DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, as reported herein, is a record of the discussions recorded at the meeting.

This transcript has not been reviewed, corrected, and edited, and it may contain inaccuracies.

Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
ESBWR Subcommittee: OPEN SESSION

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, October 22, 2009

Work Order No.: NRC-3161 Pages 1-91

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)

+ + + + +

SUBCOMMITTEE ON ESBWR

+ + + + +

OPEN SESSION

+ + + + +

THURSDAY

OCTOBER 22, 2009

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee convened at the Nuclear Regulatory Commission, Two White Flint North, Room T2B3, 11545 Rockville Pike, at 8:30 a.m., Dr. Michael Corradini, Chairman, presiding.

SUBCOMMITTEE MEMBERS PRESENT:

MICHAEL CORRADINI, Chairman

WILLIAM J. SHACK, Member

JOHN W. STETKAR, Member

CONSULTANTS TO THE SUBCOMMITTEE:

THOMAS S. KRESS

GRAHAM B. WALLIS

NRC STAFF PRESENT:

CHRISTOPHER BROWN, Cognizant Staff Engineer

KATHY D. WEAVER, Cognizant Staff Engineer

AMY CUBBAGE

IAN JUNG

DENNIS GALVIN

HULBERT LI

LAURA DUDES

ALSO PRESENT:

HERBERT BUTLER

RICK WACHOWIAK

IRA POPPEL

TABLE OF CONTENTS

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

(11:20 a.m.)

CHAIR CORRADINI: Why don't we get started? So, we're in our third day of our ESBWR subcommittee for the ACRS. My name is Mike Corradini, Chair of the subcommittee.

Today, we have a new group, or a modified group of subcommittee members in attendance. Professor Abdel-Khalik will be here eventually. I think Dr. Armijo and Dr. Banerjee may not be here, but we have a new member Dr. -- or Mr. Stetkar. Excuse me. Don't want to give you that vaunted title. As well as our consultants, Tom Kress, Graham Wallis and Bill Shack.

The purposes of the meeting again is to review resolution of reactor systems, mechanicals systems and I&C systems, and cybersecurity issues for the ESBWR design certification. I will skip over a lot of the preliminaries since we've been discussing this throughout the week. We have with us today GEH Nuclear Energy, as well as the staff, and our main focus today will be on instrumentation and control systems.

Let me remind everybody the rules of participation in today's meeting. They've been announced as part of the notice of the meeting in the Federal Register on September 28th. A transcript of the meeting is being kept and will be made available as stated in the Federal Register notice.

It is requested that speakers first identify themselves and speak with sufficient clarity and volume so that we can readily be heard. And also, I wanted to make sure everybody puts their cell phones on silent mode.

We have not received any requests from the members of the public to make comments, okay? But we do have a bridge line open. We are going to have two parts to the meeting. Before our break, we're going to have discussions on I&C that will be open, and we have an open bridge line. Then after the break, we will go into closed session because some issues that are going to be discussed are protected information, designed as part of the proprietary work of GEH pursuant to 5 USC, or security related information.

I'll ask the staff if they have any other comments before I turn it over to GEH.

MS. CUBBAGE: Sure. I'll just give a brief background of the topics and why we're here.

The first topic is a follow up from the subcommittee meeting we had almost a year ago now, December last year.

There was some specific items of concerns that were addressed by the subcommittee. I'll note that Charles Brown was one of the ones that had some significant comments, and I'll note that he's not here today. So, I hope that this information gets back to him because we're not going to be able to go through this level of detail at the full committee.

Also, we have an additional topic of cybersecurity. That's a topic report that the committee has not heard about before. So, those are the two topics today, and I'll introduce -- did you want to go ahead to GE now?

CHAIR CORRADINI: So, just go ahead to GE. Is Rick going to lead us off, or Ira? Who is --

MR. BUTLER: I'll lead off.

CHAIR CORRADINI: Herbert will be first.

MR. BUTLER: It's Skip Butler. Herbert is my full name. I'll be the lead presenter on the ESBWR Engineer Manager for I&C. On my right is Ira Poppel. He's principal engineer and lead designer for I&C on the ESBWR, and to his right is Lloyd Heckle, who is our software QA manager, and who has been instrumental

in developing some of the things that we'll present here today.

Also, you'll hear later from Matt Bohne, who is our cybersecurity lead. He'll join us at the front at that time. Okay, if we could go to the next slide, Rick?

Just to step through the high level topics, we'll talk about the changes from Rev 5 to Rev 6. They have been substantial. When we met on December 3rd, there was a lot of work in progress, but unfortunately for the ACRS committee at that time, you weren't privy to it because it wasn't part of Rev 5. But there has been a significant amount of work done over the last nine months. That's to say the 4th quarter of `08 through June, when we submitted the preliminary copy of DCD Rev 6.

We got some feedback from that meeting, from the ACRS, and we'll touch on that. We broke the pitch into three main parts: regulatory compliance, the software systems and software design process, the I&C design principles, which really focus on IEEE standard 603 compliance, which really stands the test of time, even in the digital age. Then we'll close for some questions.

So, first of all, this eye chart. I'd

just like to highlight the topics on the right. The RAIs are obviously the staff's request for additional information. The ECAs are engineering changes from GE. The cars are the corrective actions; the LDRs are minor licensing deficiency reports or tracking items.

CONSULTANT WALLIS: Let me interrupt with a question. I mean principles is a long way from final product. How do you know when the final product is good enough? You can have determinacy to infinity, or a tiny bit of it. How do you know when it's enough with I&C?

MR. BUTLER: We will present that in one of the slides, and there's actually a backup calculation that demonstrates that.

CONSULTANT WALLIS: So, you're going to get to that?

MR. BUTLER: We're going to get to that.

CONSULTANT WALLIS: Principle seems an awful long way. It's like saying you've got the general design criteria, and now you've got the answer.

MR. BUTLER: I think we have a bit more than that, and we hope to convince you of that. Okay, just to highlight on this, I would say there's been a substantial amount of work first suggested to us in

RAIs from the staff, but also we took those RAIs, and ensured through our appendix B program that the conforming changes that were necessary through the LTRs and through the entirety of the document all chapters were addressed, and that's why the GE driven component is there.

So, the guidance back from the ACRS committee on the 3rd of December can really be summarized into two main points. One was a concern about the design and development process for digital I&C for the ESBWR, and the ACRS committee asked for RAIs to help highlight and expand upon that.

Actually, the majority of those RAIs the staff had already issued to us. They just weren't ready for submittal, and so they weren't presented on the 3rd of December. The second point has to do with level of detail. Again, there were a number of RAIs culminating in our last RAI, which is RAI 7-1.139, which really spoke to additional level of detail, and we'll present that as well.

Okay, just to add some perspective around the recommendation for enhanced design process, and the DACs to support it, there was about an 80 percent increase in DACs from Rev 5 to Rev 6 for I&C, and if you just look at the perspective here, whether you

look at the DCD page count, or the chapter count, the number of DACs for I&C are 663, okay? So, I'd like to present that in a little bit more explanation. So, hold on.

So, the first part of that is that if you look at a digital implementation, a significant part of that is the applicant software that is going to be the first of a kind for any new plant to be licensed in this country. So, if you follow the IEEE standards for a system and software development process, GEH thinks that you have to have a number of specific design, audit and hold points. Those are all very well articulated in our LTRs for the software development plan, the software QA plan and cybersecurity plan.

And so, really a significant number of these DACs are specific to ensuring that all applications on all the software platforms adhere to the IEEE standards, starting with 603, and follow a structured approach with traceability.

The rest of them are based upon ensuring that functions to be performed on each one of those platforms for the safety function are met and testable. That's where the DACs and ITAACs come from, and they're really based on that, as well as the

diversity that we have in our overall system, which we'll hit later.

