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: Friday, April 24, 2015

Work Order No.: NRC-1535 Pages 1-273

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

+ + + + +

FRIDAY

APRIL 24, 2015

+ + + + +

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 BROWN, Chairman

RONALD BALLINGER, Member

DENNIS BLEY, Member

JOY REMPE, Member

STEPHEN P. SCHULTZ, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

ROSSNYEV ALVARADO, NRR/DE/EICB

MARK BURZYNSKI, Rolls-Royce*

NORBERT CARTE, NRR/DE/EICB

SAMIR DARBALI, NRR/DE/EICB

VIC FREGONESE, AREVA*

BOB HIRMANPOUR, Southern Company

JOHN THORP, NRR/DE/EICB

CAMILLE ZOZULA, Westinghouse

*Present via telephone

AGENDA

P R O C E E D I N G S

8:32 a.m.

CHAIRMAN BROWN: The meeting will now come to order.

This is a meeting of the Digital I&C Subcommittee. I'm Charles Brown, Chairman of this Subcommittee meeting.

ACRS in attendance are John Stetkar, Dennis Bley, Joy Rempe, Steven Schultz, Ron Ballinger and Myron Hecht, our consultant.

And Christian Antonescu of the ACRS staff is the Designated Federal Official for this meeting.

The purpose of the briefing is to review the staff's activities and discuss progress made to date on digital equipment computing platforms submitted for NRC review via topical report.

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

The rules for participation for today's meeting have been announced as part of this Notice of this meeting previously published in the Federal Register on March 24, 2015.

We have not received written comments or requests for time to make oral statements from members of the public regarding today's meeting.

Also, we have participants on the bridge line, I think, listening to the discussions. That's Bic Fregonese from AREVA, Mark Burzynski from Rolls Royce, Camille Zozula is from Westinghouse who's actually sitting in the peanut gallery and others from the public.

I think I got everybody else that I've been told about.

So, to preclude interruption of the meeting, the phone line will be placed on listen in mode during the discussion, presentations and committee discussions.

The bridge line will be opened at the end of the meeting to see if anyone listening would like to make any comments. People on the phone line should identify themselves by name at that time.

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 participant should first identify

themselves and speak with sufficient clarity and volume so that they may be readily heard.

To preclude disturbances and distractions, please silence all electronic devices.

We will now proceed with the meeting and with that, I'll say good morning and it's a beautiful day in the neighborhood and I will call upon -- got to have some humor, okay -- and it is a beautiful day.

MEMBER STETKAR: Was it a gray sweater?

CHAIRMAN BROWN: This is a dark gray sweater.

MEMBER STETKAR: Yes, but I mean Mr. Rogers.

CHAIRMAN BROWN: Well, I deviated a little bit from the norm here.

So, I will call upon Mr. John Thorp of the I&C Branch, the I&C Branch Chief, Division of Engineering, Nuclear Reactor Regulation Office to make an opening statement and introductions.

John?

MR. THORP: Good morning, Charles and Member of the Committee.

I'd like to introduce myself, John Thorp, Chief of the Instrumentation and Controls Branch in NRR and DE, Division of Engineering.

With me are some of my staff, Norbert Carte, to my left, Rossnyev Alvarado and Samir Darbali. And to the side table, we have our senior level advisor, Steven Arndt and just behind him, another of my senior staff, Richard Stattel.

I think we're also accompanied in the audience by member of I&C engineering staff from the Office of Reactors.

Good morning. I appreciate the opportunity for us to spend some time with you this morning to describe for you some of the digital instrumentation and controls topical reports that we've reviewed or are in the process of reviewing.

We want to familiarize you with the basic design of the digital I&C platforms involved, what we looked at or what we're looking at and where they may be used, et cetera.

So, here's the agenda, you've already seen this, I'm sure. But we worked with this out with Christina prior to today's meeting. It covers a total of our topical reports.

I'd like to -- you can see by the agenda who the speaker will be for each of the given topical reports. Norbert had the distinct pleasure of being able to speak to two of them.

So, moving on to the next slide.

I'd just briefly like to discuss the nature of the topical reports we've reviewed or are reviewing including those that we're going to describe for you today.

These reports essentially describe and we review the hardware and software design of components or complete digital I&C platforms that are or would be commonly applicable to all licensee plants who might chose to use them.

Their topical reports vary in scope, content and specificity. So the scope of the review we perform is essentially based on what the platform vendor provides to us.

The hoped for benefit of our evaluations of these topical reports and the resulting documented safety evaluation report on a platform is the ability for licensees to have that portion of a licensing review essentially already completed, reducing the review time required and, thereby, improving the review schedule, reducing as well, you know, the level of effort by my staff and reducing the cost to the licensee.

So, essentially, we're seeking a win-win, licensee and the agency.

EICB Topical Reports Update to ACRS I&C Subcommittee

John Thorp (NRC/NRR/EICB)

April 24, 2015

AGENDA

Opening Remarks	Chairman C. Brown, ACRS
Introduction	John Thorp, NRR
Regulatory Context and Approach	Norbert Carte, NRR
Spinline 3 Topical Report - Background - Description - Key Review Criteria	Rossnyev Alvarado, NRR
CPLD - Based SSPS Cards Topical Report - Background - Description - Key Review Criteria	Norbert Carte, NRR
Break	
HFC – 6000 Topical Report - Background - Description - Key Review Criteria	Samir Darbali, NRR
NuPAC Topical Report - Background - Description - Key Review Criteria	Norbert Carte, NRR
Conclusion	John Thorp, NRR
Closing Remarks	Chairman C. Brown, ACRS

Topical Reports Being Presented

- Purpose: Regulatory Efficiency

- Rolls Royce Nuclear Spinline III
- Westinghouse CPLD – Based SSPS Cards
- Doosan HFC-6000
- Lockheed Martin NuPAC

EICB Staff Presentation of Topical Report Reviews Outline

- A basic explanation of each design, how it works, and where it might be used in the reasonably foreseeable future.
  - A summary of each design from a technical engineering perspective - drawings and oral explanations that describe how each design processes signals, inter-divisional communications, interfaces between safety and non-safety signals.
  - Staff understanding of plans to implement these systems - new plants, retrofits, non-US markets, etc.

Now the topical reports we're presenting today, and you see on this slide, they represent four of the approximately 15 digital I&C platform equipment topical reports or major revisions thereto that staff has completed since 1995.

The staff is going to explain to you our consistent approach based in regulatory requirements in our evaluation of the material presented to us in these topical reports.

I want to emphasize, this is a pretty rigorous review focused on critical evaluation and, as with our other safety evaluations, we have to achieve a reasonable assurance determination and a conclusion in order to successfully issue an SER.

You'll hear about a range of digital platform topical reports, some that provide very specific detailed functions and purpose, others that are a collection of components sometimes loosely referred to as a box of Legos or a box of parts.

For platforms where the applicable vendor is seeking to maintain a wider degree of flexibility, that is the design is more general in nature and not fixed or specifically laid out as a complete particular system our resulting safety evaluation is thus more limited in scope.

So, our review will produce a greater number of what we would call application specific action items in such a case. The effect of these large number of ASAIs, Application Specific Action Items, is essentially a translation to a later date of burden to the licensee who wishes to use a given platform in an application at their site since the licensee will have to provide responses and explanations for each of those action items.

CHAIRMAN BROWN: John, let me push just a little further on this so I understand.

These are things you can see at this point would be issues for specific applications when somebody comes in with an application they may be using it somewhat differently than you expected that doesn't fit any of those.

How does the review of this fit with the review that would occur at that point in time?

MR. THORP: Well, we take into account the SE that we'd already used on -- written on the given platform. So, they come in with a particular platform for which we've already evaluated, there's a comparison process that takes place. So, we look for any differences and any gaps as well as the ASAIs being responded to.

CHAIRMAN BROWN: Let me just springboard from that for a second.

MR. THORP: Sure.

CHAIRMAN BROWN: The ASAIs, did you provide a list, I've looked at the SEs and I don't remember, okay -- my age -- seeing a summary list of all the ASAIs.

I saw some referred to through, you know, in the SE that you'd all mentioned. Hey, we covered this but we didn't do that, therefore, you're going to have to do such and such if somebody comes in an application. But I didn't see a summary list in the SE.

Is that -- is my assumption correct?

MS. ALVARADO: No, there is a list after, I think it's either before conclusions or after conclusions, a change by topical report. But there is a list --

CHAIRMAN BROWN: Well, I really missed it then.

MS. ALVARADO: -- summarizing generic items and then application specific items.

CHAIRMAN BROWN: Okay. All right, I'll go back and look at that.

MR. THORP: Yes, typically I think we try to collect all of those right at the end of the SE to make it easier for the, you know, the applicant to see what it is we're concerned about at the time.

CHAIRMAN BROWN: I saw a bunch of references but I just don't remember the ASAIs being explicit.

MR. THORP: Okay. So, well, with the concept of these ASAIs in mind, you're going to hear from my staff lead for each of these four topical reports that are noted on the agenda.

Part of this discussion is going to include the applicable, quote, unquote, key review criteria used during the review, which I believe is responsive to your original request for a familiarization presentation on the platforms.

Norbert Carte is going to describe the review scope and criteria in more detail in his discussions.

Finally --

CHAIRMAN BROWN: John, I just -- please, excuse me for a minute.

I guess one of the things, at least in my mind when we started wanting to have this meeting was that we are not going - this is me talking right now -- I did not look at it from the standpoint that we were going to, quote, give approval, disapproval, agree, disagree, whatever.

MR. THORP: Right.

CHAIRMAN BROWN: We're just reviewing --

MR. THORP: Right, this is an informational presentation.

CHAIRMAN BROWN: -- what you're all doing and then if an application comes in then we would be doing a more thorough review.

I mean we just didn't have the resources to go into it at that depth, even though we had -- it's good to have the topical reports, but --

So, it's my understand that our final Betty Crocker Good Housekeeping seal of approval on the overall thing would be based on its application in a specific design.

So, I just wanted to lay that on the table from my standpoint. If any of my member disagree with me on that? Okay.

MR. THORP: I think I agree with you. Thank you. Thank you, I think that's correct.

CHAIRMAN BROWN: Okay, thank you.

MEMBER REMPE: While you're interrupted, I'd like to ask a question.

I was at the NPIC HMIT meeting and I heard some discussion about this process. Could you remind us about how long it takes to go through a review of these topicals and is the process getting more efficient, do you think? And is the time getting shorter or is that just so dependent on what they submit you can't really comment?

MR. THORP: It really varies and depends on what is submitted. It also significantly depends on the quality of the submittal and we have continued to emphasize to potential applicants that the need to have a good, thorough, quality input to us so that we can commence our review and do that in a timely fashion, that reduces the number of requests for additional information, et cetera.

Now, one way that we have done that is to encourage and I think potential vendor applicants for these topical reports have listened and heard us and, therefore, come to see us for what we call pre-application discussions at a phase zero meetings to discuss, you know, the scope and content that's needed in an application.

Some of them start out being somewhat unfamiliar with how to go about doing that, some of the folks that aren't the large vendors.

The nominal time frame, to get back to your original question is two years to complete the review. They can't be done faster, it's I think on average about a two year time frame but it sometimes takes some vigorous extra effort on our part to iterate with the applicant and obtain the information that we need

MEMBER REMPE: Okay. Thank you.

MR. THORP: And we are, with those comments that you heard at the RIC and at the NPIC HMIT, you know, we're consistently seeking to find ways to make the process more efficient.

So, just a little note for you guys, the information that my staff is going to present to you is at a nonproprietary level in this meeting. This is a public meeting. So, if you find a need to discussion information or have questions that broach or push into proprietary areas, then we would need to make that information the subject of a separate closed meeting.

CHAIRMAN BROWN: Well, just tell us if we look like we're touching on something.

MR. THORPE: We'll do our very best to draw the line because we have to preserve the interest of those who have sought that kind of proprietary protection.

MR. HECHT: Can I ask a question in advance with respect to that? Are questions on the order the size of the designs, particularly for the FPGA designs or those, you know, from terms of the number of gates, are those considered proprietary questions?

MS. ALVARADO: Yes.

MR. HECHT: Okay.

MR. THORP: Okay, next slide?

Okay, so I'll just -- one more slide for me and then we'll kick into with the real material from my folks.

So, we understand the committee's interested in becoming more familiar with the digital I&C platforms we've reviewed and that you're interested in various aspects of the platforms' design and how they work.

We're prepared to speak to you about the items described on this slide and believe that this will give you a good understanding of what we've looked at or are evaluating in the case of active reviews.

Relative to the last bullet, we aren't always given nor are we always privy to the vendor and licensee plans for the use of these various platforms but will relay what we've been made aware of as we've worked on them, recognizing that that's not necessarily information that's in stone or for sure.

We conduct an acceptance review in topical reports. Kind of so, Joy, a question that don't provide a sufficient level of clarity and detail to allow us to even commence a review have resulted in our not accepting the topical report or the applicant withdrawing the topical report until they strengthen the content of the document.

Now, what do we review and evaluate? Well, we seek to gain a technical understanding of the platform and the hardware and software associated with it. I'd like to emphasize that in our reviews, the questions and areas concerned flow directly from the regulatory requirements laid out in the Code of Federal Regulation and it's incorporated standards, the general design criteria, standard review plan and its incorporated branch technical positions and direction from the Commission in staff requirements memoranda.

We also take into account, of course, the guidance found in applicable regulatory guides which provides methods and approaches that the staff has already examined and considered acceptable approaches.

We evaluate alternatives to guidance, applying appropriate engineering judgment as we do so.

I hope our presentations will give you and help you gain an appreciation for the scope and content of our reviews on these platforms and I look forward to the discussion with you.

Norbert Carte will now speak in a bit more detail on the regulatory framework and what we've prepared to present to you on our digital I&C platform topical report reviews.

So, Norbert, go ahead and swap out there.

MR. CARTE: Okay. My name is Norbert Carte, I'm a Technical Reviewer in the I&C Branch, which I forgot to put after my name.

And today, I'll be talking a little bit about how we use topical reports. And so, it's framing the discussions to follow in terms of efficiency and regulatory criteria that can be addressed.

And in part, this is because topical reports have different scopes and those different scopes result in us addressing the regulatory criteria to a different degree, depending on the scope of the topical report.

And I'll also discuss the technical requirements and the key review criteria.

So, obviously, all the regulatory requirements must be met, though it's probably not efficient to talk about each and every regulatory requirement, some appear to be more significant for assuring safety and we want to talk about those in particular.

And then we'll talk about how those are assessed with each topical report.

So, again, as John emphasized, the point of a topical report is to increase regulatory efficiency to allow the review of an aspect, a detail, once and the crediting of that in multiple situations.

It reduces the burden on the staff. It also reduces the burden on the applicants from preparing that material.

There is always incumbent the responsibility to evaluate the applicability of a topical report for its intended applicant in a power plant. So that is done in the licensing phase.

So, basically, the industry proposes an approach to deal with a specific subject that is expected to be used more than once. So we don't like to do topical reports for one off applications. And it must be complete and detailed information.

Recently, we presented to the ACRS, well maybe not recently, ISG-06. And then ISG-06 discusses or encourages the use of topical reports in order to reach closure on certain aspects of license amendment applications for intended use in license amendment applications.

So, in general, when we look at topical reports or at any process in the NRC, there's two aspects. There's the regulatory process and LIC-500 is an internal office instruction that guides the process of performing reviews. It does not contain technical criteria.

The standard review plan contains the technical criteria. And so the attempt is to -- the focus mainly from the technical reviewers is on the SRP, the project managers use the office instruction more than we do. Their job is to keep us in line in terms of process.

So, when we look at the topical reports scope, each one can have a different scope but we can think of them as three major groups of scope.

And one would be a digital replacement card. So, this is a case where we have an old analog system installed in a plant. The components on those analog cards are no longer available so they are left to redesign the cards.

And in some cases, they have chosen to redesign those cards using digital components. Those tend to be fit, form and function identical replacements or that's the intent and slide in the existing racks.

Yes?

CHAIRMAN BROWN: Does that -- when you talk about the digital replacements, does that imply since they're fit, form and function, if the old analog cards were analog in and analog out, obviously, you're going to get analog in, does that also mean analog out?

MR. CARTE: Yes.

CHAIRMAN BROWN: Even though you process within the card digitally?

MR. CARTE: Yes.

CHAIRMAN BROWN: Okay.

MR. CARTE: Well, to qualify analogs, there are -- analog are discrete inputs.

CHAIRMAN BROWN: Whatever.

MR. CARTE: Okay.

CHAIRMAN BROWN: But whether it's a variable signal or whether it's a discrete contact I'd think, that's the input but the output could be either one also. You don't deviate from its basic output function, in other words?

MR. CARTE: Correct.

CHAIRMAN BROWN: Okay. Thank you.

MR. CARTE: One detail which we'll get into a little later is typically with a digital card, there needs to be the ability to program the card and configure the card. So, these cards will have, in general, connectors on them that are used when the card is removed from the cabinet in order to configure or program the device. Sometimes the plant will have that capability, often it does not.

But they do have digital connectors that are not used while they're in operation or while they're installed in the rack because the old system didn't have the capability to connect to that.

Okay. So, one scope of cards, and I'll give some examples about historical ones and we'll also talk about today one of those digital replacement cards, the CPLD, a Complex Programmable Logic Device, based solid state protection system cards.

There's also a category of scope which we call system specific. So, an applicant has proposed a specific digital platform and a specific design for a specific function in a power plant. And one example of that was the NUMAC Power Range Nuclear Monitoring System Nuclear Monitor.

It's not described today, but it's an example of the system specific design. We don't have any system specific designs that we're talking about today. We're going to talk about one card and three application frameworks.

So, an application framework is a general concept in software engineering for what has been termed a box of Legos. It is a set of components and a concept for using those components to construct an application.

So, sometimes that includes a software program manual. So, the plans for developing application specific applications and sometimes it does not, depending on the scope that the applicant requested.

So, today we will be talking about three application frameworks, the HFC-6000 which has been approved and it is going through an amendment process, the SPINLINE 3 which has been recently approved as well as the NuPAC process which is the in process of being reviewed.

So, in terms of just historical perspective, so in the formal -- well, let me back up just a little bit what's not here -- as the current form of the SRP took shape in 1997 and it didn't change much in 2007.

So, what you see or what you're familiar with the SRP was established at that time.

So, before that, AREVA had proposed a digital replacement module for some Bailey modules in their protection systems. That was a topical report reviewed and approved by the staff.

It had two microprocessors in it that were auctioneered or compared. And that was actually the installed in the Delta Flux Trip function at the Oconee Nuclear Power Plant. Now that and the other analog modules got removed with the TXS upgrade that was finished in 2009 or in '11 -- '11, okay.

Also in the past in terms of digital replacement cards, there is the ASIC based, the Application Specific Integrated Circuit based replacement module for the Westinghouse 7300 cabinets.

So, the 7300 cabinets perform the bi-stable functions for reactor trip and ESF functions and those were analog cards. Components were not available and Westinghouse designed a module to replace those cards. And that was approved in 2001 and that will become interesting when we talk later in some aspects.

In terms of system specific designs, I've already mentioned the NuPAC Power Range Nuclear Monitor. It does both the power range nuclear monitoring as well as the oscillation power range monitoring which was added subsequently to the initial functions. And there are various installations of that equipment.

So, in terms of application frameworks, we can divide the application frameworks into two categories because of their fundamentally different technologies involved in each.

One is the programmable logic device category and that would include the NuPAC application that we'll talk about today as well as the ALS platform that was previously approved by the staff.

So, the ALS was first used in the Wolf Creek main steam and feedwater isolation system. This was before There was a topical report, so then the topical report was submitted and approved.

And then the Diablo Canyon application will use that topical report as a basis of the License Amendment Request that is currently being reviewed by the staff.

So, in terms of microprocessor based applications, and these tend to look like programmable logic controllers. There's the MELTAC which is currently under review by NRR staff. It's going through its acceptance review. It has not been accepted.

It is proposed for use in the US-APWR which I believe has been presented to the ACRS.

There's also the Triconex platform which was initially approved in 2001 and then was -- an updated version was reviewed and approved in 2012. It will be used in Diablo Canyon License Amendment Request which is currently under review.

Common Q is a little harder to explain. It was first approved in 2000. There were generic open items, plant specific open items. They then, in the series of submittals, they closed the generic open items except for one. And they also amended the application. And it also includes a software program manual. So, the last approval on that was in February of 2013.

So, the Common Q is used in the AP-1000 in Palo Verde for their core protection calculators which was both reviewed by the NRC.

There are some 50.59 uses of the Common Q platform. So, there are some digital installations in plants that we do not see. And one of those examples would be a post-accident monitoring system, a rod sequencer, rod position indications, those are examples that we have not looked at in license amendments.

In terms of another platform, there was the AREVA TXS platform. That was originally approved in

2000. It was the base platform for the RPS/ESPS upgrade at Oconee.

We reviewed changes to the original platform as part of that licensing review for the Oconee application.

There is also a, well, I call it an application framework, but it's a little fuzzy. The Eagle 21 system, it was designed to be a replacement for the plant protection systems. It is a digital version of the Westinghouse plant protection system.

So, in the sense it's a system specific design but it's also a little bit of an application framework.

So, you didn't have to replace the whole system. Those cards were designed to fit in the 7100 racks of the Westinghouse plant protection systems and there is at least one instance where only two trips were replaced. The other trips still rely on the Hagan module so it was almost a card replacement in that instance. But I think that required some modification outside the card chassis to do that.

MEMBER STETKAR: Norbert, you were on a roll, so I want to get to the TXS. You listed -- you said Oconee, RPS/ESPS upgrade, I'm familiar with that and 50.59. Is that for Oconee or is that for others?

MR. CARTE: Yes, I think they have a hydro application at Oconee that was installed under 50.59.

MEMBER STETKAR: Okay, okay. I think for the QOE facility.

MR. CARTE: Yes.

MEMBER STETKAR: I didn't know whether that was, you know, comma and 50.59 for other plants because I wasn't aware of it at others.

MR. CARTE: Right. I'm not aware of any other installations but we're not necessarily aware of all installations that occur under 50.59, we as the design engineering staff. The region does have some oversight and they do look at these things, but that doesn't necessarily get tallied up into a master list of who's got what where.

MEMBER STETKAR: Okay.

MEMBER SCHULTZ: Norbert, it sounded as if, as you went through these, that in some applications the topical report has been revised as a result of the application, has that happened?

MR. CARTE: No. The problem with digital I&C topical reports is obsolescence of components. So it's not that they're, in general, they always get revised and it's not because there's things that are broken and they need to be fixed.

But what happens is there is some, generally, some component becomes unavailable or some improvement gets made.

MEMBER SCHULTZ: I understand that part of it. I'm trying to understand the way in which the topical reports are applied. Because as it was originally -- as it was described earlier, these are fixed documents that are intended to be applied many times. And if you're revising them each time you have an application then it defeats some of the purpose.

MR. CARTE: Right. It's a little problematic. We approve a version of a module but that module can never stay fixed. The version number of that module is very difficult to remain fixed.

Some component gets changed, some process gets changed. That change gets evaluated but that new module can't have the same version number. It has to be updated to reflect that it's not the same thing that you shipped earlier.

So, component obsolescence results in your version numbers of modules never remaining fixed.

CHAIRMAN BROWN: With that in mind, relative to your comment, if a plant -- if an application is designed using one of the versions that they have approved using the topical report, and then the modules get revised later, three, four, five years down the stream because of component obsolescence, that module cannot be directly used in the old thing unless you all look at that again. Isn't that correct?

MR. THORP: They would have to conduct first a screening. But if you're talking about this is --

CHAIRMAN BROWN: I'm saying if you get --

MR. THORP: -- if you had a licensee that's been installed?

CHAIRMAN BROWN: Yes, a licensee has a version that is approved.

MR. THORP: Right.

CHAIRMAN BROWN: So, part of the licensing basis --

MR. THORP: So, now they talk with the vendor. The vendor says, hey, we've got this new way of replacing this particular piece that, you know, we're having some difficulty getting these parts and we want to put this new gadget, call it widget, on the board. It's going to do exactly the same thing for you, blah, blah, blah.

Well, that has to be explained to the licensee and the licensee has to evaluate that, screen it through 50.59 and if the 50.59 questions and criteria are not met, then they would have to generate a license amendment request, come back to us for our review.

CHAIRMAN BROWN: Okay. All right. Does that -- I just wanted to --

MR. THORP: Similarly, on a grander scale, the concept and the concern that we have for, you know, these technology vendors are always interested in trying to make things smaller, better, faster, cheaper, you know.

So, if they see a need in a given platform that they have that they're marketing a need to try to improve it and update it, what we've been pressing with NEI and with industry, with the vendors, is to identify a means that's systematic and clearly understood for them to examine any deltas, any changes that they've made to determine whether that has a potential of invalidating our SE on the platform and to set up a routine process by which we all understand this is what you need to go about in doing rather than waiting until the last minute for the licensee to try to catch it or whatever.

I want the vendors thinking about this and in sending us an update that they request our subsequent review.

And we also have to try to be efficient with this as well. I'm not interested in evaluating a bunch of sequential little iterations on a platform that nobody's taking on and put into their plant. I'll wait until somebody wants to put the application in their plant then we'll look at the whole thing again.

MEMBER SCHULTZ: That's why I asked the question. It's a real challenge to maintain the control over the process.

MR. THORP: It is, that's correct. And so we're --

MEMBER SCHULTZ: It's important that you do so.

MR. THORP: Yes. And in our interactions with NEI, they have agreed to and have identified a working group, but it's not their highest priority but they've got some folks in industry who are examining that.

At the same time, some of the major vendors, based on this same conversation that we've had with them in the past, have developed their own in-house means to ensure that they track and configuration manage the potential changes that they have or the changes that they want to develop in any platform they have so that they know when to come to us or to seek another review.

MEMBER SCHULTZ: That sounds more than a nice thing to do. That sounds like a necessary thing to do.

CHAIRMAN BROWN: It's a requirement. It's my understanding it's a requirement. You've got to maintain configuration control and management of each.

MR. THORP: So, they've developed actual procedures for doing this. What I want to do is have them get together and let's ensure that what they've got at least a minimum standard of how they go about doing this so that we can comprehend it and effectively process that.

MR. CARTE: Right. But I might put that a little -- frame that a little bit. I guess I understood the question a little differently.

But there are two scopes, there is one, a License Amendment Request and another is replacement module efforts installed.

During the license amendment process, we do look at changes. That is our practice. After it's installed, they go through the 50.59 process. And as he said, we're discussing what those criteria need to be for when we need to be notified about changes.

CHAIRMAN BROWN: Yes, I guess one of my

follow ons to Steve's comment, again, is, and your details of clarification of it, some of these licensees may or may not have the same level of engineering or technical capability.

Some carry some on down the stream with them but they rely more, or at least that's what I get out of some of these meetings, they rely more on the vendors to tell them, is this okay or is it not okay.

And it seems to me that's a kind of a hard spot that you all have to deal with.

MR. THORP: Well, the ultimate responsibility for the safety of the systems or components that are put into place, original installation and modifications subsequent, lies with the licensee.

And so, they do have to make sure that that conversation with vendors is a good one. And the vendors I think understand this. But some of the issues that we've had to deal with have involved exactly that in which the vendor had an impression that changes they had made simply constituted a hardware change out and then resulted in a recommendation to licensees who were going to buy this component to simply do a 50.59 screening and it was good to go.

So, that's a very short and simplified way of describing what we've seen in the past.

Now, I think, well, I'll leave it at that. But that is a concern.

MR. CARTE: Right. The vision on that is that the vendors are the experts on the hardware platform, the technology. They're responsible for evaluating and characterizing the changes that exist.

The applicant is responsible or the licensee is responsible for evaluating the effect of that and impact on their licensing documents and on safety.

CHAIRMAN BROWN: Okay. Before you leave this slide, you've talked about four different types of devices in There and there are some folks that don't necessarily know what all of those are.

You talked about FPGA, CPLDs in one framework and then you talk about microprocessors and then programmable logic controllers. They're kind of used as a mix and match.

And I read this a couple of places in your all's documents and I wanted to make sure I understood you all's distinction between an FPGA and a CPLD which are largely, in my understanding, I may be wrong so fix me, are programmed by a software to perform a series of stepped operations.

And that once you program them, that's the way they are. It's not a -- they're not software based in terms of their basic --

I know you want to leap in, just wait please.

But they're not software based in the manner that microprocessors are or, in some circumstances, maybe even programmable.

I'm trying to get a feel for myself. I know microprocessors are very, very clearly, every software, this software, that it's all buried in there, PLCs. What are the differences between the PLCs and the PLDs?

MR. CARTE: Okay. These are fuzzy sets and so it gets complicated as technology evolves.

CHAIRMAN BROWN: That's why I asked.

MR. CARTE: But, the programmable logic devices is a term that I'm trying to use as a generic term at some point it was a technology specific term.

The idea is that is a device that consists of gates that you program, that you configure or connect.

The difference between an FPGA and a CPLD is sort of a measure of complexity. The FPGAs are an order an magnitude or significantly more complex in complex programmable devices.

The concept about not having software is not a hundred percent accurate for FPGA. So an FPGA has a large number of gates on them. You can actually emulate microprocessors on the FPGA and run your regular software on those microprocessors.

CHAIRMAN BROWN: On the FPGA?

MR. CARTE: On an FPGA. That process is obviously discouraged, but it is the technology allows that. In fact, I just recently read an article where a guy on his own time used an FPGA to build a handheld Cray-1 computer.

So, the concept of an FPGA being hardware is definitely not valid. But you can implement microprocessors on an FPGA. So, it's a fuzzy class and we can get more into that different later.

But one of the main distinctions between a microprocessor and the programmable logic devices is the degree of parallelism in the device. So a microprocessor tends to have a small amount of shared resources and all process share those resources.

And on those devices, one technique that I've heard of in the past, to assure that those processes are working is a watchdog timer.

Another concept occurs in an FPGA and

complex programmable logic devices which are highly parallel devices. So, if you were to strobe a watchdog timer based on a CPLD or FPGA, you're only really confirming that a very small fraction of the circuit on that card is working.

So, watchdog timers don't have the same effectiveness on programmable logic devices because of their inherent parallel nature and you look to other sorts of checks to assure that things are fully functional, aliveness checks and self-testing and things like that.

So, there are certain technological differences, but these are basically fuzzy categories.

Now, when we talked about programmable logic controllers, that's an industry -- that's a term that came out of the automation industry.

So, computers have not always been reliable and in some senses for industrial applications, they took out the unreliable pieces. So they took away the displays, the display controllers, they took away the keyboards. They, in general, take away network connectivity and create system which was very simple, a dumbed down computer that was less prone to fail. Without a hard drive, it's not sensitive to -- as sensitive to vibration.

And so a programmable logic device is really an industrial hardened computer that has a certain architecture, no screen, no hardware, no hard drive, no keyboard, implements mainly logic.

CHAIRMAN BROWN: But it has ROM and RAM in it?

MR. CARTE: Yes.

CHAIRMAN BROWN: Okay. So, it is a software -- I understand your point.

MR. CARTE: Yes.

CHAIRMAN BROWN: Let me back up to your FPGA just to make sure I understand the FPGA, CPLD routine.

I guess in the designs we've looked at on the FPGA side, they have not been or at least they have been advertised to not have been in this fuzzy area where they implement or emulate a Cray computer.

