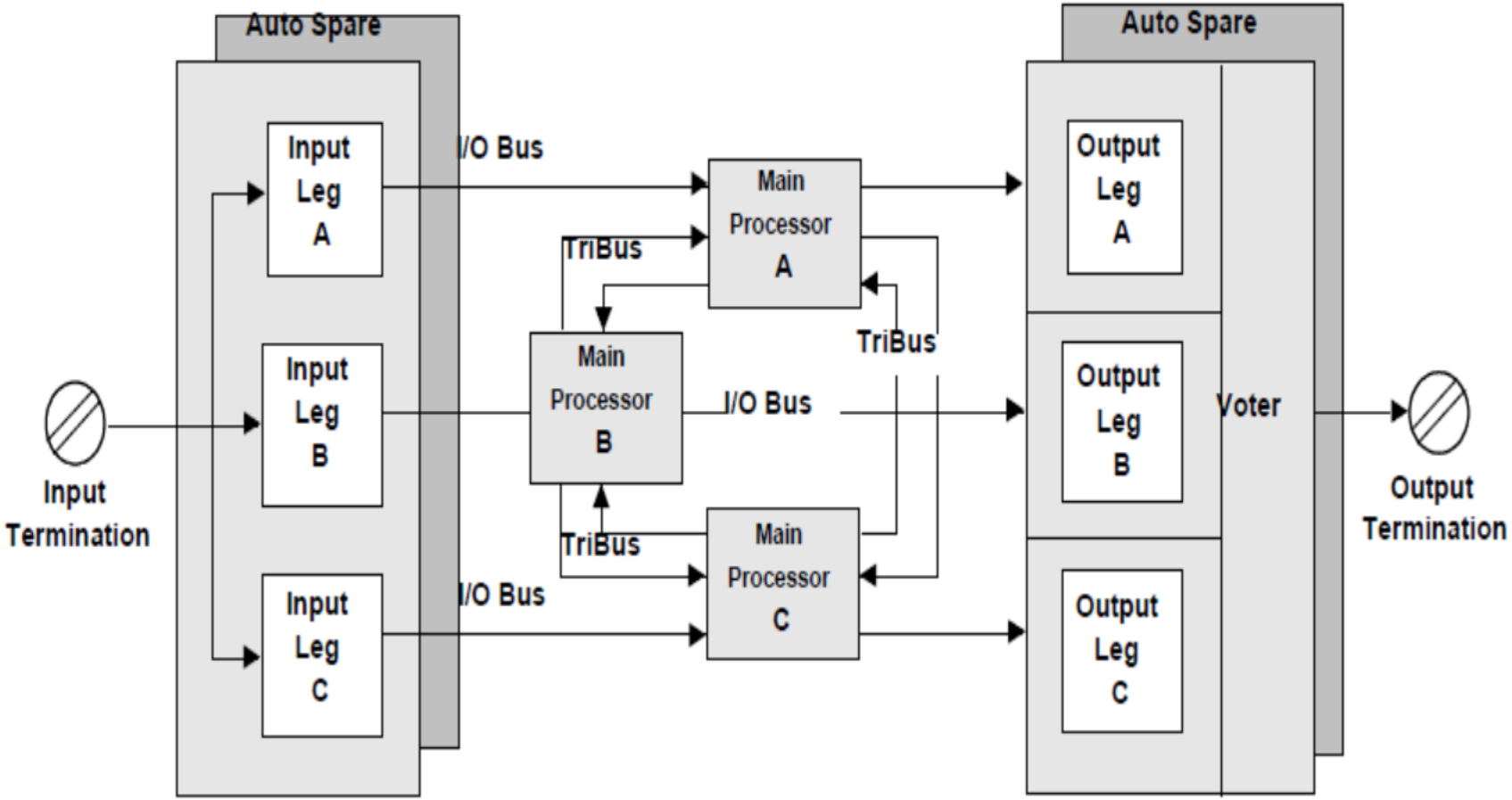
Diversity and Defense in Depth (D3)
Guidance

- **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

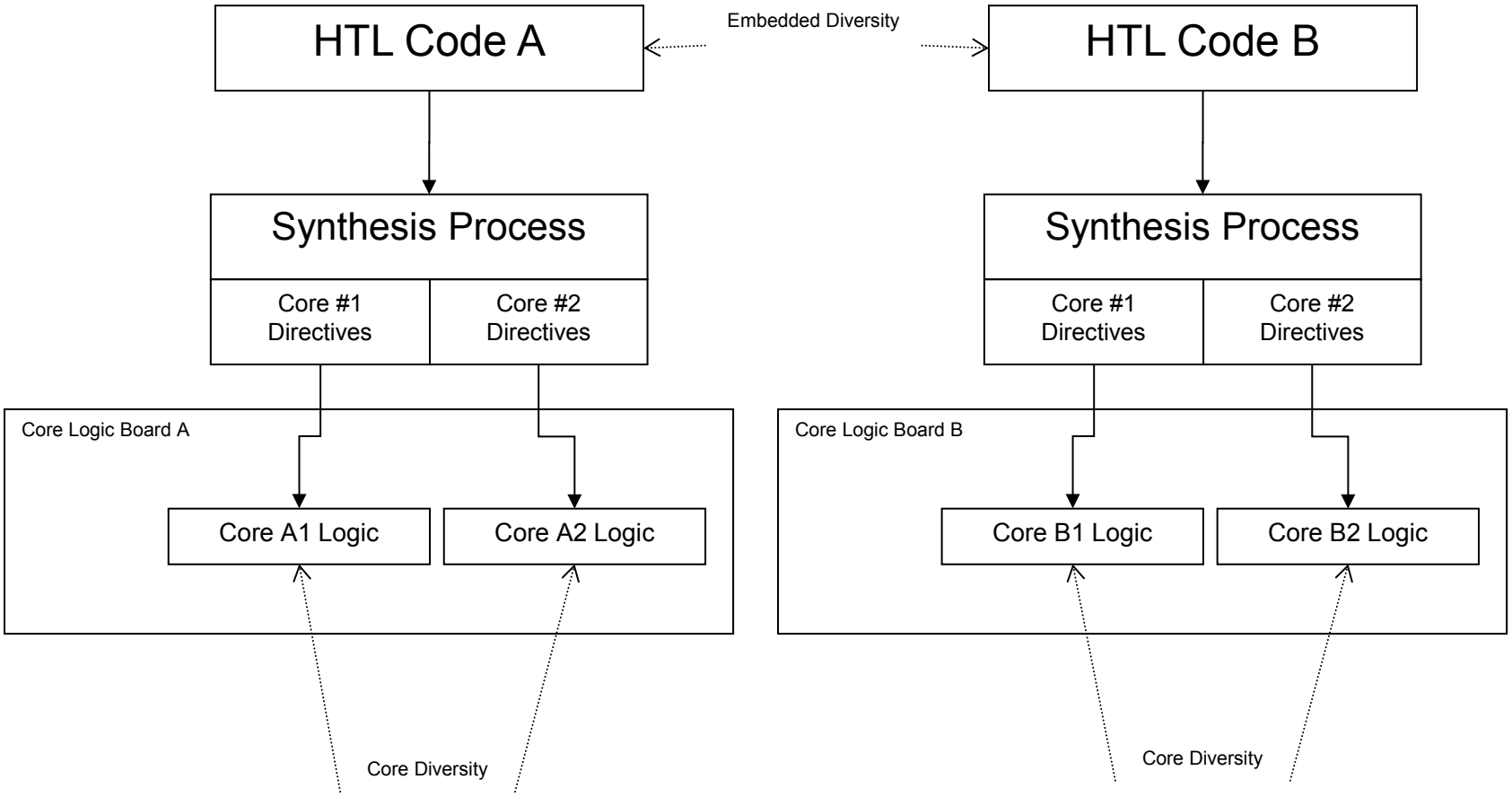
Diversity and Defense in Depth (D3)
Analysis Preformed by Licensee

- **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**
    - **Identifies Three Parameters 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**

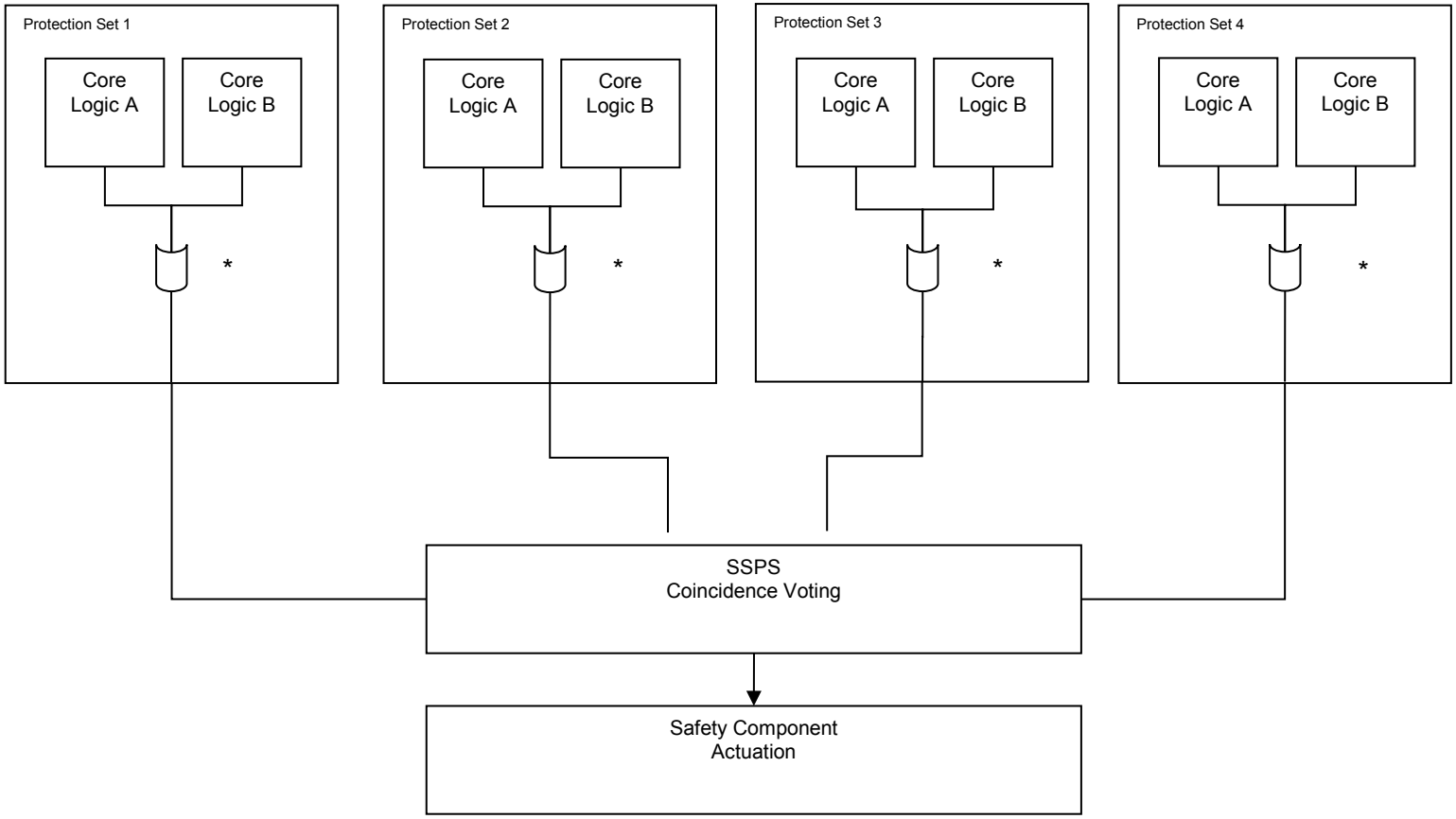
Diversity and Defense in Depth
Diablo Canyon Diversity Solution