Okay, to speak -- one example to provide additional design detail, the last RAI that we received on this topic, and there were several, is RAI 7.1-139, and specifically the staff asked us to provide additional architectural detail and design in block diagram format to ensure that there was a real design for each one of these safety functions within each platform.

And so, we've done that by adding eight new figures, revising nine figures, and obviously, there's a significant amount of table and text that goes with those revisions to the DCD.

MEMBER STETKAR: Are you going to go through some of those figures later, because --

MR. BUTLER: We can. They're in back up.

MEMBER STETKAR: Okay. Let me ask a fundamental question then because we did raise the issue about two years ago of why GEH does not include in the DCD functional logic diagrams that show the actual -- I'm not talking about details now, middle-level information, signal inputs, coincident logic, including interlocks, manual signals, automatic for each -- for all of the protection and safeguards

functions. We've been asking for that now for two years, and we still don't have it.

MR. BUTLER: I would note, and this is perhaps not tactful, that all of the other vendors are including those in their DCDs so that we can indeed look at an integrated instrumentation and controlled system design, and determine what signals are the input signals, how those signals are processed in real logic, how they're combined with both manual inputs and interlocks, time delays, and look at the output signals.

That's very, very important for a design overview to see how the integrated design will really work for pinch points. We've learned an awful lot in 30 years of experience that adhering to very focused specific design criteria for individual functions does not necessarily provide an integrated design that indeed is a -- I don't know what the correct word to use is. Perhaps prudent design is the best word.

And yet, we still don't see those logic diagrams that -- that the -- the eight diagrams that you've mentioned are not that type of diagram. They're a much simpler, higher-level non-specific type of information.

So, I guess I'm still left where we were a

year ago with respect to the information regarding the integrated design at that level of detail. And again, I'm not -- don't get me wrong. I'm not trying to emphasize detail of -- of chip sets or lines of code, or anything there. I'm back up at somewhere between the information that exists now in the DCD, and -- and basically the equivalent of the information that is traditionally provided in a Final Safety Analysis Report.

MEMBER STETKAR: So, there must've been an active decision made about why those types of diagrams were not included in the DCD, and I'm rather frustrated about that.

MR. BUTLER: Okay, so we have shared in an informal way the preliminary logic diagrams with the staff. They've been given an opportunity to walk through those. What we were asked to do in the RAIs was to provide additional detail at the level of the block diagrams. We've done that.

What we've committed to do with the extensive number of DACs is to provide the information related to the detail design, the logic diagrams, the SDSs. All of that material that you may be seeing with the other vendor submittals will be available to staff review through the DAC process. So, we're not

trying to not provide that information. We're providing that information at a later date using the DAC process, and the LTR's that we've committed to are extremely vigorous with hold points that allow for these review packages to be developed for staff audit.

MS. CUBBAGE: I just wanted to clarify. I think you said they were provided informally. They were provided on the docket, which is not part of the DCD.

CHAIR CORRADINI: Okay, say that again, Amy. I'm sorry.

MS. CUBBAGE: The logic diagrams were submitted on the docket, and provided to the ACRS.

MEMBER STETKAR: Okay, two questions. Yes, indeed, we -- we got those, and I have them. I looked at them two years ago. But it was my understanding that they were not necessarily directly related to the ESBWR; that they might be somewhat preliminary and generic in nature, at least the set that I saw.

MS. CUBBAGE: Well, they're related to the ESBWR, but they are not -- they don't have finality.

MEMBER STETKAR: Right. Well, I guess the concern that I have is that if the design is not final at that level, what design are we certifying? If the

design is not final because these diagrams are preliminary, and for whatever reason are not included in the formal design control document, what exact design are we certifying? I mean the -- because they're not final, and won't be final until apparently few -- prior to fuel load, at least on North Anna.

MS. CUBBAGE: I think it'd probably be best if we let GE continue, and you can ask that of the staff when we present.

MEMBER STETKAR: Okay.

MS. CUBBAGE: But I guess the bottom line is that's currently not a level of detail that we are reviewing for certification.

MEMBER STETKAR: Okay.

MR. BUTLER: Okay, next slide. Okay, what we wanted to show here was the rigor with which in tier 2 chapter 7, we've identified the regulatory requirements for each one of the platforms. So, in this chart, upper left, you'll see that there is a series of columns, each one of those columns represents one of the systems rolling up to one of our diverse platforms. We have three diverse safety platforms for our D3, and on the left are all the regulatory requirements specific to a digital INC, software-driven system.

The middle chart on the left takes that one step further, where we've taken all of the critical 603 criteria, and we've also associated them very explicitly with each one of the systems that roll up to the platforms. Then within each section of the chapter, there are summary regulatory conforming statements having to do with things outside of digital INC and software instrumentation and so forth.

So, that creates the entire packet for chapter 7 of the Regulatory Compliance. We've done that in a structured way so that we can have a cross-reference and traceability mapping to the Tier 1 commitments. The Tier 1 commitments basically have two components. One is the system-driven or NPL driven aspects of each one of the systems and functions for the safety system, and then the Tier 1 DAC and ITAACs. There's a complete traceability matrix for all of that.

MEMBER STETKAR: Again, I haven't been reading through your slides quickly enough. So, slow me down.

MR. BUTLER: That's okay. The first part you can take advantage of once in a while.

MEMBER STETKAR: Okay, I'll do that. Was there a change between Rev 5 and Rev 6? You mentioned

now that you have three -- you call them independent diverse platforms. In Rev 5 there were -- in my thinking, I'm not a digital INC design guy. There were three platforms. How -- have you made changes between 5 and 6 to the definition of those platforms, if I can use that term?

MR. BUTLER: No, no. The only thing that we've done --

MEMBER STETKAR: Because there's not an ICP that used to be the ATWS Standby Liquid Control System.

MR. BUTLER: Right. So, in the first slide I tried to show that there were a number of LDRs, licensing deficiency reports, that were raised internally to identify a lack of clarity and consistency with which we described the architecture in the system. So, really, from Rev 4 through Rev 6, the architecture has not changed.

MEMBER STETKAR: The architecture is basically the same, okay. That's what I thought. I just wanted to make sure that there was more of a descriptive process than kind of what you're --

MR. BUTLER: Right. And so, with that as the backdrop, what we did do with respect to an ECA was to add one additional implementation of ICP, which

is for the HPCRD. That is not an architectural change. That's an additional function to meet the requirements of the Safety Analysis in the PRA.

MEMBER STETKAR: I'd like to -- I want to make sure you have enough time to get through your presentation. I want to come back to that HPCRD in particular, because although it's a specific function, it's an example of the type of information that I'm looking for in terms of the I&C. But I know it's too detailed for now, so get through the presentation. Let's try to save a little bit of time at the end.

MR. WACHOWIAK: I think that particular is one of the items that we are going to discuss in the November meeting that specific.

MEMBER STETKAR: Okay.

CHAIR CORRADINI: Will you be here in November?

MEMBER STETKAR: Yes.

CHAIR CORRADINI: Good. Let's move on.

MR. BUTLER: So, the key takeaway here is that the regulations serve as the fundamental basis for quality, safety and reliability, and we feel very strongly that we've done an exceptional job mapping those requirements, including a 603 matrix that is traceable to Tier 1.

Okay, so we need to have a software and systems development process. Ours is IEEE compliant. We've worked on this for a number of years to ensure that we have one that will stand the test of time in an implementation for the entirety of the DCIS. What this chart tends to show is in the first waterfall model, our software management plan, which really serves as the overall framework or skeleton for the development of the I&C systems in hardware and software.

To the bottom left -- excuse me, to the upper right is our software quality assurance program manual, and the fact that these DACs and ITAACs are just a sampling of the design and hold points where an independent review will occur, either a peer review or verification review, to substantiate that the design is ready to proceed.