MR. CARTE: Right.

CHAIRMAN BROWN: They have been straight through hardware type, as you say, you discourage this other methodology?

MR. CARTE: Right. I think for a while people tried to bill FPGAs as hardware devices and in that attempt, they have never tried to emulate a microprocessor an FPGA because that would undermine their position.

So, no one has ever proposed that that I'm aware of to the NRC and we would not encourage that. However, FPGAs are very complex and, therefore, they have some of the same issues that software does in terms of the inability to completely test them as well as the reliance on software development tools.

So, we consider the software -- and in general, you load a data file on to an FPGA. There are FPGAs where you burn in connections or break fuses. But the larger the FPGA is, the less likely you are to have those type of implementations. They tend to all require loading of data file these days.

And some have some sort of processing function in there to translate and map that data file into local memory locations.

So, they are essentially software devices and require the same level of controls as microprocessor based devices, same level of process development controls as microprocessor devices.

CHAIRMAN BROWN: So, any subsequent looks we may have at an application of FPGAs really requires the committee to have a better understanding of how they are implemented because of our concerns relative to processes that may or may not stop the operation in the multiple divisions since they now have, as you're characterizing it, they are fundamentally software based, software control type devices as opposed to burned gates which was literally what I was familiar with.

MR. THORP: There are software instructions that are burned in on the chip.

CHAIRMAN BROWN: Yes, but that's -- when I hear burn in on a chip, that means breaking fuses, doing whatever it is so that you've literally fixed the number of gates that you go through and every clock stroke, every clock, you know, leading it, trailing it, whatever it is, every clock initiation or tick that you have that as you step through the operation and move the data through it was fixed.

That's old days, that's -- you go back when I first looked at these things 20 years ago. Now you're saying their more complex and there are more different -- there are different ways of utilizing them.

MR. CARTE: Right.

CHAIRMAN BROWN: Which now put them into the context of microprocessors where our concerns should possibly be more amplified.

MS. ALVARADO: Yes, but we haven't seen any application using or emulating these.

CHAIRMAN BROWN: No, I appreciate that.

MR. THORP: Some of these have functioned like a microprocessor. They're software involved in the --

CHAIRMAN BROWN: I've always loved Norbert's approach in terms of fuzzying the -- you know, giving us the true scoop here on what is going on so we understand it. I'm just trying to make sure I understand a way that I can at least ensure that the committee understands what we're doing and why we should make certain observations as part of our reviews, that's all.

MR. CARTE: Right. The technology is evolving. So, what used to be a complex device is no longer considered complex.

There's also underlying technology differences. So there are fuse, antifuse type FPGAs which you gave a familiarity with.

But there's also devices where the file isn't loaded when you power up. So, when you -- the first thing the file does, the system does, is load the file at power up.

There's other systems or configurations where there's actually flash type memory in the device and it's an instant on device and there is no loading of file at power up. It's done at the factory.

So, there are various ways that these things are implemented and that's changing or evolving over time. So there isn't a good set of words you can use that'll always hold for categorizing these into particular complexity classes or processes.

I mean obviously fuse and antifuse are words that apply.

CHAIRMAN BROWN: No, you've helped out immensely in terms of my ability to ask questions.

MR. THORP: Well, you know, recognizing that there are different approaches that can be used in the design of these systems, we expect that to be explained to us and that's the kind of things we ask questions about when we conduct our reviews.

CHAIRMAN BROWN: Well, one of the designs you're going to be presenting to us is an FPGA based design. So, you've now raised the question of what are we seeing?

Because it has a lot of little watchdog timers floating around in it. Now, I don't know, so I've got some sense of -- because they're all called the same thing, I have some sense of comfort when I read it and now I've raised my level of discomfort, that's all.

Hey, we need to move on here so we can at least for your part --

MR. CARTE: Right. Actually, you're two presentations in that vein today. One is a complex programmable logic device which is fundamentally simpler.

CHAIRMAN BROWN: That's the card replacement?

MR. CARTE: Yes. And the other was an FPGA which is fundamentally more complex. One we've completed the review, the other we're still in process. So, there's different amounts of information you'll be able to get in that.

CHAIRMAN BROWN: Okay, thank you.

MR. CARTE: Okay. So, the technical requirements fall into these basic categories.

The first bullet I just want to mention is that A figure of standard has been moved from 50.55a(a)(1) to 50.54(jj) and 50.55j. And that's the A criteria for quality standard. So it'll be designed, erected, constructed in accordance with quality standards.

So, all of these requirements must be met. Some of them have greater safety significance than others. What we do in general is or the role of the

SRP in general is to look at all the requirements, look at all the guidance regarding those requirements and distill it down to a set of guidance for the reviewer.

So, it attempted to harmonize all those different requirements into one set of review criteria for the reviewer to follow.

Chapter 7 has a unique organization. It has a set of review criteria based on function such as reactor trip or engineering safety features. It also has a set of criteria by topic such as BTB 717 for development processes.

So, we would look at the development process criteria for reactor trip system and in the ESF system. So, the reason it was developed that way is to try and reduce the amount of repetition in the SRP.

MR. HECHT: Can I ask a question about the quality review process and how it differs between software development and FPGA development? Is this an appropriate time or should I wait until --

MR. CARTE: Well, we can wait a little bit.

But so, quality has actually two definitions. One is a process. So sometimes we think of -- we use the word quality to refer to Appendix B and it also has other characteristics.

So, 603 talks about low failure rates and minimum maintenance requirements, the fact that -- and the GDCs talk about you'll develop things in accordance with codes and standards.

So, you'll specify the functions and you'll specify features that ensure high reliability, low failure rates.

So, in terms of process, software development processes, we don't really make much of a distinction between FPGAs and microprocessors.

Now, so we look at the same -- we apply the same criteria for software development processes whether it be FPGA or a microprocessor based system.

Now, there are technical differences between the two. So, you can't exactly apply the same criteria. You have to apply some engineering judgment in your evaluation of the implementation of that criteria.

MR. HECHT: Well, there are two steps in the FPGA process that I see are different than the software development process and one is the development of net lists and then finally it's the actual development of the files which fuse or antifuse the chips themselves and then there's the burning of those chips.

MR. CARTE: Right. But in some senses, I

mean if you think of a process where you write in C code of VHDL, they're both essentially software. Then you're talking about a set of tools which translate that software representation and if you look at VHDL it looks just like software, right, it is software.

There are different tools that translate those functional requirements onto a specific implementation on the chip. And so, yes, there are fundamental differences in those tools. But, in essence, there are software, there are very large degrees of similarity in the development process all the way to the source code, the VHDL or C code.

In fact, there are tools where you can take a C code and burn it onto to a chip so you don't have to write in VHDL.

And so, the line is fuzzy. So you want to differentiate between the software instructions that you write and the underlying implementation. And yes, there are different tools and different processes.

MR. HECHT: Okay. So, if putting it another way, you would consider the net list generation and the files to burn the FPGAs as the equivalent of a compiler that you can kind of trust?

MR. CARTE: Correct. Compile, link and load essentially. We treat them as comparable tool sets.

MR. HECHT: Okay. And I guess the distinction is that when you're writing VHDL, that's a human process just like writing C is a human process, so that's where you spend most of your time?

MR. CARTE: Actually, we in a regulatory space, we don't review the source code in that sense. We try and keep our review at a higher level than that. We review the processes, review that they actually test, do code reviews and things like that, but we don't actually evaluate the source code.

MR. HECHT: Well, but you do do thread audits?

MR. CARTE: Yes. And that would go down to -- that can go down to the source code and it goes over to the test -- the testing of the requirements.

MR. HECHT: But you don't look at the tools and the quality of the tools that are being used below that or how do you assess that? You must assess that somehow.

MR. CARTE: The applicant has to assess the tools and to the extent that they rely on the tool or accredit the tool for meeting a safety requirement, then they need to qualify that tool for its ability to do that.

To the extent that they can independently confirm the output of that tool, then they don't need to do that. So, there are different approaches that people take and some people look at developing a test suite in accordance with safety related requirements and they use that test oracle or suite to confirm the actual code works correctly.

So you have two independent Appendix B development processes. The other ways would be to use two independent non-safety related tools to compare the outputs against each other and then use those to confirm.

But there's different processes and it's hard to generalize but the requirement is that they evaluate the tool and if they rely on the tool, then they have to qualify the tool for what they rely on it for.

MR. HECHT: And do you provide -- is the regulatory guidance saying, for example, you and use two non-qualified processes to compare against each other versus --

MR. CARTE: Yes, yes. No, the regulatory guidance does not talk about that. The regulatory guidance just basically says that either you qualify the tool or you independently confirm its output.

CHAIRMAN BROWN: Can we go on?

MR. HECHT: Yes, go ahead.

CHAIRMAN BROWN: Okay, thank you.

MR. CARTE: Okay. So, the specific review criteria we'd like to talk about today, we feel are more significant and that's why we'll talk about them.

Some of them are a little bit of a matter of interpretation. So, when we say design bases, there's two ways you can think about that.

You can think about the design bases of the plant and that's documented in the FSAR and you can think about the design bases of a system.

So, a system is built in accordance to some specification. There needs to be a one for one correspondence between what the system does or features it has and the documentation that describe the system.

So, that description, the documented description of the system and the reason for those features existence, we consider to be the design bases of the system which is different and distinct from the design bases of the plant.

So, what happens is, in general, when we compare, we're looking at topical report, we can assure that the equipment matches the description of the equipment, that the paper matches reality.

And in general, when they set up the criteria for that system, say in an equipment qualification, they will look at the worst case seismic loading that they anticipate, they will specify that as the design basis of the system.

The plant then, the licensee, has the obligation to ensure that the intended installation of that equipment is bounded by the qualification of the plant.

So, it's a two-step process. We ensure the equipment matches the paper and they ensure that the paper matches the needs of the plant.

So, single failure criteria is one of the important criteria. There are some requirements for redundancy explicitly in the GDCs and 603. However, redundancy is more strongly -- redundancy and independence are more strongly implied or required by the single failure criteria.

In other words, if you're not redundant, it's hard to argue that you can withstand a single failure.

So, the quality we look at is not Appendix B quality QA. We look at are the technical processes associated with software development appropriate for the tools that they're using? Are they crediting the tools in the right way? Are they evaluating the tools correctly?

So, in terms of equipment qualification, there tends to be two types of qualification, one which we call environment or can be called environment and the other would be performance. So, response time behavior is considered a performance requirement.

Environmental is a little of a fuzzy term. Sometimes people consider atmosphere different from radiation or seismic requirements.

So, for instance, GDS 2 talks about protection against natural phenomenon and GDC 4 talks about environmental design dynamic effects. So, in that case, we're thinking about environment in two different categories, things that are naturally occurring like earthquakes and things that are a result of accidents.

But in reality, there's a set of temperature radiation, humidity, vibration requirements placed on the equipment in a particular location and that's what's qualified, too, even though the descriptions come from different areas.

When we talk about independence, the criteria talks about independence between redundancies, between the equipment and the design basis events and you can do that by qualification testing and between the safety systems and other systems.

When we think about electrical independence in these areas, we think about electrical independence, we think about physical independence.

Generally, physical independence is addressed at the plant level where they end up installing equipment in different cabinets, in different rooms, different fire zones, depending on the level of physical independence that's required.

And that provides you immunity against things like fire or accidents that could occur, running a forklift into a cabinet, for instance.

We also consider communication independence and the independence between protection and control. So, we think about all these aspects when we think about independence.

We also consider the secure development in an operational environment. And the way we look at that is that there's no unwanted, undocumented, unneeded code in the system.

So, in essence, we're confirming that there's a one for one correspondence between the features of the system, characteristics features, and the design basis documentation for that system.

How that system is used and whether that meets the needs of the plant is evaluated at the time license amendment request.

We also sometimes look at diversity and defense in depth, if it is proposed. So, some applicants propose that they have enough inherent diversity in the system to eliminate consideration of common cause failure per the guidance in the Standard Review Plan Branch Technical Position, BTP 719, and some applicants do not.

But in the end, diversity in defense in depth is a plant level criteria that needs to be evaluated at the license amendment.

MEMBER BLEY: The previous bullet that you went through, does that imply you're actually rummaging through code or just descriptions of the code looking for unnecessary things that might be in there?

CHAIRMAN BROWN: The SDOE, is that what you're talking about?

MR. CARTE: Yes, there's two aspects. There's one what we do look at a little bit at the processes that they have in place for not introducing code as well as in general, there are code review requirements.

When you look at software development processes, you basically must code reviews. And so, someone is responsible for evaluating the code against the software design description. We check that they have done that and that evaluation should consider --

MEMBER BLEY: That's really looking at their documentation?

MR. CARTE: Yes, sir. We're looking at their documentation, their evaluation.

MEMBER BLEY: Okay.

MR. THORP: Those kind of things get discussed during our audits, threat audits and we try to see how they're handling the code, how they're protecting it, how they're ensuring that it doesn't get corrupted. You know, are there extra gadgets, you know, nice to have things that really don't belong there but maybe they offer to non-nuclear customers, that kind of thing.

MEMBER BLEY: Historically, there's been a lot of that.

MR. CARTE: Right. Well, effectively, or in summary, we evaluate that they did their job correctly. We do not do an independent review.

So, we predominantly are making sure that they have procedures in place and that they do their job thoroughly and if we find holes, we keep digging because we should not find anything. If they've done a good job, we shouldn't -- in a short audit, we should not be able to find a single problem and, if we do, we just keep pulling the thread.

MEMBER BLEY: Okay.

MR. CARTE: Okay. So, in essence, what happens is how the criteria are addressed depends in part on what is requested to be addressed in the topical report as well as the general categories that we've talked about.

A digital replacement card, for instance, we'll never look at digital communications because the analog didn't allow for that. So, it doesn't exist in those cards.

The application framework, it's hard to determine exactly what you're going to -- how you're going to use that card, so some criterias are left open. System specific has the most information in it.

And, again, when we talk about a License Amendment Request, it in essence, must address everything not addressed by the topical report.

So, a topical report closes something, everything else is required to be addressed in the

License Amendment Request. And, in general, they'll confirm what the TR bounds that the needs of the plant.

So, I tried to create a little bit of a matrix in terms of how these different criteria are addressed at the different types of review and I'm not sure I want to talk about all of them.

But one area that's interesting is, for instance, single failure criteria. A digital replacement card cannot met the single failure criteria. It is a component that is used in the system.

However, one of the aspects of the single failure criteria is that there are no undetectable failures. So, in general, all systems get a failure modes and effects analysis and that analysis is accompanied by some evaluation that identifies how each failure is identified so that the system does not have any unidentified failures in it.

So, in general, to address the single failure criteria, we look at the FMEA at the digital replacement card and at the application framework. If we had a system design, we can look at more details and, obviously, a license amendment, we can look at everything.

The criteria for quality is addressed similarly for all applications. We assure that what they did within the scope of the topical reports meets the quality criteria in the SRP.

There's nothing really system specific about quality. It's safety related, non-safety related but besides that, it's difficult to partition in terms of the quality of a reactor trip function versus and ESF function. There is no distinction.

Independence is also an interesting criteria to evaluate. So, for instance, in an application framework, since you don't know the application, you don't know the information, you don't know what information will be transmitted, all you can evaluate is the mechanism or communication. And for microprocessor based systems that tends to be a separate communication processor and dual port RAM.

In terms of digital cards, they meet the same functional requirements. There are really no independence criterias to check.

And I think that's really all that I wanted to talk about on this slide. But this give sort of a feeling that we address the same criteria differently depending on the scope of the application.

We have the acronym list and then I guess questions.

CHAIRMAN BROWN: If we have no questions, we'll move on to Rossnyev. Is she next?

We're about 20 minutes behind, so we will try to maintain some decorum in our questions, not decorum but --

MR. THORP: Well, we'll try to maintain that as well.

CHAIRMAN BROWN: -- quality in our questions here.

MS. ALVARADO: Okay.

CHAIRMAN BROWN: So, the floor is yours, excuse me.

MS. ALVARADO: I'm sorry.

I'm Rossnyev Alvarado, I'm a Technical Reviewer in the I&C Branch in NRR and I was the lead reviewer for the Rolls Royce SPINLINE 3 digital platform.

Next slide?

This slide just summarizes the outline for my presentation. It's pretty much based on what Norbert described previously.

Next slide?

So here is the background of the SPINLINE 3 platform. We issued the safety evaluation in September of 2013.

This platform resulted from the evolution of several I&C systems that Rolls Royce have installed in France. And because of this, it was designed based on European Nuclear and Quality Standards like the IEC-880. Now it's IEC-6880, but at the time this was developed, it was still the old format.

MEMBER STETKAR: Rossnyev, are these, you said installed in France? These are in EDF plants, nuclear plants?

MS. ALVARADO: Yes.

MEMBER STETKAR: They're back fits for AREVA?

MS. ALVARADO: Well --

MR. THORP: They've actually been through, my understanding --

MS. ALVARADO: Several evolutions.

MR. THORP: -- several evolutions, several generations of SPINLINE digital I&C platforms. They also do, there's a segment of their business that is involved with neutron monitoring systems and things like that.

MEMBER STETKAR: Neutron monitoring is usually often on the side.

MR. THORP: So, they are through a majority of the EDF plants.

MEMBER STETKAR: Is that right? I didn't

know that.

MS. ALVARADO: Yes, but going back to your question, in 2011, EDFs selected SPINLINE to replace the reactor protection system in at least 20 units in France. So, they're going through that replacement now as we speak.

MEMBER STETKAR: Thanks.

MS. ALVARADO: So, when we did our review, the French equivalent of the NRC, the regulators, they participated in our audit and we also talked and exchanged information with what we were reviewing and what they were reviewing.

So, they went with your guys when you went to France for the audit.

MR. THORP: Yes, they joined us for that week of the audit.

MEMBER BLEY: Is their approach reasonably similar to what we're doing?

MEMBER STETKAR: The review approach, right?

MR. THORP: Yes. I think they -- I can't give you a detailed explanation but I think that they expressed a lot of the same questions and concerns and wanted to look into a lot of the same things that we were looking into. So, that gave me a sense that there was a pretty roughly good parallel approach to things.

Now they may emphasize some things more than others that I'm not familiar with and I don't know whether our SL, who's perhaps more familiar with some of the things that they do over there.

MEMBER SCHULTZ: In timing, their review and our review is in parallel? When did this start?

MS. ALVARADO: It overlapped.

MR. THORP: Well, they expressed an interest knowing that we were going to do the audit. Right? So they --

MEMBER SCHULTZ: Not just the audit, I meant the topical review.

MS. ALVARADO: They overlap. They started before because --

MEMBER SCHULTZ: That's what I would have thought.

MS. ALVARADO: Right, because they were awarded this to Rolls Royce in 2011. But I cannot tell you exactly when they started.

MEMBER SCHULTZ: When was the topical submitted to us?

MS. ALVARADO: 2010.

MR. THORP: '09 or '10.

MS. ALVARADO: It's a long story.

MR. THORP: It has an ugly history.

MEMBER SCHULTZ: Okay. So there's some work that was done in parallel and some that was not, I guess?

MS. ALVARADO: Right.

MR. THORP: Right. There was some fits and starts in the whole process of trying to get this particular platform evaluated.

MS. ALVARADO: So, the SPINLINE platform has been qualified and is accepted to use in safety related applications for U.S. nuclear power plant and it's now maintaining their QA program compliance with Appendix B.

Next slide?

So, I'm trying to present in this slide a summary of the description of the system. The SPINLINE is based on microprocessor technology. It's a modular system that can be configured in different sizes according to the application.

So, to do this, what we receive in the topical report with no specific system architecture, instead they describe the different components and how they can be put together for an application in specific.

So, what we did was evaluate these components and some of the suggested architectures but we didn't evaluate a specific architecture for the system.

So, the manner in which these components are put together and how they interact will have to be evaluated when we get a license amendment using the SPINLINE system.

MR. THORP: So, this relates to my comment earlier about the desire of the vendor to have a maximum flexibility so that they can tailor their product to the needs of customers that might have varying desires in the requests.

CHAIRMAN BROWN: Okay. I guess I understand when I looked at the topical report and it talked about the CPU and the actuator card and this and that and the voting card and on and on and on.

But, they did have a couple of figures which, if you look at them, both the single division figure as well as what I would call a 4-channel figure relatively conventional application. Now, they didn't identify on there which card was doing what in this ting.

So, when you all looked at this, did you all look at the application of this card in terms of how it is or did you just look at each card as an --

I'm trying to put this into perspective.

I'm saying here's a car, I've got a carburetor, I've got some brakes, I've got a radiator and I've got -- so we looked at the radiator, we looked at this, we looked at that. But that --

MS. ALVARADO: Right. We didn't look at those examples that they provided. They just provided those to illustrate how they can put these parts together.

So, all we did is what you're saying, like the different parts. You picked the example of a car, you know, do they have a carburetor, they have a motor and they have wheels and we just look at each one of them and then they put together sort of like this chassis that you see here in which they performed the testing and the equipment qualification and how they operate it. And that's what we evaluated. We did not evaluate that.

MR. THORP: So, the purpose and the function of each of these separate cards and components and how they typically fit together and how information is transmitted and processed was explained to us and I think in the functional description, you're going to hear from Ross how this thing is designed, the basic functional design.

CHAIRMAN BROWN: Okay. The reason I ask

is because these do identify what they call one way communications. I think there's an internal network of some kind, is this the NERVIA one?

MR. THORP: The NERVIA.

CHAIRMAN BROWN: The NERVIA thing which was never stitched together into any understanding of how this thing munched around with all these cards. Is the one of the stations?

MS. ALVARADO: We will get there when we get to the communications.

CHAIRMAN BROWN: Talk a little bit about that?

MS. ALVARADO: Yes.

CHAIRMAN BROWN: But it's the one way communications was a thing of interest as well as they refer to the watchdogs on some of the components, particularly, I guess, the --

MS. ALVARADO: CPU.

CHAIRMAN BROWN: -- is it the UC25 N+ CPU?

MS. ALVARADO: That says video card.

CHAIRMAN BROWN: Oh, yes, I'm sorry. Well, that's just the name of the card. That shouldn't be too bad, I guess.

MS. ALVARADO: That's in the CPU card. Yes, we'll talk -- I will talk about that.

CHAIRMAN BROWN: All right, I'm just -- all I'm trying to do is get some concept because there's a couple of features relative to the discussion that were kind of interesting.

MS. ALVARADO: Right. And there is a system description in the safety evaluation where I go and try to describe that figure, but it was just -- this is what we can do.

CHAIRMAN BROWN: Okay.

MS. ALVARADO: The staff did not evaluate it.

CHAIRMAN BROWN: All right.

MS. ALVARADO: Because we didn't have enough information to evaluate it.

MEMBER SCHULTZ: Please interrupt us if we go into proprietary information.

MS. ALVARADO: Oh, I will.

CHAIRMAN BROWN: Please do that.

MS. ALVARADO: Don't worry, I will.

So this slide shows an example of a chassis. So, in the front of the chassis, what they have is what they call the main or daughter boards. These boards, what they do is signal conditioning.

Then in the back, they have the interface boards. And the interface boards, all they do is capture the signals from the sensors and perform some periodic testing, provide power supply if they need it and perform EMC filtering.

In between these two boards, is the backplane and they use the backplane, they has a bus for the backplane and that bus is the one that communicates the data from the I/O board to the CPU. This is separate than the NERVIA network and I'm going to talk about it when I describe the communication.

MR. CARTE: Can I interrupt just for a second? You know, one of the --

MS. ALVARADO: You cannot ask questions, you know. You're on this side of the table.

MR. CARTE: I'm using your slide, though, to answer a question that happened -- that Charlie asked.

In terms of what is a PLC, if you're looking at this box, this is the general thing what you'd expect to see when you see a PLC. So, it's a 19-inch rack, almost everything is 19-inch racks, they may have different heights but they basically have sometimes a card for a power supply. They have a microprocessor card, they have analog input cards and output cards.

This basic look and feel is what is a PLC. You can argue about -- get more precise but fuzzy, that's what a PLC looks like.

MR. THORP: I'm going to budget you on the use of the term fuzzy for the rest of the meeting.

MS. ALVARADO: Yes.

CHAIRMAN BROWN: But this is also a microprocessor based system here?

MR. CARTE: Yes.

CHAIRMAN BROWN: so, we'll unfuzzy that part of it.

MS. ALVARADO: Yes, but just a caveat, there are some of these cards that had FPGA on it and CPLDs and we evaluated them.

So, in the next slide, just to summarize this list, the boards that we evaluated that were submitted in the topical report and we look at, as I mentioned, some of these modules, the I/O modules, have programmable logic devices like CPLDs and FPGAs.

This is where fixed logics and they didn't change so they were part of the acceptance process that SPINLINE did for the operating system software.

So, we look at these logics and see what they do. But this is pretty simple what they do is pretty much conditioning of the I/O signals, that's what these logics are doing.

Next slide?

So, in this slide, I want to just briefly describe the software architecture and the configuration.

A SPINLINE -- Rolls Royce uses a tool called Clarice as assistance software development environment to develop, build and configure the system software.

So, they have, let's say, like two components, the OSS which is the operating system software and the application software.

The application software will depend of their requirements for the data, particular application in a plant.

The OSS is the one that we look at and they went through a very extensive verification and validation process.

So, this software did not change with the application, this is fixed. This is what they have as the operating software.

The operating software can be configured to use different I/O modules and this is the flexibility that they have depending on the application that you have. For example, if you need to use an actuator, then in your OSS, you would tell this configuration, this application doesn't have an actuator and the OSS will not look for that kind of thing.

And the way they perform this is that they have tables inside the OSS, well, I put it on the outside like this hardware configuration tables, for example, on the top.

What it does is it will tell the operating system what I/O boards are installed and where they're installed in the rack.

Now, you have the system data which is information that the OSS uses to determine hardware status and communication with the network status.

Then you have this interface table which is a table that is going to exchange the data between the operating system and the application software.

And last but not least, we have the application data which is application specific that the application software is going to need depending on the requirement that the licensee establishes.

MR. HECHT: Can I ask a question?

CHAIRMAN BROWN: Go ahead.

MR. HECHT: Okay. This is I think a good time to talk about the issue of obsolescence and changes and how the topical report might move off because, based on my reading of this document, this has a 68040 processor on it.

MS. ALVARADO: Right.

MR. HECHT: Which I remember being very excited about when it was new but I guess none of us are new -- some of us are not new anymore.

And I think it's growing long in tooth, is it not? What would be the process here when they replace that 68040 processor?

MS. ALVARADO: I cannot talk in terms of SPINLINE, right, because maybe they decide to maintain it. I don't know if they can.

But I can tell you what we've seen with Diablo Canyon, for example, and I think it will be something like that.

So, when we got the Triconex, the first time was in 2001, right, and that Version 9. In 2011, Invensys submitted Tricon Version 10.

So, what we did was evaluate the different between Version 9 and Version 10 and we evaluated that delta and did a safety evaluation based on the delta.

For Diablo Canyon, they are using Version 10.2 or 10.3. So, what we did was like, okay, we approve Version 10. For Diablo Canyon, we are looking evaluated the deltas between what we approved in the platform, right, when we looked at the Version 10 versus what they are using for Diablo Canyon which is as 10.2.

And there were just some changes in some cards and stuff like that.

So, I would think in this case, it's some sort of similar process. So, if the microprocessor were to be changed, then they will have to submit another topical report describing what they're using and we will have to evaluate the deltas because it might as well be that they're just changing the microprocessor, but then they are using the same I/O boards. So, I don't need to evaluate the I/O boards, I just need to evaluate the new microprocessor and if it works and communicates with the existing cards if that's what they are doing.

MR. THORP: So, I don't want to get into too much detail and stop me if I -- not that I have a lot of detail in my head, I was a supervisor, but I participated in this audit.

And we pulled threads and delved into this whole process significantly because we saw that there was, as you said, some things that appeared to be kind of long in the tooth in terms of the actual technology and I won't want to get into numbers and that kind of thing.

But we verified that they have a very solid approach and a plan in terms of life cycle maintenance of these systems where such that they're not too worried about obsolescence on this stuff.

And I can't get into the detail about how they prepared themselves to deal with that but they have and they're ensuring based on the number of plants that they've got these things installed in that they can fully satisfy the needs of these systems for well beyond their designed lifetime.

MR. HECHT: Okay, well, hypothetically --

MR. THORP: So, what I'm telling you is I guess, not that we would anticipate that they wouldn't change their design to make something newer, better, faster, cheaper, smaller like I talked about.

And so, we have processes to deal with that and to look at the deltas.

MR. HECHT: What I'm trying to do is I heard, in general, the process described. You evaluate the changes and based on those changes, you do that.

What I was hoping to get out of this discussion was here in the specific case, you've changed the processor, you get a different instruction set and maybe other differences in the processor besides merely the instruction set.

What criteria would be used in this case if they were to make a change in the process rather than just saying, in general, evaluate? I mean can you get into more detail saying how you would approach that problem?

MS. ALVARADO: That's what I just described with the Tricon, that's what we did with the Tricon. We have to go --

MR. HECHT: Oh, you said you sent from Version 9 to Version 10.2 but you didn't say if in Version 10.2 they took an 80.86 and put in something else.

MS. ALVARADO: Well that's getting into the details of what they did. I cannot discuss that but I can tell you that from Version 9 to Version 10, we did look at all the changes that they did and evaluate it.

MR. THORP: There was essentially a decade of time between Version 9 for Triconex and Version 10. So, rather than a focused sort of little delta review, we essentially did a full blown topical report review of Version 10 and reestablished sort of a baseline and wrote and SE reflecting that version.

MR. HECHT: So, they need --

MR. THORP: So, now with the little delta between Version 10 and the little improvements that they've made in 10.2, 10.3, we looked at those deltas as well for Diablo.

MR. HECHT: So, the answer is when you replace a processor, you write a new topical report?

MS. ALVARADO: The vendors do, yes.

MR. HECHT: The vendors do?

MR. THORP: The vendor has to decide how to treat that.

MR. CARTE: I mean a topical report is strictly a vendor pool thing. We review a topical report when we get one. If they choose to update it, fine. If they don't, fine.

Our next shot at is the license amendment if they do not choose to update a topical report. So, if they have not updated the topical report, then we will consider that in the license amendment process.

If they choose to update the topical report, that will make license amendment process quicker and we would evaluate at that time. The criteria is not different. It's one set of criteria for power plants. It doesn't matter whether it's in the initial application or an update.

So, when they changed processors, there was a set of regression testing that they had to do and a set of documentation that they have to do and that

-- it's the same as the original set.

So, we would review it against the criteria that we would do review against the initial applications.

So, in essence, there's no difference in how we should review things. It's one set of criteria. It doesn't matter whether it's the topical report, an amendment to a topical report or a license amendment, it's one set of technical criteria.

CHAIRMAN BROWN: I'm going to have to -- we're going to have move along here. Go ahead, Rossnyev.

MS. ALVARADO: Okay. Next slide?

So on this slide I'm just describing how the system operates. Right?

So, the first step is that when you pretty much turn on the system, the systems goes through an initialization process where it goes into initializing the code, verifying internal operation of the CPU, then it goes and initializes all the I/O boards. Right?

And it's using the hardware configuration table to identify the boards that are installed and start testing for communication with the I/O board. And then, it sets the hardware watchdog of the CPU board at this point.