Diversity and Defense in Depth
Diablo Canyon Diversity Solution

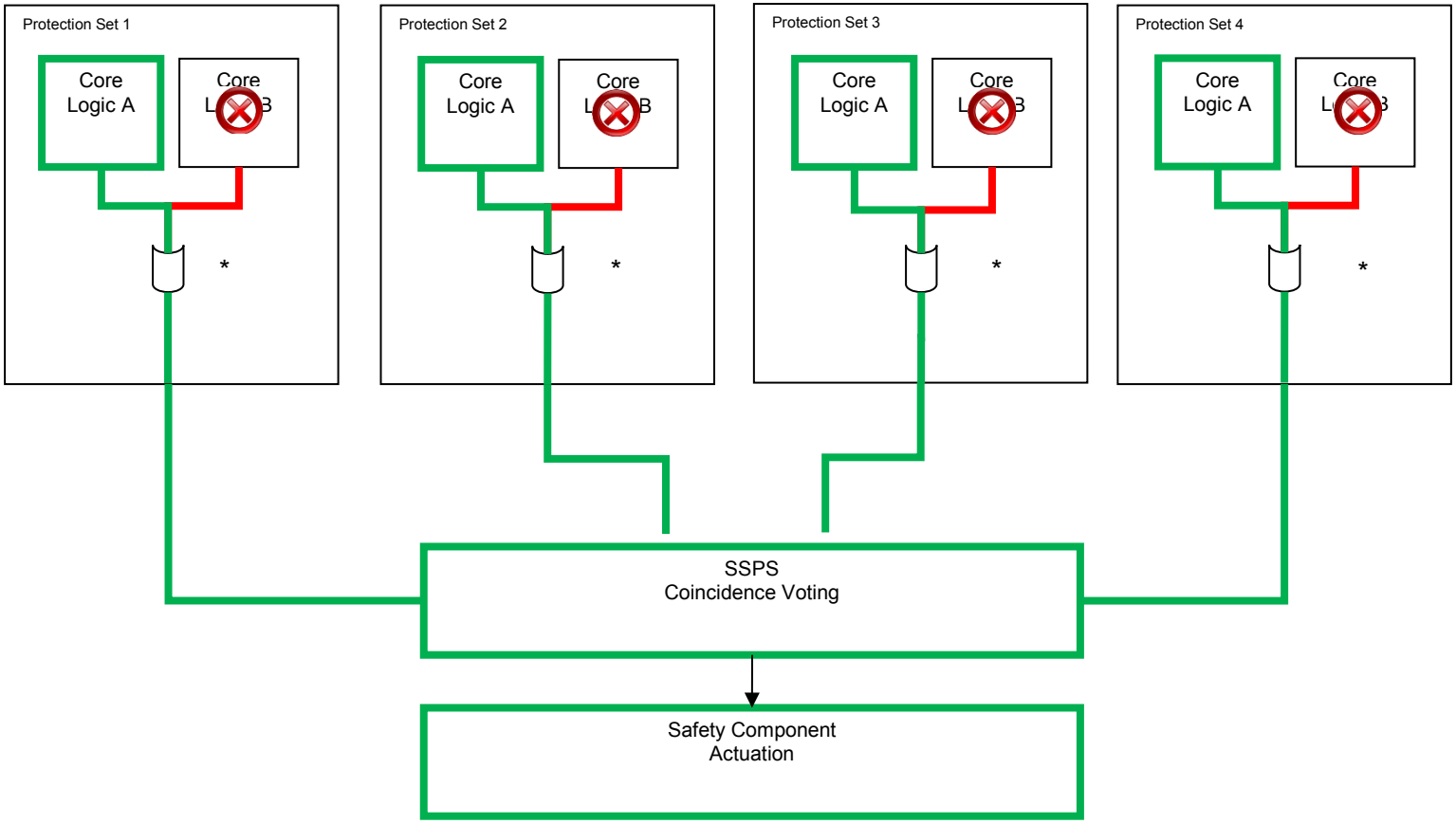


Diversity and Defense in Depth
Diablo Canyon Diversity Solution



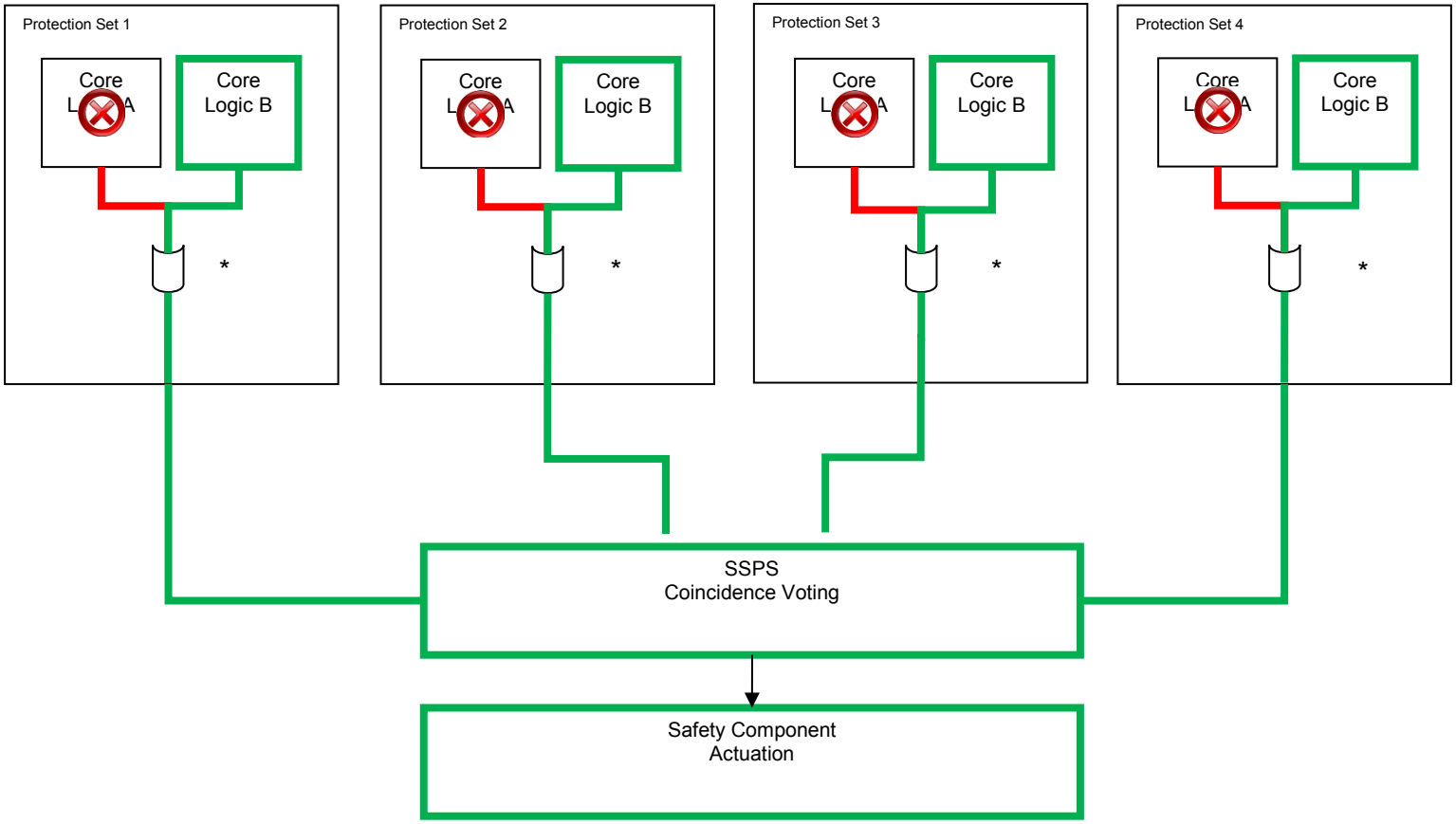
* OR function is accomplished by DO contacts in series for De-energize To Trip (DTT) or in parallel for Energize To Trip (ETT) function.

Diversity and Defense in Depth
Diablo Canyon Diversity Solution



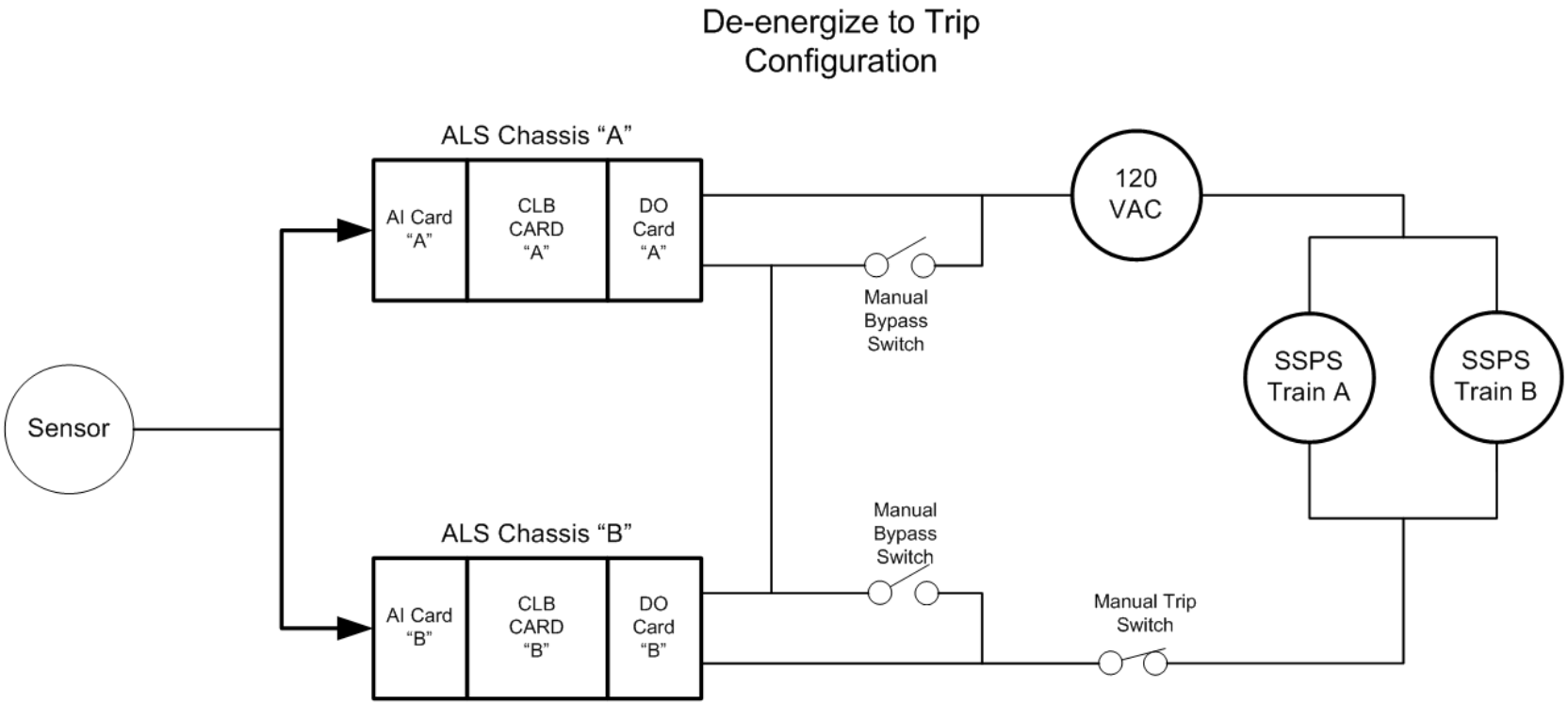
* OR function is accomplished by DO contacts in series for De-energize To Trip (DTT) or in parallel for Energize To Trip (ETT) function.