Then in the bottom left is the cybersecurity program plan. You'll hear more about that in our closed session.

The important thing here is that these three documents work together so that all of the entrance and exit criteria to a review step are integrated with one another; they're traceable, and they're documented with reports and bases documents in

our documentation control system.

Okay, so for the procedure design and the design principles, really we wanted to focus on five main themes: simplicity, independence, redundancy, determinacy or deterministic behavior, and diversity.

CHAIR CORRADINI: This looks like something I have at the university. I like this foundation.

MR. BUTLER: We try and have one.

CHAIR CORRADINI: Thank you.

MR. BUTLER: Otherwise, we wander.

CONSULTANT WALLIS: It's so high-level. This looks like a preliminary lecture, though.

CHAIR CORRADINI: Well, this is -- I understand this. Keep on going.

MR. BUTLER: Okay, so -- all right, so the next -- okay, so it's sometimes useful to define our system based upon what we do, and what we don't do. So, I just want to make it very clear to the staff, and to the ACRS committee that is reviewing many designs, both in the retro-fit fleet, and new units.

What we don't do: we do not mix signals of safety and non-safety in a prioritization module concept. That is not what we do for the ESBWR. We keep each one of our safety functions, subsystems and

platforms independent, separate, isolated and diverse to achieve all the safety functions including diverse actuation.

Okay, so let's take a look at RPS, Reactor Protection. This is a derivative block diagram from 7.2-11a, which is in the back up, and what we try to convey here very clearly is everything is broken down into simple blocks for sense, command and actuate. Each one of these functions is clearly defined in the system design descriptions, and the logic diagrams, and in the implementation and hardware that we have that is targeted. Mike?

CHAIR CORRADINI: No, no. I'm just --

MR. BUTLER: Okay.

CHAIR CORRADINI: I'm trying to look for things as you're talking. I'm sorry. Excuse me.

MR. BUTLER: Okay. So, what we're trying to convey here is that is that an implementation of a power plant's DCIS is a very complex endeavor, and will be a very complex delivery, but you need to break it down into simple parts.

So, we have a lot of simple parts, but each one of the simple parts basically follows this approach: there is a solution to be achieved. There is a platform, a diverse platform, picked to implement

it on. It is broken down into system functions and components, and each one of them is clearly identifiable, and where appropriate has an audit and hold point in the three LTR's, and a sample thereof is in DAC or ITAAC.

Okay, go to the next chart. Okay, independence: this is a bit of an eye-chart, but you'll see at the bottom below the big, dark line, the safety system and the four divisions. So, each one of the shades of green represent a clear and distinctly separate implementation per division for the three diverse platforms.

So, we'll see this chart again when we talk about diversity, but it's important to note that the only communication that is allowed to occur between RTIF, NMS, as well as in that layer and between SSLC/ESF and the four divisions of that layer is the two-out-of-four voting, which we've had in the analog days as well. That is the only thing that communicates between those four divisions. Nothing in the safety system communicates with DPS, which is in the shaded blue.

Okay, so the next chart. Okay, in the area of redundancy, first of all, all of the safety DCIS meets the redundancy principles in IEEE-603 for

censors, controllers and actuators. In particular, for SSLC/ESF, that has -- within each division, it is self triply redundant, and that's to ensure that we do not have an inadvertent actuation because that system has the capability of firing the squibs, which of course we want to happen when it needs to happen. You absolutely don't want it to happen when it shouldn't happen.

Similarly, all safety DCS design is single failure proof, and this is -- okay, and this is to ensure that there is no unintended, inadvertent actuation throughout -- throughout the system. Okay, in short, the DCIS does not act as a credible initiator to an inadvertent event.

Okay, all of it is redundantly powered, primary power, as well as power in the cabinet or the chasse. So, that's to ensure that there is absolutely no reason that safety power doesn't reach the controllers or the IO packs, or anything else. Also, on the non-safety side, we are also redundant. Either dual redundant, or triply redundant.

Okay, determinacy or deterministic systems: This was an interesting topic for discussion on the 3rd of December. We do make a commitment to deterministic behavior for the digital I&C, both the

controllers as well as the networks.

We wanted to clarify for the Commission, as we have for the staff, that for us, a deterministic behavior for digital I&C is not that something happens absolutely at the same point in time, but it happens predictably based upon inputs and outputs in the required period of time. This is a pretty common definition for all digital systems.

What we would like to say in conclusion for this definition at a high level is that we don't perform control functions, closed-loop control over some sort of common network. All of the control loops are on their own dedicated network.

Each one of those dedicated networks or network segments is specifically engineered, and controlled, and is not changeable so that we assure determinacy in all of the communication channels, which it's for the RTIF, system platform, or the SSLC/ESF system platform. And they are not shared between division, or between platforms. They're dedicated networks designed and controlled to ensure a deterministic behavior for the exchange of data.

Okay, the controller. Again, we had a lot of conversation on the 3rd of December about deterministic behavior and the controllers. What we

would like to convey very clearly is that for the safety system controllers, as well as for DPS, the communication is buffered or isolated from the controller in its program loop so that the program loop in the controller will always proceed through it's algorithmic process in the stated period of time, independent of whether or not data comes in or not.

Of course, the application layer code will look for is the data present, and is the data what I expect? But presence or not of data on the memory busses that the controller can read is not in any way going to adversely affect the programming loop of the controllers used in the safety system or DPS.

CONSULTANT WALLIS: Do I misunderstand that is you're asking something to control, the position of a control rod, you can tell it -- you have an input, and then you have to measure where the control rod actually is, and have some feedback that goes back to --

MR. BUTLER: Correct.

CONSULTANT WALLIS: So, it's not -- it needs the data in order to control properly, doesn't it, to know that it is controlling properly?

MR. BUTLER: It does, right.

CONSULTANT WALLIS: I get the impression

it's also the forward stuff here. You have to have this feedback --

MR. BUTLER: Well, we actually have an animation, but we're not allowed to share that with you. But what I would say is that --

CHAIR CORRADINI: That helps, thanks. Go ahead,

MR. BUTLER: The point that we're trying to convey here is that the data that is required for the application program to run the logic to perform the safety function is made available. Ira, the little pointer? Is made available outside the controller on these shared memory locations. The shared memory location is an implementation to ensure that the data that is required will appear in the memory register that will be read by the controller, but in a controlled way so that this is isolated so that there's no way for data coming in from this data feed for the data acquisition can interrupt the programming or the memory used to run the program.

The controller is isolated from that portion of the world that it needs to interface with.

CONSULTANT WALLIS: But whether it works or not cannot be independent of the mechanics of the thing it's controlling, can it?

MR. BUTLER: Again --

CONSULTANT WALLIS: I don't see how I&C can ever be designed by itself, because it's controlling something which itself has response characteristics.

MR. POPPEL: There are -- there are two answers -- directions your answer can go. The first thing is these are safety systems, and as indicated, VPS. Okay, they're doing things like saying, we need to make sure that when the reactor level gets here, the reactor scrams. Okay, that's the control loop. They -- the visions acquire their own data at a specific time in the --

CONSULTANT WALLIS: It tells a lot about the thing which is measuring the level, then this can affect the whole system, can it not?

MR. POPPEL: For that division.

CONSULTANT WALLIS: Yes. So, you have to know something about things that can happen to the way in which you measure the level, and when you design the controller, don't you?

MR. POPPEL: Yes.

CONSULTANT WALLIS: Or, is it completely independent?

MR. POPPEL: No. We have data quality

checks, okay? But for example, we can't fix or deal with a broken transducer.

CONSULTANT WALLIS: No.

MR. POPPEL: If the transducer is erroneously indicating level, okay, then we say, there's our divisional failure. We've got three other divisions where -- and in our case, we could have two other divisions that are -- assume correctly indicating level, and that two-out-of-four voting logic in all divisions will result in the right thing.