After the system is initialized, it goes into the cyclical mode of operation. Right? And it's showing it in the blue line in the arrows above.

So, we have the first step is the cycled time management. This is a function that the system has to manage the time of the system. So, when you are designing the system, you say, well, my predefined value for the operation is this many seconds of microseconds or whatever you want or milliseconds, I'm sorry.

If the cycle time is longer, then the CPU will stop and an indication will be shown to the operators.

Then the next function is test and self-test diagnostics. This is to detect different failures in the system. So, once as set of failures is detected or if there is there some sort of problem, the system will go into some sort of defined state. This defined state on how the errors are managed is application specific.

So, we didn't go into review of how the failures are managed because they said that it will depend on each application.

But if there is a problem with the watchdog timer, the CPU will stop. That we evaluated.

Then next step which I'm showing in a bigger scale is the part of data acquisitions. So the system pretty much --

CHAIRMAN BROWN: Rossnyev, we said the watchdog timer, you did evaluate that. Did you evaluate what it does if it's not strobed or if it's not reset?

MS. ALVARADO: Yes, it will stop the CPU.

CHAIRMAN BROWN: Well, it stops what, the CPU?'

MS. ALVARADO: Yes. It will stop the CPU.

CHAIRMAN BROWN: Is that all it does?

MS. ALVARADO: And it will drive the output to define safe condition, like a predefined value.

MR. THORP: And that is relative to the application.

MS. ALVARADO: Right and then --

CHAIRMAN BROWN: No, I understand that, but I mean is the design of the system such that you can establish whether it triggers an alarm or whether it actually triggers a voting trip and a reactor trip system where it says, hey, okay, I have to consider this channel tripped or whereas if it's just an alarm, does it have that capability to go --

MS. ALVARADO: It has that capability, but again, it would depend on the application. But they --

CHAIRMAN BROWN: All I wanted to know was does -- I mean it has multiple ways that it can provide and output, that's all I was trying to look for.

MS. ALVARADO: Yes, right, yes.

CHAIRMAN BROWN: So, I think you answered that.

MR. THORP: We assured ourselves.

MS. ALVARADO: You get an alarm that can be sent to a plant computer system. They have an LED indicator that is if the system is operating right, it will stay illuminated. If the watchdog fails, that will go off.

And then, it will also drive the outputs to a safe condition.

CHAIRMAN BROWN: Yes, which could be, if it was a reactor trip function, it could be a voting trip?

MS. ALVARADO: Right or something like that, right.

CHAIRMAN BROWN: If it was a safeguard, it could be just an alarm. It could be whatever. Okay, that's all I -- I didn't see it explicitly covered in the discussion that's in the SER, the nature of the output.

So, go ahead, you're fine.

MS. ALVARADO: So, the system will acquire the data, right, it will go from the sensors and it is showing it in the bottom part how the data goes from the sensors eventually into the input boards then to the application software where it's processed and then the application software will create outputs if necessary to drive the actuators.

The next function will be the LDU data exchange which we did not look at. I looked at -- I evaluated from the point of view of the operating system but I didn't look at the LDU -- LDU means local display unit -- because, again, the configuration of the local display unit is application specific, so we didn't evaluate these.

I just look and from the part of the OSS, how data is collected and then how it can be exchanged.

So, I want to emphasize that these functions are executed in every cycle in the same order and are independent of input and external event.

The cycle time is fixed during this time and if this time is not met, then like I said before, the watchdog timer will time out and, as I described before, you have the LED will go off and then the outputs will go into a safe condition.

The system is continuously informed of the status of the communication interface. So, the system retains the ability to perform a safety function without reliance on data from the outside.

The SPINLINE system does not use interrupt to manage self-test programs. They use interrupt only when the system fails and needs to drive the outputs to a predefined safer state and this will be defined for an application specific.

Next slide?

So, in the next slide, I summarize the different system communications that we evaluated. I'm going to talk in detail about the first two but regarding the last two, there are some passive communication hubs and converters.

These components do not use embedded logic, they are just passive components, all they do is just pass the signal.

There are two serial links in the front of the chassis and these are RJ45 connectors and how these are used is a plant specific application.

Next slide?

So, on this slide I'm going to talk about the backplane bus communication, and simpler, it's called BAP which stands for backplane. This is a passive bus communication that the system uses to collect data from the I/O boards and transmit it to the CPU.

It's a master/slave bus with the CPU being the master and the I/O boards the slave, which means that the CPU will request information from the I/O boards and the I/O boards have to respond to the master.

The bus uses this connector, so you can see a mark XF1 and XF2 for data transmission.

The way the data flows is like from the input, they said like the input terminals that I have here, they go from the fuel sensors to the interface board, right, and from there, it goes into the main board or the daughter board through the XF2. That's with the red arrow that you have in the slide.

It goes into the main board where it goes through signal conversion or conditioning and from the main board though XF1 which is the one with the blue arrow, that's where it's transmitted through the backplane bus to the CPU.

It will be the opposite direction like reversing direction for the output board.

There's two of the boards that do not

communicate with the backplane bus and these are the RTD, the temperature board. It doesn't communicate directly with the CPU using the backplane bus, it uses the analog card to communicate.

And the other one which I'm going to talk in more detail is the CPU board. The CPU board does not communicate directly for the NERVIA communication through the backplane bus.

The backplane bus uses a predefined configuration for data --

MR. HECHT: Could I ask a question? The NERVIA network you said it was a one way --

MS. ALVARADO: That's in the next slide.

MR. HECHT: Oh, I'm sorry.

MS. ALVARADO: Can you hold it until the next one?

MR. HECHT: Okay.

MS. ALVARADO: Okay. The backplane bus uses a predefined configuration for this data exchange and the operating system ensures that the communication between the CPU and the I/O boards occurs in a predefined time.

Next slide?

Here we are going for NERVIA.

Interesting, Member Brown is not here and he wanted to know about this.

MEMBER STETKAR: He'll be back soon.

MS. ALVARADO: Okay. He will be back when I'm done.

MEMBER BROWN: Speak slowly.

MS. ALVARADO: Okay. So, this is intra-divisional communication for these Rolls Royce using the NERVIA network which is a proprietary dedicated network. It was developed using the open system interconnection model.

As I mentioned, this is used to exchange information within a division, nonetheless, they can use it if they want it for division. However, Rolls Royce did not request approval for intra-divisional communication above the following new year.

So, they defined two components for the NERVIA which is what we call a station which is on your left side which is pretty much the part that is the NERVIA board and the NERVIA interface board. And then they have another one which is called the unit which is pretty much where CPU board is. Okay?

MEMBER STETKAR: So you said they have the capability for using the network for intra-divisional but as far as the topical, they didn't --

MS. ALVARADO: No, they didn't.

MR. THORP: They didn't request our review of that aspect about the this.

MS. ALVARADO: So, they're not going to use it.

MEMBER STETKAR: They're not going to -- they'll physical disable it?

MS. ALVARADO: Well, they didn't physical disable because you have the network there. It's just that they're not going to use it so when we get a license amendment, we have to be -- to evaluate that they're not using it for that purpose.

CHAIRMAN BROWN: But could it be used by mistake?

MS. ALVARADO: Yes?

CHAIRMAN BROWN: Could it be used by mistake?

MR. THORP: But there's an SDOE question.

MS. ALVARADO: Right, exactly. We'll evaluate it for that purpose.

MC. HECHT: Can I ask a question about the implementation and you'll tell me if I'm going into proprietary territory?

How is it that they get the guarantee the one way communication? Is that --

MS. ALVARADO: That is proprietary, yes.

CHAIRMAN BROWN: That answers that question.

MS. ALVARADO: Yes.

CHAIRMAN BROWN: We'll move on, that was one of my questions.

MS. ALVARADO: Well, I mean they have ways to configure, as I was saying this station, they will configure the station to make it one way only. But, yes, that's proprietary.

MR. THORP: And they described for us in great detail in how they specifically manage data communication and cycle time and things like that.

CHAIRMAN BROWN: Is it proprietary whether it's software or hardware configured?

MS. ALVARADO: What is software?

CHAIRMAN BROWN: The one way communication? That's pretty high level, is it hardware or is it software configured?

MS. ALVARADO: It's software configured.

CHAIRMAN BROWN: Okay. I won't make no further comments on it.

MS. ALVARADO: Okay.

CHAIRMAN BROWN: We'll move on.

MS. ALVARADO: The NERVIA is an Internet based network that uses a time based token pass protocol. The way this works is the token is transmitted from one station to another and a station is allowed to transmit the data when that station has a token and it's only allowed to transmit the data for a specific period of time.

So, when a station is transmitting, the message is received by all other stations that are connected to the network.

The stations that are not transmitting are listening for messages and they have to wait until that period elapses and to get their turn in the network to transmit their messages.

The cycle time for transmission is defined during this time but this cycle time is also monitored by the station and it's communicated to the unit so the CPU will know about it.

The network station are always transmitting in the same order, so you define it when you are defining the network in your design for the station on top is the station one then the station two, so they will always transmit in the same order.

The network design establishes the sequence and is always defined during the design.

The NERVIA network does not have direct access to the backplane bus as I'm showing in this slide. Communications between the CPU and the NERVIA network always happen through the dual port memory which is static and doesn't change during program execution.

They have an arbiter which, and just before you ask, I cannot go into details because that part is proprietary. They have an arbiter that is responsible for monitoring this data exchange and that there is no data collision in the DPM.

Once the data is copying the station, this information is available to be broadcasted to the network.

I want to point out that the processor time for the unit is different than the station processor time. So, if the station were to fail, this will not affect the operation of the unit or of the chassis, it will continue to operate because they are separate, they have separate transmission times and operation times. They only way they exchange data is just through the DPM.

Both cycle times are fixed and are monitored and is always executed at the same time for both the processor and for the station.

If an application uses the SPINLINE, then the NERVIA network has to be evaluated as a part of the full response time for the system because then your response time will vary, depending if you use the NERVIA network or not.

I can just mention this going back, is, yes, a station, the NERVIA can be configured as a one way communication but that will go in to proprietary information.

The NERVIA processor performs different diagnostics to confirm the data. For example, it performs cyclic redundancy checks and the received message, it will flag erroneous data or if the data is stale so it's not used by the CPU.

And it's always checking for communications, so the NERVIA station has also watchdog timer.

Next slide?

So now --

MEMBER BLEY: Before you leave that slide, you talked about the communications and with the tokens. Is that essentially the same scheme that was the old IBM toke ring bus communication protocol?

MS. ALVARADO: This is more like a star communication.

MEMBER BLEY: Okay.

MS. ALVARADO: So you have the token and

I give the token to Samir because it's in order, it's always in order. Right? So now, when he has the token it's the only time that he can transmit.

MEMBER BLEY: It sounds the same, though.

MS. ALVARADO: Yes, it's --

MR. HECHT: On the software level it is. IBM did have that token ring.

MS. ALVARADO: Right, right.

MR. HECHT: But it's -- that was a physical layer difference.

MEMBER BLEY: Yes, that's right, it was a long time ago.

MS. ALVARADO: Did that answer your question?

MEMBER BLEY: Yes, thank you.

MS. ALVARADO: Next slide?

So regarding the key review criteria, this other criteria that Norbert described before, we look at independence for the communication comparability and SDOE.

Regarding redundancy and diversity, there are features in the system to implementing this but these are application specific, so we didn't review it and we left it as an applicant specific action item. It will depend on how the platform is used.

Next slide?

In independence, we evaluated two different things, one was electrical independence and the other one was regarding communication independence. This summarizes our findings.

The SPINLINE platform meets the criteria for electrical independence. They did multiple tests and we looked at the tests and saw how they performed these and they met the criteria in IEEE 384.

The system provides digital communication that can support independence, it just depends on how this is used. So we will have to evaluate that for an application when someone submits a license amendment.

And we looked at the features for non-1E components but until we see how this is implemented, we couldn't evaluate it at this time. So, we'll have to see when a licensee submits a license amendment how this is implemented.

Next slide?

MEMBER SCHULTZ: So, does the SER associated with the topical specify provide guidance to the licensee as to what they need to provide specifically --

MS. ALVARADO: Yes.

MEMBER SCHULTZ: -- to satisfy the

communication concern?

MS. ALVARADO: Yes, throughout the safety evaluation, there are a specific guidance that we say this is an application specific action item and then at the end of the safety evaluation, there is a chapter where it tells you in detail, you know, for communication, you need to look at the following actions.

MEMBER SCHULTZ: Okay, thank you.

MS. ALVARADO: So, yes.

Predictability and repeatability, we evaluated how data communicated and the response time characteristic of the system. But this is always going to depend of how the system is going to deal with an application.

But we do observe that the software runs sequentially, deterministically and periodically. The cycled time is fixed and the functions are executed in the same order.

So, the system is behaving in a deterministic way. The unit processor is independent of the station processors and data exchange between the unit and the station is to the DPM. Those are the ones that are very important to summarize.

Next slide?

Regarding SDOE, this slide summarizes our findings for the SDOE. But the software is configured in Rolls Royce in France. We looked at the different access controls that they have. They have a secure environment to do the software application.

The software, once it is in a system, it cannot be modified by an operator when the system is running online because of the way the system is configured. And the system includes features that can apply to demonstrate protection against undesirable behavior of other connected system and prevention against inadvertent access.

MEMBER SCHULTZ: So, there is -- is there something the licensee needs to do to take credit for that or is it --

MS. ALVARADO: Yes, it is identified -- because one of the things is like because of the flexibility of the system that they can install different I/O configuration, they have some --- they have the code for all I/O modules, right, so what they do is the deactivate the code that they're not going to -- for the modules that they are not using.

So we identified this as an application specific item, look, depending on your configuration, you need to go and be sure that the code is deactivated and it's not going to create unevaluated.

MEMBER SCHULTZ: And with regard to the environment that is demonstrated to be secure, is that monitored in a certain fashion or is there -- what is provided to assure that that environment is stable over time?

MS. ALVARADO: Well, we looked at the software tools that they use and the --

MEMBER SCHULTZ: No, I know what you've done.

MS. ALVARADO: Right.

MEMBER SHULTZ: I know what you've done, but --

MR. THORP: You're talking about at the licensee's level?

MEMBER SCHULTZ: Exactly. Is that something for the licensee to do or is there --

MR. THORP: Well, they're certainly going to have to have their piece of that. This would be the secure operating environment, right, for this platform. And that would be something we would look at in their application to us about how they intend to install and use and assure SDOE at their facility.

MS. ALVARADO: Right, but what we look at is like how they do it at the like the applicant, in this case, Rolls Royce, how they control their software, who has access to the software.

MR. THORP: This is one of the --

MS. ALVARADO: When they are programming the logic, who are the people that have access to modifying the code and that they're following their configuration.

MR. THORP: This is one of the key aspects of the audit that we performed.

MS. ALVARADO: Right.

MR. THORP: At their facility.

MS. ALVARADO: And the last slide, this is just a summary of the different applications that can be done with the SPINLINE platform.

There is none installed in the U.S. and we don't know of any licensee -- no licensee have come to us saying that they want to use the SPINLINE. However, this is installed in several places in France and in Eastern Europe and also in operation in China.

And that concludes my presentation. Questions?

CHAIRMAN BROWN: Okay. Norbert, this is your opportunity to shine and be crisp.

MR. THORP: At this point, could I --

CHAIRMAN BROWN: I think we should take a break. We will -- since this is a break and we're running --

MR. THORP: A little late?

CHAIRMAN BROWN: Yes, I know, well, I went ahead and took my break. We will recess the meeting for 15 minutes until, actually 13 minutes until 25 minutes of 11:00.

MR. THORP: Okay, thank you.

(Whereupon, the above-entitled matter went off the record at 10:21 a.m.)

MR. CARTE: So I'll be talking about the SSPS CPLD-based topical report. So when I talk about this, first I want to give a little background about the solid state protection system itself and then I'll talk about the topical report and the criteria applied.

So in terms of the SSPS, the first voting systems for Westinghouse plants were basically relay voting systems. For a plant that consisted of 14 cabinets, testing took about four hours. There were about 1,000 conductors involved in the communication of status information at control board and plant computer. There are approximately 750 relays with 4,000 contacts.

So in January of 1971, Westinghouse proposed the topical report solid state protection system that replaced these 14 cabinets with six cabinets, two trains, that is three cabinets in each train. And these cabinets consisted of an input cabinet, a logic cabinet and a relay cabinet.

The circuit boards all predominantly fit in the logic cabinet. Testing time was also automated with a semi-automatic testing board. And that reduced the testing time to approximately 10 minutes per train. And through multiplexing, they reduced the number of conductors to about 42.

So in 1974 that was approved and applied subsequently in new Westinghouse plants.

So this is a picture of the SSPS cabinets. The center two cabinets are the SSPS cabinets. The two, one on the left, one on the right, are the demultiplexers that the SSPS communicates with. So if we look at the cabinet, there is an input bay, each which is compartmentalized into four separate sections, one for each of the input channels from the plant protection system.

There is a logic bay. And in this logic bay there are some circuit cards. And these are the cards that were being changed in the topical report. There is also a relay bay. Now, these circuit cards, the status information from these circuit cards is communicated out to the plant control board through the demultiplexer cabinet -- and I will talk about that -- as well as the plant computer through a separate demultiplexer.

Basically, one train communicates to the control board, the other train communicates to the plant computer. There is some coordination between the trains so that there the information is synchronized. In a later slide what we are going to see is we are going to see these, these same cabinets, one rotated clockwise at the top of the display and the other one rotated -- no, sorry -- counterclockwise at the top and clockwise at the bottom. But let me get into that.

So, in essence there are eight boards, circuit boards involved in these cabinets. One is the universal logic board which does the voting. The safeguard driver which drives the ESF relays, the undervoltage driver which powers your after-trip breakers, the semiautomatic tester which is used during surveillance testing, the clock counter board which is both used during surveillance testing and is used for status indication. And I will describe that a little bit more in detail. We also have a decoder board.

So what the clock counter board does is it has a clock and a counter and it increments, the decoder board translates that incremental number into addresses to use for multiplexing and testing purposes.

The memory board is the one non-safety board in this set-up. This is the board in the demultiplexer cabinet that holds the status information that is communicated from the SSPS cabinets. And the isolation board is --

CHAIRMAN BROWN: From/to where?

MR. CARTE: From the SSPS cabinets to the demultiplexer cabinets. And those, I will show that in the next slide.

CHAIRMAN BROWN: Thank you.

MR. CARTE: And then there is an isolation board which does 1E electrical isolation.

So when we talk about the SSPS in context, so the six cabinets that I talked about are here: input bay, logic bay, relay bay. The plant protection system consists of four channels here so the plant sensors get wired into the four different channels of the plant protection system. So Westinghouse plants generally have a one out of two trips for start-up and intermediate source range. They have two out of three trips and two out of four trips. So that's why they have four channels of information.

Those binary inputs go into the input cabinets where there is isolation between the different channels and as well as between the circuit boards. And that binary status information then goes into the solid state protection system cards, the relay cards, the voting cards. And then depending, if appropriate, the safeguards or ESFS, RPS system gets actuated.

So when we talked about the different cards, in here we have the logic card as well as the driver cards. We have the isolation cards that communicate status information to the demultiplexer cabinet. We also have a connection between different redundancies. And that's through an isolator card in order to co-ordinate that each train is indicating the same information.

So if we --

CHAIRMAN BROWN: Before you leave that, understanding the left-hand channel 1, 2, 3 and 4, the vertical --

MR. CARTE: Yes.

CHAIRMAN BROWN: -- right outside the little half partial ring.

MR. CARTE: Yes.

CHAIRMAN BROWN: That's sensors coming in?

MR. CARTE: Right. These are the sensors and this is the plant protection system.

CHAIRMAN BROWN: So that takes the ana -- that's still all analog?

MR. CARTE: Yes.

CHAIRMAN BROWN: And it sends out this little bi-stable signal shown by these relays?

MR. CARTE: Yes.

CHAIRMAN BROWN: And under the master and slave relay thing?

MR. CARTE: Yes.

CHAIRMAN BROWN: So are those still contacts like that?

MR. CARTE: Yes.

CHAIRMAN BROWN: You said they were binary --

MR. CARTE: Yes.

CHAIRMAN BROWN: -- so I presume they're still the relay contacts?

MR. CARTE: Yes.

CHAIRMAN BROWN: And that's what and then so all this replacement goes into the solid state logic in the voting?

MR. CARTE: Yes.

CHAIRMAN BROWN: Okay.

MR. CARTE: One qualification: the plant protection system, these four cabinets are not part of the review. In some plants they're analog, they're 7300 cabinets, in some plants they're Eagle 21's such as Diablo Canyon where they're being ripped out and replaced with Triconex and ALS.

CHAIRMAN BROWN: Okay.

MR. CARTE: So they still produce binary signals for voting purposes.

CHAIRMAN BROWN: Okay, thank you.

MR. CARTE: And there's this, the input bay is the isolation for that.

CHAIRMAN BROWN: All right.

MR. CARTE: So this signal, there's sort of two configurations in which the ESF -- sorry, SSPS is used. One is in operation and the other is testing. So we'll talk about how the cards are used in operation.

The orange cards are basically the cards that process the safety functions, so the discrete inputs come into the ULD card which is voted. And depending on the vote, it actuates either the ESF or reactor trip breakers.

The blue cards are used for status indication. So in the upper left is the clock counter board. Using a clock and a counter it creates a sequential number which is decoded by the decoder board into addresses. And those addresses are used in order to provide multiplex information out to the memory board which is used for status indication on the main control board or on the plant computer.

That information is coordinated because the clock counter also sends the count out to a decoder board which sits in the demultiplexer cabinet in order to -- so that they both are sending and receiving information at the same address.

MEMBER BLEY: Is indication always non-safety? I was just curious why the number is non-safety. It's only used for indication.

MR. CARTE: That is correct. Plant computer and control board indication, yes. In general, I think that it is not required to be safety.

MR. THORP: I think generally speaking it is considered non-safety. Like the annunciators on the control board.

MR. CARTE: As long as the plant computer is not doing anything --

MR. THORP: Correct.

MR. CARTE: -- picking safety up.

MR. THORP: And I think, I think the

plants -- this is just a philosophical point, real brief -- that they, they prefer to have their plant computers be non-safety related so that, so that they can update them more rapidly and use the plant computer for all the different purposes for which it could be used such as trending information and --

MR. CARTE: Main control board information --

MR. THORP: And, yes, illuminate control boards with the annunciators, for example. Those are considered non-safety related.

MEMBER STETKAR: Annunciators are, I mean the indications on the board are usually powered by safety-related.

MR. THORP: The actual indicators are, you know, process status like a steam-generated level or something like that. Those you would have your safety-related channel displays and those would lbe safety related.

MEMBER STETKAR: Yes. Equipment that starts is all safety. Those indications would be safety-related.

MR. THORP: Right.

MEMBER STETKAR: Okay.

MR. CARTE: Okay. And so the other configuration is when it's in surveillance testing. So in that case the clock counter board or the count is basically input to the semiautomatic test board in order to generate all permutations and combinations of inputs. As well as the semiautomatic tester then looks at the response of the tested boards to assure that the outputs are correct.

So those are the two configurations in which the cards are used.

Okay, so in terms of -- so that's, that doesn't change; new boards, old boards, that's the way the SSPS system works. In terms of the programmable logic devices, some sort of history on that is needed.

So in February of 2001, we approved the ASIC base replacement module topical report. So this was an ASIC, had ASIC chips. These cards had personality modules. Neither the application nor the NRC review identified those components as containing software. Although if you look at the position today, we would consider that to be software because you are loading a file onto those devices.

So shortly after that approval, the PWR Owners' Group decided to develop new cards for the SSPS cabinets. And they decided to make that CPLD based. And they considered that to be hardware only. And in light of that recent ABRM decision, that was not an unreasonable position for them to take.

So in November -- so to put this in context, in November of 2006 industry came and talked to the Commission and said there was too much regulatory uncertainty with design C. That resulted in a steering committee and tasked working groups which resulted in the ISGs that we can talk about later or will come up shortly. As well as in March 2007 to March 2009, the Wolf Creek application or main steam and feed water isolation system came in.

So in that time frame we were discussing programmable devices and that the staff considered them to be, or considered the processes for them to be reviewed against the same criteria as software development processes. I believe that was first published in ISG-4 at Rev. 0, September 2006 -- seven.

To put that in context, in July 2010 to 2013, the ALF topical report was reviewed in accordance with software development processes. Then in 2013, February, there was a CDBI inspection of Harris. This inspection identified that these cards were installed in a plant using only a 50-59 screening. And that was in August determined to be a violation.

In that year 2013 we had four meetings with the PWR Owner's Group, Westinghouse, to determine what the best path forward would be. And that, it was decided that a topical report would be the best approach for that. So in February of 2014, Westinghouse docketed a topical report for the CPLD-based SSPS cards.

So these cards basically, the old cards basically used Motorola high-threshold logic so that it was basically 15-volt logic. And it was at that time envisioned to be better for noisy shop floor environments which I guess is not really directly applicable but they made that decision.

The new cards were designed to be form, fit, function identical to the old cards. So the design basis of the new cards is the design of the old cards. There are eight new cards. Seven are installed in the existing SSPS racks; and those are listed below. As well as one is installed in the non-safety demultiplexer cabinets.

Now, with respect to these cards, the ISO card is the only one that we would not consider to have software. It was strictly electrical isolation, no CPLDs. The other cards all have complex programmable logic devices on them. The three cards that were most critical for performing safety function are the universal logic board, the safeguard driver board and the undervoltage driver board.

Those cards actually have two CPLDs on them. One is the main CPLD and the other is a test CPLD. So the test CPLD generates all permutations and combinations of inputs to test the main CPLD. It compares the main CPLD outputs with its model of what the outputs should be and, therefore, it is involved in continuous self test of all circuits involved on that card, on the main CPLD.

The cards also include a watchdog timer which if it times out it goes to both the main CPLD and the test CPLD, and if it times out there's also an LED on the card edge.

So the main enhancements on these cards are, as might be said, some improvements to single point vulnerabilities. So some drivers were duplicated, output drivers were duplicated, some power supplies were duplicated. And this was to make the cards more reliable, not an attempt to make any individual card satisfy the single failure criteria.

So on these three cards if -- three cards, if the test CPLD finds, fails one test and you get an E1 LED, a red LED that says you have failed a test, if you fail ten tests in a row you get an E10 LED that indicates the status of that card. These, these health-monitoring features are not connected to any control board indications, they are local only to the cabinet in terms of card edge LEDs.

So in terms of design basis, it's the original card design, the form, fit, function identical. There were some instances where that was not quite achieved but that's documented and identified. So some cards need to be replaced in pairs.

Single fire criteria was not evaluated, in essence because the cabinet itself addresses that criteria. Individual cards do not address that criteria.

MEMBER STETKAR: Can I interrupt you just a second? What you said about, you know, it fails ten functions you get some color light on --

MR. CARTE: Yes.

MEMBER STETKAR: -- card edge. Operators don't know about that. Does, if it fails ten times in a row what does the card do, just keeps processing?

MR. CARTE: It continues to perform its function, yes.

MEMBER STETKAR: Okay.

MR. CARTE: So, the issue is as a form, fit, function replacement the original cards did not have health-monitoring circuits to that extent and had no way to indicate them out. There are processes actually in the works, and that will probably come in for license review, license amendment request or a topical report in order to provide indications for these self-help, self-help monitors. But that would require some changes to the cabinets as well as to the control board in order to provide that indication.

So that needs to be, it's a separate item, but that was not envisioned at the time.

MEMBER STETKAR: They do not aggregate them into a general trouble alarm train, you know, Channel 1, Train A, or something like a trouble alarm?

MR. CARTE: There is a trouble alarm but that puts you in half trip. And the decision was made -- and in fact all of these are wired that way. And all they have to do is remove a jumper and any of these would give them a half trip.

MEMBER STETKAR: But they don't do that.

MR. CARTE: But they don't want the half trip --

MEMBER STETKAR: Okay.

MR. CARTE: -- on a single test failure.

MEMBER STETKAR: Good to know. Thank you.

MR. CARTE: Okay, so single failure criteria. The boards were evaluated in a couple of different ways to ensure, basically to ensure that they had no undetectable failure modes. And as well as to ensure that the test circuitry would not compromise the main functional circuitry. That was done by a look at the drawings on the audit.

The quality was reviewed against the -- it was based mainly on engineering judgment against the underlying regulations as opposed to software development reg. guides.

The equipment qualification, we looked at what we believed to be the bounding envelope for all Westinghouse plants and compared their qualification environment to that bounding envelope. And I think there were a couple points that we noted that needed specific evaluations by specific plants. But in general we thought the equipment qualifications bounded all known installations. But it is still the applicant's responsibility to ensure that when they do the install the cards.

These cards can be installed one card only or you can replace an entire train.

The independence criteria was the same as the independence criteria of the previous cards. The isolation card performs that function. No circuit -- no CPLDs involved in that function.

The secure development operational environment was basically the cards have a CRC check number on them so they confirm the right version of software is installed on the cards at the time of manufacturing. In general, the plants don't have the ability to change that software. They don't have the tools. They don't have the equipment. So that is not changeable at the site.

In terms of diversity and defense in death, we use BTP 719 criteria to evaluate their testing. And we felt that they met the criteria for eliminating consideration of common cause failure because they had effectively analyzed all permutations and combinations of inputs. There were a few combinations associated with the reset of the safeguard driver function that were not explicitly tested. However, they were evaluated and determined not to impede the safety function.

I was trying to make up some time.

CHAIRMAN BROWN: No, you did fine.

MR. CARTE: Okay.

CHAIRMAN BROWN: And so I have a question.

MR. CARTE: Okay.

CHAIRMAN BROWN: The watchdog -- let me backtrack. Go to your -- where's the diagram.

MR. CARTE: This one or?

CHAIRMAN BROWN: Yes, that one. Okay, I'm on the wrong frame here. Come on. Windows 7.

In each of these you've got train A, train B.

MR. CARTE: Yes.

CHAIRMAN BROWN: And I guess there's a universal logic board --

MR. CARTE: There are several universal logic boards.

CHAIRMAN BROWN: Each train?

MR. CARTE: Yes.

CHAIRMAN BROWN: Okay. And there is a watchdog timer associated with those?

MR. CARTE: Yes.

CHAIRMAN BROWN: And you talked about the light illuminating. But one of the other things that was talked about in the device, it de-energizes the board interlock relay or something?

MR. CARTE: Right. There's an interlock -- okay, so the normal warnings that exist with the semi-automatic test board is that once you're in test or once you pull a card you effectively go into a half trip condition. And those, that's the indication or availability that exists in the cabinet today.

Those warnings for watchdog E10 alarm are wired into that signal but they're not active -- you can activate or deactivate that half trip based on a jumper on the board. And so, yes, the capability exists to generate a half trip based on those functions. I do not believe that it's implemented in the plant because it's undesirable.

CHAIRMAN BROWN: A half trip would mean --

MR. CARTE: Well, if you get a --

CHAIRMAN BROWN: I mean even one out of two is a half trip, is a trip.

MR. CARTE: Well, a half trip would be that, right, the fundamental requirement is that you have two trains operable. But you can have one train inoperable for a short period of time in order to do surveillance testing. In that mode you are basically almost tripped. And if you get another signal or another test action from the other train, you trip.