Diversity and Defense in Depth
Diablo Canyon Diversity Solution

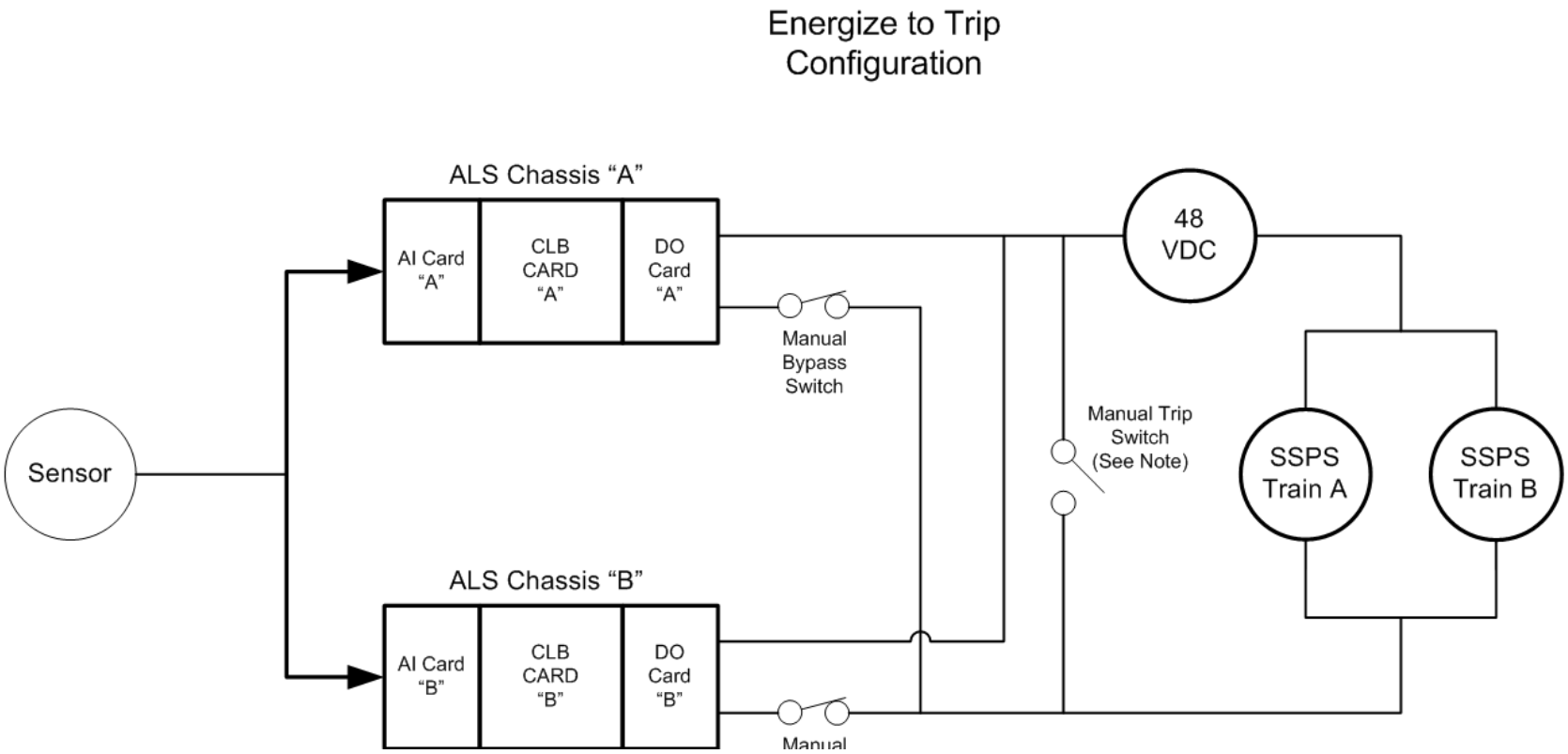


* OR function is accomplished by DO contacts in series for De-energize To Trip (DTT) or in parallel for Energize To Trip (ETT) function.

Diversity and Defense in Depth
Diablo Canyon Diversity Solution



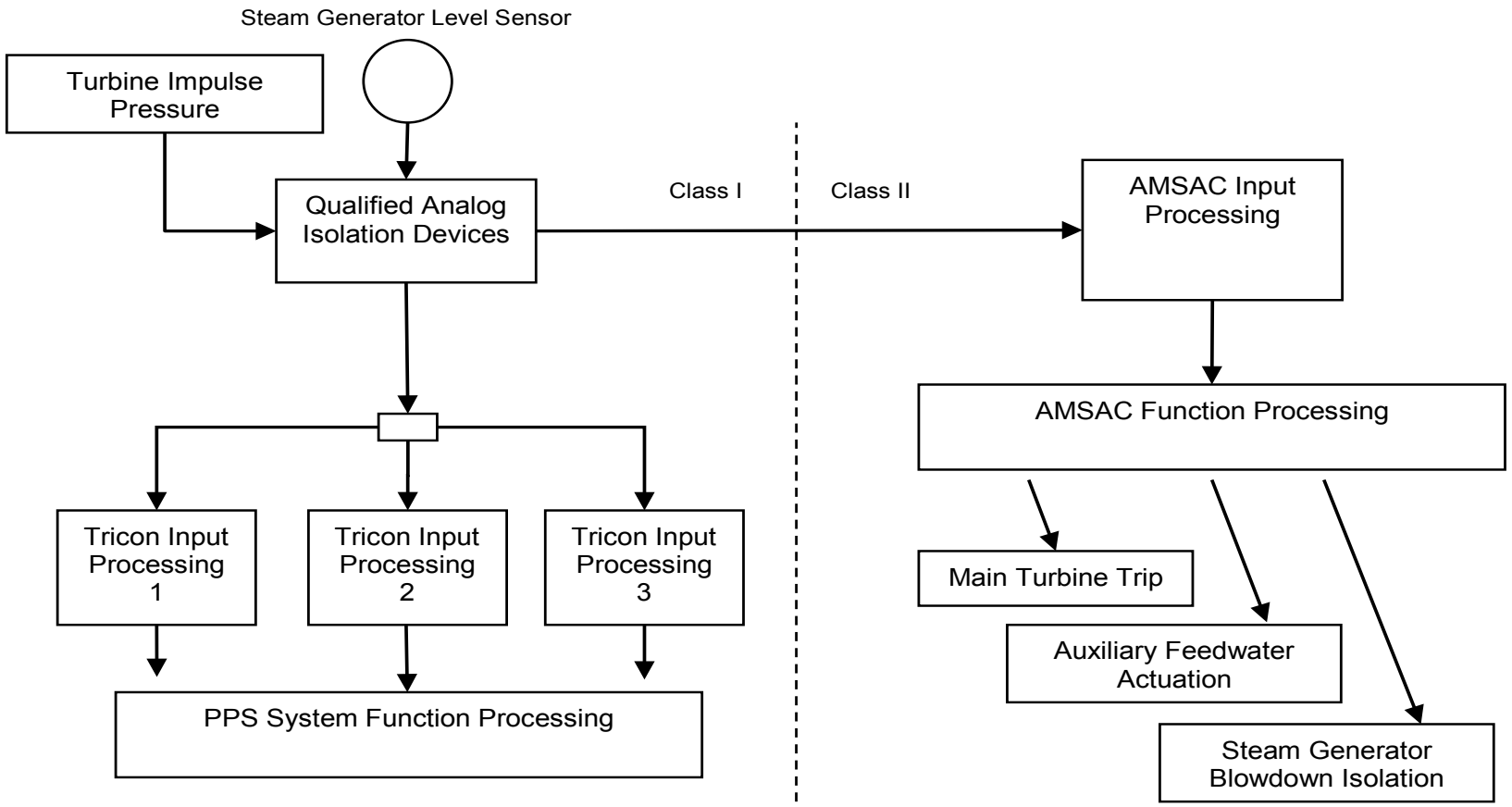
Diversity and Defense in Depth
Diablo Canyon Diversity Solution



Diversity and Defense in Depth
Anticipated Transient Without Scram (ATWS)

- The design architectures are completely different.
- The two PPS subsystems were developed by vendors that were different than the vendor that developed the AMSAC system . *
- The AMSAC system uses different microprocessors which are produced by different manufacturers than those used in the Tricon subsystem.
- The diverse AMSAC system is powered by a non-safety related source.
- The quality of components in the AMSAC system is based on selection of known process electrical components that have proven reliability.
- The diverse AMSAC system initiation path is separate and independent from the Tricon PPS system processors which are subject to a SWCCF.
- The diverse AMSAC system initiation path is separate and independent from the ALS PPS system Core Logic Boards.
- Though the AMSAC system shares the same Steam Generator Level sensors used for the PPS system, these sensors are not digital devices and are not subject to the effects of a software CCF.
- 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
Anticipated Transient Without Scram (ATWS)



Diversity and Defense in Depth
Manual Operator Action

- The new Diablo Canyon Digital Process Protection System eliminates the need to perform 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.