The point is the acquisition of level in -- within the division is the control loop. The data coming in horizontally, the two-out-of-four data from the other divisions trip data is asynchronous. Division 1 can't control or ask, or deal with when Div 2 sends it in. It's just that Div 1 looks, and it's memory location 3, and sees that there's two trip data without any indication of how it got there, when it got there, or why it got there, okay? And so, that's this.

The thing you mentioned about control rod positioning isn't a safety system in the ESBWR, and you are correct that obviously if you're positioning a control rod, you need to have feedback where it is. That reverts to Skip's previous comment in that the

reactor can -- the rod control and information system, RCIS, is its own system.

In other words, it needs to know where control rod position is. It measures control rod position redundantly. It pulls it. So, RCIS is saying, I'm responsible for knowing where it is. And by the way, I'm not getting that data from some other system over the network. It's my system.

Okay, now I happen to send that data to other networks so other people can see rod position, but I don't care whether other people see rod position. I can control rods whatever happens to the data once it leaves me.

And so, yes, we do have that, but that's non-safety. It's not quite the same thing as this, but we don't mix control over the network. Another way of saying that is our non-safety networks can go down, and all the controllers will control autonomously. Completely they could go down.

They won't go down because they're redundant. They've got all kinds of good stuff that Skip mentioned, but nevertheless, we are not dependent on them for anything but operator input, alarms and stuff like that. Plant stability and control is assured without the networks.

CHAIR CORRADINI: Okay, go ahead.

MR. BUTLER: Okay, determinacy in the communications. So, we have a lot of communication data links. We call them networks or network segments. We wanted to show some examples, and to discuss briefly how they are deterministic.

So, in RTIF, there are intradivisional communications. We're showing those in blue, and we have interdivisional for the two-out-of-four voting. And we have a safety network, which is communicating to the non-safety, and that's in green. The green and blue are implementations in Scramnet, which is a brand name for Reflective Shared Memory, which is a mechanism whereby you design and configure the network and its nodes so that it's deterministic what the network it, and when you configure and deploy the network, it becomes totally hardware based. There's not a software overhead that runs, and the communication happens by having each node broadcast to the appropriate nodes that it needs to place data in.

That process happens on the order of nanoseconds, tens of nanoseconds depending on the size -- no it's microseconds. Sorry, yes. Sorry.

MR. POPPEL: Next year will be nanoseconds.

MR. BUTLER: Yes, next year will be nanoseconds.

CHAIR CORRADINI: No, I'd just rather have a design that any time -- go ahead.

MR. BUTLER: Okay, so microseconds. So, for the purposes of the cycle time required, or response time for the reactor protection system, which for a BWR is in tens of milliseconds, this system is deterministic once deployed and configured. It is hardware based, and it's an order of magnitude, or two or more faster than is required by the reactor protection plant process response times.

Okay, that's how we share the data between the divisions, and how we share the data from the RTIF platform to the non-safety broadcast elements in green. Okay, so that's one example of a network implementation that is totally dedicated to this technology platform.

In the next slide, we'll show the diverse communication network protocol for the SSLC/ESF. If you go to the next slide, which is 2 of 2. So, again, we have to have a way for the is SSLC/ESF to perform the two-out-of-four voting. We are using Ethernet to do that, and the way in which we assure that this protocol and media is deterministic is to control what

is going to be put on the network.

So, the message and its content size and the transmit rate that is required in order to achieve the response time for the functions that's being implemented. So, here we have an Ethernet network. It's 100 megabits or more, depending on when we implement the first one. And it only is running an infinitesimal amount of data so that for all practical purposes, collisions or the probability of a collision is infinitesimal. So, this will always deliver the message between the divisions.

MEMBER SHACK: This does nothing but deliver the result of the voting?

MR. BUTLER: It does nothing but carry bypass status, trip status and message authentication and quality. So, it only carries three things. This network, once set up, is between the four divisions of SSLC. Nothing else will be allowed to be on this network, and it is configured and locked down at the time the system is deployed and tested.

It does not communicate with any other network in the safety systems, or a shared non-safety network anywhere.

MR. POPPEL: Another way of saying that it doesn't communicate is there isn't any other

components of any other network on this network. The only thing on it is Div 1, Div 2, Div 3 and Div 4. That's why we're very sure that it's not going to be communicating with anything else.

MR. BUTLER: Okay, so the next one. So, diversity: we feel very strongly that diversity is a critical aspect of safe and reliable digital nuclear power plant. This chart, which is presented both in Chapter 7, Tier 2, as well as in the D3 LTR is our concept for diversity.

You'll see on the safety side there are three clearly diverse platforms, RTIF NMS, SSLC/ESF, and the independent control platform. And on the right are the non-safety platforms. The most important one is the DPS in terms of providing for the overall safety functionality of the plant.

So, if you go to the next slide, what we've tried to do here is bring this into a derivative graph of Figure 7.1-1. So, here, we're presenting the horizontal layers to clearly communicate that the ICP's in dark green, they are microprocessor and operator -- operating system-free implementations and programmable logic.

They are diverse from the RTIF NMS platform, which itself is diverse from the SSLC/ESF

platform; each one of them being modular in their own right, in a different technology stack in hardware and software, each one of them not communicating between the layers. And of course diverse protection system. Okay, next chart. Any questions?

CHAIR CORRADINI: John?

MR. BUTLER: We have backups of many functional diagrams. I think in terms of -- while John is thinking, I'll fill the non-awkward silence space, and say that I think in terms of the key questions that we saw with the staff from the ACRS meeting on the 3rd of December, particularly the comments provided to us by Charlie Brown, we've tried very hard to address them in quite a few RAIs, and self initiated corrections to Tier 1 and the LTRs, and to serve -- have that serve as the basis for the Tier 1 DAC and ITAACs, which particularly on the DAC side should assure that the design is safe and fit for use.

CONSULTANT WALLIS: So, there's no measure of success at the end? I mean in all design processes I'm familiar with, you have your potential for design, and you set out some specifications and all that stuff. Usually, they have some numbers with them. When you get to the end, you say, did my design meet my objectives? And I've got some measurement I

compare it with, specifications, and probabilities of success, and failure and all that stuff, and I know the thing will work according to the way I want it to work.

At this time, I don't have any measure of whether it will work according to the way I want it to work. That's the problem I have with the I&C, and I'm just an outside looking in from another field. Is it ever going to happen that you're going to have this sort of --

MR. BUTLER: Yes.

CONSULTANT WALLIS: -- measure of how well you're doing at the end of it?

MR. BUTLER: Yes, and the -- the formulation of those detailed documents are done as part of preparing for each one of the baseline record review events that are part of the life cycle steps that we go through. All of that is identified in the SMPM principally, but complemented by the SQAP, and then the cybersecurity --

CONSULTANT WALLIS: I don't know what those mean.

MR. BUTLER: Okay, those are the licensing topical reports that describe in detail what the development process is, and for each one of the six

primary system and software development lifecycle states, there are clearly described minimum entrance criteria and exit criteria with the requirement that the design basis is thoroughly documented, and that summary audit packages are presented for licensing and staff review.

MR. WACHOWIAK: And so, let me -- let me take that one step further, going into what's in our Tier 1 document. Skip mentioned earlier that there are many, many times now in Tier 1 associated with this, and it's just exactly what you're talking about there. There's the step to take the currently reviewed document, like the software management program plan, one of those. It says you need to do something for this platform.

We do the something, and that's one of our line items in Tier 1 that gets checked as part of the DAC closure. Then you take that, and you do something else with it. In some cases, it's a -- it's the factory acceptance test. I'll jump down to some of the other steps.