It's not that, it's not the, it's not the functional trip, it's more of a self-help trip. So if both trains indicate a health problem then you enter a tripped state. But it's not the functional trip state associated with --

CHAIRMAN BROWN: It's got to be found by a health evaluation.

MR. CARTE: Right.

CHAIRMAN BROWN: So if one of them's already got, if you converted the other train effective to a one out of one, or whatever tells it whether it's a health trip or whether it's a functional trip.

MR. CARTE: Right. They have that capability. And I don't believe that they are exercising that capability.

CHAIRMAN BROWN: Okay. I lost my other question.

MR. THORP: So the prior version of the SSPS cards was the same --

CHAIRMAN BROWN: No, I understand. You didn't change, functionally this is the same as when you were just all analog.

MR. THORP: Right.

MR. CARTE: Yes.

MEMBER SCHULTZ: Norbert, would --

CHAIRMAN BROWN: How --

MEMBER SCHULTZ: I'm sorry, Charley, go ahead.

CHAIRMAN BROWN: Just one more. How does the operator know that the -- you said it's a card edge LED that goes off.

MR. CARTE: Right.

CHAIRMAN BROWN: And I think you asked that question but I didn't get all of it.

MR. CARTE: Previously the old cards didn't have any card edge LEDs. And so these were basically added for the timely identification and repair criteria. The operator does not know unless they go to check, but basically they do functional testing on a six-month staggered basis. So they're in the cabinet every six months to do surveillance testing.

The active trip testing I think is also on a four-month schedule. So they're in there doing testing every four months.

So there is an opportunity at least at that point to check the LEDs. They could check them more frequently but that was not specifically addressed in the topical report.

CHAIRMAN BROWN: But it takes ten triggers to get the watchdog LED to trip?

MR. CARTE: Oh, no. There's several different LEDs. One is an E1, so you fail one test, it lights. So if you failed any test in the last six months you'll get that little light on.

CHAIRMAN BROWN: Okay, that's a test. So what about the watchdog? What about the watchdog?

MR. CARTE: Yes, because of the parallel nature of the CPLD, the watchdog essentially just confirms that those circuits are working. It --

CHAIRMAN BROWN: If it trips, what do you get? You get one light that lights up?

MR. CARTE: Yes.

CHAIRMAN BROWN: But you might not see it for six months? Or four months?

MR. THORP: I don't think it's --

MR. CARTE: Correct.

CHAIRMAN BROWN: It's only part --

MR. THORP: I don't know that we can predict exactly how the licensees are using these. We can probably try to find out but we don't know specifically how the operators -- like my experience is that our licensed operators would go down and examine into the cable spreading room to look at the RPS and S -- well, RPS is in the control room, but S class cabinets down in the cable spreading room and look for any indicators that there was some problem with any of the cards, any of them.

But that was viewed and viewable from the cabinet face. Now, I don't know whether it's a card edge --

MEMBER BLEY: If they're open cabinets.

MR. THORP: -- LEDs are something you would have to open the cabinet door and get in the back to see, in which case it would require --

CHAIRMAN BROWN: What it sounds like.

MR. THORP: -- a look by the instrumentation and controls engineers conducting their periodic maintenance examinations and tests. And how often those happen, it depends on the requirements that they're fulfilling, you now, for those surveillance tests and things like that. I wouldn't say that it was necessarily six months. I wouldn't say that it's a month. But it would depend on the licensee.

MR. CARTE: Right. Generally we know that their functional testing is about every six months. And so they're in their cabinet for that. And their trip breaker testing is every four months. So they're in the cabinet periodically, on those intervals at least.

MEMBER STETKAR: If they're closed cabinets, people don't like for you to touch them.

MR. CARTE: Right. Right.

MEMBER STETKAR: And they won't.

MR. CARTE: Right.

MEMBER STETKAR: If they happen to be open, open racks then it's pretty easy to tell somebody to go look at the light. But a lot of them aren't, aren't open racks.

MR. CARTE: Right.

MR. THORP: And I guess the point is that prior cards they didn't even have card edge LEDs to tell them anything.

MR. CARTE: Right.

CHAIRMAN BROWN: Well, they didn't have --

MR. THORP: CPLD.

CHAIRMAN BROWN: -- solid state. They didn't have CPLDs in them either. And right now the purpose of the watchdog timer according to the Westinghouse P.R. says it's there to supply a confidence level that both the main and test CPLDs are operational. And I just question --

MR. CARTE: Right.

CHAIRMAN BROWN: -- you're not going to know it.

MR. CARTE: Right. Well, one issue is that. And the other issue is that the problem is about parallel processing. In order to strobe that watchdog it goes through a subset of the circuits on the CPLD. All you're confirming is that that subset of circuits works, as well as a clock. You have to in order to check that's working you need a clock.

So you're not really confirming every function, you have to rely on the test CPLD which does all permutations and combinations to confirm the health of every function. And, yes, that only results in a card edge LED.

MEMBER BLEY: Are they different LEDs --

MR. CARTE: Yes.

MEMBER BLEY: -- or is it the same LEDs?

MR. CARTE: Different LEDs.

MEMBER STETKAR: Will the watchdog --

MEMBER BLEY: But nobody's watching them, so --

MR. CARTE: Yes.

MEMBER BLEY: -- doesn't matter.

CHAIRMAN BROWN: With the old analog system how often did somebody actually perform a functional test on a train? I don't know.

MR. CARTE: The functional testing

requirements has not changed. There was an intent originally and we did not review that. There was a desire to eliminate some of that functional testing based on the self-testing capability. And we did not review that. They did not ask for credit for that. No one to my knowledge has done that on the 5059.

CHAIRMAN BROWN: So under whatever administrative requirements there were to go perform --

MR. CARTE: Yes.

CHAIRMAN BROWN: -- the testing, that has stayed --

MR. CARTE: Yes.

CHAIRMAN BROWN: -- that has not changed with these.

MR. CARTE: Correct. That was not addressed by the topical report; right. And they can't change the tech specs without coming in for license amendment. So, yes.

CHAIRMAN BROWN: All right.

MR. HECHT: Can I ask a question about the SDOE comment you made? You said that they, that the cards will basically check the version of the software prior to running. And I was trying to understand which cards those would be here.

MR. CARTE: Right. So there are seven cards with CPLDs. Two of them have two CPLDs. So for each CPLD the version is checked and documented at the time of manufacturing. So you load the software, you then read back your CRC version of the software and then you can run through your complete functional test or manufacturing test of that card. And then it shows.

MR. HECHT: Oh, I see. So this is at the factory.

MR. CARTE: That's correct.

MR. HECHT: The software at the factory would read the cards.

MR. CARTE: Yes, load --

mR. HECHT: There is not run-time software at the plant when the cards are prepared.

MR. CARTE: Right. And these CPLDs are instant-on devices. So some, some devices you can load a data file at the power-up. These CPLDs have flash memory and they're loaded at the factory once and only once.

MR. HECHT: Okay.

MR. CARTE: Yes.

MR. HECHT: Yes, I'm sorry, that's what I thought and I didn't understand. Okay, I've got it.

MR. CARTE: So they load the software from a controlled file and that should be good enough.

MR. HECHT: But you could have processes with your load so you do a CRC check after you load it and then you do a full functional test so you know it loaded properly and you know it's working. And then it ships. And the licensee does not have the tools, unless they bought them separately, but they were not supplied with the product to make those changes, to make any changes.

MEMBER SCHULTZ: With regard to the 5059 implementation at Harris, was that considered to be an isolated instance or?

MR. CARTE: No.

MEMBER SCHULTZ: Did you go into the process with Westinghouse because something needed to be done with regard to appropriate implementation?

MR. THORP: Well, there was, there was -- it's an interesting question -- there were seven, I believe seven or eight other licensees who were in one stage or another of implementation of these cards. Some had not yet put any in. Some had only put a card in on one train. And I think that was the case of Shearon Harris, they put it in on one train, if I remember correctly.

MEMBER SCHULTZ: Well, yes, we don't need to go into detail. I think it's a good example.

MR. THORP: You know, the issue was it was useful, we thought the most useful thing rather than dealing with each plant individually, writing separate violations for each one and going through the whole "let's review your situation individually" --

MEMBER SCHULTZ: Right.

MR. THORP: -- would be, since they all are using the same product, to have the PWR Owners' Group and Westinghouse develop this topical report problem.

And that fixed the problem generically in combination with the development of what we call an enforcement guidance memorandum, an EGM. And we worked with the Office of Enforcement so that that provided a limited period and very specific criteria that needed to be met for a six-month time frame for those who were not -- were technically considered in violation but then would be able to satisfy the issue by conducting another 5059 evaluation referencing the topical report and the --

MEMBER SCHULTZ: And somewhat it's parallel with the topical submittal and so forth? In other words -- well, we don't have to get into that detail right now.

MR. THORP: We completed our review of the topical report before the EGM was issued. So that it was a sequential thing.

MEMBER SCHULTZ: Okay, I understand.

MR. THORP: So they, they had to hold and stand by. In one case a plant that had put these cards in had actually experienced a problem; it wasn't really related to the SSPS software or anything like that. But they pulled those cards, put back their old SSPS cards in place and then they held in place and waited for the outcome.

MEMBER SCHULTZ: Thank you.

CHAIRMAN BROWN: Okay. We will move on to Samir and the HFC-6000; correct? You gained a couple of minutes here thanks to Norbert.

MR. DARBALI: Yes. So good morning. My name is Samir Darbali. I am a clinical reviewer in the I&C Branch in NRR. I will be talking today about the HFC-6000 safety system platform.

Next slide.

This is a brief outline of what I'm going to be talking about.

Next slide.

So some background information. The HFC-6000 platform is a modular rack-mounted platform that is housed in cabinets and is intended to serve as a qualified generic digital I&C platform suitable for use in safety-related applications at nuclear power plants.

The platform was developed by HF Controls Corporation, or HFC, which is owned by Doosan Heavy Industries & Construction Company. The platform is based on product line developed by Forney Engineering which date back to the 1980s.

Possible applications and use of the HFC-6000 platform would include a reactor protection system, engineered safety features actuation safety functions, and a post-accident monitoring system.

Next slide.

This slide shows the components that are within the scope of the -- sorry about that.

So continuing on the background, the HFC-6000 topical report was submitted for review in March 2008. The technical review was contracted to Oak Ridge National Lab and NRC technical monitoring of the contract was performed by EICB.

The safety evaluation for the topical report was issued in April 2011 and included six generic open items related to equipment qualification testing.

Regarding operational history of the HFC-6000 platform, these systems are currently installed in 24 South Korean nuclear power plant units. However, none have been installed in U.S. nuclear power plants and currently there are no license amendment requests for installation in the U.S.

MEMBER STETKAR: Samir, I haven't looked at any of the data to get the acronym so I will call it the Korean 1400 new design certification. Is this system included in that, do you know?

MR. DARBALI: I don't have the specifics of which design is --

MEMBER STETKAR: I'm just trying to figure out how soon we might see it.

MEMBER BLEY: Yes, the reactors in Dubai? No, the Korean reactors; right?

MEMBER STETKAR: The Korean reactor has been submitted for design certification here.

MEMBER BLEY: Yes, for us. Yes. Yes.

MEMBER STETKAR: So I don't care about Dubai.

MEMBER REMPE: APR-1400.

MEMBER STETKAR: APR. Thanks.

MR. DARBALI: Right, I don't have any specifics on which design.

MR. THORP: I was kind of looking around, Charley, because I had seen Terry Jackson sitting back there before. But I think he's not here right now, so. I was going to ask him about it.

MEMBER STETKAR: I was just curious because it sounds like a comment from --

MR. HIRMANPOUR: Bob Hirmanpour with Southern. DCD got accepted for review recently but they haven't done Common Q at this time.

MEMBER STETKAR: Common Q.

MR. HIRMANPOUR: Platform independent.

MEMBER STETKAR: As far as the DCD is concerned?

MR. HIRMANPOUR: Yes.

MEMBER STETKAR: Okay, thank you.

MR. DARBALI: Okay. This slide shows components that are within the scope of the topical report. The HFC-6000 is a generic application framework platform for which final configuration is dependent on an application-specific design.

The platform is composed of microprocessor-based modules providing control, input, output and communication functionality. The base platform consists of an equipment chassis housing tool, redundant controllers, dual ported memory, input/output modules and power supplies.

For safety-related use, internal redundancy is provided as part of the base platform architecture through redundant controllers, redundant inter-channel connections, redundant bus links to input/output modules and redundant power supplies.

Listed in the table are the 15 components that are within the scope of this topical report. The main components we'll be addressing in this presentation are the SBC06 controller module and the EPM06 dual=ported memory module.

This slide identifies some of the areas which are out of the scope of the topical report, including the application software which is necessarily specific to a plant system.

The following slide will better show what is and what is not within the scope of the topical report.

So this is sort of a busy slide but it illustrates an example of a 4-channel safety system architecture based on the HFC-6000 platform. The green box you see there illustrates one HFC-6000 rack in a redundant controller configuration. And by redundant controller I mean you can see in there there are two controllers, two primary, there's a primary and a secondary controller. And we will discuss redundancy later.

MR. CARTE: They are identical though?

MR. DARBALI: They are identical, yes.

The red box identifies the scope of the topical report and illustrates how the HFC-6000 can be used to implement one redundancy in a parallel redundancy system architecture.

Intra-channel communications are included in the scope of the first topical report. However, inter-channel communications via the gateway controller are out of the scope of the approved topical report.

CHAIRMAN BROWN: Do you want to repeat that again? The intra-channel --

MR. DARBALI: Right.

CHAIRMAN BROWN: -- those are within?

MR. DARBALI: Correct.

CHAIRMAN BROWN: The inter-divisional communications are --

MR. DARBALI: Are out of the scope.

CHAIRMAN BROWN: -- are outside?

MR. DARBALI: Right.

MR. THORP: That would be application specific.

MR. DARBALI: Right.

CHAIRMAN BROWN: Yes, okay. I just wanted to make sure it sounded the same as what I read.

MR. DARBALI: Right.

MR. THORP: Yes.

MR. DARBALI: Also, peripheral and field devices like sensors, voting logic, actuators, human/machine interface displays, and control interfaces are out of the scope.

Regarding communication links, the platform provides a redundant intercommunication link bus which is the ICL bus between the input/output modules and the controller modules. And also provides intra-channel communication link, which is the C-link to the right of the controller modules. These communication links will be further explained in the following slides.

I mentioned earlier that the gateway controller, which is the blue box that allows for inter-channel communication is out of the scope. But HFC came with an amendment to the approved topical report which does include that channel gateway controller. Now we, we're in the process of performing an acceptance review on that amendment to the topical, so we haven't reviewed it yet.

Next slide.

So this slide focuses on the contents of the green box we saw in the previous slide. The main equipment chassis, which is the box on the top right, provides two slots for SBC06 controller modules and one slot for a dual-ported memory DPM06 module. This redundant controller assembly constitutes the base CPU module for the safety platform.

In the CPU module configuration, one SBC06 module acts as the primary or active controller and the other SBC06 module serves as secondary or standby controller. The main equipment chassis also has the capacity for a maximum of 11 input/output modules.

The expansion chassis, which you can see on the bottom right, has capacity for a maximum of 14 input/output modules. The chassis backplanes receive operating power from the power supply module, which you can see on the left. Your redundant power cables get attached to a connector on the back of the chassis. The 24-volt DC operating power and the 48-volt DC auxiliary power are routed to each module via redundant rails on the backplane.

CHAIRMAN BROWN: Question. Back on your previous slide --

MR. DARBALI: Yes.

CHAIRMAN BROWN: -- you show the green-dotted area.

MR. DARBALI: Right.

CHAIRMAN BROWN: And now flip over to the next page, page 8, and I show the green-dotted area.

MR. DARBALI: Right.

CHAIRMAN BROWN: Are those equivalent?

MR. DARBALI: Yes.

CHAIRMAN BROWN: One, the page 7, shows a primary and a secondary controller.

MR. DARBALI: Okay.

CHAIRMAN BROWN: And in page 8 it does not show --

MR. DARBALI: Yes.

MR. CARTE: Go to page 8.

MR. THORP: You see the little green boxes there, Charley?

CHAIRMAN BROWN: Oh, that's where it is?

MR. DARBALI: Right. So the green --

CHAIRMAN BROWN: It's located in the same chassis then?

MR. DARBALI: Right. So the previous slide was more synchriotic.

CHAIRMAN BROWN: I got it. Thank you very much.

MR. DARBALI: Okay. So right, so your green boxes are the SBC06 controller modules. And that --

CHAIRMAN BROWN: I got it.

MR. DARBALI: Okay. So going back to the

power module, each HFC-6000 module performs diode auctioneering of the redundant power as well as voltage level conversion to obtain the operating power needed for onboard hardware.

The CPU module communicates with the input/output modules via redundant serial ICL traces on the backplane. ICL communications are shown in the figure below and to the left of the SBC06 modules. So those are the red ICL. And that's a communication to and from the input/output modules.

Redundant ICL connectors on the rear of the backplane enable expansion of the ICL bus to local expansion chassis by twisted pair ICL cable or to remote expansion chassis through an optical repeater.

The safety communications link indicated in the figure above the SBC06 modules is the C-link communication which interconnects with safety controllers to enable broadcast of data and status information among safety controllers within the same channel. In the following slide we'll discuss more ICL and C-link communications.

So again in this image you can see the two SBC06 controllers. On top of those you can see the C-link communication that performs broadcast communication between the two redundant controllers.

Below you can see the ICL links that go from the input/output modules to the SBC06 controller modules.

The C-link is an Ethernet-based network employing a proprietary token-passing protocol to implement deterministic communications. The C-link provides a path for the transmission of data and information among SBC06 controllers within a channel.

And there's a separate subordinate processor within the controller module that serves to process these signals and buffer the main processor from communications.

The ICL, which is the one below and connects between the input/output modules to the controller modules is a serial bus used to interconnect these modules. This communication is accomplished using a master/slave polling protocol so only the controller can initiate communications. And that's also a separate processor that handles ICL communications.

Next slide.

MR. HECHT: Can I ask a question?

MR. DARBALI: Yes.

MR. HECHT: If you have the C-link why do you need the dual-ported memory?

MR. DARBALI: Right, and we'll talk about that. But basically the two controllers are redundant but only one acts as primary. The second one is secondary standby. So the dual-core memory has a CPLD chip that handles the failover transition.

So all of the data that the primary controller has is being passed to the secondary controller through the dual-ported memory.

MR. HECHT: Okay, so that's where the state data is kept?

MR. DARBALI: Right.

MR. HECHT: If you will.

MR. DARBALI: Right.

MR. HECHT: So why can't you -- why didn't they do that over the C-link? Or what does the C-link do -- I'll ask it the right way. What does the C-link do that the dual-ported memory does not do?

MR. DARBALI: It provides broadcast data between the two controllers. But it does not handle the failover mechanism.

CHAIRMAN BROWN: Just between primary and secondary.

MR. DARBALI: Right.

MR. THORP: It's information sharing but not, not --

MR. DARBALI: Right.

MR. THORP: -- information actuation in

terms of having the secondary replace the primary if there's a failure on the primary.

MR. HECHT: But doesn't the dual-ported memory provide that information sharing function?

MR. DARBALI: Well, okay, it does but if you go back to your, to the big diagram that talks about the scope. Okay, so yes, the dual-ported memory handles communication between the two controllers. If you look at the blue box that says Channel A gateway controller, that also has a node to the C-link.

So if you were going to do inter-channel communications you would have to use the C-link as well through that gateway controller.

MR. HECHT: Okay, so it's the same information that's going to the C-link as in the dual-ported memory? Maybe I'm not -- maybe it's not --

MR. CARTE: No, I think the issue is that it's a bandwidth issue. So if you think about the dual-port memory is there to allow failover, bumpless transfer failovers, so in that sense the state of the primary controller needs to be reflected in dual-port memory. And to maintain that state you have a lot of communication that's going on. If all that communication was happening on the C-link you wouldn't get, you wouldn't be able to communicate any other information on the C-link because you would be using up all your bandwidth.

So I think that it's probably an architectural issue.

MR. THORP: So that's what is maintaining that tracking function. And that eats up a lot of information --

MR. CARTE: That would eat up all the C-link bandwidth. And it's used in that base so you have timing issues with that.

MR. HECHT: Thank you.

MR. DARBALI: So we're in slide 10.

So this drawing shows the processors and complex programmable logic devices for CPLDs that are part of the SBC06 controller module. So as you can see, the SBC06 module has three processors and four CPLDs. The dual-ported memory, which is the orange box on the bottom, has one CPLD.

The SYS or system processor, which is the top-left box, processes -- monitors overall status of the controller module, services watchdog timers and executes the application program code.

The ICL processor handles communication on the ICL to obtain field data from and send operational commands to the input/output modules.

And the C-link processor is responsible for regulating messages sent over the C-link.

And other functions that are performed by the CPLDs is, for example, in the dual-ported memory it manages failover mechanism. And in the controller module, one of the CPLDs handles shared memory, which you can see better in the next slide.

CHAIRMAN BROWN: They're still using 386's?

MR. DARBALI: Yes.

Okay, so this slide shows you can see on the top-right it's what you would see as the modules. And in their redundant configuration you would have another SBC06 controller to your right. And on the SBC06 controller, the blue highlight is the architecture related to the system processor.

On the top-left you see the architecture related to the C-link processor. And on the bottom left you see the red highlight which is the ICL processor architecture.

There is a shared portion in the middle that's overlapped by all three, and that's a public memory that's shared between all of them. And access to that memory is controlled by that access controlled CPLD.

CHAIRMAN BROWN: That's still within one

platform, all of one division, whatever you want to call it?

MR. DARBALI: That's all within one SBC06 controller.

CHAIRMAN BROWN: Okay.

MR. DARBALI: So you would have the same architecture on all of them.

CHAIRMAN BROWN: That's a shared resource is what -- the public thing is a shared resource then?

MR. DARBALI: Yes. It's shared between all three processors. However, all three processors have their own private memory that's not shared. And the system processor is the only one that handles the application-specific code.

CHAIRMAN BROWN: Okay. Thank you.

MR. DARBALI: Next slide.

So in this slide you can see better the two redundant controllers and the dual-ported memory card in the middle. And so the -- it's a bit complicated, and that's why I highlighted the lines that go into the dual-ported memory. But what happens is the system processor strobes the watchdog timer. And when it -- and that sends what is called a sanity signal.

Once it fails to strobe the watchdog timer it times out. It sends a not sane -- I'll try, an insane signal to the failover CPLD. And then there's a sanity CPLD on the controller. Once the watchdog timer times out there's going to be a flag and that no longer is going to be your primary controller.

So you're going to have bumpless transfer to the second controller and then that primary or PRI signal coming from the main controller, that's the yellow highlight, that's going to be false. So it provides the logic to transfer primary control of the controller.

MR. HECHT: Does that mean that there's a single point of failure here?

MR. DARBALI: What do you mean?

MR. HECHT: Okay. I would see two. And maybe this is a not a design review but maybe I would just ask if you considered that? Two cases of controller B spuriously wants to take over and what prevents it from doing that?

And then case two, controller A has failed but sanity CPLD doesn't want to let go?

MR. DARBALI: Well, control -- when you initialize both controllers, the first one to strobe the watchdog timer is going to take the primary. The secondary is not going to ask to become primary.

MR. HECHT: All right, fair enough.

MR. DARBALI: As far as the sanity CPLD failing --

MR. THORP: Well, the acute failure is essentially in that controller; right?

MR. CARTE: Right.

MR. THORP: You'd have a problem with a controller and then you'd have a problem with the sanity side, so.

MR. CARTE: You've got to put this in context. This is one rack, one redundancy equipment.

MR. THORP: Right.

MR. CARTE: The rack is not designed to be single failure proof. This design is for high reliability bumpless transfer. It's not, it does not address the single failure criterion.

So there may be more than one possibility, and that's perfectly allowed for a single failure that disables this rack. And so it's -- reliability issue is not single failure criteria that is being addressed.

MR. THORP: Okay.

MEMBER STETKAR: Well, single failure criterion in the sense of plant application.

MR. CARTE: Yes. Right.

MEMBER STETKAR: But not in the sense of this architecture.

MR. CARTE: I've heard the term single vulnerabil -- single point vulnerability to be more accurate.

CHAIRMAN BROWN: Well, if you go back to slide 7, there is within one channel of four there are two of these --

MR. DARBALI: Right.

CHAIRMAN BROWN: -- units. So that if the upper one within the green box turns to stone, I have no idea what the second one is doing because we haven't talked about it.

MEMBER STETKAR: Those two are the, those could be the function --

CHAIRMAN BROWN: Well, that's not what it looks like. It's got the same sensors, the same outputs and all of that.

MEMBER STETKAR: One could be a reactor clip, the other could be a safeguard.

MR. DARBALI: Right.

MEMBER STETKAR: So that's different.

MR. DARBALI: It's design specific.

CHAIRMAN BROWN: I understand that. But I'm just saying there is --

MR. DARBALI: Right.

CHAIRMAN BROWN: -- there are two of these redundant. There's redundant within one thing and then there is another pair of redundant.

MEMBER STETKAR: The bottom, outside of the green box in my interpretation is not redundant. Inside the green box --

CHAIRMAN BROWN: But it didn't say that in the report explicitly so I didn't read that.

MR. DARBALI: Right. What the report covered was communication between HFC-6000 racks within the same channel which would be also through this C-link. So that's another thing the C-link does.

But it doesn't say if it's going to be a redundant to the first iteration, first rack, or if it's going to be a separate function.

MEMBER STETKAR: It could be. I mean people have done -- it's a functional redundancy like low pressure versus, you know, high temperature or something like that. But that's, that's application specific; right?

The whole point is the channel A can be failed and still -- you know, that's the single failure.

CHAIRMAN BROWN: Well, I understand the point about the bottom part could be processing other functions, okay, and sending it out to whatever the topical report voting logic is for whatever controls you need.

MR. THORP: Reliability redundancy is between those two controllers --

CHAIRMAN BROWN: Yes. I got that.

MR. THORP: -- inside the green box.

MEMBER STETKAR: The single channel failure, the single failure in the sense of plant applications is out in channel 8 blue box, if you will.

MR. THORP: The single channel failure is the red box. So typically you have one battery-backed power for each channel, for instance; right? So you could lose power and lose all of these racks in that channel and that's your single failure. And then they have dual redundant power supplies, but that's the concept of a channel, that that whole box is vulnerable to single failures.

CHAIRMAN BROWN: The red box.

MR. THORP: Yes. The red box.

MEMBER STETKAR: The single failure box.

CHAIRMAN BROWN: We got that. But if you go up into the just the green, you can go back to that little, what is it, slide 12, and you have the way your report, it's not your report but that's your report, in the topical report, the control array goes, you know, the sanity check fails, fails overflow channel there to the controller B. Shut off controller B. Then it just stops.

MR. DARBALI: Right.

CHAIRMAN BROWN: Everything stops.

MR. DARBALI: Right.

CHAIRMAN BROWN: It didn't really define what "stops" means in any great detail, just other than it stops.

MR. DARBALI: Right.

CHAIRMAN BROWN: And so that's still open.

MR. DARBALI: Right.

CHAIRMAN BROWN: It's an open issue when you get to application --

MR. DARBALI: Right.

CHAIRMAN BROWN: -- specific stuff. I just, I was just trying to make that point.

MR. DARBALI: Right.

CHAIRMAN BROWN: That comment.

MR. DARBALI: The only thing it does say that if you have one of the two controllers fail, because the system allows you to do the maintenance failover if you wanted to work or take out your controller A module then you would do a maintenance failover to controller B. If one fails you get an LED light on your dual-ported memory module, you can't do that. You can't do a maintenance failover if one module fails.

MR. THORP: The system has to be healthy in order to try to exercise one for maintenance or testing.

CHAIRMAN BROWN: Yes, but it also says if you get a fail on the second one that the whole, the whole string just stops.

MR. THORP: It fails, yes.

CHAIRMAN BROWN: It didn't really -- But I just wanted to make sure I understood that point.

Okay, go ahead.

MR. DARBALI: Okay. Next slide.

So this slide highlights the cycle of operation of the SYS or system processor. So you can see there the cycles are set at 100 milliseconds. And it has eight tasks numbered zero through seven where zero, task zero through six are diagnostics and they take the first 10 milliseconds of the cycle. So you have about 90 milliseconds to run your last task, task seven, which is the application program.

Now, the -- Go ahead.

CHAIRMAN BROWN: That's interesting you say that because on page 118 of the report it talks about application loading can only operate up until 50 percent --

MR. DARBALI: Right.

CHAIRMAN BROWN: -- of the total process.

MR. DARBALI: Yes.

CHAIRMAN BROWN: Not 70 -- not 90 percent.

MR. DARBALI: Right. So you have, you have 90 percent --

CHAIRMAN BROWN: I mean this is a highly event-driven interrupt system, highly interrupt. It's got event-driven interrupts in it. And you've got, you've got limitations on the application code in terms of the application being --

MR. DARBALI: Right.

CHAIRMAN BROWN: -- able to be loaded into your processing time in order to meet these.

MR. DARBALI: Right. So you have 100 milliseconds. Ten are taken over by your diagnostics, and then you have 90 milliseconds to run your program once from start to finish. Once that's done it's going to keep running your application program until the end of the cycle.

So --

CHAIRMAN BROWN: What defines a cycle then, not the 100 milliseconds?

MR. DARBALI: Yes. So it, let's say, takes you 10 milliseconds for your diagnostics, it takes you 20 milliseconds to do your application task, you're going to keep running that 20 millisecond application task until the end of the cycle.

The 50 percent of the remaining 90 percent is an application-specific action item that's to guarantee you're running your application at least once completely.

CHAIRMAN BROWN: Every 100 milliseconds.

MR. DARBALI: Every 100 milliseconds. You need to allocate -- that application has to be 50 percent of the 90 milliseconds.

MEMBER BLEY: No more.

CHAIRMAN BROWN: No more than 55 milliseconds.

MR. DARBALI: Right.

MR. THORP: In other words no more than 45 milliseconds.

MR. DARBALI: Right.

MR. THORP: Otherwise it wouldn't be able to run its task necessarily on time --

MR. DARBALI: Right. So if --

MR. THORP: -- full through.

MR. DARBALI: So if it's 70 milliseconds and you run it once, the second time you run it, you start it, it gets paused. When you go to your next cycle you continue it but you're not running the full one. So you need it to be under 50 milliseconds -- or under 50 --

CHAIRMAN BROWN: Percent.

MR. DARBALI: -- percent of the remaining time for it to run at least once completely. And then you can run it and pause it, go to the next cycle, continue.

CHAIRMAN BROWN: But you're -- okay, let me, let me rephrase. If say you're application code ran 60 milliseconds, that would mean you would go 10 with the diagnostic.

MR. DARBALI: Right.

CHAIRMAN BROWN: Sixty for the one complete running through it, all functions.

MR. DARBALI: Right.

CHAIRMAN BROWN: You'd have 30 milliseconds into the leftover. It would start its application again but then it would stop, it goes into the next one, goes through 10 milliseconds of diagnostics, then starts someplace?

MR. DARBALI: Right.

CHAIRMAN BROWN: Where? At the end of the 30 milliseconds?

MR. DARBALI: Right. It starts at the end of where you left off.