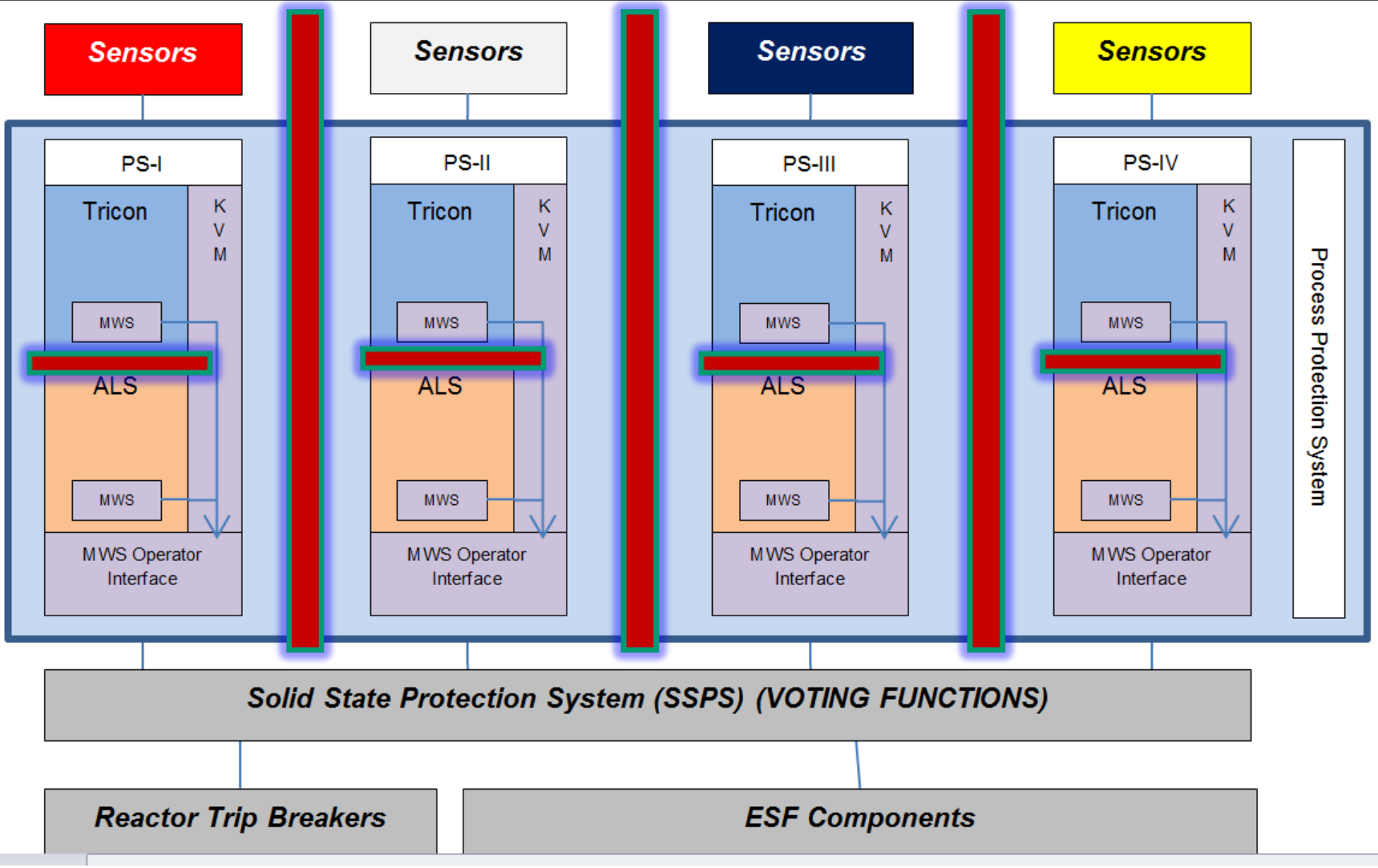
  – Existing component and division level actuation capability at the main control boards will be retained

Communications

Communication
Guidance

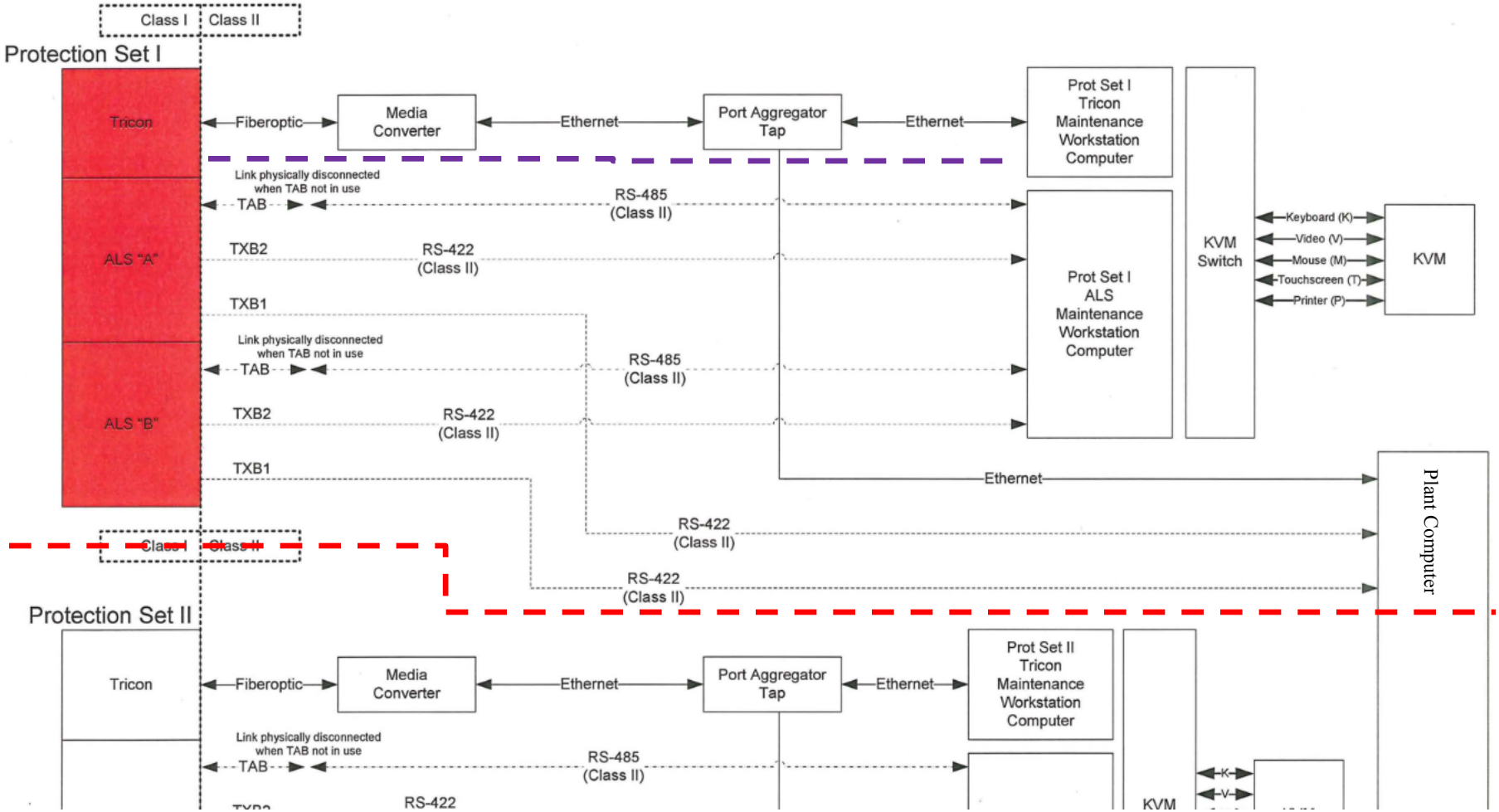
- Guidance for Communication
  - IEEE 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”
  - IEEE 7-4.3.2, “Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Station”
  - DI&C-ISG-04, “Highly Integrated Control Rooms-communication Issues”

Overview of Diablo Canyon Application
PPS System Architecture

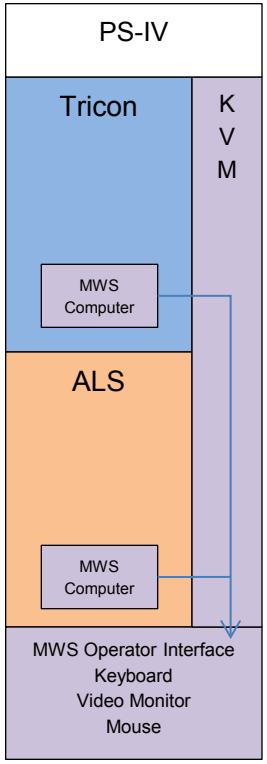


Communications Architecture

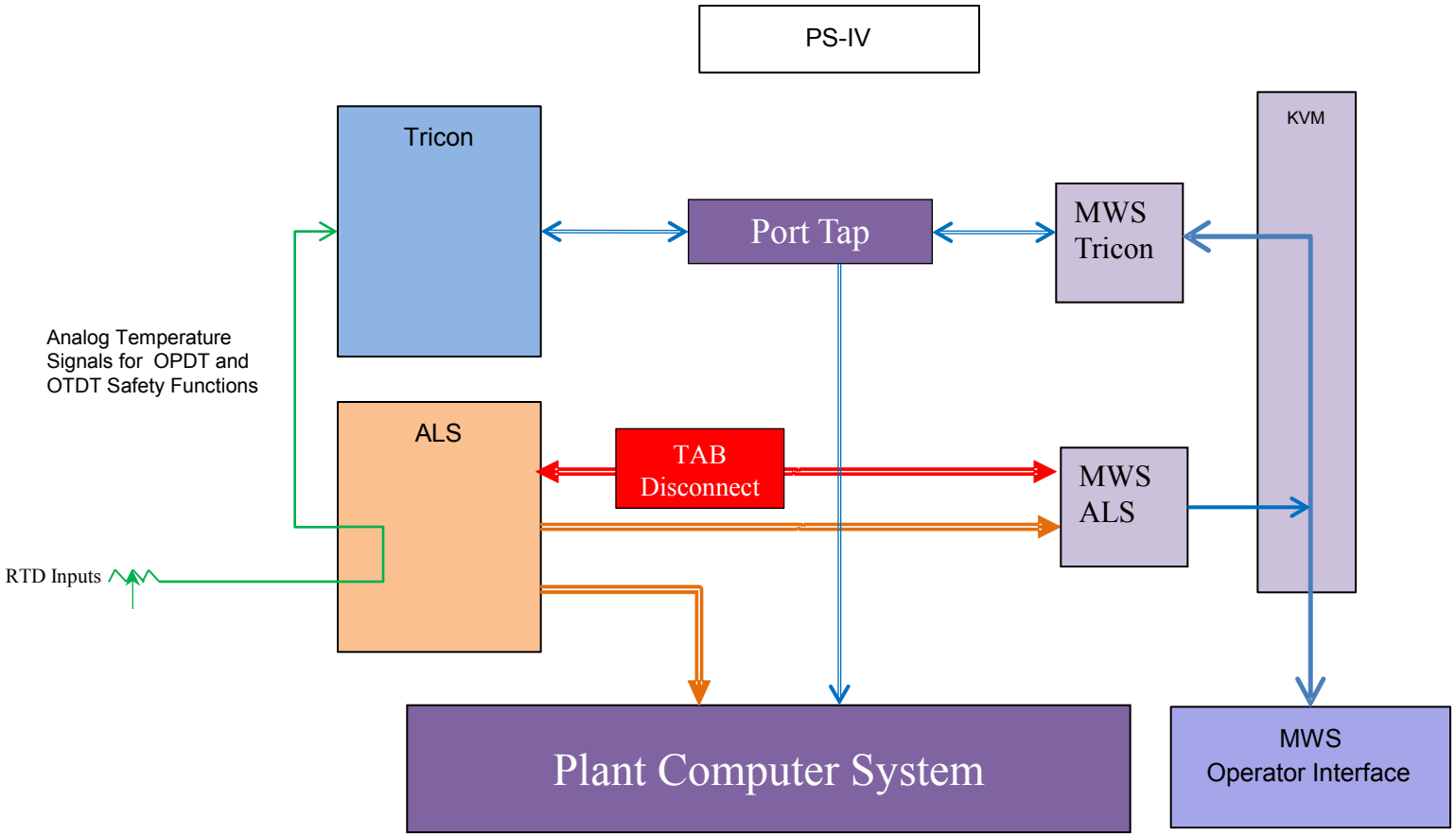
Figure 3-3 PPS Replacement Communications