Factory acceptance test: that's in Tier 1. We get the factory acceptance test done, and that piece is done as part of the ITAAC closure. Overall, it flows down through the entire I&C platforms. Each

one of them has all of the different checkpoints, and in the end, it rolls into the human factors evaluation, verification and validation of the entire thing, which then covers exactly what you're saying you'd have, but it's done in steps that are now, we think, excruciatingly detailed, laid out in Tier 1 so that everybody knows where all the checkpoints are, and what needs to be looked at to be sure that you can proceed onto the next stop.

CHAIR CORRADINI: So, I guess the one thing that you said, since again I'm not very good at this, this was not in Tier 1 previously?

MR. WACHOWIAK: In Tier 1 previously, we had the high level -- we had high level statements that said, for all the platforms, you do this kind of thing. And it -- it -- the concern was it was not explicit enough that you could go and say, what document do I have to have in my hand to say that we did this thing for all the platforms?

It is now very explicit in Tier 1 which information you have to have to say that that particular element is closed, and you've gotten through that step in the lifecycle process, and could move onto the next step.

CHAIR CORRADINI: John, did you have a

question?

MEMBER STETKAR: I do, but I don't know quite how to formulate it, and it's not so much a question. It -- I'll defer to Charlie Brown on the independence and communications. I think he may still have some questions about the interdivisional communications, but that's -- that's his issue, and I'm not going to speak for him in this forum. And he's not here, so he had an opportunity.

My concern still remains at the area that I mentioned at the outset, and that is that looking at the instrumentation and control system design, I see a lot of very typical high-level information regarding design principles and -- and functional requirements and things like that, as would apply to any fairly complex system.

I now see more detailed information where commitments to confirm that those details are in fact actually implemented according to all of the design criteria, and all of the requirements. It's the equivalent of saying that, I'm going to drive from New York to Los Angeles, and then obey every single vehicular rule in every single locality that I pass through.

At a high level, I'm going to drive from

New York to Los Angeles. At the detail, I'm going to verify that I -- that I obey every single rule; that I stop at every single stop sign, and that indeed there's a check that I do that.

The problems is that I don't know if I'm going across the United States. I don't know if I'm going through Mexico. I don't know if I'm going through Canada because I don't have that intermediate set of information to tell me how the integrated design will be implemented.

I don't actually have that travel route, or I can't find it. And that's -- that's not a question. It's still that same basic concern that -- that when being asked, at least at the level I tend to think of a design when being asked to certify a design, I'm missing that fundamental intermediate information.

CONSULTANT WALLIS: My -- my problems is I don't know what's my probability of actually getting there. That's what I'd like to --

MEMBER STETKAR: Probability is a different issue. We need the route to lay out the probability.

CONSULTANT WALLIS: What can go wrong along the way as I take the route?

CHAIR CORRADINI: Can we just go back -- let me just go back to your comments. So -- so, now I understand the comments. So, the question to them versus the staff is?

MEMBER STETKAR: No, it's -- I don't have a question. That's -- I prefaced by saying I don't really have a question. It's a feeling of uneasiness, and it's probably more a question to the staff in terms of what level of assurance does the staff have, and we probably should get the staff up here, and ask them. What level of assurance does the staff have that they have sufficient information at that level? Because I don't have it.

I do, as a matter of fact, have copies of those preliminary logic diagrams. I would be pretty happy if they were in the DCD, but apparently GEH doesn't think that's appropriate.

CHAIR CORRADINI: So, let me just turn the question so I understand it, John -- or your comment. So, the point is that between the high level, the overall level, and the details, there are examples of the intermediate. But to use your analogy, they may take Route 94, but then again, that's not set in stone. They may decide to take Interstate 70.

MEMBER STETKAR: That's -- that's exactly

it.

MS. CUBBAGE: And I think that the DAC approach is when you take a route that gets you to a safe end product. We don't ascribe that we need to know whether it's this route or that route.

MEMBER STETKAR: I think my concern, Amy, and maybe it's better if you come up, but it's for both. It's that 25 years ago, early `80s, we saw several examples where people followed every single detail, deterministic design criterion, and still had a design that followed all of the rules.

They stopped at every stop sign, but that particular design had -- had vulnerable pinch points in it, or perhaps from an integrated operational -- when I say operational perspective, I don't mean operate the plant, produce megawatts. I mean functional operation of the system.

There were things that were overlooked until somebody stepped back and took an integrated look at that design, and said, okay, the decision has been made to actually use this particular route. And indeed, that route is an acceptable route.

MS. CUBBAGE: And that information will be available before they install equipment; that information will be available to the staff as part of

the ITAAC closure process.

MEMBER STETKAR: Except it's my understanding, and this is part of the concern about DAC closure, the discussion we've been having, that if I'm convinced that information will be available, the question is when will it be available, and what will be done with it by whom when it becomes available? Because in particular for the ESBWR, it is not available at the COL stage.

MS. CUBBAGE: That's right.

MEMBER STETKAR: It will only be available some time prior to fuel loading. Therefore, there will be no --

MS. CUBBAGE: Well, step back. It's not -- it's not going to be all of the stuff is dumped on us a month before fuel load.

MEMBER STETKAR: No, no. There's a schedule.

MS. CUBBAGE: This is going to be made available to us well in advance, and with the whole points, they're going to get -- they're going to engage the staff in the inspection process before they go and install the equipment.

CHAIR CORRADINI: But the -- if I might just interject? I -- we're a bit off topic, but

you've actually gone the other branch, which I think staff is aware of and we're aware of, which is this is now more generic to all the certifications --

MS. CUBBAGE: Yes.

CHAIR CORRADINI: -- and how that inspection or -- I'm afraid I'll use the wrong word, but how that looking will be done.

MEMBER STETKAR: That's absolutely true, Mike. It is -- it is not ESBWR specific. The only difference with ESBWR, and I hate to say this again, is that the ESBWR is the only DCD that I've seen --

MS. CUBBAGE: Big objection to that. I don't think that's necessarily true that all of the DCDs have a complete --

MEMBER STETKAR: I'm saying the last two years.

MS. CUBBAGE: Well, are they using the DAC approach?

MEMBER STETKAR: They claim they're trying not to, but that's their own decision.

MS. CUBBAGE: That's their choice. If we're using a DAC approach, we've concluded that we don't need that information.

CHAIR CORRADINI: Was there something else that -- Ian, did you want to say something?

MS. CUBBAGE: Well, I think if you want to switch --

CHAIR CORRADINI: Well, just for a minute, organizational standpoints. So, you don't have any questions of the folks up here at this moment?

MEMBER STETKAR: I don't at this moment.

MR. WACHOWIAK: I think to get back to your comment on that you said you didn't see it, it -- it depends on where you're looking to find what the I&C system is supposed to do, okay? So, if you look in the analysis sections, it will tell you what the SSLC/ESF system is supposed to do. You won't necessarily find those step-by-step things what it's supposed to do in chapter 7 with the I&C. You find that in the sections that describe the analysis that we did for the plant.

So, in part, that was why the transmittal of the simplified logic diagrams, if you will, took place. The staff said, we see this in these other sections. How do we know that in your design process, you're actually putting that into the design? We showed them the intermediate step, said, okay, we see that what you said it's going to do is being put into your process, as our process that they're certifying describes.

So, that -- that's how that gets together. The problem in putting the simplified logics into the DCD while we're using the DAC process is that you -- you or someone else can not only infer from those logic diagrams what the system is supposed to do, but you can also make judgments of what it is not going to do.

We run the risk of misleading you because not all of the things are there. You might decide that it's not going to do something, where in fact it may do that.

So, in your analogy, what do you do when you get to the big pothole that you can't drive over? We wouldn't have that in there, but you have to -- you have to deal with that when, through -- when you're doing the final logic diagram, and we might have to put something in that you would think is not there by looking at the simplified volumes.