CHAIRMAN BROWN: There was another comment in here about the interrupt-driven part where it says there's a contact switch --

MR. DARBALI: Right.

CHAIRMAN BROWN: -- which if that gets triggered then what it does, it stops everything and re-starts the task control at the beginning of the sequence, not wherever it left off. That was on page 117 of something. I think it was the SE. You all were very detailed in your description.

MR. THORP: And while Samir is looking at that, I will, I will inform the group that he's had to work harder than anybody here on this, in his efforts --

CHAIRMAN BROWN: I can understand that.

MR. THORP: -- because he didn't actually do the original evaluation of this. He's been doing homework to try to catch up on what was, what was approved before, so.

CHAIRMAN BROWN: Yes, we don't need to go resolve that. I'm just pointing out that --

MR. DARBALI: Right.

MR. THORP: No.

CHAIRMAN BROWN: -- I'm just bringing a number of issues that -- no, not issues, principles that have been stated in some of the past --

MR. DARBALI: Right.

CHAIRMAN BROWN: -- past design reviews is that, number one, you wanted to avoid event-driven interrupts.

MR. DARBALI: Right.

CHAIRMAN BROWN: You wanted to avoid interrupts other than maybe there are some, there are good interrupts. You have to have some interrupts, some time-based interrupts to do some things.

MR. DARBALI: My understanding is when the topical reports talks about a contact switch it's the cycle. And the interrupt is not mentioned, from what I remember for this SYS processor, it's not mentioned as event-driven but time-based.

MR. THORP: Right.

MR. DARBALI: So the 100 milliseconds, or whatever your cycle is going to be, you have an event-based interrupt. That's going to stop your application from running, it's going to start again, and it's going to continue the next cycle.

MEMBER REMPE: It's a cycle.

MR. THORP: It's a cycle time interrupt, not really an event, but something else happened that interrupts it.

MR. DARBALI: Right. There are

input/output modules that have event-based interrupts. But that's a separate one.

Again, if I can remember correctly, the contact switch is the cycle time and it's an event-based interrupt.

CHAIRMAN BROWN: Well, we went through this on the Common Q platform which has had a loading requirement in its topical report for the Common Q processor method. And we actually, they actually ended up running a test to verify that it would complete its -- if you exceeded the 70 percent loading requirement will it still work, or would it really work even within the 70 percent as it hadn't been done. And they, they came up with a test to do that. So I'm just identifying this as an issue, a downstream issue when we ever get to a specific application.

MR. DARBALI: Right.

CHAIRMAN BROWN: Which will probably have to be resolved when it was, in my estimation, if it ever came to fruition while I'm still alive.

Samir, we can go on, okay. I just wanted to bring it because that was a point that I noticed going through this.

MR. DARBALI: I have a paragraph from the topical. I just didn't know exactly from where but I can find out. But it says, "The HFC-6000 operating system uses the time-based interrupt from the realtime clock to trigger a contact switch. The contact switch results in suspension of the continuous loop execution of the application task to restart the task control sequence from the beginning. After the short interval to accomplish the execution of the utility task and any time-based routine, application task execution is resumed at the point of interruption."

CHAIRMAN BROWN: My point being, yes, the point being is you stop, you're in the middle of processing a trip.

MR. DARBALI: Yes.

CHAIRMAN BROWN: The time-based then comes through and stops the process.

MR. DARBALI: Right.

CHAIRMAN BROWN: Not a good idea.

Then it goes and does all this other stuff that it's supposed to be doing in this little thing. And then it says, Aha, I've got to come back and finish my reactor trip calculation and whether it's really a trip or not.

MR. THORP: This is this design. I don't know that we can conclude here in this forum that it's not a good idea.

CHAIRMAN BROWN: I agree with you.

MR. THORP: Right.

CHAIRMAN BROWN: I'm just saying it's an issue. I'm just putting it on the table for downstream if we ever get around to doing it.

MR. THORP: A question to pursue.

CHAIRMAN BROWN: We would like to pursue that.

MR. THORP: Okay.

CHAIRMAN BROWN: That's if we ever get there. That's all.

MR. THORP: Thank you, Charley.

CHAIRMAN BROWN: So we ought to keep on moving here.

MR. DARBALI: Okay. Well, a key thing on this one that if the application task, that task seven is not completely performed from start to beginning at least once per cycle you do get a flag and a false identification.

Next slide.

MEMBER BLEY: Is that a permanent thing, the flag and the false indication? Or is that like the last one we were talking about where we get an LED --

MR. DARBALI: If it goes off.

MEMBER BLEY: -- on the card somewhere?

MR. DARBALI: I'd have to go back and check.

CHAIRMAN BROWN: If there's a way to resolve these, if you go back and you do a platform reset, I mean you can go back and reinitialize and restart depending on how long it takes to do it. I mean if it takes 10 minutes to do it like it does on some platforms, then that's a problem. But if it takes 30 microseconds, that's a different problem. It just -- anyway.

MR. DARBALI: Okay. So this slide lists some of the predictability and repeatability features of the design, deterministic behavior supported by design measures such as sequential execution of tasks, continuous loop execution of the application function, regular schedule for time-based routines, diagnostics that confirm the execution of the safety function, and deterministic communications with preconfigured architecture.

Also, the SYS or system processor, which serves as the safety processor, is buffered from communication transactions through the use of interposing communications processors, or the ICL and C-link processors.

MEMBER SCHULTZ: So, Samir, is this, is this a representation of the conclusions that were drawn from the -- in the SER from the review of these criteria?

MR. DARBALI: It's part of it, yes.

MEMBER SCHULTZ: Part of it.

MR. DARBALI: Yes.

MEMBER SCHULTZ: I just wanted to understand what, because there is a time difference here between what we've heard this morning earlier about the review and the review criteria and then what presents here in summary fashion. You've drawn some information from the SER --

MR. DARBALI: Right.

MEMBER SCHULTZ: -- in here as an example --

MR. DARBALI: Right. There's a lot of --

MEMBER SCHULTZ: -- of what is being used.

MR. DARBALI: -- proprietary information in the determinism portion of the safety evaluation.

MEMBER SCHULTZ: That, there's that aspect too. Thank you.

MR. HECHT: Can I ask a question? This is a method, a process issue and your, and how you do things as opposed to Charley's question. But given the fact that there is some non-deterministic aspect of what happens when a task is interrupted by the time tick, how do you treat that?

MR. DARBALI: I believe the safety

evaluation concluded that to be deterministic.

CHAIRMAN BROWN: There was a statement in one of the pages where they evaluated these, each of these little factors and then they made, drew a conclusion. I'd have to go back and find that particular part of it. It was very complete so it was a good, good discussion.

MR. THORP: Because it was cyclical and based on time, it was deterministic.

CHAIRMAN BROWN: Right.

MR. HECHT: It was cyclical and based on time but if there was an interruption of the last link task, it seemed to, seemed to be resumed rather than terminated, which would indicate that resumption could happen anywhere within that last task.

MR. THORP: We would have to get into the design to talk about the way it pauses and how it resumes right where it left off. And I don't know that we can do it.

CHAIRMAN BROWN: No, we -- yes, I agree. I mean I agree the point is along the lines I was talking about.

I just think I just wanted to get these points of the design out so that we could cover them when we come around at some other time if this comes up as part of our application. And you all have got right now a design of something docketed which I guess we are going to be looking at at some point in the future maybe. Maybe.

So I think we need to go ahead and roll on. Thank you.

MR. DARBALI: Okay, next slide.

This slide lists some of the SDOE features that are part of the design. For example, any firmware change requires physical replacement of the PROMs. And application software for the module can be installed via PROM replacement or download to dedicated flash memory. But either of these modification processes for application software are intended to occur while the module is out of service or out of the cabinet.

MEMBER SCHULTZ: Samir, with the SPINLINE discussion we had earlier there was a -- the audit that John described related to a secure development environment. Any indication that that was done here? Or was it at a time when the conclusion that, oh, it was burned in and can't be altered in the field was sufficient?

MR. DARBALI: Well --

MEMBER SCHULTZ: Things have changed in the last three or four years of that.

MR. THORP: Think about the time frame of the review that was done on those.

MEMBER SCHULTZ: Yes.

MS. ALVARADO: I don't think they did an audit.

MEMBER SCHULTZ: Whether they did an audit or not I don't know.

MR. DARBALI: No, I think there was an audit. But again, Oak Ridge National Lab was the reviewer.

MR. THORP: Yes, so it might be something we can find out for you.

MEMBER SCHULTZ: I wanted to understand if we were maintaining a consistent review going forward in some fashion. I mean we don't have any applications here but it might be something to consider when it's related to this design.

MR. DARBALI: Section 3.6 of the safety evaluation to the topical report addresses secure development.

MEMBER SCHULTZ: Okay.

MR. DARBALI: And it's quite a few pages on that.

MEMBER SCHULTZ: All right.

MR. DARBALI: So I think that what I pointed out here covers more of the secure operational environment.

MEMBER SCHULTZ: Understood.

MR. DARBALI: But on the secure development there is, there is discussion on that.

MEMBER SCHULTZ: Thank you.

MR. DARBALI: The final slide.

So after NRC approval of the, review and approval of the topical report, HFC came with two amendments. If you recall, the original NRC safety evaluation had six generic open items related to equipment qualification. HFC came back with an amendment that addressed those items. And the final safety evaluation for that amendment was issued this week actually.

And there is a second amendment that the staff is performing an acceptance review currently. And that addresses new modules that HFC would like to incorporate into their design. Some of the modules are changing because of obsolescence. And, for example, the main SBC06 module that we have been talking about, those four CPLDs are being replaced now with one FPGA.

So the staff is currently performing the acceptance review for this amendment.

CHAIRMAN BROWN: Is that it? Any questions leftover here?

(No response.)

CHAIRMAN BROWN: Okay, we will turn it back to Norbert to rescue the time line for the NUPAC.

MR. CARTE: Okay. So this is an application that is currently under review. So we'll go through the same structure: a little background, a little description, and discussion of review criterion.

So the background on this topical report is that it was originally docketed in 2011. It, due to other workload requirements we didn't start reviewing that until 2012 where we did the acceptance review that was issued in May of 2012. We issued the RAIs in May of 2013.

In 2014 the review was suspended to work on other higher priority items. Since there is no applicant associated with this topical report it falls to the bottom of the food chain.

In September of 2014 Palo Verde docketed a letter intending to use this application. And we will see how that develops. And they said they wanted to start doing that in 2016. So that might give us a greater sense of urgency.

So we recently just completed the first audit. And we anticipate there should be another audit in September or the fall. And we hope to have the final

SE issued by June, depending on the timing of the docketed information. We may get documents as late as December of this year. And so that might be a little bit aggressive depending on how much we get in December.

So in terms of a high level description, this is an application framework. So it is a set of parts and concepts about how you use those parts. It does not have a microprocessor or any emulation thereof. There is no system-specific design associated with this.

It does have a digital communication mechanism. And we are looking at that mechanism. It does not address diversity and defense in depth; in other words they're not trying to claim 100 percent testing or inherent diversity.

It does not address electrical isolation so it was stated that they intend to use, if needed, fiber optics isolation modules, whatever is acceptable for electrical isolation outside the cabinet.

It also at this time does not include the power supplies for the racks.

The description of the topical report consists of three main items as three primary bullets: a chassis and backplane, and in that chassis is where the power supplies would be mounted; a generic logic module which is really a card assembly. It consists of two types of things, a logic mezzanine as well as I/O cards. It can hold up to eight I/O cards of six different types; as well as a real transition module.

So when I display that this is what it -- the three pieces that we talked about: the rack and backplane, the generic logic module, which is an assembly. We'll get into that more later. As well as the real transition module for connecting the field inputs into the chassis.

So let me back up just for a second. So one of the things that you need about a FPGA design like this is that it is possible to implement a reactor trip function on one generic logic module card.

Some functions require a larger number of inputs and would require multiple cards. But you could go to a function by function implementation by card so that, therefore, if you have a problem you could remove one card and not impact the other functions, which is similar to the analog systems today. So it has that potential, although that isn't -- this is an application framework and the specifics would depend on the application.

So in this description of this card you basically see the pieces and parts on the left and the assembly on the right, which means so there's a carrier card which is a card that has sets of slots on it that you can plug in other cards to. The cards plug in horizontally and are called mezzanine cards for that reason, rather than perpendicularly.

So this is what it looks like. The carrier card that was on the previous slide, typical mezzanine cards. You see the connectors that connect into their location. The top card populated with a chip.

In terms of the logic card there are -- there is a core logic which basically does the built-in test and communication functions as well as an application-specific logic which will implement the application program.

You put this stuff together and you get a generic logic module.

So in terms of what happens on this logic module, it supports various forms of unidirectional communication. So in the backplane each card has different infrastructure associated with eight one-way outputs and eight one-way inputs into the backplane. So this allows for communication to other cards in the rack. It also has some non-volatile memory on the card, but this non-volatile memory is protected by a physical disconnect of a write protect which is carried to outside the card through the backplane.

As we can see, on the card it has a core FPGA. This core FPGA is used to communicate to the other cards through the backplane or to the I/O cards. And those I/O cards can then get communicated external to the cabinet through the rear transition module.

There's also an application-specific FPGA which right now they built a test specimen in order to do their qualification testing. They haven't completed their qualification testing yet. But that's just so that they could do some E-cubed testing basically.

So this is an other logical depiction of that. Basically the point here is that the logic mezzanine communicates with the I/O cards. The I/O cards then feed through the midplane or backplane to the rear transmission -- transition module and out to the field to the field wiring.

So, okay, then we talk about criteria. So in terms of independence, the only criteria we can evaluate right now for independence is the serial communication through the communications card. And that's an RS-422 card. And the communication mechanism implemented at the application level is at a byte level so that it's a start bit, a stop bit, a parity bit. And each byte communicated is confirmed at that level.

The message level communication will be configured in the application. And there will have to be appropriate schemes in the application such as CRC checks of the message content, serial or sequence numbers on the message so that you can tell if a message is repeated as opposed to not incrementing.

So what happens on these highly parallel systems is you rely on built-in tests to a much greater degree than you do on microprocessor-based systems. Most microprocessors today have implemented some self-testing on the chip itself. And many microprocessors raise a flag to the outside of the chip once they fail their internal tests and have decided to halt. So that's one form of testing that's done on a microprocessor.

Operating systems and applications programs can do other forms of checks such as memory checks. But in general we don't talk about those built-in tests because we sort of, I guess, assume they work and are not really crediting them. And some people credit watchdog timers to be strobed as a form of a health monitoring.

The problem with highly parallel systems is that unless you figure out a way to route that watchdog signal through every circuit on that parallel system it doesn't confirm everything. So a strict reliance on the watchdog is not -- doesn't give you much and you have to build in self-testing features to actually confirm the functionality that's in place. And so there's a greater reliance on the self-test.

For instance, on the CPLD card that we discussed previously there was a separate self-test CPLD that queried everything, every function on the main CPLD. And there will be some need to do that. The exact scheme to do that at the application level is going to application specific. And we have not really gotten into the review of that yet for the core FPGA.

Well, what we do know at this point is that they will be using a state machine. So if you read the literature on what you do with FPGAs there's a couple generally-accepted approaches, and these tend to be in not redundant architectures but they would be in single architectures. One is a triple modular redundancy: you implement everything on the FPGA three times and then you vote the output. That's not the approach that they're using here.

The other option is to do a state machine and have built-in tests associated with assuring that you're in the right state.

So different processes are developed. Different state machines, there's various state machines implemented on the chip to implement processes. Some of those processes are independent. So if you find a fault on that particular state machine you can reset just that process and not affect the other processes. Some processes are interconnected and so you would need to re -- if you found a fault in one of those state processes you would need to restart all the associated processes.

And then in the worst case, you could envision a condition where you would have to restart or reset the whole FPGA itself.

Those aspects, that's the general concept of how this issue is handled in the industry. And if you read the write-up on FPGAs they're trying to address single-event upsets, but it could address other types of problems. That's what we're thinking. We're not very far along in that review but we are focused on the built-in tests to assure that the continued operability of the system.

And in terms of severe development operational environment, basically it will be a one-for-one correspondence check. So there's nothing in this system that was not in the design document, and nothing in the design documentation that's not in the system.

I guess that was a quick blow-through of that argument. Any questions?

CHAIRMAN BROWN: Only one. Your early slide you said this is microprocessor based -- no, it's FPGA based. No microprocessor or emulation thereof; does that mean it's not fuzzy?

(Laughter.)

MR. CARTE: So one choice would be to implement a microprocessor. They have explicitly stated that they are not going to do that, yes.

CHAIRMAN BROWN: Yes, okay. So this is a non-fuzzy application --

MR. CARTE: Trying not to use that.

CHAIRMAN BROWN: -- with all of its other r--

MR. CARTE: Trying not to use that word anymore.

CHAIRMAN BROWN: All right.

MR. HECHT: Can I ask a question?

CHAIRMAN BROWN: Depends on how long the question's going to take. You've got 37 microseconds.

MR. HECHT: Okay. This is a fairly complex design when you come down to state, the solid state machines itself if you've got things like shift registers and memories and lots of other things. Yet they're talking about what do you do about that with respect to how you assess the completeness of the verification, particularly when they do their testing. I mean they can't test for all the states internal to this ASEP -- not the ASEP, the FPGAs.

MR. CARTE: Right. I think their approach is basically they do what everybody in the industry does for FPGAs, they do simulation in design life cycle. And in fact on top of the standard industry is a random analysis technique used for FPGA. They slapped on top the whole D&D process. So that's a completely independent process that goes through and assesses it after the design team is done.

So they're doing more than is typical but they're doing everything that is typical, typically done. And, yes, we haven't gotten any details but that's my level of understanding and that's what we'll be looking into.

MR. HECHT: Okay.

CHAIRMAN BROWN: Okay, first object here is to check whether anybody in the local public arena here would like to make an observation or a comment? You have 39 microseconds.

MEMBER BLEY: And he gets cycle three-plus.

MR. HIRMANPOUR: So staff mentioned that --

CHAIRMAN BROWN: Just identify yourself again.

MR. HIRMANPOUR: This is Bob Hirmanpour with Southern Company. Staff mentioned I have less reliance on the watchdog timer for FPG application with the technology time frames of the design change. I have a question, as far as the staff position and the requirement for having the watchdog timer and is it acceptable to have no watchdog timer for FPGA is the diagnostic and other handling routines are robust enough? Thank you.

MR. CARTE: Well, that is an evaluation that will be made by the staff on a case by case basis. You have to demonstrate predictability and reliability -- repeatability and reliability. If you can do that there is currently no explicit regulatory requirement for a watchdog timer. There are requirements for predictability and repeatability.

MR. HIRMANPOUR: Thank you.

CHAIRMAN BROWN: Hearing no more from the public is there anyone on the phone line? Can you say hello? Just me know that the phone line is on if you're out there by saying something. I'll give you another millisecond.

MR. BROWN: The bridge is open.

CHAIRMAN BROWN: Thank you. That's Theron.

All right, hearing nothing we'll close the bridge line. We'll go around the table to see if there's any comments from the members.

Joy?

MEMBER REMPE: I just want to thank everyone for their presentations and time. It's a learning experience.

CHAIRMAN BROWN: Ron?

MEMBER BALLINGER: No. Thank you for the presentations.

CHAIRMAN BROWN: John?

MEMBER STETKAR: No. And, again, thanks. This was part of the morning people who sort of precipitated this. And I really appreciate the effort that you folks put into this. I think it was you crammed a lot of information into three-and-a-half hours.

MR. THORP: Thanks, John.

MEMBER SCHULTZ: We really do appreciate it.

MR. THORP: We were meeting your objectives for --

MEMBER SCHULTZ: Yes. Oh, yes, yes.

MR. THORP: -- for this effort.

CHAIRMAN BROWN: Dennis?

MEMBER BLEY: No additional comments. But thanks, it was informative.

CHAIRMAN BROWN: Steve?

MEMBER SCHULTZ: I agree with John. A very complex issue to describe in a short period of time. And at first I was concerned that you took so much in such a time span of pieces to put together here. But the puzzle fit together very nicely and you demonstrated what you've done in the past and how you're doing things today. It did come together very, very well. And appreciate all the work that was put into the development of the presentations. And they were well delivered.

Thank you.

CHAIRMAN BROWN: Myron, do you have any other observations?

MR. HECHT: No. Just in general I was glad to see that there's a recognition that when you put in an FPGA you don't get rid of the problems that you normally associate with the sequential execution software. That was recognized.

And the other thing is that I'm glad to see that there is recognition of the fact that there are some differences in the development process between FPGAs and software which are being recognized. And I would imagine that the staff is capable and competent to handle that.

MR. THORP: Thank you, Myron.

CHAIRMAN BROWN: I had I'm not sure whether it's two or three comments. I will start with one of them.

First of all I thought --

MR. THORP: We're keeping count.

CHAIRMAN BROWN: Keeping count. Okay. That's terrible.

I appreciated all the paperwork you all, documentation you all got to us. It was, I thought the SERs that you all had completed or at least partially completed provided a lot of assessment of the topical reports and brought out some points that weren't necessarily obvious in the topical reports in terms of how things were stitched together.

The other -- so I thought that was well done. And I thought the presentations were well done. I will just echo my compatriots' comments also. It was very informative, good interchange and dialog on questions.

The other thing was this, to echo John, we were both, we're both -- all the I&C guys obviously are very interested in having future discussions or interchanges for information like this on other, whether they're topical reports on platforms or other specific related issues that you guys see are coming to the fore as being critical or important in terms of the performance and how we apply the digital systems to the plants.

I mean we don't know everything you are doing down in the birds nests of your offices. And so --

MR. THORP: We're feathering things.

CHAIRMAN BROWN: Yes.

MEMBER STETKAR: Well, it's that time of years.

CHAIRMAN BROWN: Exactly. And so I mean if there's other items like this that you're working on, please, we'll probably have Christina strobe you all every now and then to see what else is going on. But we'd like to have the opportunity to have this type of an interchange. It's very informative for us to see where we're going and where the staff is going.

Any other related comments from those comments? Comments of some of the members rather. Excuse me.

(No response.)

CHAIRMAN BROWN: With that I will close the meeting. Thank you very much.

(Whereupon, the above-entitled matter went off the record at 12:09 p.m.)

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

EICB Topical Reports Update to ACRS I&C Subcommittee

John Thorp (NRC/NRR/EICB)

April 24, 2015

AGENDA

Opening Remarks	Chairman C. Brown, ACRS
Introduction	John Thorp, NRR
Regulatory Context and Approach	Norbert Carte, NRR
Spinline 3 Topical Report - Background - Description - Key Review Criteria	Rossnyev Alvarado, NRR
CPLD - Based SSPS Cards Topical Report - Background - Description - Key Review Criteria	Norbert Carte, NRR
Break	
HFC – 6000 Topical Report - Background - Description - Key Review Criteria	Samir Darbali, NRR
NuPAC Topical Report - Background - Description - Key Review Criteria	Norbert Carte, NRR
Conclusion	John Thorp, NRR
Closing Remarks	Chairman C. Brown, ACRS

Topical Reports Being Presented

- Purpose: Regulatory Efficiency

- Rolls Royce Nuclear Spinline III
- Westinghouse CPLD – Based SSPS Cards
- Doosan HFC-6000
- Lockheed Martin NuPAC

EICB Staff Presentation of Topical Report Reviews Outline

- A basic explanation of each design, how it works, and where it might be used in the reasonably foreseeable future.
  - A summary of each design from a technical engineering perspective - drawings and oral explanations that describe how each design processes signals, inter-divisional communications, interfaces between safety and non-safety signals.
  - Staff understanding of plans to implement these systems - new plants, retrofits, non-US markets, etc.

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

Regulatory Context and Approach

Norbert Carte (NRC/NRR)

April 24, 2015

Outline

- Use of Topical Reports (TRs)
- Topical Report Scope
- Technical Regulatory Requirements
- Key Review Criteria
- How Criteria are Addressed

Use of Topical Reports

- Increase in Regulatory Efficiency (elimination of redundant reviews)
- Reduce Burden on Licensees (reduction of redundant preparation)

- Industry Proposes for Licensing Use
  - Deals with a specific safety-related subject
  - Expected for multiple use
  - Complete and detailed information

- Digital I&C-ISG-06 encourages use of platform topical reports

Topical Report Scope(s)

- Topical Reports in General
  - LIC-500 Rev. 5, Topical Report Process
  - SRP, Technical Review Criteria
- Digital Replacement Card
  - CPLD-Based SSPS Card
- System Specific
  - NUMAC PRNM (Not described today)
    - Power Range Neutron Monitor
    - Oscillation Power Range Monitoring System
- Application Framework
  - HFC-6000
  - SPINLINE 3
  - NuPAC

Topical Report Scope - Historical

- Digital Replacement Cards
  - AREVA Safety Star (August 1995)
    - Installed in Delta Flux Trip at Oconee, prior to TXS Upgrade
  - ASIC Based Replacement Module (ABRM, February 2001)
    - Replacement for Westinghouse 7300 cabinet modules (50.59s)

- System Specific
  - NUMAC PRNM (November 1997)
    - Power Range Neutron Monitor
    - Oscillation Power Range Monitoring System
    - Various Installations

Topical Report Scope - Historical

- Application Framework
  - Programmable Logic Device (PLD – e.g., FPGA & CPLD) Based
    - ALS (September 2013)
      - Wolf Creek MSFIS & Diablo Canyon PPS
  - Microprocessor Based (PLC –Programmable Logic Controllers)
    - MELTAC (under review)
      - US-APWR; NRR: Topical Report in acceptance review
    - Triconex (2001 & 2012)
      - Diablo Canyon PPS
    - Common Q (August 2000 – February 2013)
      - AP1000, Palo Verde CPCs, 50.59 (PAMS, Diesel Sequencer, Rod Position Indication)
    - TXS (May 2000)
      - EPR, Oconee RPS/ESPS Upgrade & 50.59
    - Eagle 21 (Early 1990s)
      - Various Westinghouse Plant Protection Systems (PPSs)
      - Predated Topical Report Process
      - Approved by Precedent

Technical Regulatory Requirements

- 10 CFR 50.55a
  - (a)(1), Quality Standards
    - Now 50.54(jj) and 50.55(i)
  - (h), Incorporates by reference:
    - IEEE 279-1971, Protection System
    - IEEE 603-1991, Safety Systems
- 10 CFR 50 Appendix A
- 10 CFR 50.34(f) – TMI Action Items
- 10 CFR 50.62 – ATWS

- All requirements must be addressed

Key Review Criteria (General)

- SRP
  - Addresses all regulatory requirements and guidance (at time of issuance)
  - Provides one set of review criteria for each aspect being reviewed
  - Matrix organization
    - By Function (e.g., Section 7.2, Reactor Trip, Section 7.3, Engineered Safety Features, …)
    - By Topic (e.g., BTP 7-14, Development Process Reviews, BTP 7-21, Real Time performance)

Key Review Criteria (Specific)

- Design Bases
- Single Failure Criteria
  - Implicitly requires redundancy and independence
- Quality
  - Specifications and standards
- Equipment Qualification
  - Performance (e.g., Response Time)
  - Environment
- Independence
  - Between Redundancies, Design Basis Events, & Other Systems
  - Electrical, Physical, Communication, Protection and Control
- Secure Development and Operational Environment (SDOE)
- Diversity and Defense-in-Depth (D3)

How Criteria are Addressed

- Topical Reports (TR)
  - Digital Replacement Card
  - Application Framework
  - System Specific

- License Amendment Requests (LAR)
  - Everything not addressed by TR
  - Confirm TR bounds Plant design basis

Criteria Evaluated in Topical Reports (TR)

	Digital Card	System	Application Framework	LAR
Design Basis & Qualification	**Plant Specific:** Each TR addresses design basis and qualification requirements that are believed to encompass all future applications.			Ensure application is bounded by TR
Single Failure	FMEA	Reviewed	FMEA	Reviewed
Quality	Each item within the scope of review is reviewed against SRP criteria for quality.			
Independence	Mostly NA	Information	Communication Mechanism	Physical & Information
Performance Requirements	Component	System	Component	Design Basis
SDOE	Control of physical access to equipment is plant specific; however, I&C technical review ensure there is no unwanted, undocumented or unneeded code.			
D3	**Plant Specific:** However, each application may try to eliminate CCF from consideration by inherent diversity or testing.			