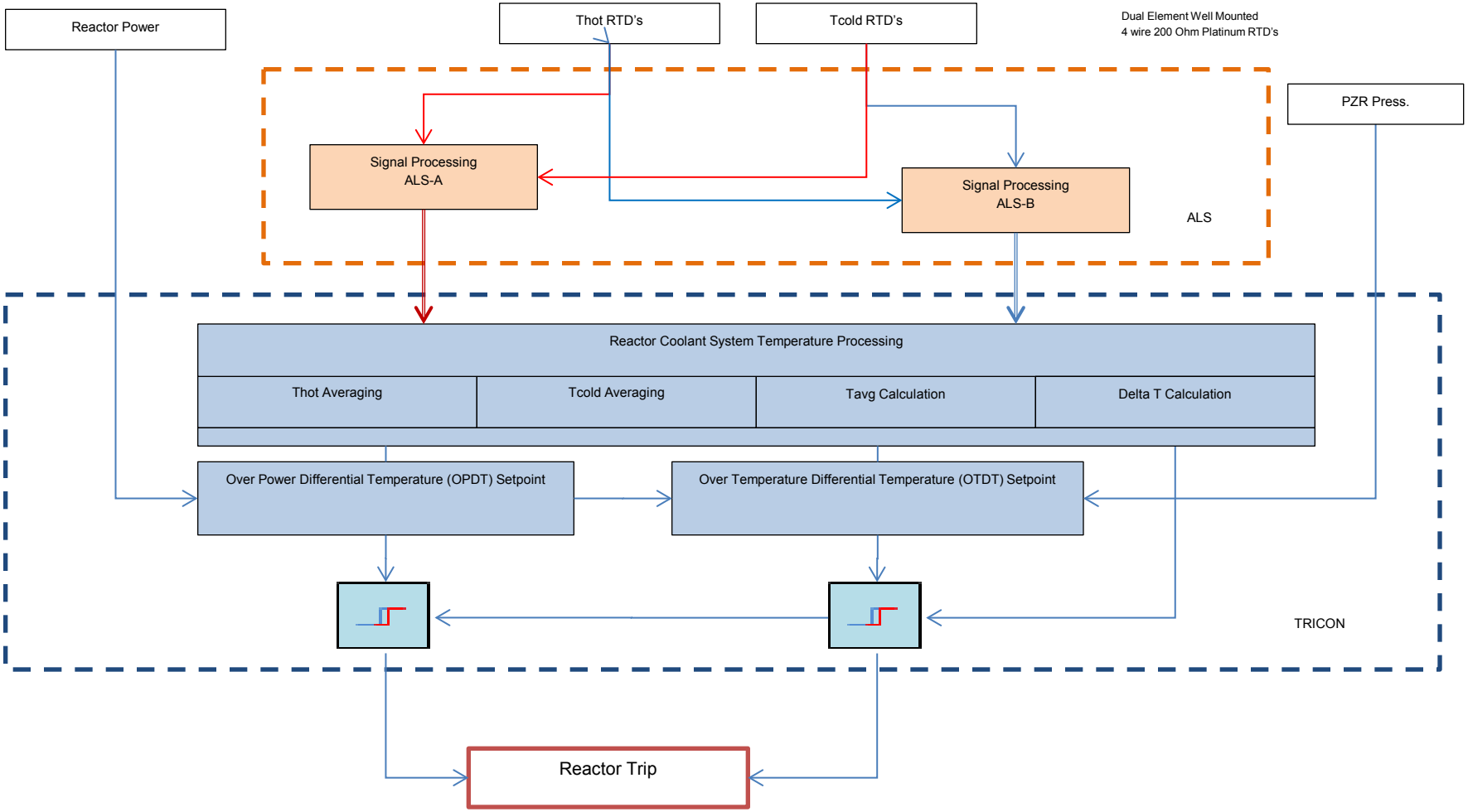
Overview of Diablo Canyon PPS Application
Safety to Non-Safety Communication Architecture



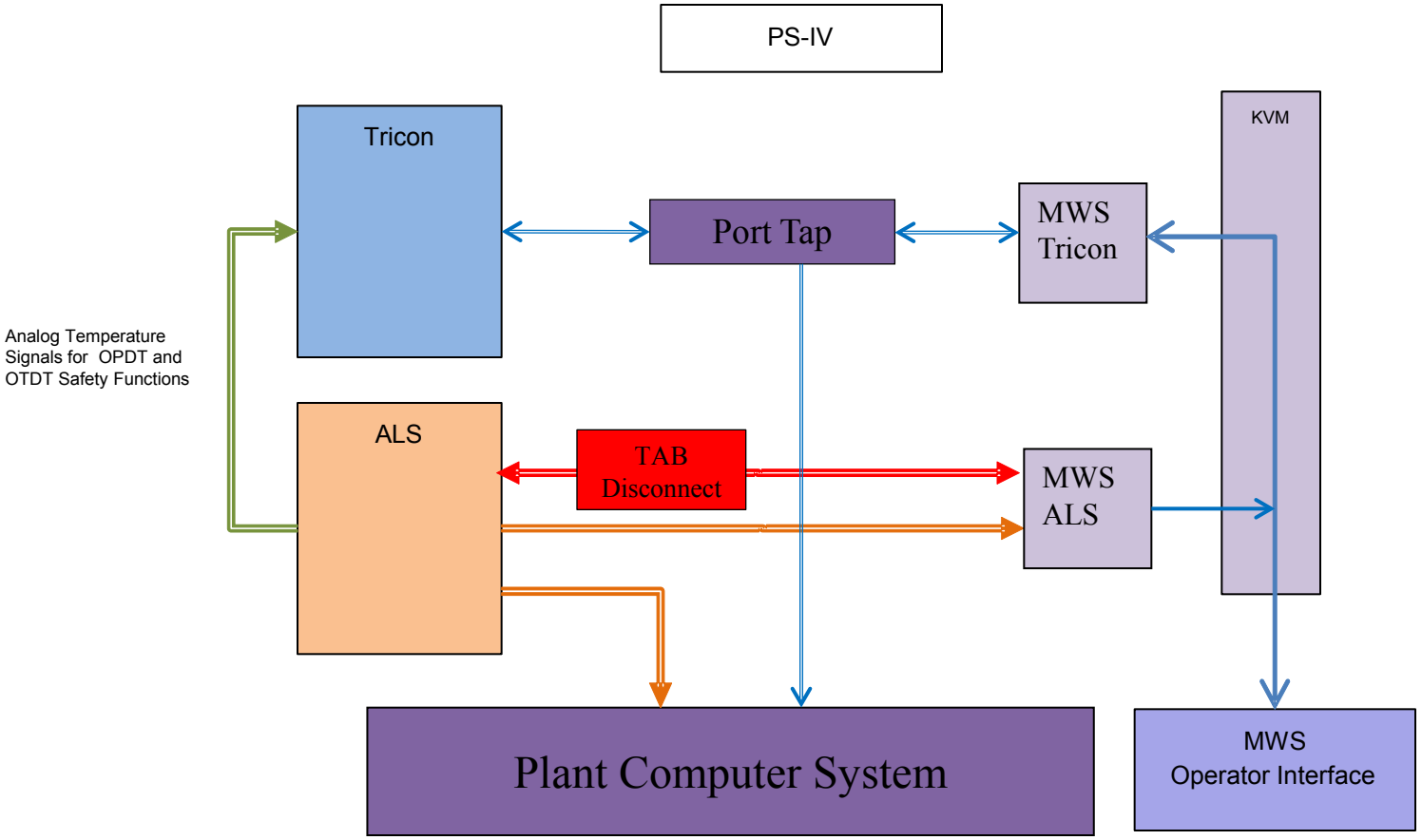
Overview of Diablo Canyon PPS Application
Safety to Non-Safety Communication Architecture