MEMBER STETKAR: That's fine. I'm glad you made that -- that distinction. I guess my concern is that I would like the opportunity to at least ask you the question at this point in the review process whether or not you've thought about the fact that there might be a pothole. Because under these conditions, if there is a pothole, it seems like it

could be a problem. It's taking this travel analogy a little bit overboard, but it's --

MR. BUTLER: We know that there will be potholes, and we feel very comfortable with the fact that the structured process that we define, and that we've committed to will allow us to discover those potholes, and document our solution to them as DAC.

MR. WACHOWIAK: So, for one example of a pothole that is known now, which I think Skip covered in his presentation: the issue of data storms. Right? That is a pothole that we know about with digital I&C systems. We've designed our architecture such that the communication and the -- and the way that the application program processed the communication does not -- is not amenable to data storms, being interrupted by data storms.

So, we saw that one now. We know how to -- how to implement that, and we give a requirement for the system that says, that operating system has to continue to perform its application function over and over and over again independent of whether there's data there or not.

So, we can see the potholes that we can see now, but the ones we don't see, our process is what handles dealing with them.

MEMBER STETKAR: Let me back you up to a bigger one, and pushed it off to November a bit, but it -- it's -- it relates to my concern about the information for the digital I&C design. Not so much digital, the I&C design. And that is the new function for isolating CRD under certain conditions, and then bypassing the isolation of CRD under other conditions. This seems to be something where someone has identified an issue, and the plant design has been changed because new valves have been installed, both isolation valves and new bypass valves. So, there's been physical hardware changes, and of course the I&C has been changed appropriately to implement those necessary functions.

It's difficult. I understand the signals that are being used. I can read the words. I don't see the logic diagram that I'd like to see. Several of the same signals are being used for both isolation and bypass, low GDCS --

MR. POPPEL: You mean same parameters, not same signals.

MEMBER STETKAR: That's the information that I'm looking for. But I could see --

MR. POPPEL: We said that the ICP bypass is implemented on the independent control platform.

It's very clear the independent control platforms are in fact independent, have their own censors, and are not using common hardware, software with SSLC/ESF. That is clearly stated in the DCD.

It is impossible for anybody to believe that we're using the same transmitter in both systems. It's very clear that --

MEMBER STETKAR: When you say it's impossible, it isn't impossible.

MR. BUTLER: The words that we tried to write were an attempt to clearly communicate, along with our commitment to IEEE Standard 603 that we have independent censors with independent signal path for IO to the controllers for everything. Everything is kept separate down to the instrument.

MEMBER STETKAR: It's just really hard for me. It's difficult to see that just by reading the words in all of the places in the document. It's -- it would be nice to see --

MR. POPPEL: But I mean if for example we had a picture, and it showed a common transmitter feeding the ICP and SSLC/ESF, you could rightly say, how come you said over here they were separate, and over here you do the same one? And you say, boy, did we get screwed up. You caught us. But we didn't feel

we actually had to draw a picture of that, because we said here they weren't going to be the same. We're very clear about it.

MEMBER STETKAR: Okay, I guess I'll have to go back and search to make sure that is --

MR. POPPEL: But that is one of the valid potholes that you would -- you would say. If we're going to have this thing that does all these, one of the things you have to consider is independence of the signal because the signal is what could've gotten you there in the first place.

So, when we went through our portion of the design for this, and decided what platform to put this on, we adjusted to that pothole by saying, it has to go on one of our independent platforms that does not use the same signals, just for the specific reason that you've pointed out there.

So, I think where we are now is a question of how do you find this information, rather than it not being there?

MEMBER STETKAR: That is exactly right. That's exactly right.

CHAIR CORRADINI: Okay, so a lot of what you're asking I think we really need the staff's discussion. So, do you have -- does this committee

have anymore of the folks from GEH before we ask the staff to come up? No? Ian, you were going to say something. Are you going to wait until -- do you want to wait until --

MR. JUNG: Wait until the introduction to ask people.

CHAIR CORRADINI: All right, so why don't we start the switching around? Thank you very much. I appreciate it. Don't go far. Familiar faces are coming up.

MR. JUNG: Thank you, Chairman. As my staff gets set up and gets ready, I think the key message I want to send to ACRS is Mr. Brown and John and subcommittee provides us with smart advice. We heard your -- we heard your issues, and we responded, and we worked with the GEH.

We spent a significant amount of time. Level of detail has been -- there's some subjectivity as I discussed in earlier meetings, and staff struggled the last couple of years regarding level of detail that we felt that we needed. And when the ESBWR certification came in, there was an expectation of design detail. It wasn't quite there, but given Part 52 framework of the design acceptance criterion ITAAC, staff had to make some decisions on some of

these elements.

But I think we've gotten to a point where we have to make some decisions, and I know -- I know it's not John's comments. I see some points, but when we talked to GEH, we had some points given their design stage. And we got a significant amount of information. We consider the earlier simplified logic diagrams submitted to the staff twice in Revision 3 or earlier, and Revision 5 stage.

We looked at both stages to see how they're progressing. We looked at the issues in terms of it's still something that used to be in the DCD or not? And we clearly made a decision it's not. We felt it's going to change as the design gets implemented as it goes.

CHAIR CORRADINI: So, just one clarification for John to make sure. You said there were two submittals from your version, Rev 3 and Rev 5. Have you seen both, John?

MEMBER STETKAR: No.

MS. CUBBAGE: After the meeting in December --

MEMBER STETKAR: I've seen Rev 5.

MS. CUBBAGE: That would've been some time about nine months ago.

MEMBER STETKAR: About a year ago. So, it's probably time.

CHAIR CORRADINI: I'm sorry. I didn't mean to interrupt you. Go ahead.

MR. JUNG: Yes, thank you. I think that overall, ACRS' comments resulted in enhancing the DCD, and it provided additional confidence to the staff based on the results. I think the overall Safety Evaluation Report improved, and I'd just to thank you for that. I think the staff is ready to provide you with the side of the story regarding these issues.

MS. CUBBAGE: I'd just like to follow up with one comment related to what Ian was saying. It's that we can't lose sight of the fact that the DCD becomes the FSAR, and there has been a lot of work in previous years on working one what level of detail is appropriate for an FSAR, and we take a look at some other FSARs, and that's part of our consideration. So, let the staff go ahead.

CHAIR CORRADINI: So, may I just -- just as a kind of point of organizing the discussion, there will be certain things that we will start bleeding back into the generic issue of -- of if one goes down the path of staying with DACs, and the staff is reviewing that relative to attributes and some design

details, as examples or maybe even some specificity, how does one -- if it doesn't end up being design -- the design set at the DCD stage, how does one go through the verification and validation beyond that?

That's a generic thing that if we go that route, you guys may know something. We can discuss it, but that's another committee, another group that is essentially going to look at it for all the various certifications, versus clarifications here that the committee needs to feel more comfortable with what's going on.

So, we'll go back and forth, but I guess for my mind, I just want to make sure that I get it clear because I don't want to necessarily leave it in GEH's or the applicant's corner relative to the generic issues. So, is it --

MR. GALVIN: Hulbert is going to speak to that. I mean each design chooses a different set of DAC for their level of design. So, it's not just a generic issue in the sense of, you decided to give us this level of design, and they've given us this level of DAC. All the other design centers have done something different. So, I mean it's --

CHAIR CORRADINI: Right, but it's --

MR. GALVIN: It might be a match. Now, of

course the whole verification process is --

CHAIR CORRADINI: That's what I'm talking about. It's not so much that the details are different. I'm aware of that. It's more a matter of given there are certain things that are left to ITAAC, to DAC and ITAAC verification, that process, we can talk about it, but it's over here. We're not going -- we're not going to worry about it today.