Acronyms

ALS – Advanced Logic Systems
ASIC – Application Specific Integrated Circuit
CPLD – Complex Programmable Logic Device
D3 - Diversity and Defense-in-Depth
EPR – Evolutionary Power Reactor
FMEA – Failure Modes and Effects Analysis
FPGA – Field Programmable Gate Array
HFC – HF Controls
ISG – Interim Staff Guidance
LIC – Licensing
MSFIS – Main Steam and Feedwater Isolation System
NPP – Nuclear Power Plant
NRC – Nuclear Regulatory Commission
NRR – Nuclear Reactor Regulation
NUMAC – Nuclear Measurement Analysis and Control
NuPAC – Nuclear Protection and Control
PAMS – Post Accident Monitoring System
PLD – Programmable Logic Device
PPS – Plant Protection System
PRNM – Power Range Nuclear Monitor
SDOE – Secure Development and Operational Environment
SRP – Standard Review Plan, NUREG-0800
TR – Topical Report
TXS - Teleperm XS
US-APWR - US Advanced Pressurized Water Reactor

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Rolls-Royce
SPINLINE 3 Digital Platform

Rossnyev Alvarado (NRC/NRR/EICB)

April 24, 2015

Outline

- Background
- Description
- Key Review Criteria
- Application

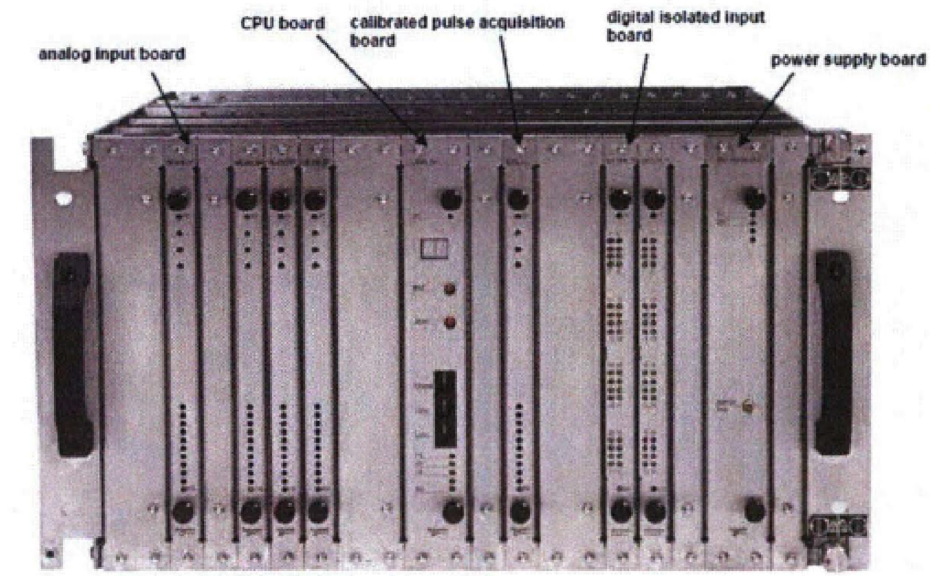
Background

- The Safety Evaluation of Rolls-Royce SPINLINE 3 Platform was issued in September 2014
- This platform resulted from the evolution of previous Rolls-Royce I&C systems
- This platform was designed, implemented, and qualified in compliance with European Nuclear and Quality Standards (e.g., IEC-880)
- The SPINLINE 3 platform has been qualified and accepted for use in safety related applications for U.S. Nuclear Power Plants

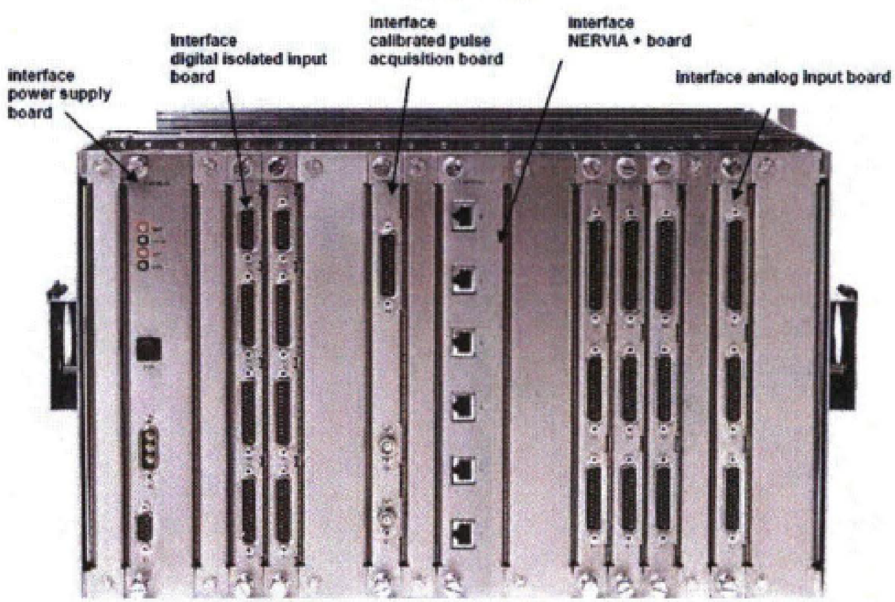
Description

- Based on microprocessor technology
- A modular digital system that can be configured in different sizes according to the application
- Components: interface boards, daughter or main boards, power supply modules, communication modules, operator interfaces, and a chassis with a backplane board

SPINLINE 3 Chassis



Front View



Rear View

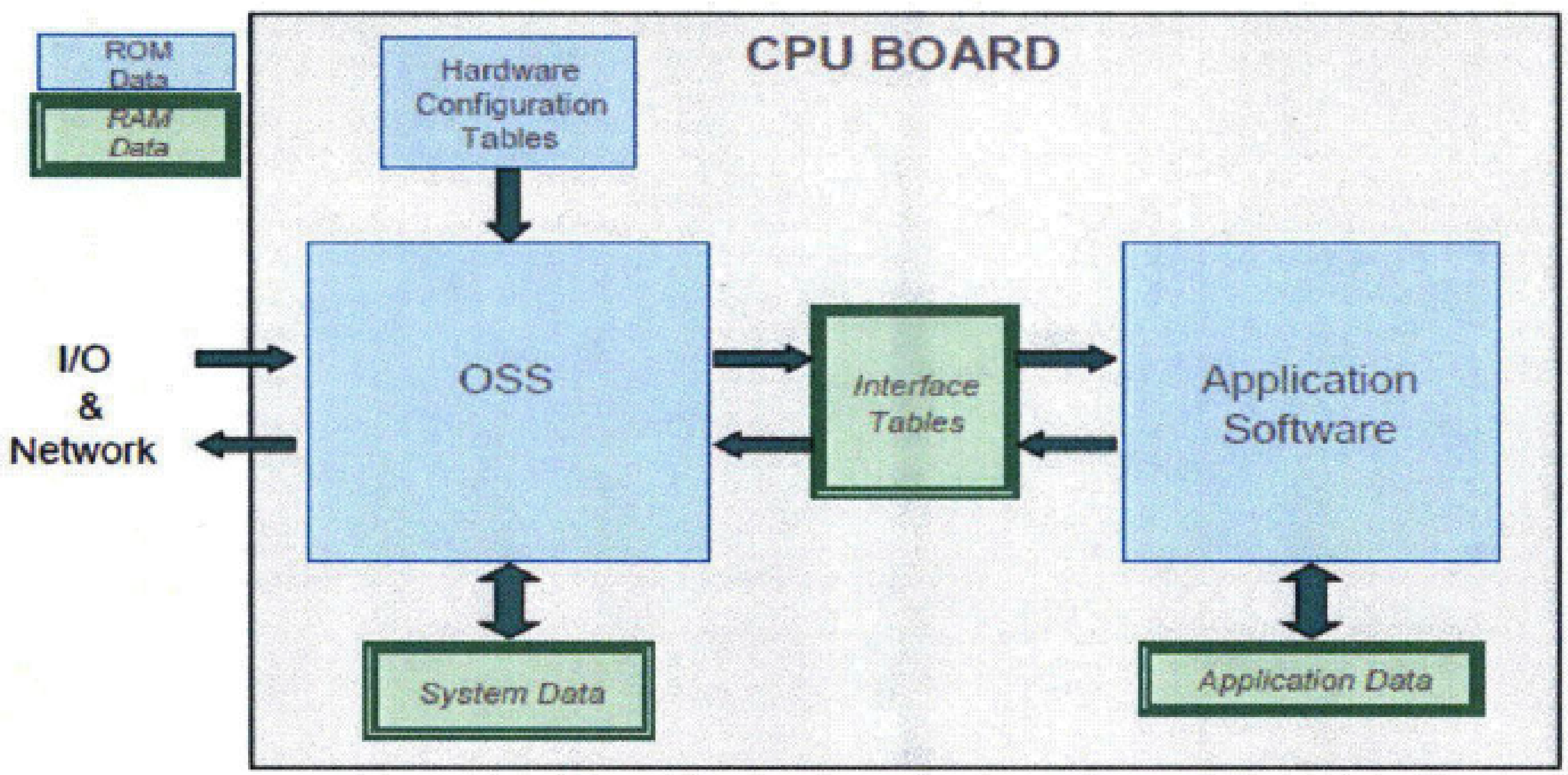
Main or Daughter boards

Interface boards

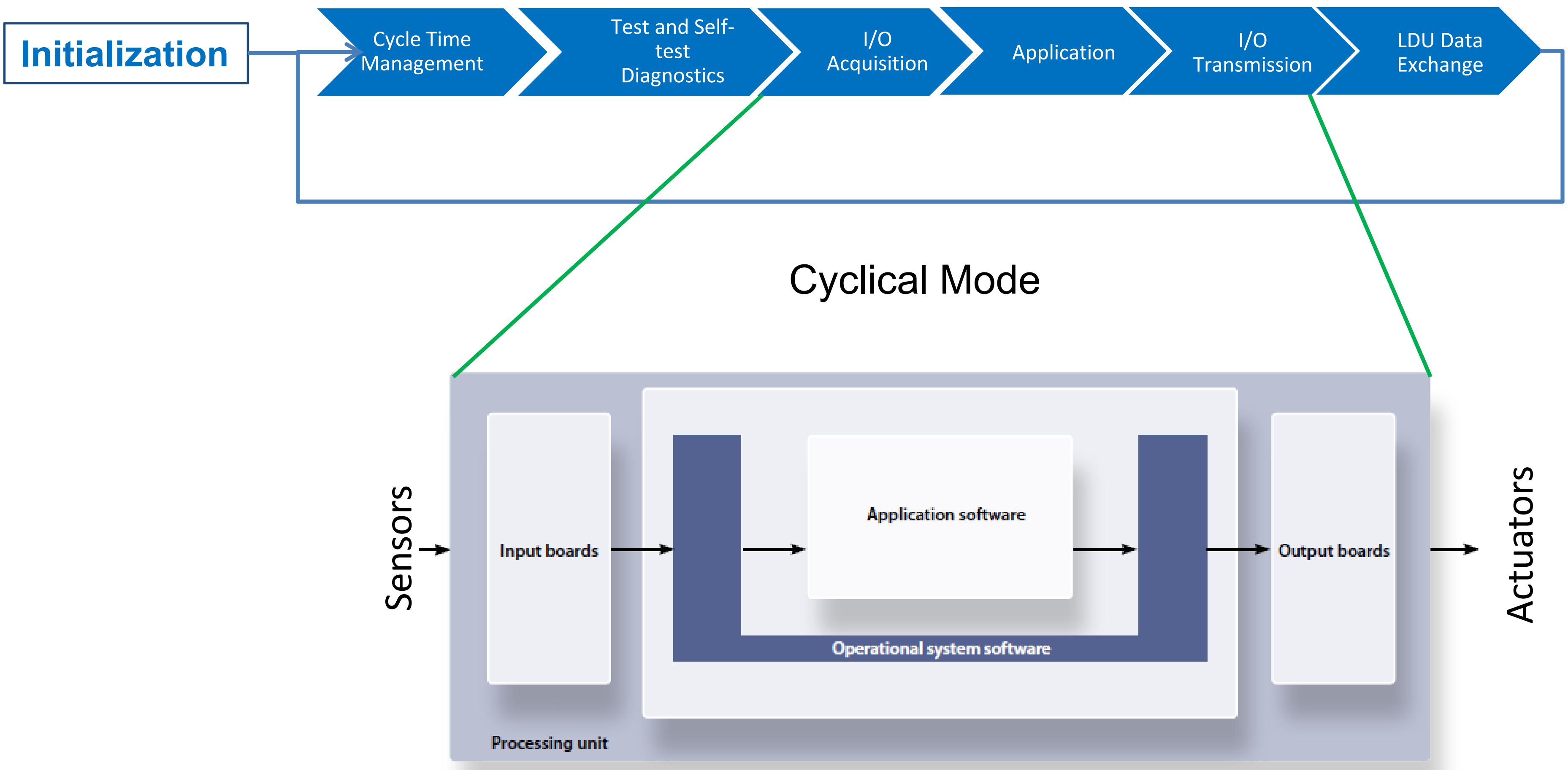
SPINLINE 3 Components

Component ID	Name	Type
8PT100	RTD board	Conditioning
I.8PT100 Interface board		Interface
16E.ANA ISO	Analog input board	Main
I.16EANA Interface board		Interface
32ETOR TI SR	Digital isolated input board	Main
I.32ETOR TI interface board		Interface
ICTO	Calibrated pulse acquisition board	Main
I.ICTO interface board		Interface
32ACT	Actuator drive board (Discrete output)	Main
I.32ACT interface board		Interface
6SANA ISO	Analog output board	Main
I.6SANA interface board		Interface
UC25 N+	CPU board	Main
NERVIA+ board	NERVIA+ communication board	Main
I.NERVIA+ interface board		Interface
ALIM 48V/5V-24V	Power supply board	Main
I.ALIM 48 interface board		Interface

Software Architecture and Configuration



System Operation

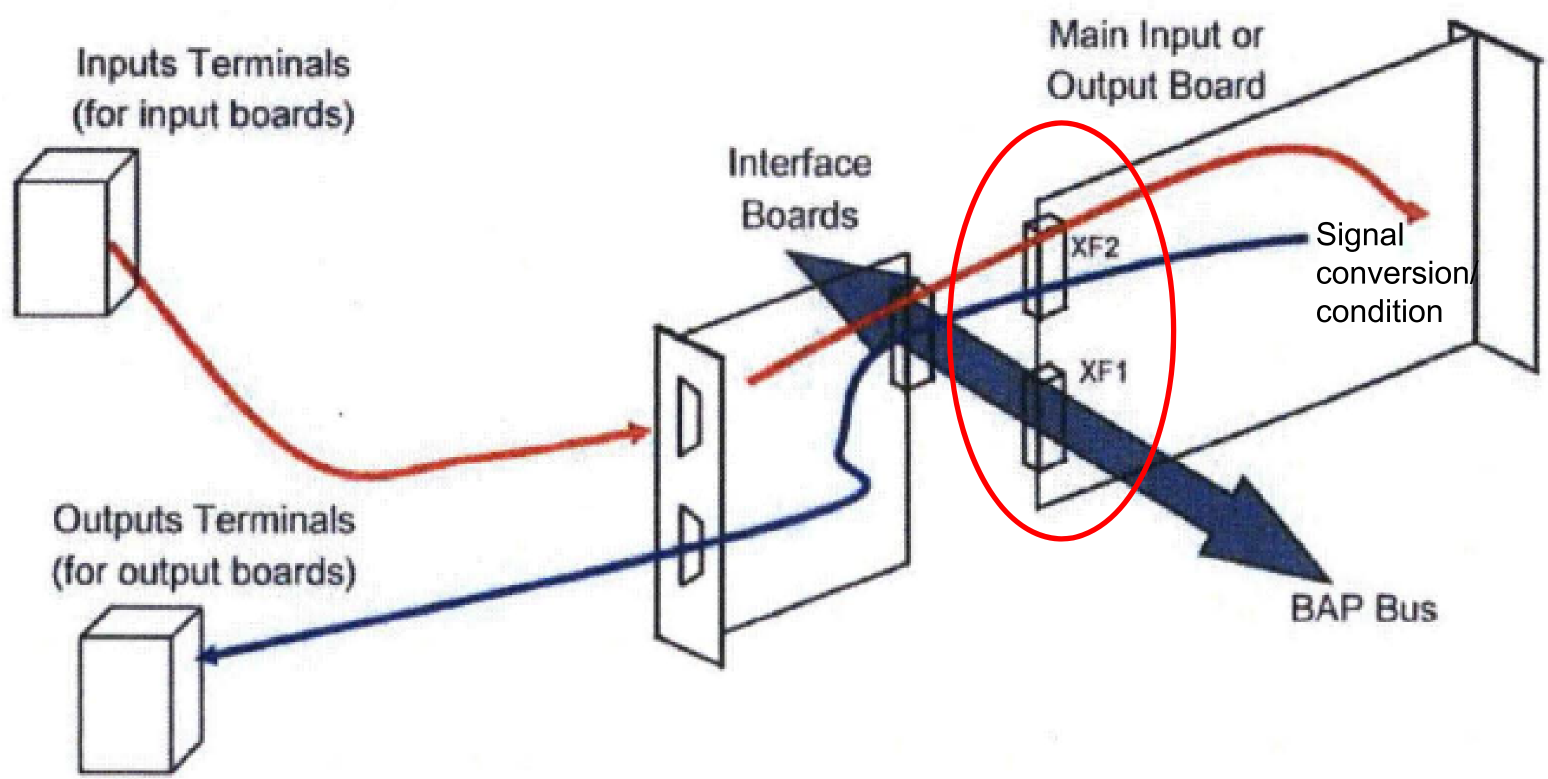


Lower figure taken from Spinline ™ Technical Sheet , www.rolls-royce.com

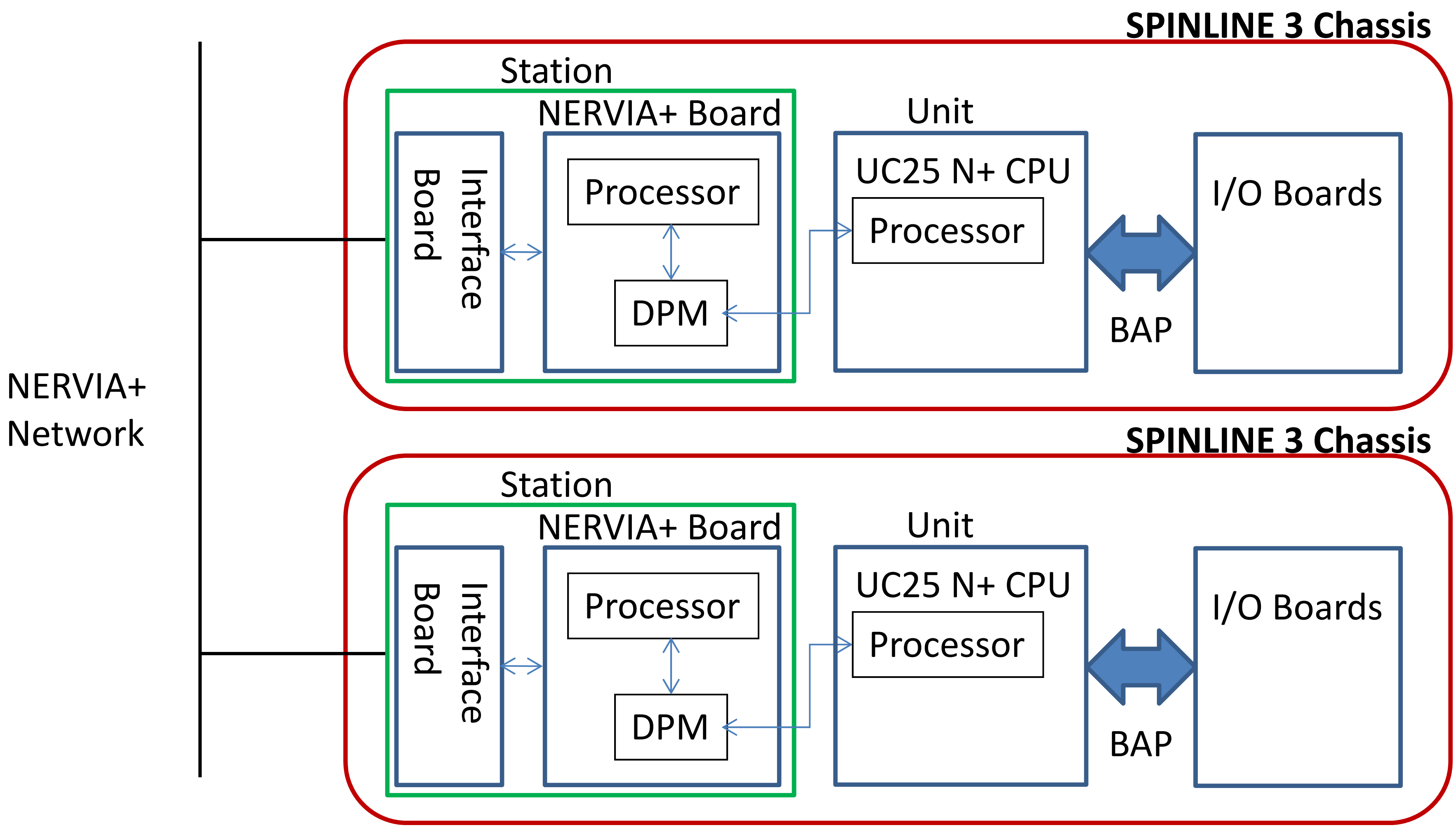
System Communication

- Backplane (BAP) Bus
- Intra-Divisional Communication (NERVIA+ Network)
- Passive Communications, Hubs, and Converters
- Serial Links

Backplane Bus Communication



Intra-Divisional Communication



Key Review Criteria

- Independence
- Redundancy(Application Specific)
- Diversity (Application Specific)
- Predictability and Repeatability
- Secure Development and Operational Environment

The TR did not address specific applications or establish a definitive system architecture. Therefore, the evaluation against the review criteria was limited to consideration of the means provided within the platform.

Independence

- The design permits Non-1E connections to the analog and discrete output modules, mechanical output relay interfaces, and the NERVIA network
- SPINLINE 3 platform met the criteria of IEEE Std. 384-1981 and Section 6.3.6 of EPRI TR-107330 for electrical independence
- SPINLINE 3 platform provides digital communication design features that can support independence between an SPINLINE 3 platform-based safety system and other interfacing systems
- Although the system includes features for one-way communication to non-1E components, the TR did not provide enough information to evaluate communication between safety and non-safety components

Predictability and Repeatability

- Software runs sequentially, deterministically, and periodically
- System's cycle time is fixed and functions are executed in the same order
- The system's cycle time performance is deterministic and defined during the system design
- The Unit's processor is independent of the Station's processor
- Data exchange between the Unit and the Station is via the DPM
- Data exchange between Stations and Units is not synchronized
- The system uses the BAP bus for data exchange with I/O modules
- NERVIA network is a time-based bus protocol
- The actual response time of an SPINLINE 3 platform-based system will be determined by its overall configuration

Secure Development and Operational Environment

- The SPINLINE 3 OSS and plant-specific application software for a SPINLINE 3-based system are developed in-house by Rolls-Royce (France)
- The manufacturer developed the SPINLINE 3 platform under a secure environment which controls the access to the facility, the facility LAN, the development environment, quality records, and the configuration management system
- The software cannot be modified on-line by operators
- The SPINLINE 3 platform includes design attributes and features that a licensee could apply and credit to demonstrate protection against undesirable behavior of connected systems and the prevention of inadvertent access
- The NRC staff determined a secure development environment had been established for the SPINLINE 3 platform that is consistent with the regulatory positions found in RG 1.152, Revision 3

Application

- Can be used in protection systems, such as RPS, NIS, Process Instrumentation System, ESFAS, and Diesel Load Sequencing System
- None installed in the US
- Installed in more than 50 PWR in France and VVER nuclear reactors all over the world
  - In 2011 EdF selected SPINLINE 3 to replace the RPS of the 1300MW French nuclear reactors (20 units).
- Used by 8 Neutron Instrumentation Systems in operation in China. Also to be installed as the NIS of 20 reactor units currently under construction.

Acronyms

BAP – backplane

CPLD – complex programmable logic device

CPU – central processing unit

DPM – dual port memory

EdF - Électricité de France

ESFAS – engineering safety actuation system

EPRI – electric power research institute

FPGA – field programmable gate array

I/O – input/output

NIS – neutron instrumentation system

OSS – operating system software

PWR – Power Water Reactor

RAM – random-access memory

RG – regulatory guide

RPS – reactor protection system

ROM – read-only memory

RTD – resistance temperature detector

SR – safety related

NSR – non-safety related

TR – topical report

VVR – water-water energetic reactor

Westinghouse SSPS Board Replacement Licensing Summary Report

WCAP-17867-P-A Rev. 1

Norbert Carte (NRC/NRR/EICB)

April 24, 2015

Outline

- Background - SSPS
  - Solid State Protection System (SSPS) History
  - SSPS Cabinets
  - List of Circuit Boards
  - SSPS in Context
- Description – CPLD-Based SSPS Topical Report
  - Timeline: Regulatory Positions for PLDs
  - Summary Description
- Key Review Criteria

SSPS History

- RTS & ESFAS Voting
  - Relay Voting (First Westinghouse plants)
    - 14 Cabinets
    - 4 hour per train test time
    - Monitoring Information – 1,000 Conductors
    - 750 Relays with 4000 contacts
- January 1971 – Westinghouse SSPS TR
  - Solid State Voting
    - 6 Cabinets (2 Trains – 3 Cabinets each)
      - Input, Logic, Relay
    - 10 minute per train test time
    - Monitoring Information – 42 conductors (Multiplexed)
- March 1974 – SSPS TR Approved

SSPS Cabinets

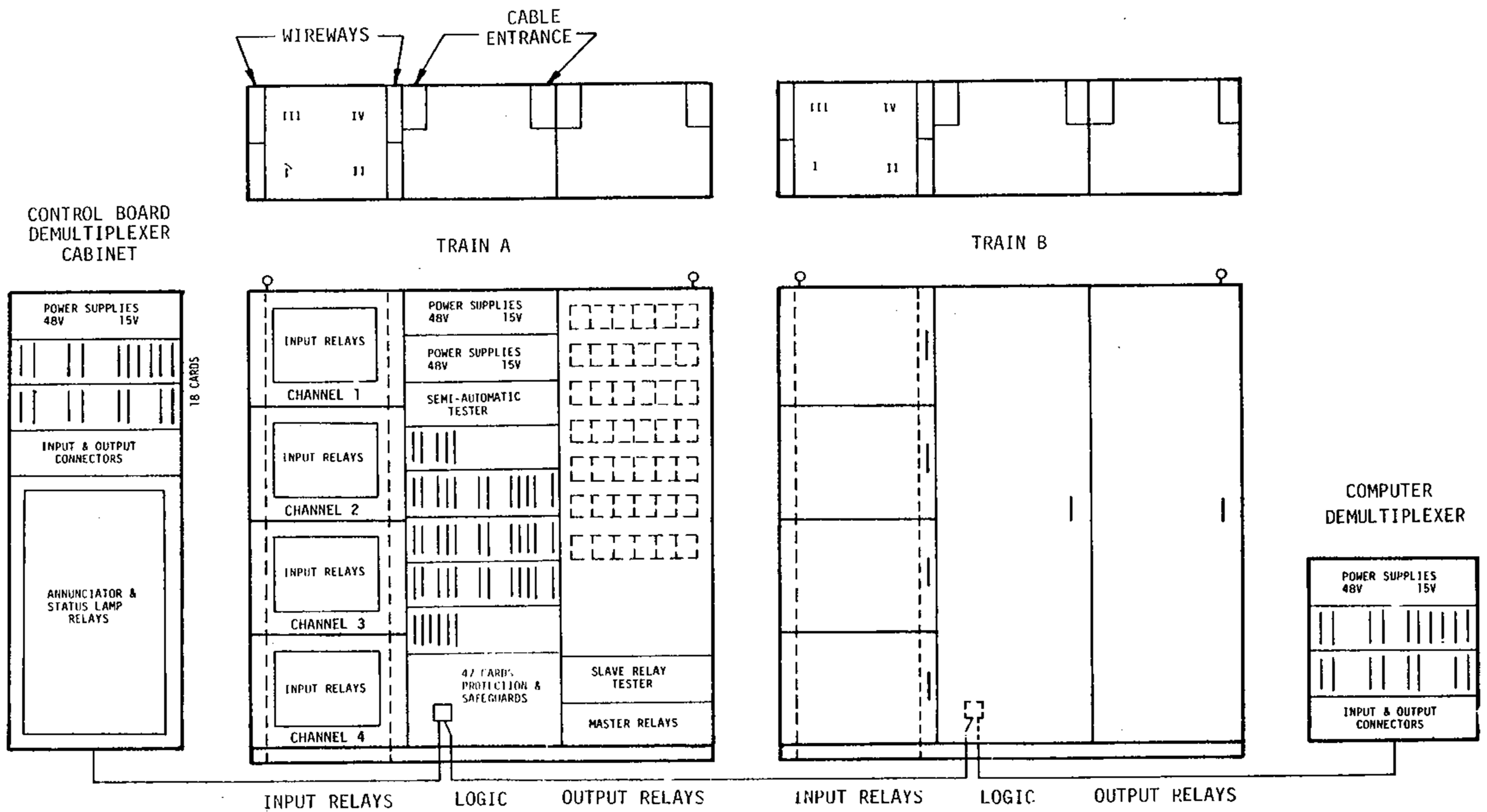


Figure 2. Solid State Protection System Equipment Layout

List of Circuit Boards

ULB – Universal Logic Board (voting)

SGD – Safeguard Driver (drives ESF relays)

UVD – Undervoltage Driver (powers trip breakers)

SAT – Semi-Automatic Tester (surveillance testing)

CCB – Clock Counter Board (test & status indication)

DEC – Decoded (decodes clock counter for status indication)

MEM – Memory (non-safety status indication)

ISO – Isolation (electrical isolation)