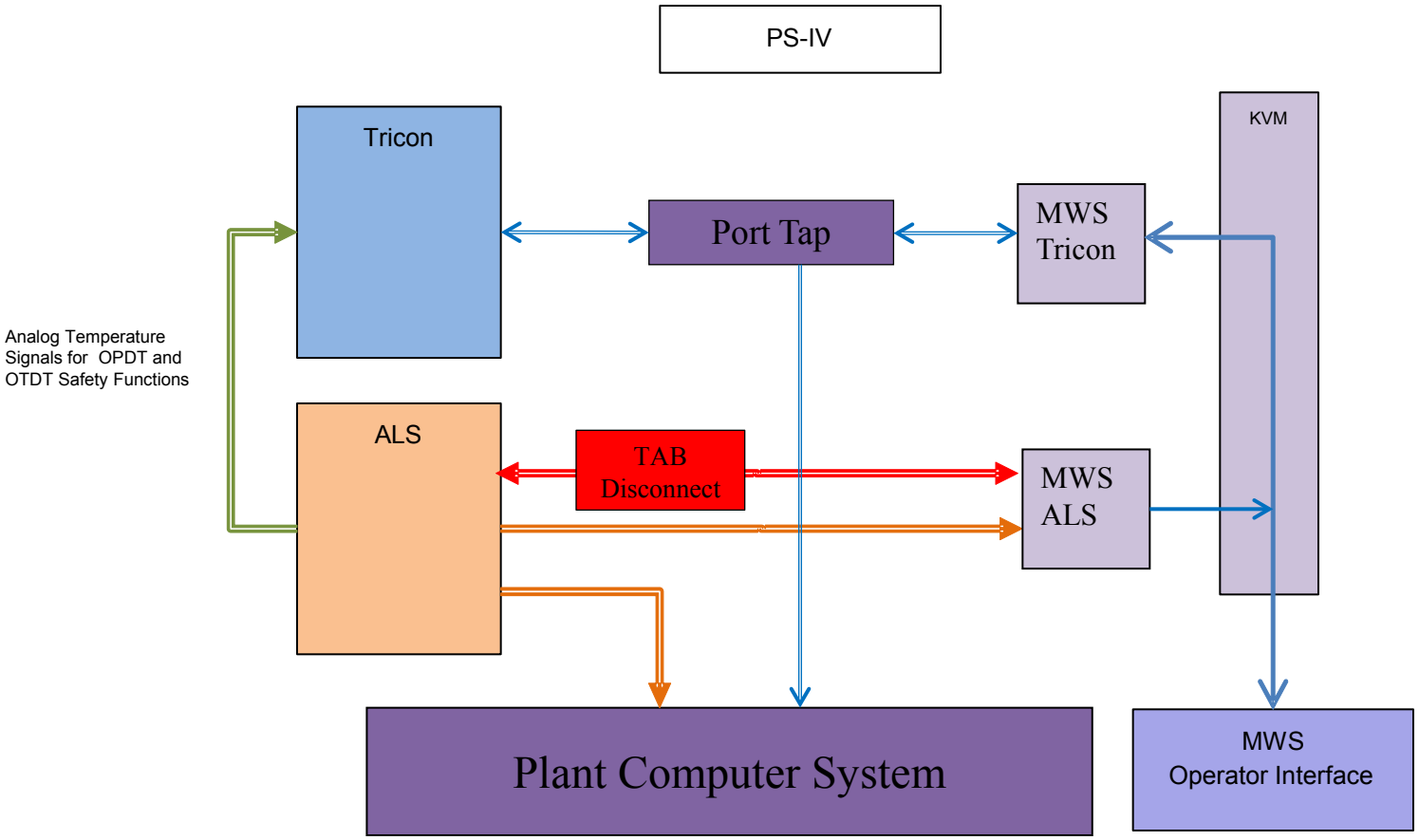
Overview of Diablo Canyon PPS Application
OPDT and OTDT Functions



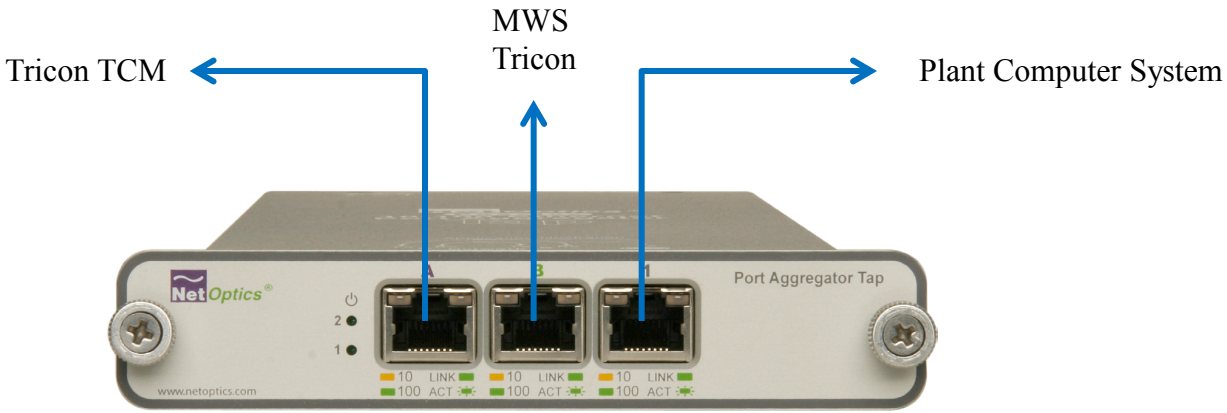
Overview of Diablo Canyon PPS Application
Safety to Non-Safety Communication Architecture

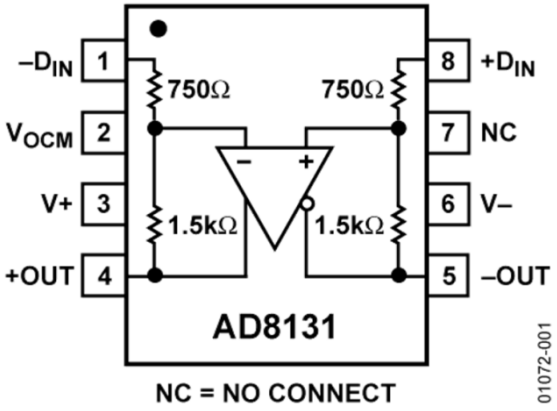


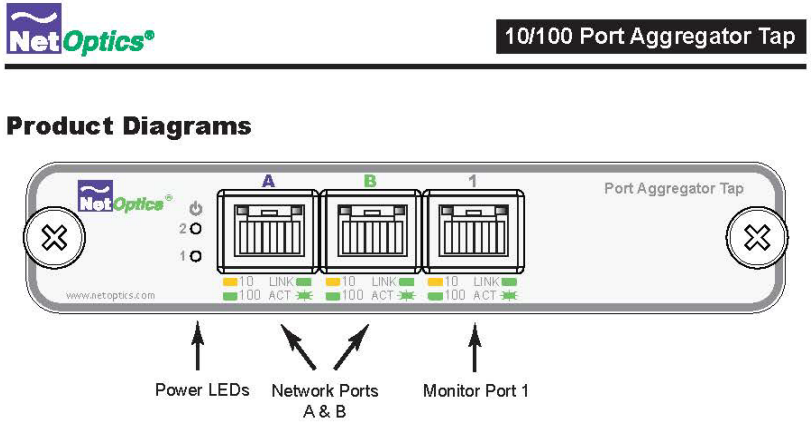
Overview of Diablo Canyon PPS Application
Safety to Non-Safety Communication Architecture



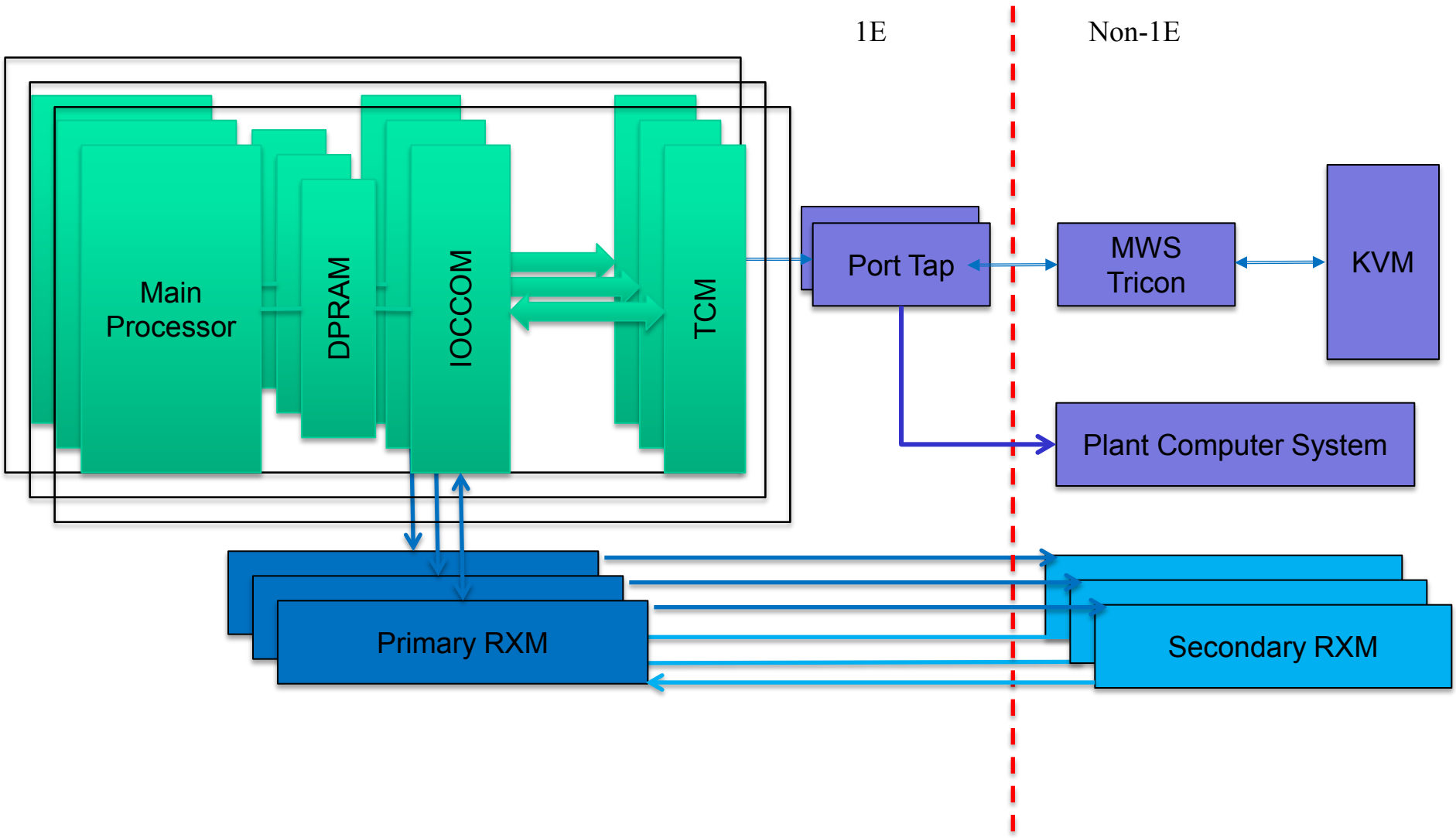
Port Aggregator Tap







Overview of Diablo Canyon PPS Application
Safety to Non-Safety Communication Architecture



Overview of Diablo Canyon PPS Application
Safety to Non-Safety Communication Architecture

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)

Communication
Path Forward

The NRC staff is currently reviewing and documenting the evaluation for DI&C-ISG-04 adherence points in regard to the Diablo Canyon PPS system Design.

Communication
Current NRC Assessment (In Progress)

- The Diablo Canyon LAR appears to adequately address each of the twenty adherence points listed in DI&C-ISG-04, with the exception of Staff Position 1, Point 10.

- Staff Position 1, Point 10, states that safety division software should be protected from alteration while the safety division is in operation.

  - Deviation in Diablo Canyon LAR
    - The Tricon Maintenance Workstation will be connected to the TRICON system during plant operations.
    - The ALS RTD signal processing functions will remain operable during specified surveillance tests performed on other ALS functions. Thus, the licensee is taking a limited exception to this criteria.