MS. CUBBAGE: Right. I think what Dennis is trying to emphasize is that it's a give and take between Tier 1 and Tier 2 and the DAC. If they'd give more detail here, you'd get less detail in the DAC.

CHAIR CORRADINI: Sure, okay.

MS. CUBBAGE: It's a different approach.

CHAIR CORRADINI: Great. Thank you. So, go ahead, Dennis. Do you want to --

MR. GALVIN: Well, the staff here will brief you on the follow up to the December 2008. Hulbert is going to go through some of the issues you raised, and the staff overall review, and the follow up to your issues. Hulbert?

MR. LI: My name is Hulbert Li. I'm the lead reviewer for ESBWR I&C systems. The purpose of today's meeting is to brief the subcommittee on the issues brought up last December, and also we'll

address some of the staff's perspective with four pillar and plus one design principal, bring up Mr. Charlie Brown. Also, we request the advice of the subcommittee on the I&C systems.

The committee members, Dennis and myself and Leroy Hardin, will address the cybersecurity area, and we also have Joe Ashcroft on the committee. This is in-line with today's subjects, and last December SCS meeting, and we used the transcript to relay the message to GEH, and also follow up with additional requests for additional information/questions.

GEH responded to our questions, and also updated the DCD Revision 6 and also implement additional detail information. The first question the subcommittee pointed out is the cross reference between Tier 1 and Tier 2. It's not clearly related in this Revision 4, Revision 5 DCDs.

So, GEH made improvements in Revision 6, and they provided cross-reference, and the obvious one is the table 7.1-2 and 14.3-1a, and the 7.1-2 gave the reference for all these IEEE Standard requirements, how to detail -- detail address in the Tier 2 sections. So, it's very helpful information for staff because we will be able to find out precisely, but the ESBWR design implemented those IEEE-603 requirements.

The 14.3-1a gave cross reference to Chapter 15 analysis requirement. This Tier 1 section how to verify that there was -- there was analysis requirements. So, staff found these cross-references very useful. These are just two examples. There are many other references in Revision 6.

The second comment from SER is there's no -- the documentation is not complete, and at that time, we still had questions for GEH to request for consistency between the DCD sessions. So, in Revision 6, GEH provided detailed consistent checks for all these sessions, and this example I'm putting up is Tier 1, Section 2.2.15. It addressed the applicability matches for the IEEE-603 requirements.

They identified all the requirements in 603, and also cross referenced to every safety system, how they implement those IEEE-603 requirements.

The second session is Tier 1, Section 3.2, and the software development. They provided detail, instructions how to verify each platform goes through every lifecycle to the final product, to demonstrate how they achieve those lifecycle design process. So, staff reviewed those in detail, and found those acceptable.

The third question is additional

information on the architecture of the I&C system, and appropriate ITAAC and DAC should be added. As in the presentation earlier, there was detail of the ITAAC diagrams provided in the DCD, and those are in the block diagram form in Section 7.1, 7.2, 7.3 and 7.4. This block diagram form is compatible to the other design certification application.

I was also the lead reviewer for AP1000. I think those block diagram types of drawings are compatible in the AP1000.

MEMBER STETKAR: Excuse me, very compatible with a very high level set in the AP1000.

MR. LI: Right.

MEMBER STETKAR: But those are -- those are very high-level principles. It says, we have four signals from some censors coming into something that does some processing, and it sends a signal out to some individual division. That's -- I can draw those diagrams.

MR. LI: Yes, I think --

MEMBER STETKAR: The AP1000 also has the functional logic diagrams.

MR. LI: It's docketed information. It's not part of the design certification.

MEMBER STETKAR: I understand that.

MS. CUBBAGE: I don't think that's the same information as docket --

MR. LI: Let's go to the next one. We can address that.

CHAIR CORRADINI: Okay, all right.

MEMBER STETKAR: No, no, no. It's in the DCD on the AP1000.

MR. LI: It's the drawings --

MEMBER STETKAR: The drawings that I'm looking for are in the DCD. They're in the design -- I wouldn't have this discussion if they weren't. They are. They also have the high-level diagrams. The ones that you're --

CHAIR CORRADINI: Okay, so you're going to address this? Hulbert, you're going to address this?

MR. LI: I'll address this issue. We go through twice: first in the DCD Revision 3 stage. We requested -- basically, we tried to compare with the DCD description whether those diagrams reflect the DCD description. And then, Revision 5 of DCD, they make lots of changes in the DCD. So, we request again for those diagrams.

Those diagrams are a little bit lacking because they constantly working on the DCD itself first. And then after that, finalize of the third

stage, then they update the drawing. So, the drawing reflects the DCD itself. So, for our minds, DCD is the appropriate design certification document. Drawing is just supplement to make more clear to read, but not necessarily represent everything discussing the DCD.

MS. CUBBAGE: This is comparable to the systems reviews where PNIDs, etcetera, are available for audit, and are not part of the certification.

MR. LI: But we anticipate there are more refinement for those diagrams when the design is getting more mature in the final stage. And so, we plan to have an audit of those final logic diagrams in our high-tech resolutions stage, rather than put a design certification. The problem is putting the design certification -- if they change something, and forget changes something, then making contract, this conflict statement.

That happened in the -- in our early review. We consistently had a problem because some other -- Chapter 7 discusses something in I&C, not necessarily consistent with what Chapter 7 says.

So, we bring up these to the -- and they tried to consolidate all the I&C related information into Chapter 7. So, Chapter 7 became very -- so, any

change, they just go to one place to make change. Don't have to -- you know, they may miss somewhere.

Another concern is the design certification is for a long time, maybe 15 years, even longer, and the technology may change. The logic diagram I reviewed 30 years ago with operating plan. It's quite different from current language.

MEMBER STETKAR: I'm sorry, Hulbert. The logic diagrams that I looked at 30 years for operating plants look an awful lot like the logic diagrams that I see for new designs coming in. I'm not saying we're going to use an oxcart or a horse, or a Maserati or a jetpack to get across the United States. That's technology.

The fundamental best route across the United States has not changed, and the depiction of that logic, how we take input signals, what input signals we use, whether they're pressures, temperatures, levels, flows and what combinations of those particular input signals I decide to use to implement a particular function, such as injection or isolation, that's fundamental safety system design. That is not based on rapidly changing technology because next year we might have even yet a faster processor.

If you're saying they're changing the fundamental logic because of chip speeds, that's a real problem.

MR. LI: They way they present on the diagram has changed. It's not the same. It used to be draftsman drafted, and now they computerized everything. It's a software-driven drawing. This current -- that background does not necessarily need adjustment to anything. It's a computer-based drawing.

So, the symbols of how these are is not quite the same as how they were in the past.

MEMBER STETKAR: It's true the symbols look different. I'm concerned about -- I'm not concerned about whether I have a comma, or a period or a semicolon. I'm not concerned whether I have a computer that drew a triangle instead of a parallelogram or something. I'm concerned about how the basic fundamental safety system actuation logic is implemented, and that doesn't change -- that shouldn't change whether I have a CAD program drawing the drawings, or whether I have a draftsman sitting in a room with a pencil drawing the drawings. It's the same drawing. It's the same logic.

MR. LI: This is the detail discussed in

how they foresee their design. Logic diagram is the tool for the designer to implement the requirements.

MEMBER STETKAR: It is, but the problem that we've seen in the past is that people who look at each function individually, and many people do, specify criteria for that function within -- within the boundary conditions that they use for that particular function, and that is done function by function by function.

At some point, there is an integration process where all of those functions are integrated into the logic. Someone decides that indeed some input signals may be shared among functions. Some input signals -- some functions may indeed require separate input signals.

There may be particular interlocks or time delays that are inserted, and until you see -- until you're able to see the whole system in front of you, I guarantee you that reading words about individual signals and individual functions you will not see the problem.