SSPS in Context

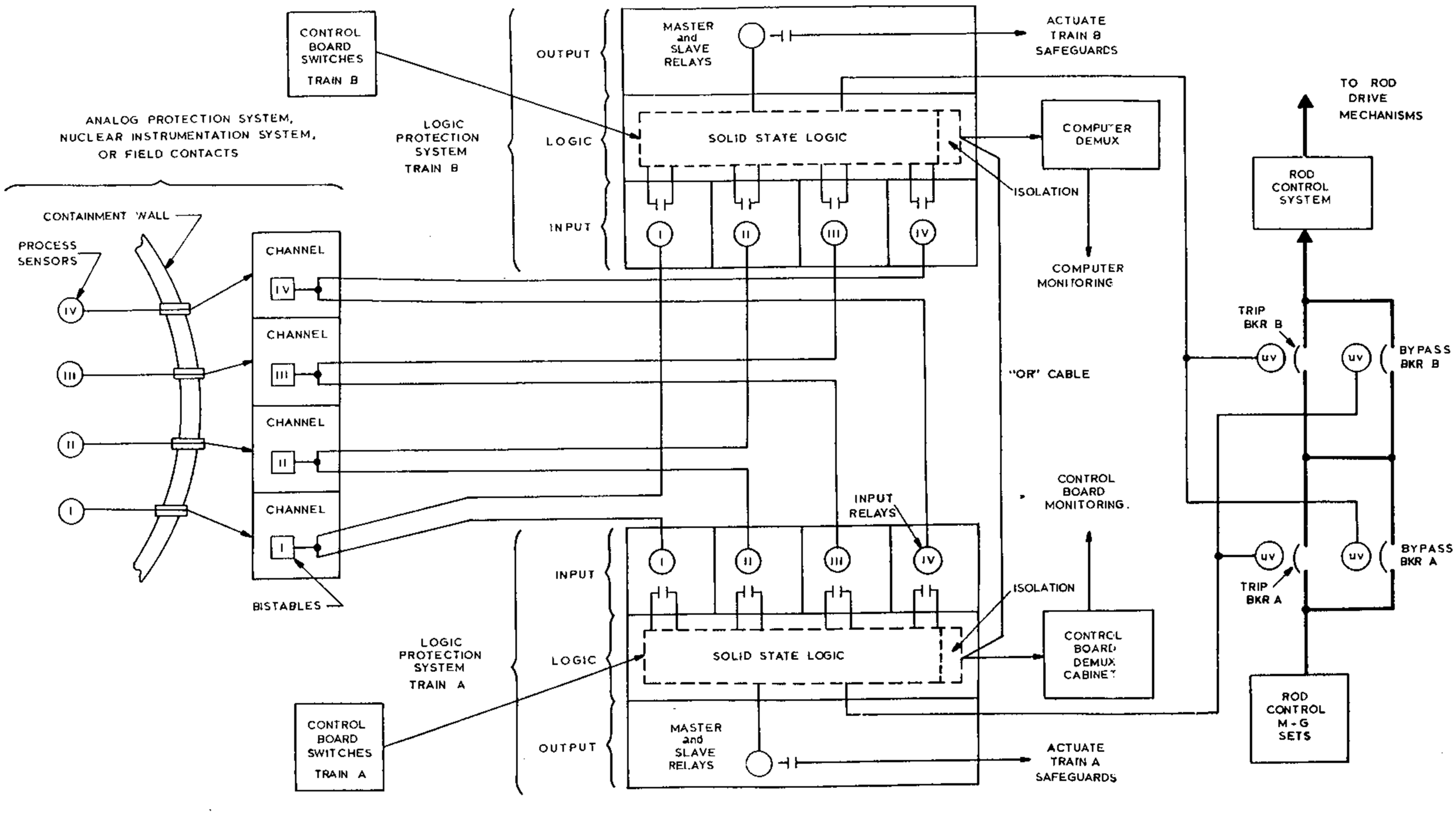
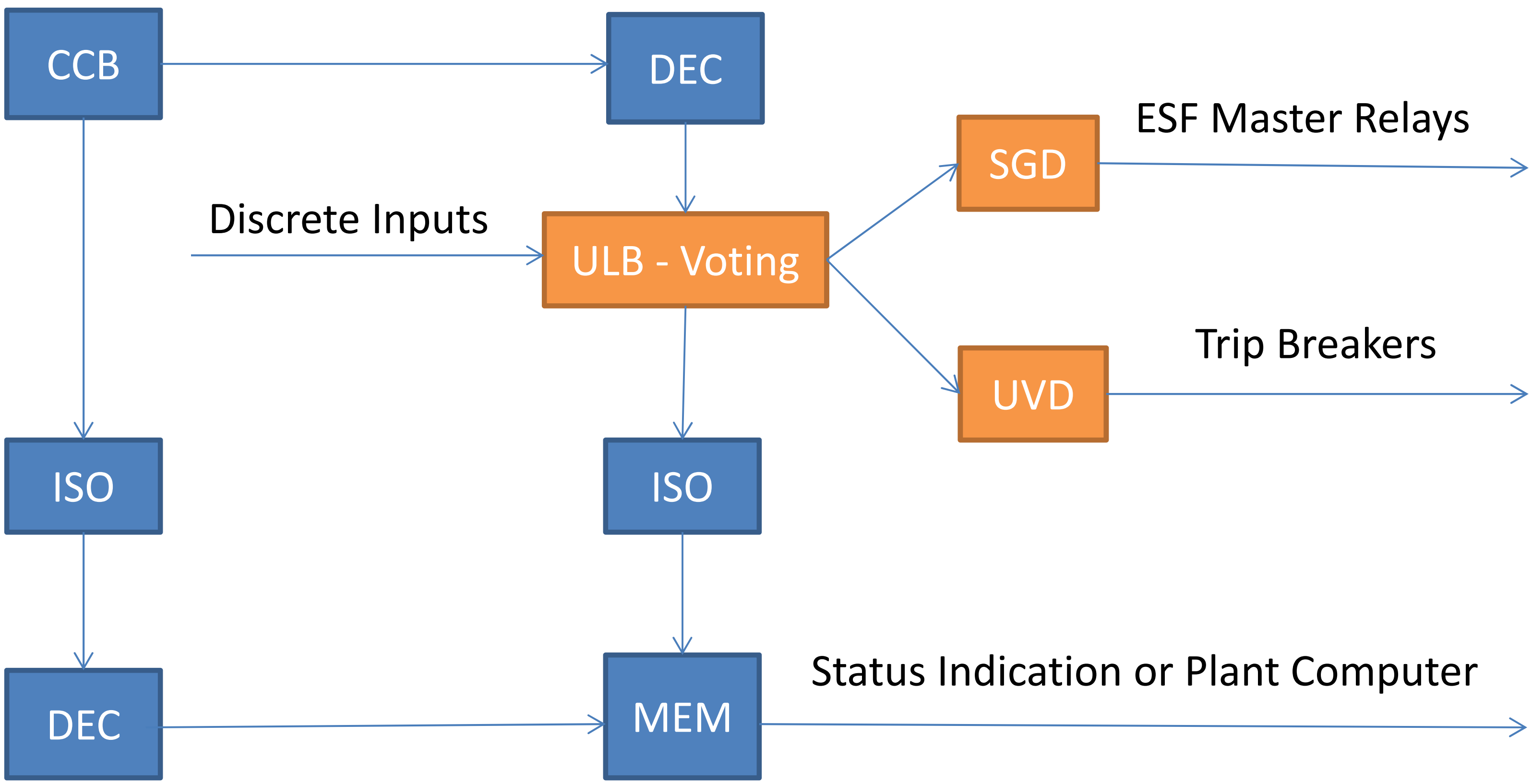
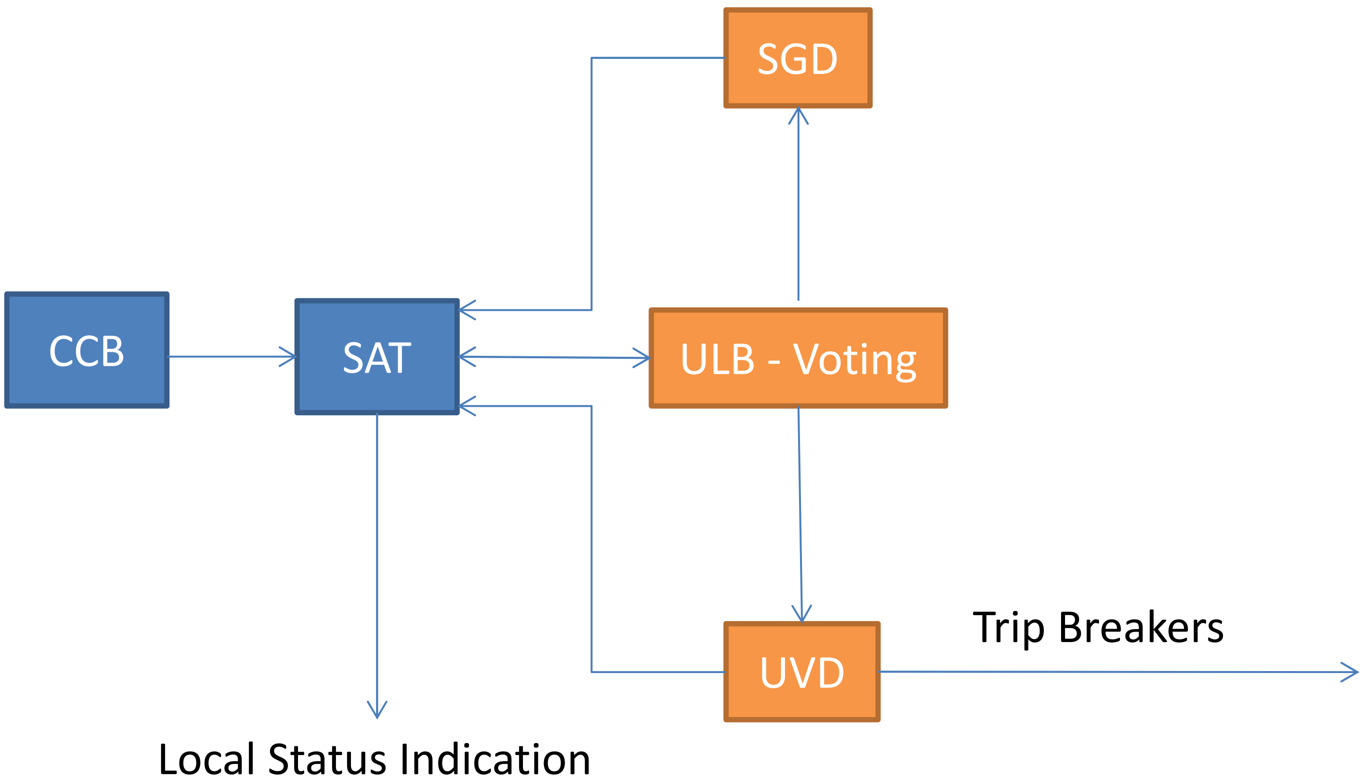


Figure 1. Solid State Logic Protection System Block Diagram

SSPS Cards Used When Operating



SSPS Cards Used When Testing



Timeline: Regulatory Positions for PLDs

- February 2001 – ABRM TR Approved
- April 2002 – CPLD-Based SSPS Card TR Funded
- November 2006 – Industry Met with Commission
- March 2007 → March 2009 – Wolf Creek MFSIS Review
- September 2007 – ISG-04 Rev. 0 Issued
- July 2010 → September 2013 – ALS Topical Report under Review
- February 2013 – CDBI Inspection at Harris
  - Four meeting regarding condition
  - Decided topical report was most efficient approach
- August 2013 – Violation issued to Harris
- February 2014 – CPLD-Based SSPS Card TR docketed

Summary Description

- Digital Replacement Cards
  - Old Cards used MHTL Logic Chips (No longer available)
  - New Cards perform identical functions
- 8 New Cards
  - 7 Installed in Existing SSPS Racks
    (ULB, SGD, UVD, SAT, CCB, DEC, & ISO)
  - 1 Installed in Non-safety demultiplexer cabinets (MEM)
  - 3 have CPLDs and they process safety signals
    - Universal Logic Board (ULB)
    - Safeguards Driver Board (SGD)
    - Under Voltage Driver Board (UVD)

Key Review Criteria

- Design Basis
- Single Failure
- Quality
- Equipment Qualification
  - Performance
    - CPLD based
    - No Interrupts
    - Aliveness checks - LEDs
- Independence
- Secure Development and Operational Environment (SDOE)
- Diversity and Defense-in-Depth

Questions?

Backup Slides

PLDs vs. Microprocessors

- Microprocessors
  - Share resources
  - Watchdog Pulse process is last in big loop
- Programmable Logic Devices (PLDs)
  - Implement microprocessor
    - Watchdog may be appropriate
  - Highly parallel
    - Watchdog does not provide much assurance

ULB – Universal Logic Board

- Three Discrete Voter Logic Circuits
  - One 4-input: two out of four
  - Two 3-input: two out of three
- Six Test Points
  - Output of each voter (3)
  - Address inputs to multiplex circuits (3)
- Enhancements
  - Card edge LEDs
  - Redundant components to address single point vulnerabilities
  - Self-test CPLD

SGD – Safeguards Driver Board

- 8 drivers to actuate ESF master relays
  - Include Reset input
- Enhancements
  - Card edge LEDs
  - Redundant components to address single point vulnerabilities
  - Self-test CPLD

UVD – Undervoltage Driver Board

- “Ors” up to 22 inputs (ULB voted outputs)
- Single Driver, maintain undervoltage coil of reactor trip breakers
- Enhancements
  - Card edge LEDs
  - Redundant components to address single point vulnerabilities
  - Self-test CPLD
  - Short Circuit protection

CCB – Clock Counter Board

- Inputs to SAT board
- Inputs to multiplexing for status indication
- Enhancements
  - Improved enable signal
  - Card edge LEDs
  - Redundant components to address single point vulnerabilities

SAT – Semi-Automatic Tester

- Monitors board health
  - Cabinet self-heath
  - Test switch position
  - Card status condition
- For Surveillance testing of ULBs
  - Inputs from Clock Counter board
  - Generate test sequence
  - Evaluate test results
- Enhancements
  - Card edge LEDs
  - Redundant components to address single point vulnerabilities

DEC – Decoder Board

- Decodes clock counter bits to address signals
- Enhancements
  - Manual test feature
  - Card edge LEDs
  - Redundant components to address single point vulnerabilities

MEM – non-safety Memory

- Receives multiplexed data from ULB
- Outputs data to:
  - Control Board & Plant Computer
- Enhancements
  - Card edge LEDs
  - Redundant components to address single point vulnerabilities

ISO – Isolation Board

- Electrical Isolation
  - Between Redundancies
    - Required to ensure coordination of plant computer and main control board information
  - Between SSPS & Demultiplexer Cabinets
    - Between ULBs and MEMs
- No CPLDs
- Enhancements
  - Redundant components
  - Redundant error indication
  - Status indications
  - Test points

Acronyms

ABRM – ASIC Based Replacement Module
ASIC – Application Specific Integrated Circuit
CPLD – Complex Programmable Logic Device
FPGA – Field Programmable Gate Array
ISG – Interim Staff Guidance
NPP – Nuclear Power Plant
NRC – Nuclear Regulatory Commission
NRR – Nuclear Reactor Regulation
NuPAC – Nuclear Protection and Control
PAMS – Post Accident Monitoring System
PLD – Programmable Logic Device
PPS – Plant Protection System
SRP – Standard Review Plan, NUREG-0800
TR – Topical Report

ULB – Universal Logic Board
SGD – Safeguard Driver
UVD – Undervoltage Driver
SAT – Semi-Automatic Tester
CCB – Clock Counter Board
DEC – Decoded
MEM – Memory
ISO - Isolation

HFC-6000
Safety System Platform

Samir Darbali (NRC/NRR/EICB)

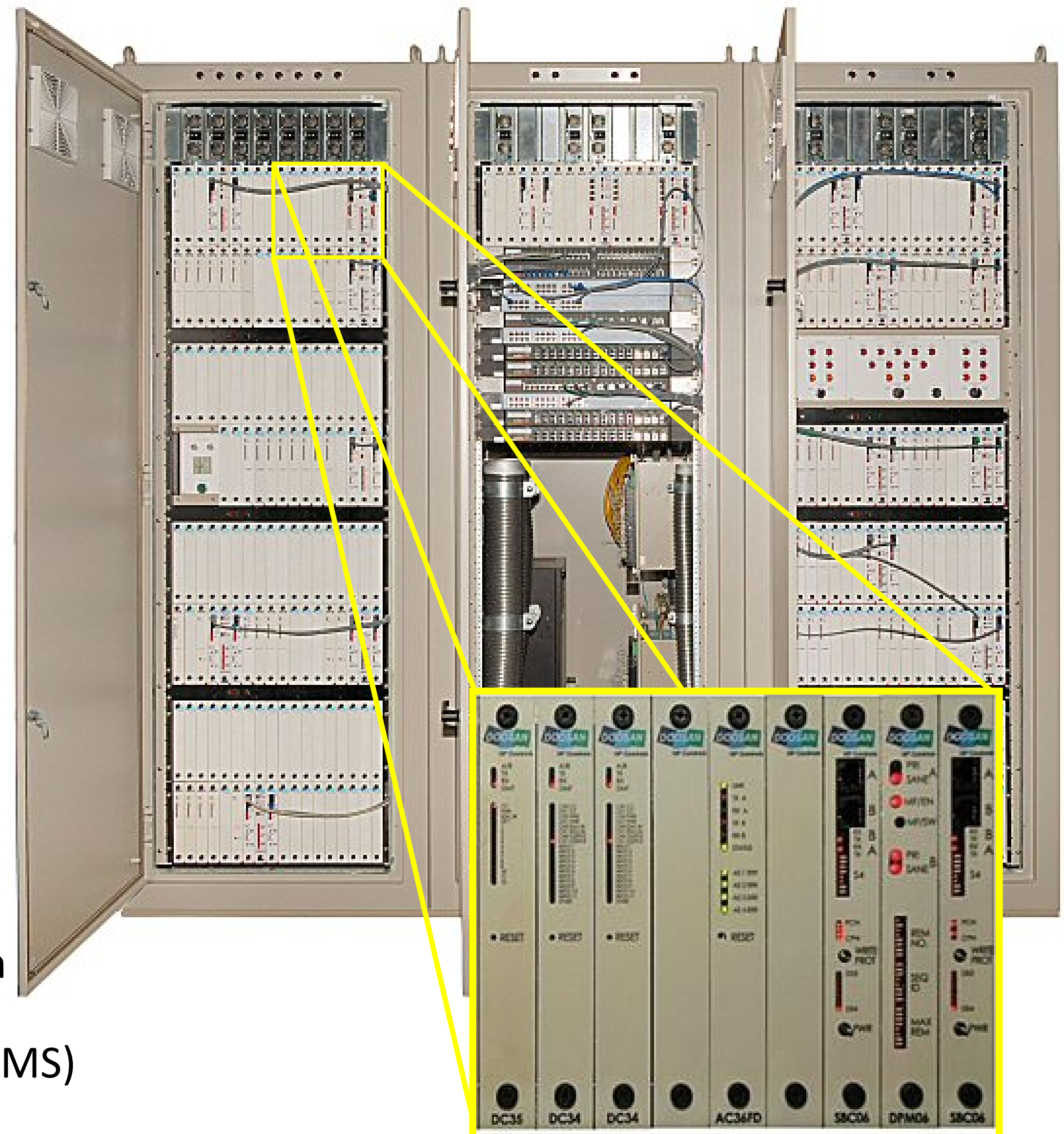
April 24, 2015

Outline

- Background
- Description
- Key Regulatory Criteria
- Amendments to the HFC-6000 Topical Report

HFC-6000 Background

- HFC-6000 is a modular, rack mounted platform that is housed in cabinets
  - Developed by HF Controls (HFC) Corporation, owned by Doosan Heavy Industries & Construction Company
  - Based on product lines developed by Forney Engineering Company dating back to the 1980s



- Applications could include:
  - reactor protection system (RPS)
  - engineered safety features actuation system (ESFAS) functions
  - post accident monitoring system (PAMS)

HFC-6000 Background

- Topical Report (TR) submitted for review in March, 2008
- Technical Review contracted to Oak Ridge National Lab
  - NRC Technical Monitoring of contract performed by NRR/DE/EICB
- Safety Evaluation (SE) issued in April, 2011
  - SE included six Generic Open Items related to Equipment Qualification Testing
- Operational history:
  - HFC-6000 platform-based systems currently installed in 24 South Korean NPP Units
  - Not installed in any US NPPs
  - No license amendment requests for installation in US NPPs

HFC-6000 Platform – Topical Report Scope

- Application Framework
- Redundant (Microprocessor-based) Controllers
  - Operating System Software
- Dual Ported Memory (DPM)
- Input / Output Modules (Analog & Digital)
- Redundant Power Supplies
- Equipment included in the TR:

HFC-SBC06 (Controller Module)	**HFC-DI16I** (Digital Input Module)
HFC-DPM06 (Dual-Ported Memory)	**HFC-DO8J** (Relay Digital Output Module)
HML 601-5 (24 V Power Supply)	**HFC-DC33** (Digital Control Module for MOVs)
HML 601-8 (48 V Power Supply)	**HFC-DC34** (Digital Control Module for EOBs)
HFC-BPC01-19 (Controller Backplane)	**HFC-AI8M** (RTD Input Module)
HFC-BPE01-19 (Expansion Backplane)	**HFC-AI16F** (Analog Input Module)
HFC-AI4K (Pulse Input Module)	**HFC-AO8F** (Analog Output Module)
HFC-ILR06 (I/O Link Fiber-Optics Repeater/Terminator)	

MOV - Motor Operated Valve EOB - Electrically operated breaker RTD - Resistance temperature detector

Out of Scope of the Topical Report

- External Communications
  - Between HFC-6000 Channels
  - Between HFC-6000 platform and other systems
- Human-Machine Interface
- Displays
- Any Application-Specific Software
- Multi-Channel Operation (i.e., Voting Mechanism)

Safety System Architecture Example Based on the HFC-6000 Platform

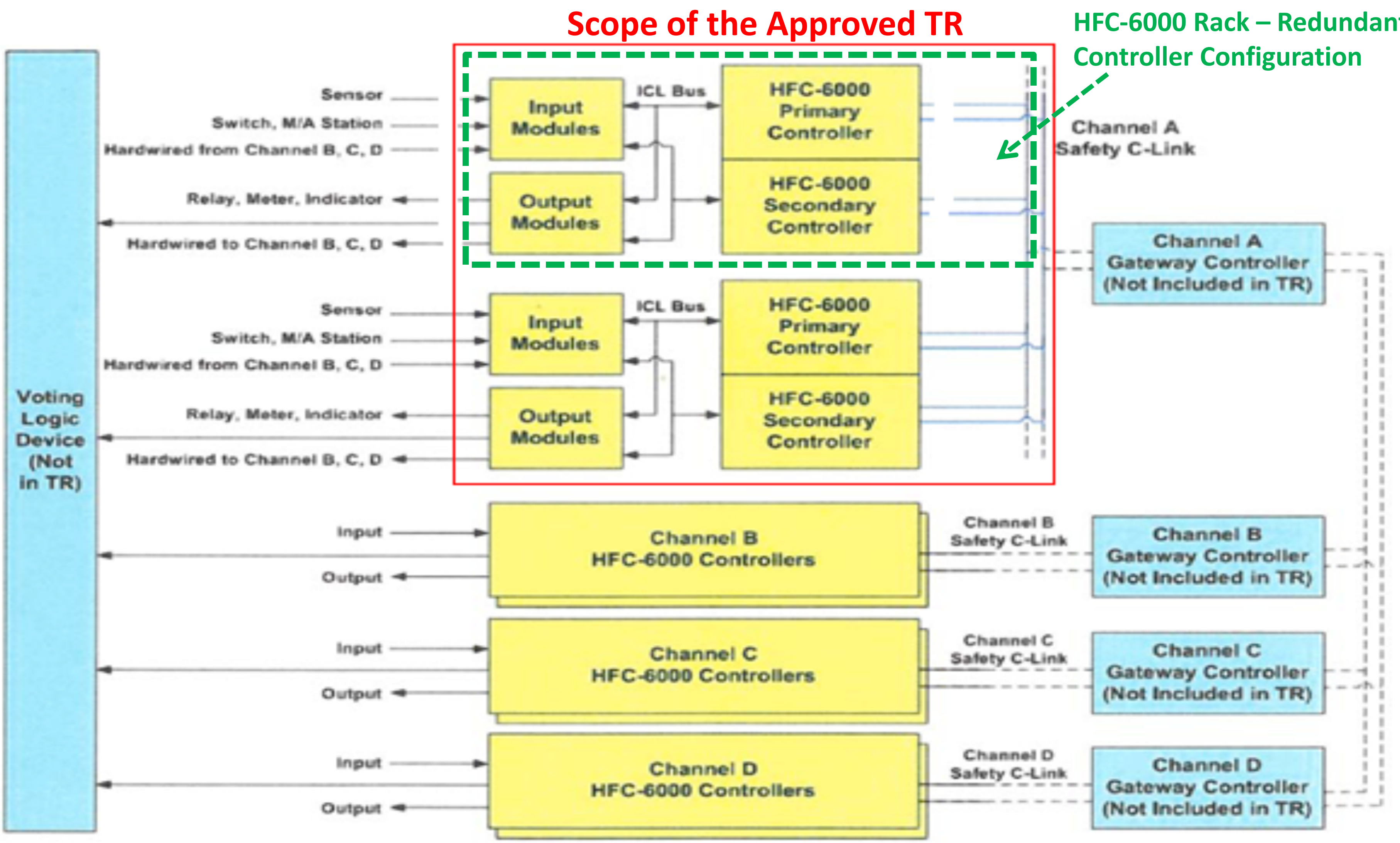
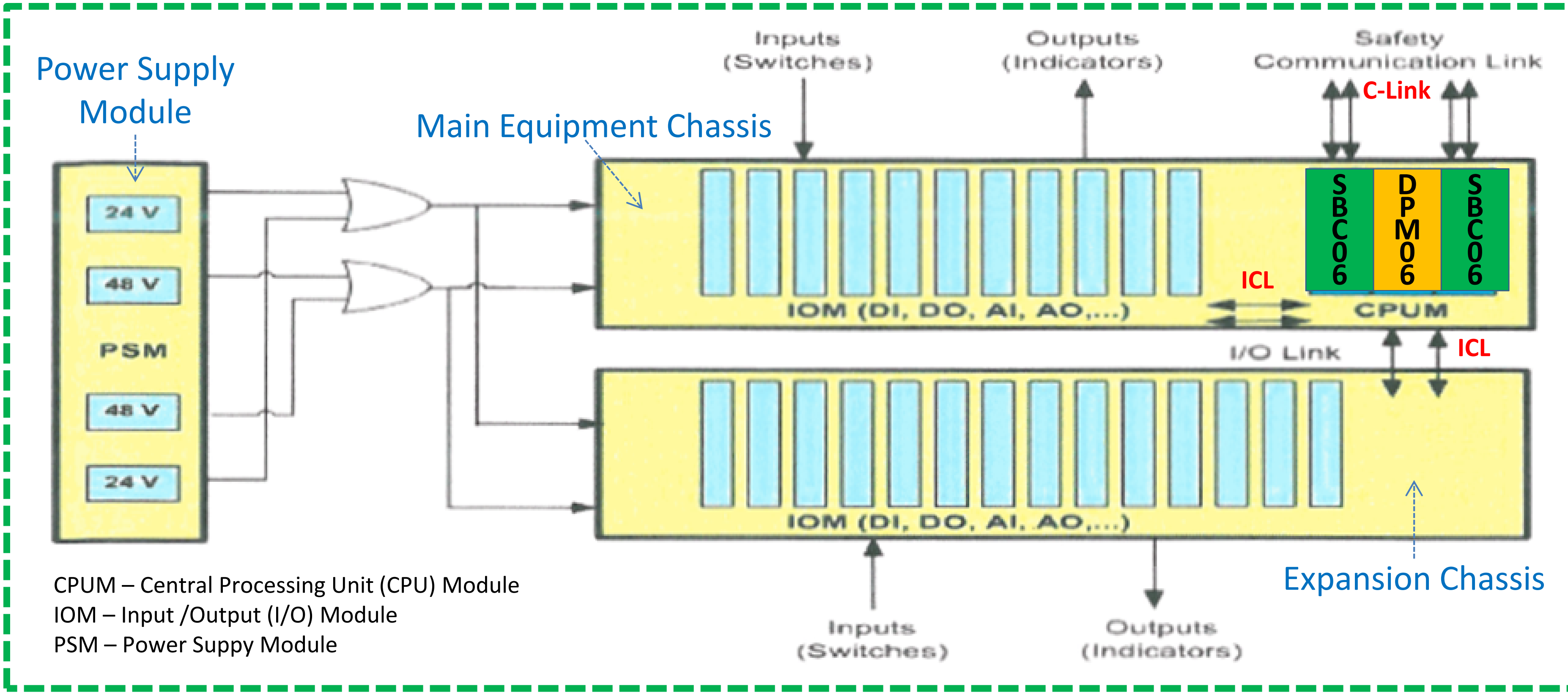


Figure 1 of HFC-6000 SE (ML110831017)

Hardware Arrangement for the HFC-6000 Platform

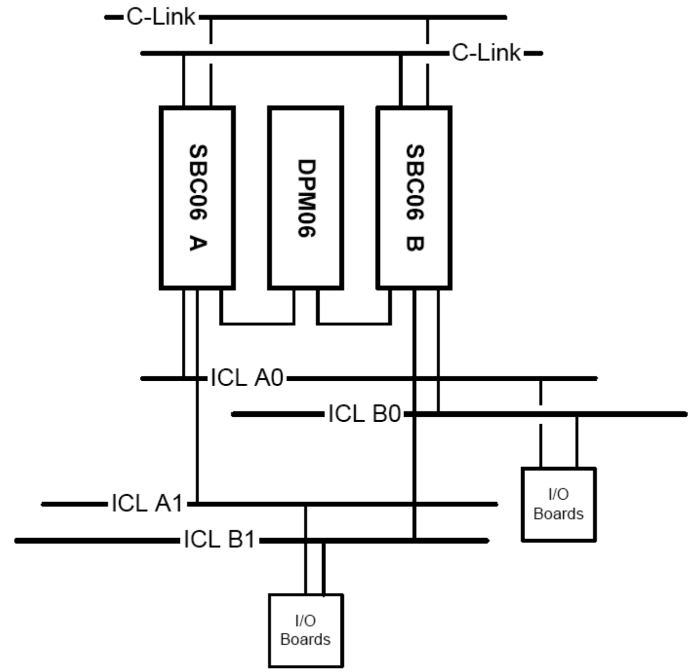


- CPUM and IOMs (up to 11) are housed in the main equipment chassis
- Additional IOMs (up to 14) implemented in an expansion chassis
- PSMs in a separate power rack that provides redundant 24 VDC and 48 VDC power via separate backplane traces in each equipment chassis

Figure 2 of HFC-6000 SE (ML110831017)

Communications

The HFC-6000 platform provides two communication interfaces:



- **Intra-Channel Communication link (C-Link)** - Transfers information among safety controllers (SBC06) within a channel to provide status information and operational data. The C-Link is a redundant Ethernet-based network employing a proprietary token-passing protocol to implement deterministic communications.

- **Backplane interconnections/ Intercommunication link (ICL) -** Supports transmission of data between the CPUM and IOMs to allow periodic polling to update I/O data. The ICL bus implements a proprietary deterministic protocol based on a poll/response approach to communication.

Figure 4 of HFC-6000 SE (ML110831017)

SBC06 and DPM06 Modules

SBC06 Controller Module

SYS Processor (64-bit)

Monitors overall status of the controller module, services watchdog timers, and executes the application program code.

ICL Processor (32-bit)

Handles communication on the ICL to obtain field data from the IOMs and to send operational commands to the IOMs.

C-Link Processor (32-bit)

Responsible for regulating messages sent over the C-Link.

SBC6_CHSEL CPLD

Provides the logic necessary to perform various functions for the SYS processor.

PBUSIF CPLD

Provides the logic to interface the SYS processor local bus with components on the common bus.

SBC6_386C CPLD

Provides board management functions for the ICL and C-Link processors.

SBC6_SHARB CPLD

Provides arbitration for all memory access across the common bus by each of the three processors.

DPM06 Dual-Ported Memory

SBC6_DPM CPLD

Manages the failover mechanism between redundant controllers.