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 unneeded, unwanted and undocumented code 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

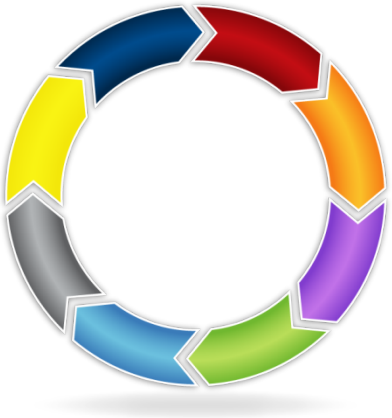
Secure Operational Environment (Control of Access)

- 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

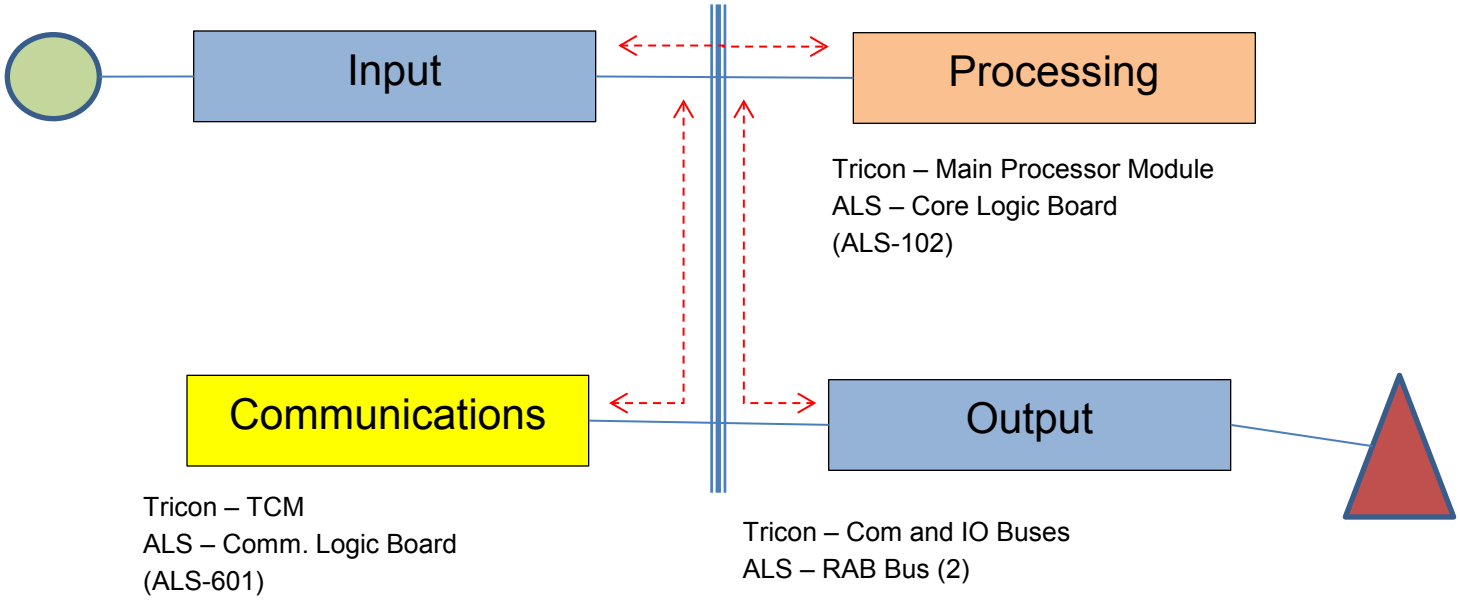
Deterministic Performance of PPS



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

PPS Deterministic Performance Characteristics



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

ALS Deterministic Performance Characteristics

Access Time: The board access time is the fixed interval allocated to exchange data with an individual board using the Reliable ALS Bus (RAB) protocol.

Frame Time: The frame time is the interval between accessing each specific board so information will have been read once from all application input boards and written once to all application output boards.

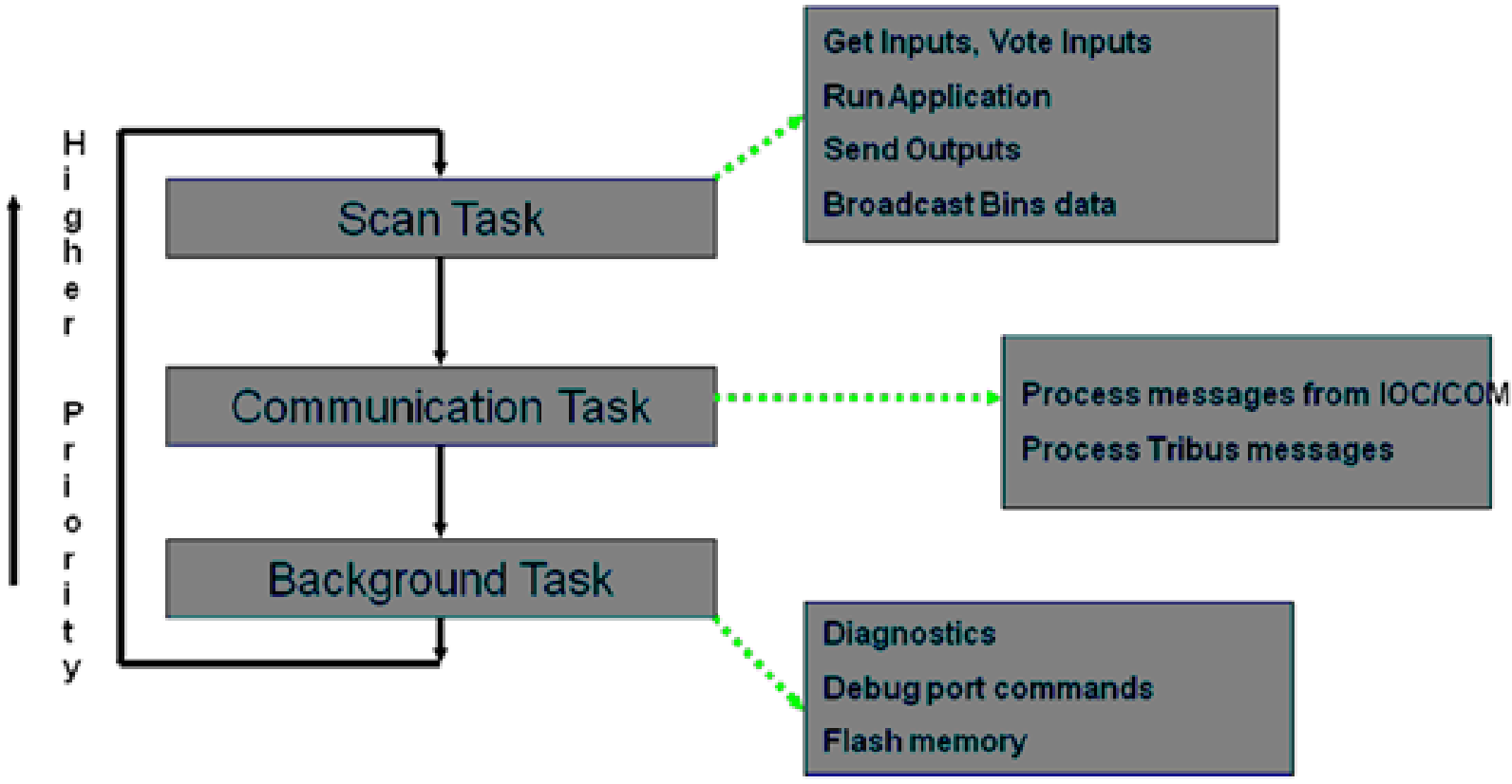
Tricon
Deterministic Performance Characteristics

- **Tricon scan cycle is predictable and repeatable from scan to scan**
- **Event Driven Interrupts are not used in the Tricon**

TASKS BY PRIORITY	INTERRUPTS BY PRIORITY
SCAN	WATCHDOG
COMMUNICATIONS	START SCAN TASK
BACKGROUND	START COMMUNICATION TASK

Tricon
Deterministic Performance Characteristics

ATTACHMENT 6
INVENSYS RESPONSE TO RAI No. 6



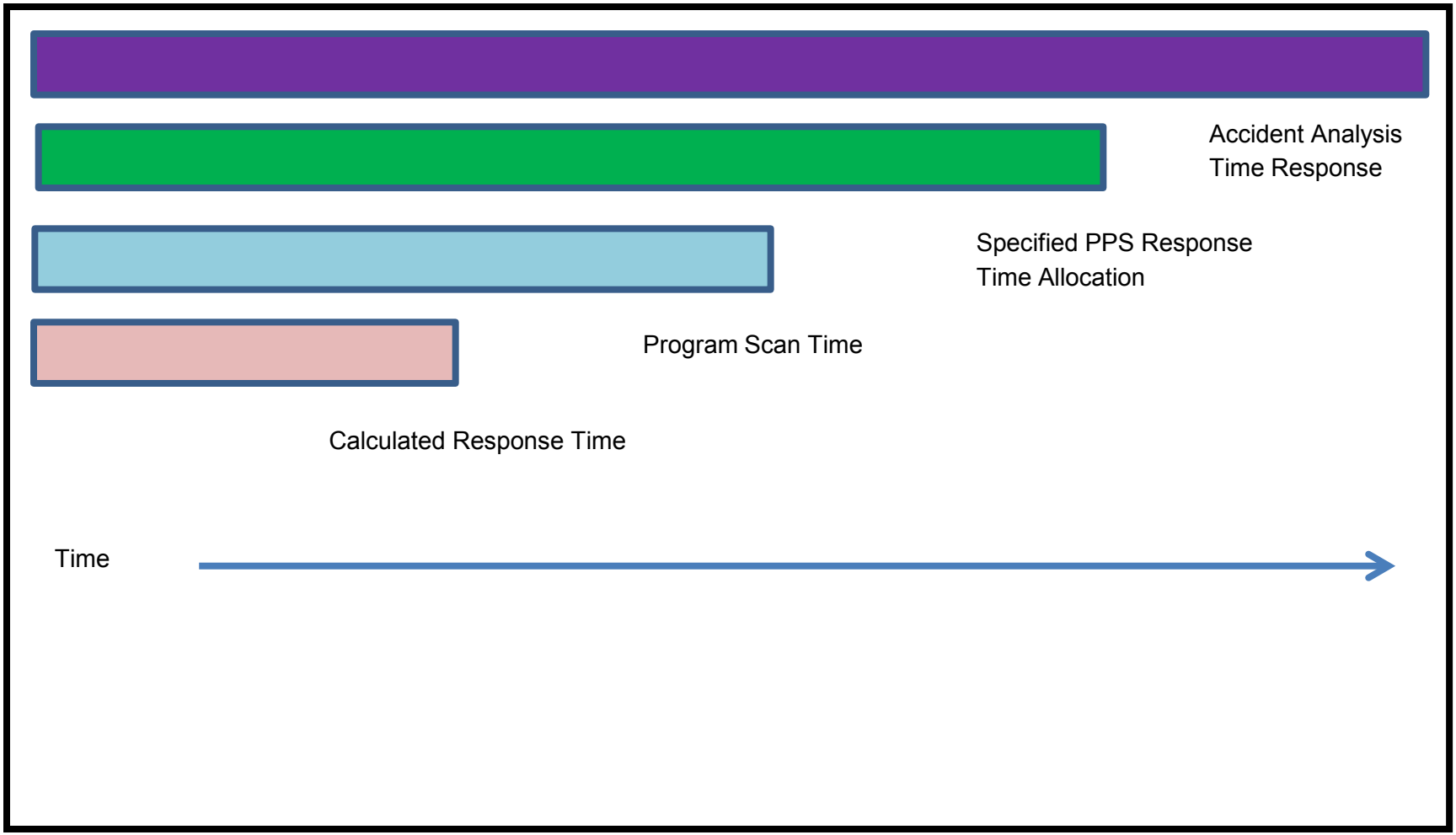
Tricon
Deterministic Performance Characteristics

- The Tricon application program (calculational cycle) cannot be interrupted by any of the lower priority tasks during the program execution cycle.