SYS Processor - Intel Pentium µP
ICL, C-Link Processors - Intel 386EX µP
CPLDs - Xilinx

SBC06 and DPM06 Module Architectures

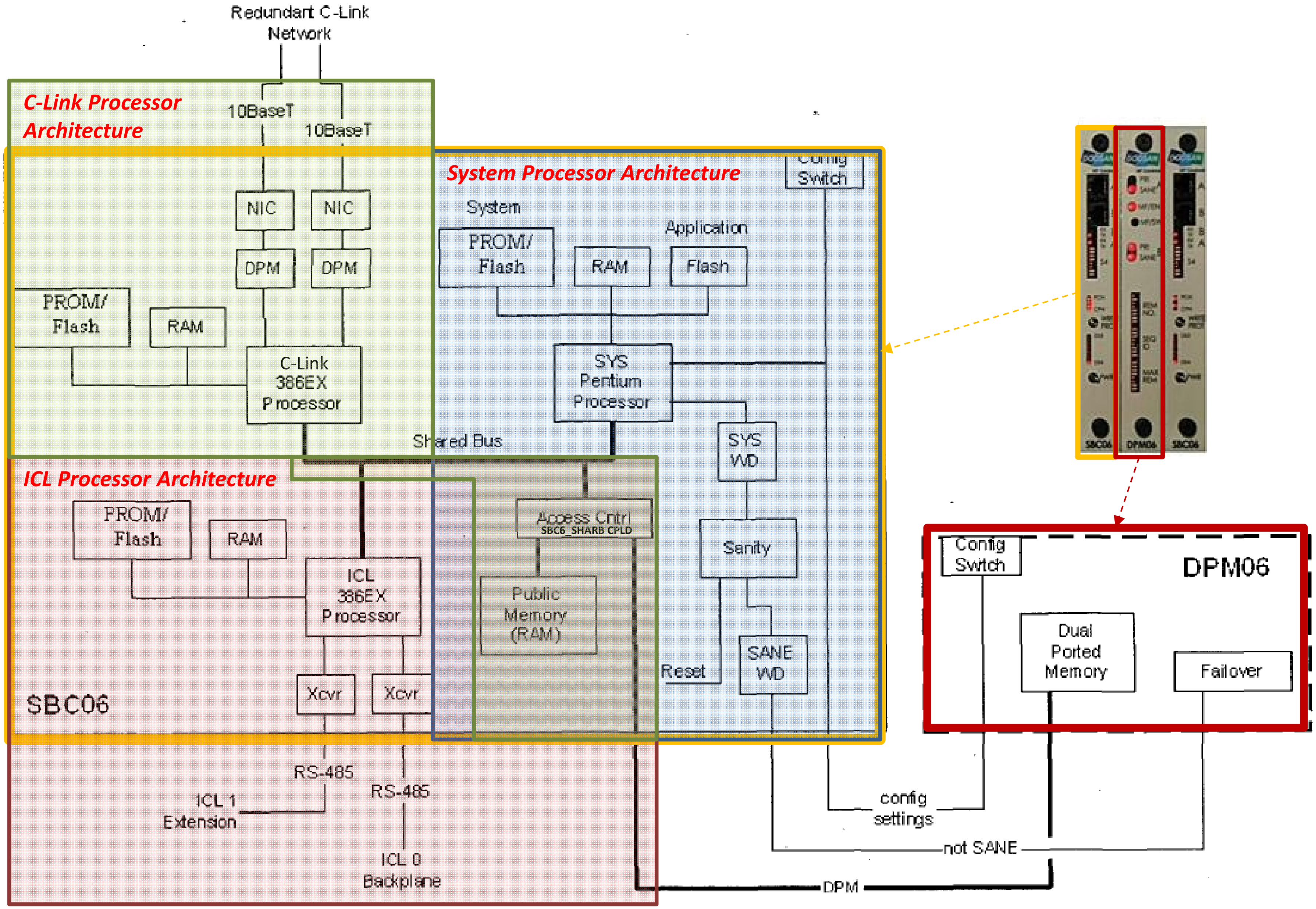
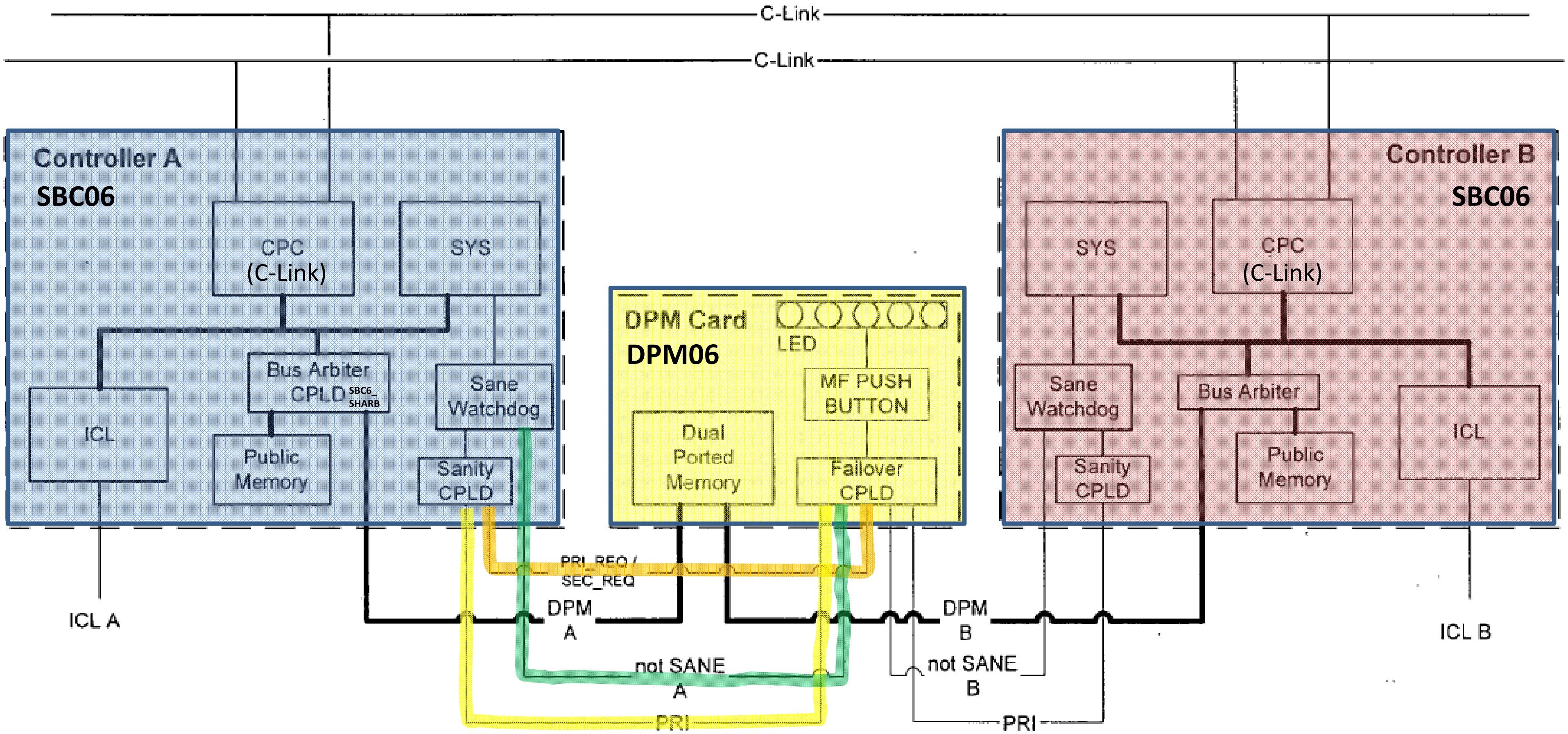


Figure 5 of SBC06-DPM06 Design Specification (ML091480158)

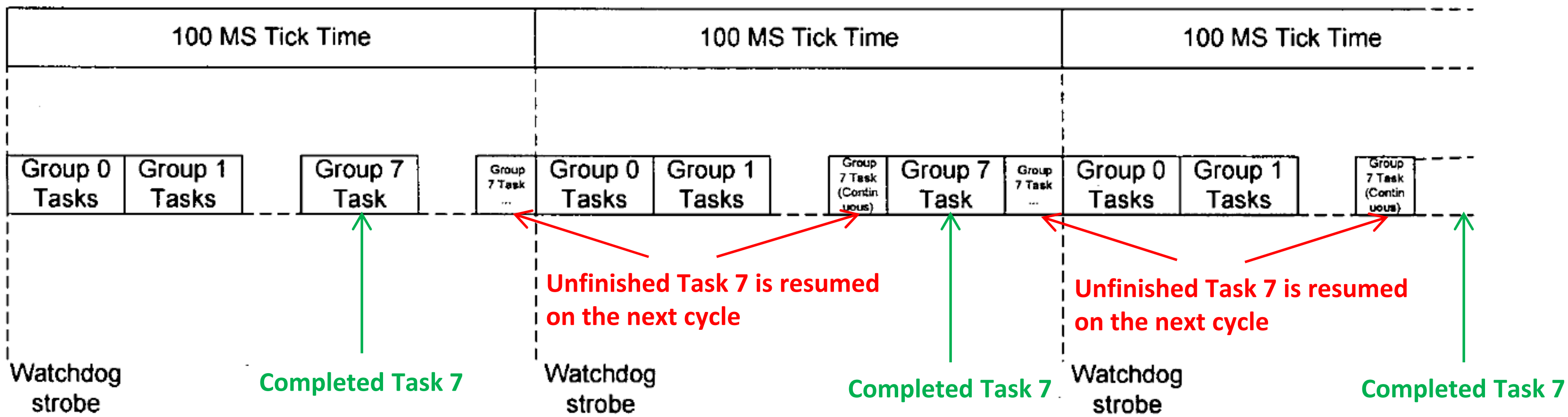
Redundancy and Failover



- Logic to determine controller operation mode: Primary or Secondary
- Controller failure detection mechanism
- Failover mechanism on failure of primary controller
- Mechanism to ensure a smooth transition of control during failover
- Manual maintenance failover

Figure 18 of SBC06-DPM06 Design Specification (ML091480158)

Execution Sequence for Tasks in the SYS Processor



- Operating cycle of the main (SYS) processor is 100 ms
- Task groups 0-6 are diagnostic tasks (nominally 10 ms)
- Task 7 is the application program
  - A check is performed to ensure that Task 7 is fully executed at least once each cycle
  - If not, a system alarm flag is set for fault identification and handling
  - Task 7 may be executed more than once, in a continuous loop, until the end of the cycle
  - An unfinished application task is resumed on the next cycle

Figure 5 of HFC-6000 SE (ML110831017)

Predictability and Repeatability

- Deterministic behavior is supported by design measures such as:
  - sequential execution of tasks
  - continuous loop execution of the application function
  - regular schedule for time-based routines
  - diagnostics that confirm the execution of the safety function
  - deterministic communications with preconfigured communications architectures (i.e., predefined nodes and addressing)
- The SYS processor, which serves as the safety processor, is buffered from communications transactions through the use of interposing communications processors (i.e., the ICL and C-Link subordinate processors).

Secure Development and Operational Environment (SDOE)

- The system software for the HFC-6000 platform is burned into PROMs that cannot be altered in the field.
- Any firmware change requires physical replacement of the PROMs.
- Application software for a module can be installed via PROM replacement or download to dedicated Flash memory. Either of these modification processes for application software are intended to occur while the module is out of service (i.e., out of the cabinet).
- A write protect switch on the faceplate of the HFC-SBC06 controller module allows for preventing modification (i.e., overwrite) of the application executable in Flash memory during online, in-service operation.

Amendments to the HFC-6000 TR

- After NRC approval of the HFC-6000 TR, HFC submitted two amendments to the approved TR for:
  - The closure of the six generic Equipment Qualification open items
    - Final Safety Evaluation issued in April, 2015 (ML15064A002).
  - The inclusion of additional modules that can be used with the HFC-6000 platform
    - For example, in a newer version of the SBC06 controller module, the four CPLDs are replaced with one FPGA.
    - EICB staff is currently performing the acceptance review for this amendment.

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Nuclear Protection and Control (NuPAC)

Norbert Carte (NRC/NRR/EICB)

April 24, 2015

Outline

- Background
- Description
- Key Regulatory Criteria

Background

June 2011	Topical Report (TR) Docketed
May 2012	NRC Accepted TR for Review
May 2013	NRC Sent RAI
Feb-Sep 2014	Review Suspended
Sept 2014	Palo Verde Intent to use
April 2015	First Audit
Sept 2015	Second Audit
June 2016	Evaluation to be Completed

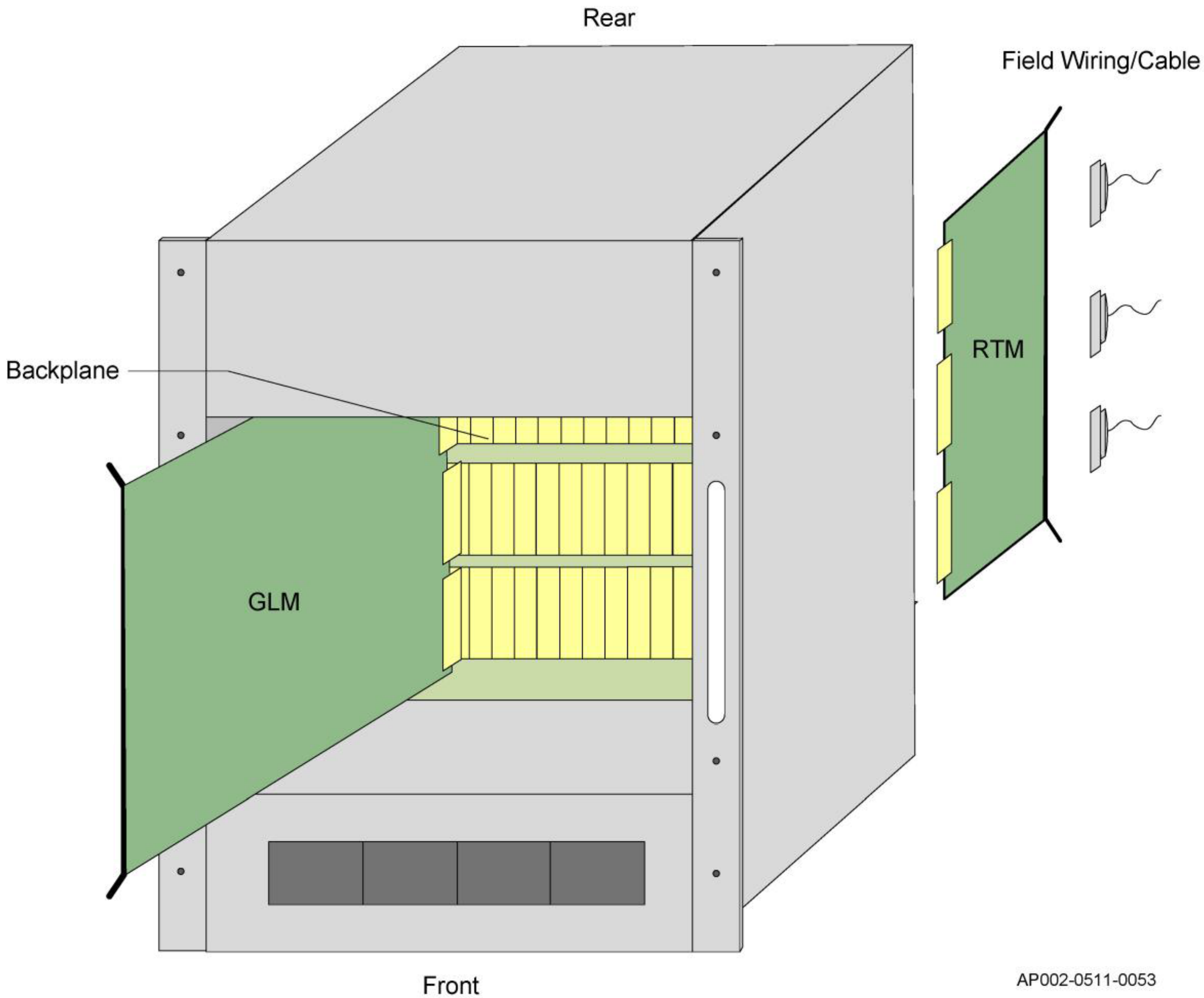
Description

- Application Framework
  - FPGA-based (no microprocessor or emulation thereof)
  - No system specific design
- Digital Communication Mechanism
- Does not Address Diversity and Defense-in-Depth
- Does not Address Electrical Isolation
- Does not Include Power Supplies

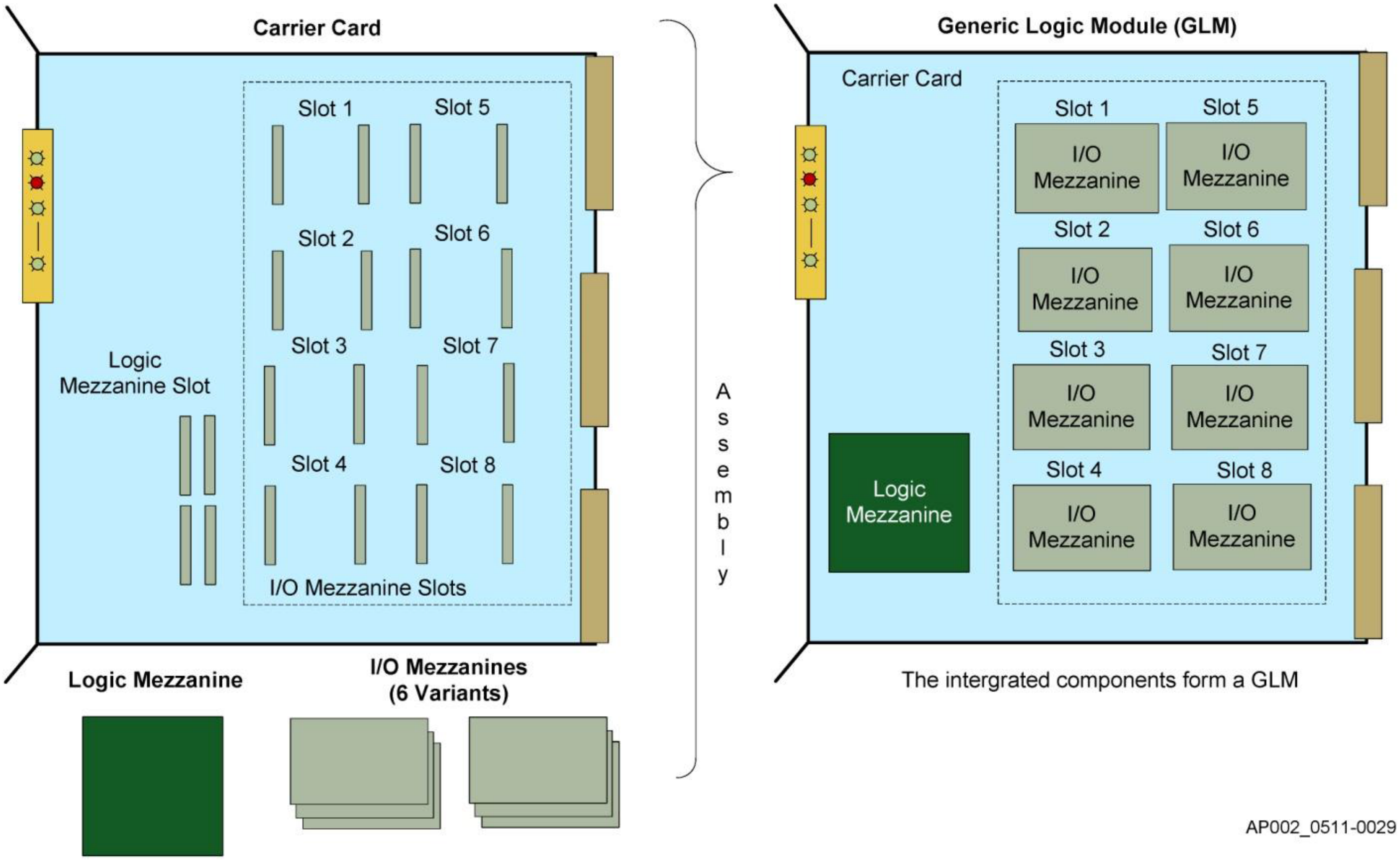
Description

- Chassis & Backplane
- Generic Logic Module - Carrier Card (Supports mezzanine cards)
  - FPGA-based Logic mezzanine
    - Parallel Processing
    - No Interrupts
  - I/O Mezzanines
    - Serial Communication RS-422
    - Analog Input and Analog Output
    - Discrete/Pulse Input
    - Temperature Input
    - Solid State Relay Output
- Rear Transition Module

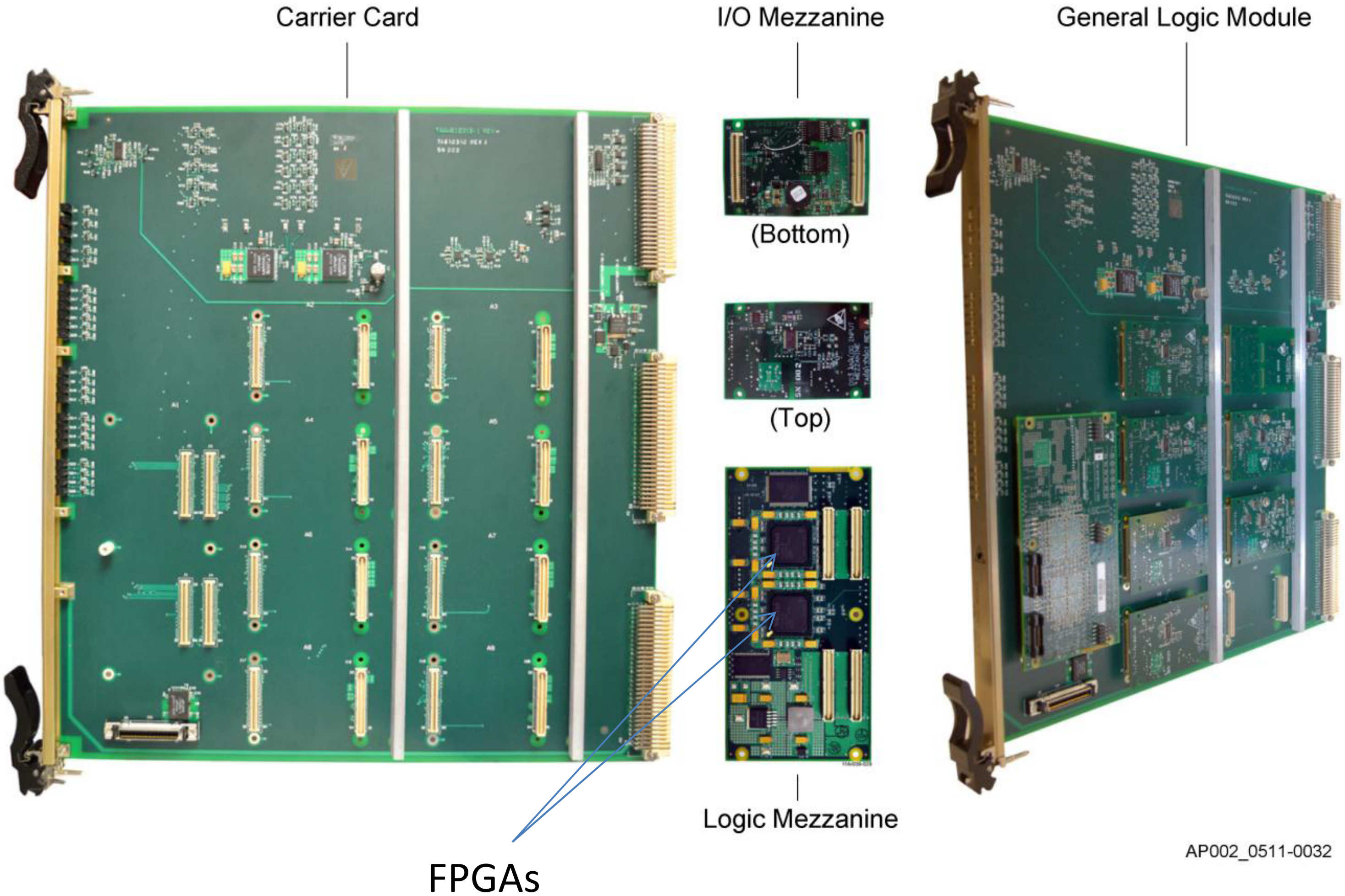
Description



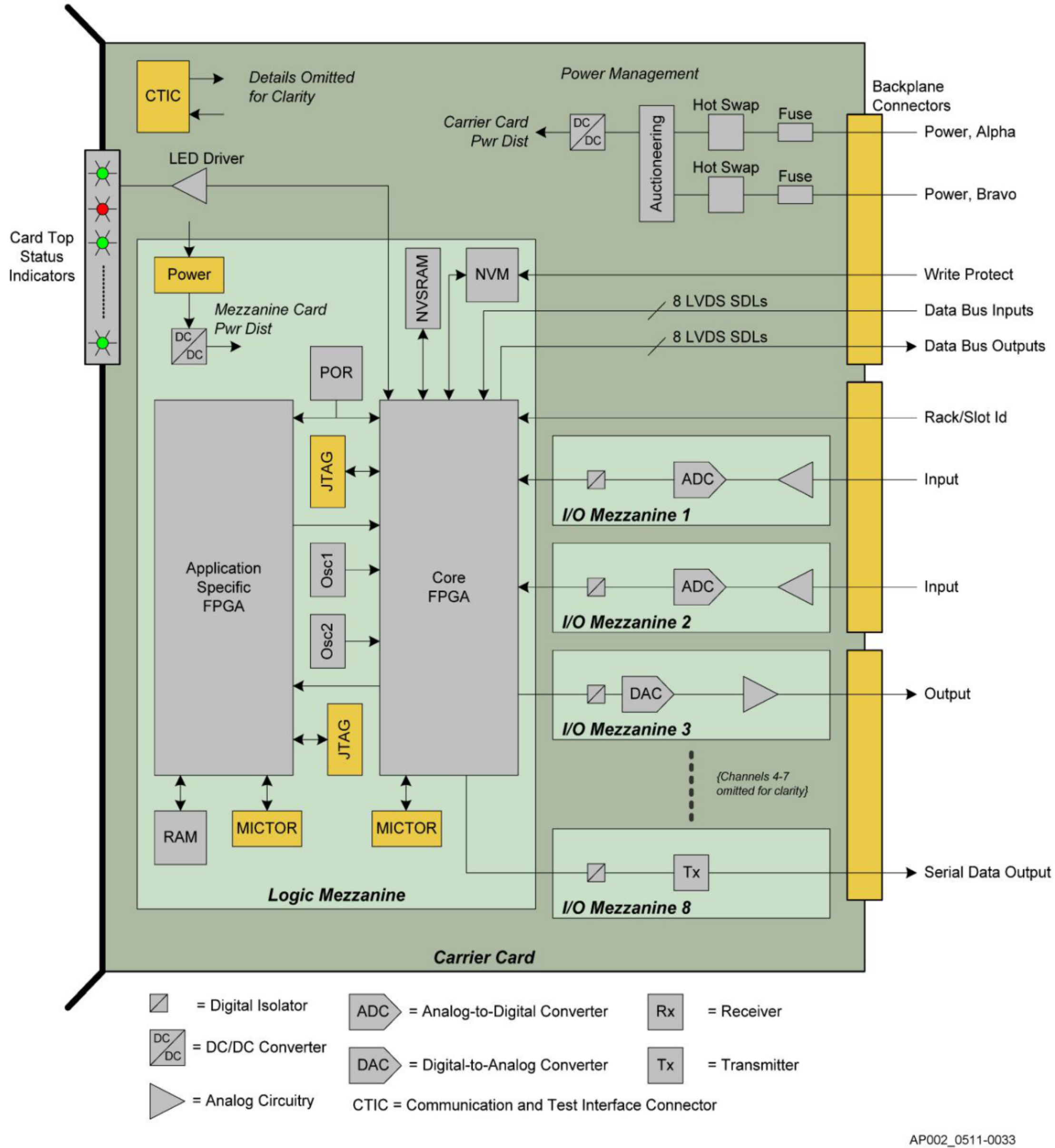
Description



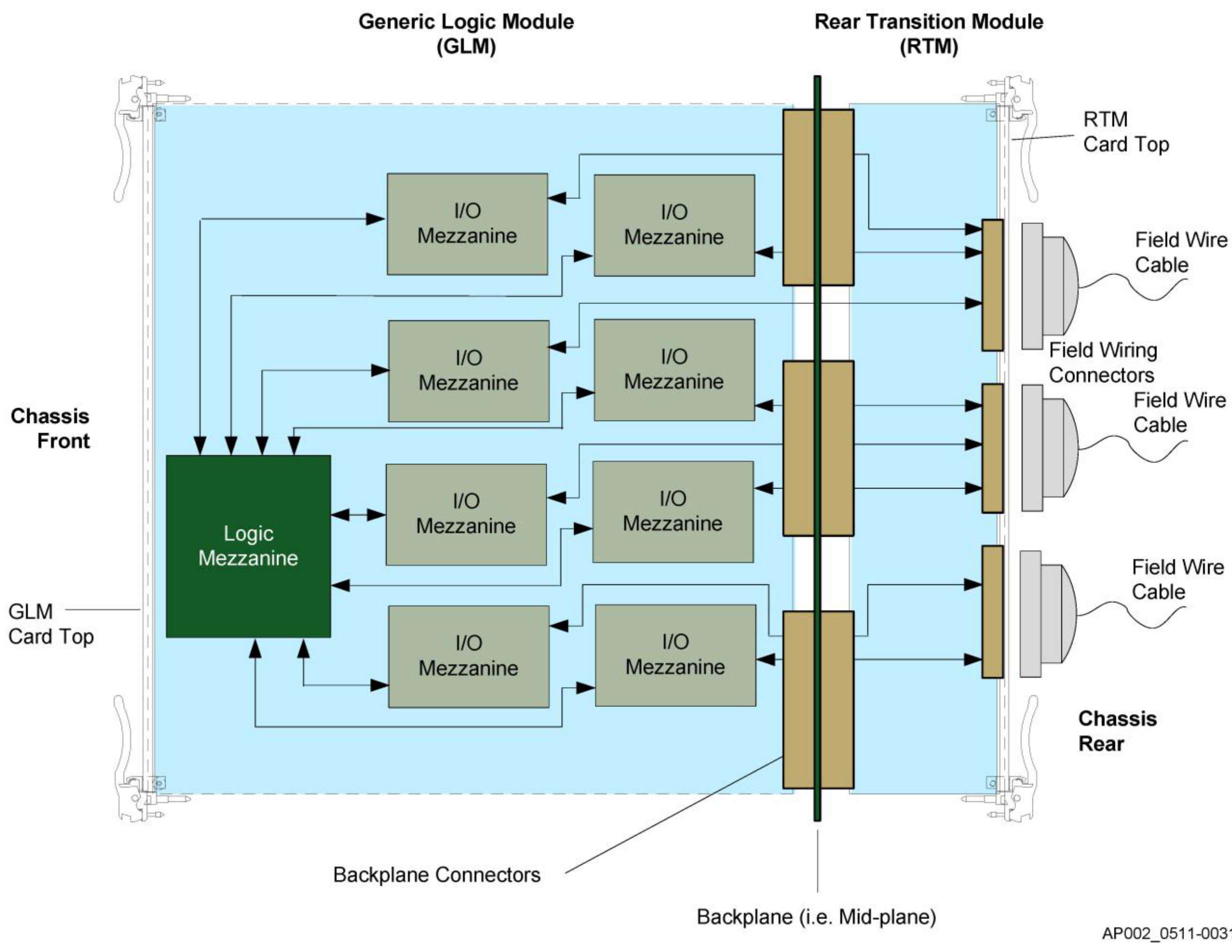
Description



Description



Description



Key Regulatory Criteria

- Independence
  - ~~Electrical~~
  - ~~Information~~
  - ~~Segregation (physical independence)~~
  - Communication Mechanism
    - Serial Communication Card (RS-422) & Core FPGA
    - Byte level
- ~~Redundancy~~
- Predictability and Repeatability
  - Communication heartbeat
  - Invalid state machine detection
  - Analog output control loss (WD)
- Secure Development and Operational Environment (SDOE)
- ~~Diversity and Defense-in-Depth (D3)~~

Questions?

Backup Slides

Embedded Microprocessor System Determinism

- Microprocessor / Interrupt Based Paradigm
- Common processing provides all functions
  - Serial Execution
  - All function share limited resources
- Independent watchdogs can mitigate risk
  - Function stalls results in watchdog action
  - Potential to interrupt functions

NuPAC Platform FPGA Determinism

- Latency Requirements
  - Declared for each FPGA functional requirement
  - Resource Allocation
    - Dedicated to function if necessary
    - Shared among functions if necessary
    - Allocation performed to guarantee max required latencies
- Dedicated Resources
  - Custom Finite State Machines (FSM)
  - Fixed / Tightly Controlled State Sequences & Latencies
  - Massively Parallel Function Execution
    - Provides very low latency
- Resource Sharing
  - Equal and repetitive access to all functions
  - Deterministic sharing of resources achieved through fixed sequence dedicated access

Verification of Deterministic Performance

- Covers each and all required functions
- Constrained Randomized Stimulus
  - Includes randomized injected errors
  - All functions execute simultaneously
  - Verifies required latencies
- Randomized and Repeatable

Acronyms

ASIC – Application Specific Integrated Circuit

CPLD – Complex Programmable Logic Device

D3 - Diversity and Defense-in-Depth

FMEA – Failure Modes and Effects Analysis

FPGA – Field Programmable Gate Array

ISG – Interim Staff Guidance

LIC – Licensing

NPP – Nuclear Power Plant

NRC – Nuclear Regulatory Commission

NRR – Nuclear Reactor Regulation

NuPAC – Nuclear Protection and Control

PLD – Programmable Logic Device

SDOE – Secure Development and Operational Environment

SRP – Standard Review Plan, NUREG-0800

TR – Topical Report