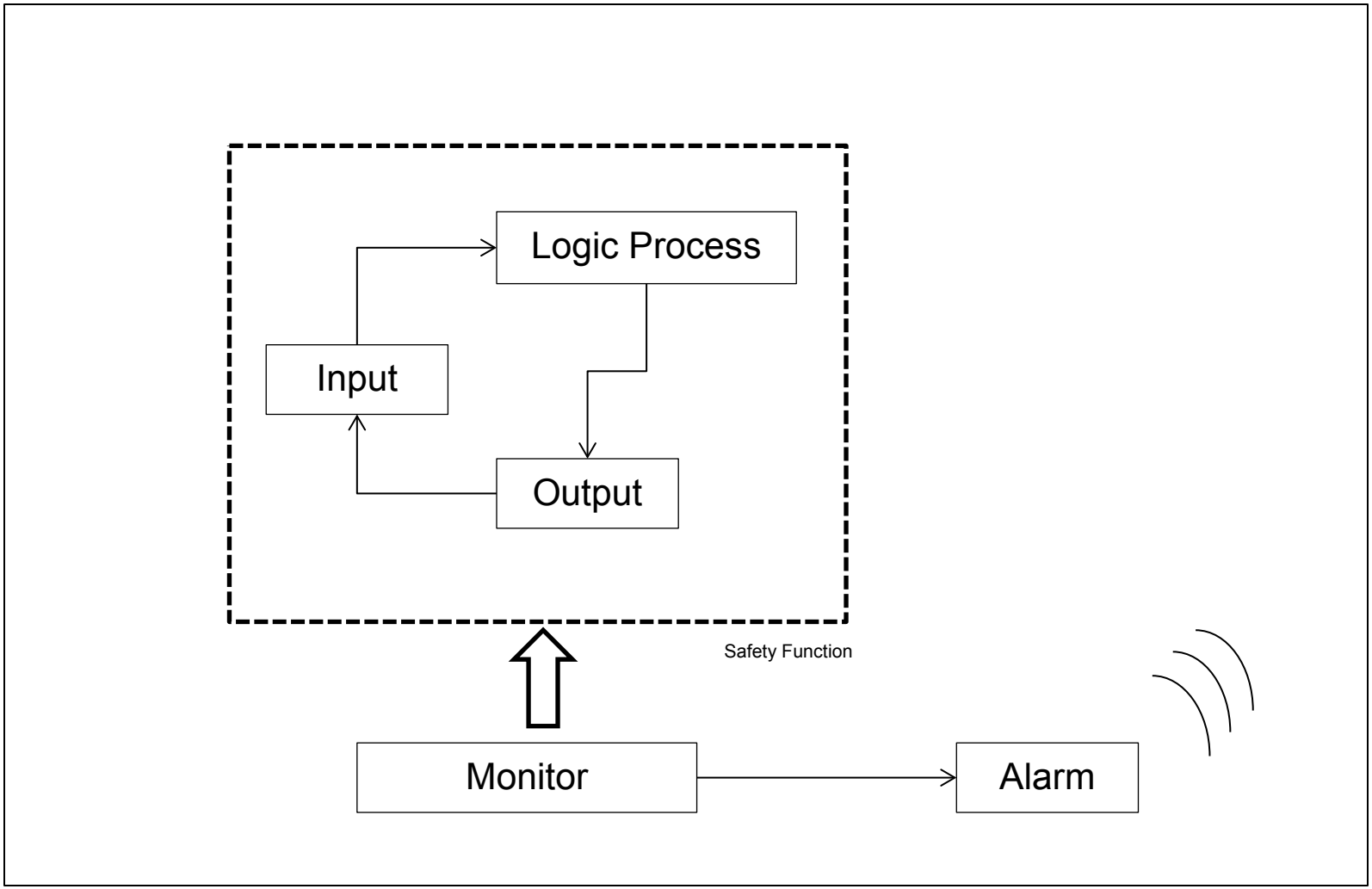
- Actual processing time is established during program development.

- Once application program development is complete, the cycle time does not vary as a function of calculational loading of the system.

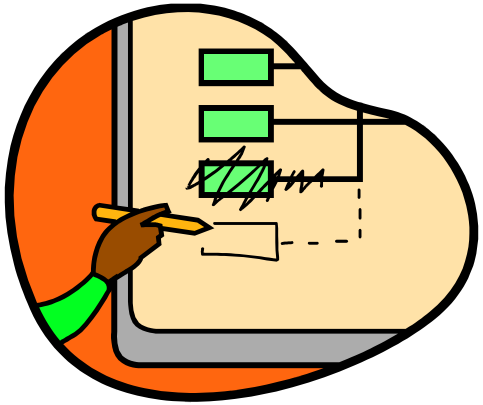
Tricon
Deterministic Performance Characteristics



Failure to Perform Deterministically



Platform Changes



Changes to ALS and Tricon Platform Criteria

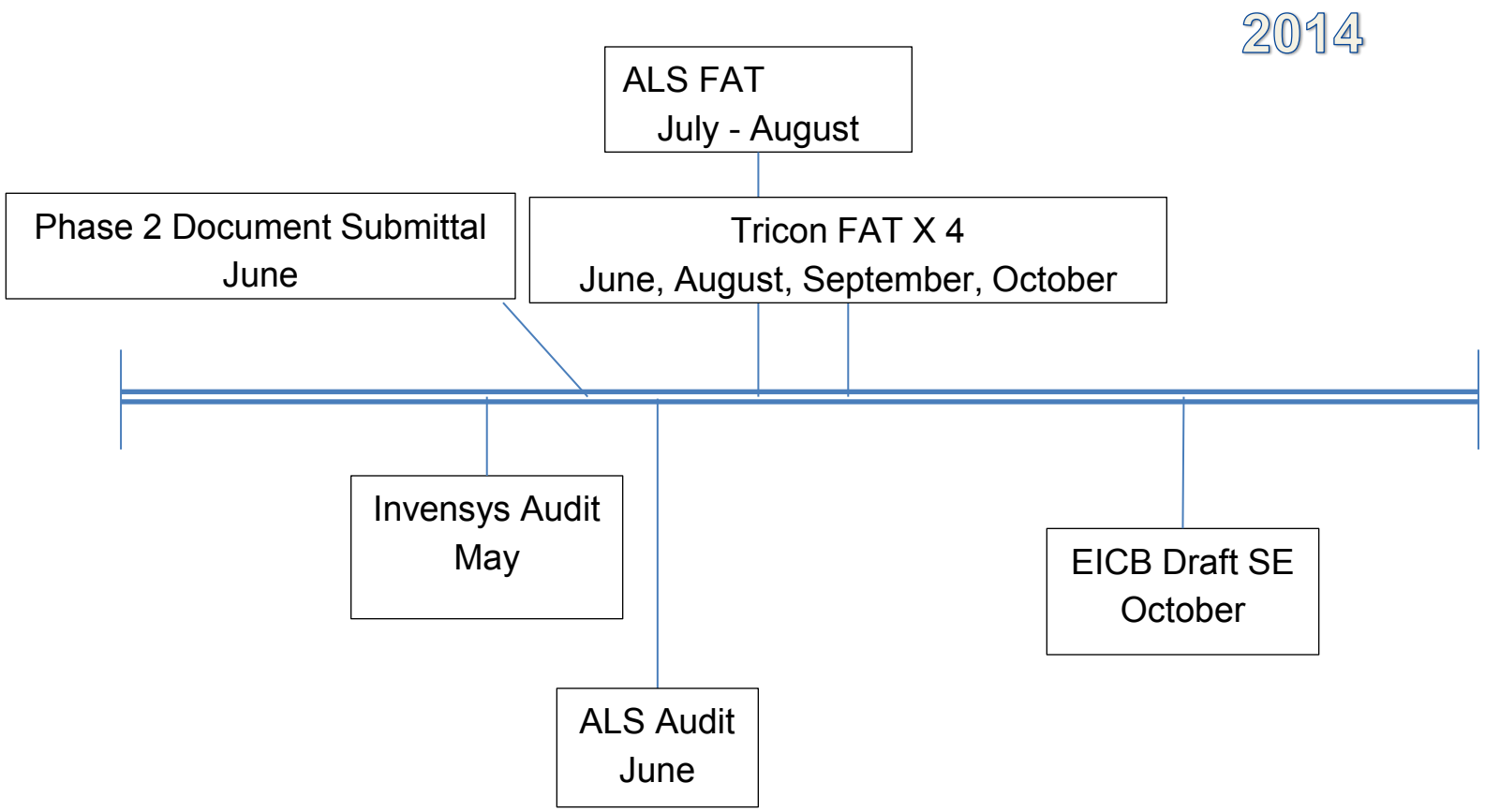
- The Tricon V10 Topical Report and Safety Evaluation were issued in April of 2012

- Since then, changes to the approved platform have been made due to advancements in digital technology and improvements in development processes. These changes include:
    - Hardware
    - Software
    - Procedure

- A Review of these changes to the approved platform is necessary to assure the changes are acceptable.

- The Staff is reviewing documentation associated with these changes and is drafting a Platform Changes chapter within the Safety Evaluation.

Project Schedule



Summary

Summary

- **Path forward for D3**
  - **The Licensee has provided all of the necessary documentation to support the Diablo Canyon D3 Position including a comprehensive D3 analysis approved by the NRC in 2009.**
  - **The Staff is reviewing this documentation and is drafting the Diversity (D3) portion of the Safety Evaluation.**

- **Path forward Communications**
  - **The NRC review staff is documenting the evaluation for each of these 20 ISG#4 positions in regard to the Diablo Canyon PPS system design.**

- **Path Forward for Determinism**
  - **The Staff is reviewing this documentation and is drafting a system determinism chapter within the Safety Evaluation.**