MS. CUBBAGE: I think --

MEMBER STETKAR: I don't know --

MS. CUBBAGE: I don't think anyone is disagreeing with you that that has to be done. It's a

matter of timing.

MEMBER STETKAR: It is. It is.

MS. CUBBAGE: So, the question is do we feel comfortable --

MEMBER STETKAR: That is the question, yes.

MS. CUBBAGE: Do we have a comfort level with the level of detail that's been provided, plus the verification process that will happen through the ITAAC inspections to have confidence that GE will in fact implement this design as advertised in the DCD? And we've gone to an excruciating amount of detail looking at their topical reports that document the design process that they're going to follow to make sure that these outputs are going to be appropriate, and we have hold points to make sure that we have an opportunity to inspect this information before they install it in a plan.

That is kind of the fundamental place where we're at.

MR. WACHOWIAK: This is Rick Wachowiak from GEH. Is it on? Wrong trajectory. Rick Wachowiak from GEH. And so, since we're licensing -- we're certifying the process right now, as Amy said, there was a test in there. They read the words for,

for example, how the ECCS system is supposed to actuate, signals and things like that. They look at our process that says it will be translated into logic diagrams.

They asked us for the interim logic diagram. They reviewed that logic diagram, and yes, indeed it did do what the DCD said, and it didn't have these issues that you're talking about. And so, they -- what they're saying is this process is sufficient to produce an output, a result, that we can all live with as long as we check it at these interim points.

So, that -- that process there was tested, and it -- and we believe that with the DAC that we're proposing, that the process that we're certifying is appropriate with the Tier 1 information that we have in our documents.

MS. CUBBAGE: And I will also take it to the parallel situation with the rest of the plant. They may have a system that may say there's going to be a valve. Well, they don't have to specify today that it's going to be what kind of valve, etcetera, etcetera. But we've gone out; we've done audits are part of the design certification. We've looked at their design specifications. We've looked at the drawings they have for the specific components, but

that level of detail doesn't become part of the certification.

MEMBER STETKAR: Sure.

CHAIR CORRADINI: Go ahead.

MEMBER STETKAR: Are you done at that point? Should we go forward?

CHAIR CORRADINI: Let's go forward because I think we're okay on time. Go ahead, Hulbert.

MR. LI: Thanks. The staff conclusion basically summarized the requested information from GEH a picture of I&C and other levels of detail question based on SER's recommendation and meeting transcript.

The DCD's Revision 6 provides information described in Chapter 7 one through four. DCD Revision 6 ITAAC verify the 603 requirements for every safety related assistance. And also, they give the lifecycle implementation verification ability. It's easy to verify each life cycle.

So, staff concluded substantiate I&C design information DCD including DAC and ITAAC conforms to the regulatory requirement under Part 52, and provides reasonable assurance of safety. The implementation of DAC and ITAAC will be inspected by the staff to ensure the appropriate design

implementation and as-built design will be verified.

MR. GALVIN: If I could just clarify the third bullet. You won't see all 603 requirements in Tier 1. You know, something like QA and what's the other one? Equipment qualification are covered by other -- other sections of the Tier 1. So you won't see a one-to-one correlation of every --

MEMBER STETKAR: In the tier for I&C.

MR. LI: It will be a different. Next few slides we give a fresh perspective for the four pillar and platform design principles. And the redundancy, because they follow 603 requirements, and they are safety related I&C system are physically and electrically separate in four divisions, located in four corners, also the fire protection requirement.

And the ITAAC commits to FMEA to confirm the safety related I&C system satisfied single failure criterion. And non-safety system network segments are either triple redundant, or double redundant for most occasions. The staff found the I&C design redundancy design principle.

Independent: staff reviewed the independent design principle based on the DCD design information and the DAC/ITAAC verification process. From the earlier presentation, the intradivisional

data like trip and bypass is same for the two-out-of-four voting logic. So, they are -- it's very limited intradivisional communication.

The reactor trip and these independent control platforms is point-to-point data link, and then the SSLC/ESF platform uses the Communication Interface Module, and those are to be verified in the ITAAC stage.

So, staff carefully reviewed the DCD information, which included statement of communication independence; found that I&C design made that communication independent principles.

Dependency: DCDs state that Q-DCIS internal and external protocol are deterministic. In GEH's definition, determinism means a specific function always be accomplished within that required time period or space of time. And this character, deterministic character will be inspected during the ITAAC resolution process because each platform defines a specific function to be performed at certain times, and those are part of the V&V, verification and validation process.

So, during the ITAAC closure stage, we will review those baseline reports to verify they do have those determinants building into their systems.

Defense and depth in diversity: The license topical report provided these three analyses for the Standard Review Plan's BTP 7-19 guidelines. The specific method is the NUREG-6303. It's the chapter 16 analysis scenario to analyze defense and diversity ability in the ESBWR I&C system.

The diverse protection system design document in Tier 2, Section 7.8, and associate ITAAC is documented in Tier 1, Section 2.2.14. Staff has reviewed these three designs and finds them acceptable, and we addressed them in our SER.

Simplicity: Basically, the ESBWR designs follow IEEE-603 design requirements. So, it's -- in earlier presentation, they showed the sense, command and actuate approach. This design made the independent isolation separation requirements. Intradivisional communication is very limited. So, staff concluded this design followed the simplicity principles. This concludes my presentation. Any questions?

CHAIR CORRADINI: John, or any members?

MR. JUNG: John, if I may, I want to speak to some of your thinking earlier regarding adding -- potentially adding things to the logic diagram.

You mentioned that it's really hard to

fully grasp integrated -- look up the I&C systems. I think we have to look at it from the other way, and as part of our staff review process, we went back to earlier operating reactor FSARs from the `70s to some of the late `80s. Some of them in the `80s became quite expensive, and agency went backwards a little bit.

Agency realized that it's very hard to maintain licensing basis, and any time certain changes are made in a FSAR, they have to come in for licensing reviews and things. So, some of the late `80s, `90s, the agency began to allow some of the detailed information off of FSARs. For example, PNIDs and things in many cases are not part of the FSARs in current operating reactor.

Looking at the ESBWR FSAR and the DCD, right now Tier 2 is about 500 pages now.

MS. CUBBAGE: Chapter 7.

MR. JUNG: Chapter 7. And Chapter 7 also is part of the supporting function for supporting system, and in a way I&C system force the design basis safety functions in Chapter 15.

So, Chapter 15, Chapter 6, it's -- when you got to those chapters, when you talk about certain sections, it talks about I&C, and then I&C says, refer

to Chapter 7.

In Tier 1, Tier 1 contains not just the commitment, but overall in Part 52 design certification itself is a sort of design commitment by itself because the Atomic Energy Act says, 185B says, this is a design that will be constructed down the road. But in Tier 1, it still has a high level description, functional arrangements, interlocked bypasses and testing requirements, and then it goes into ITAAC.

That's probably for I&C areas; it's probably 200 to 300 pages. So, when the ACRS think about adding more into the DCD, it's -- I know you have the benefit of having more confidence and clarity, but if you think about it carefully in the sense that does it -- this area eventually might get into thousands and thousands of pages if some of the design details are implemented, and all the FSARs are implemented.

So, something to think about is already it's very complex to understand that, and then down the road, none of us are here, and inspectors are looking at it, and trying to see how -- they're trying to inspect the plant. It's going to be even harder for them to inspect and find out the significant

elements of the design they need to look into, and more than likely the licensee themselves are going to have a difficult time.

So, the reason I'm mentioning this is that some of the FSARs, if you go back to some of the very early FSARs, it's only this thin. The ECCS system does this. Very high-level statement description that eventually got into a lot more details.

But I think the question is in terms of additional information, and I've been asking to Hulbert and my staff, do you guys have sufficient information to make a reasonable-assurance finding based on the DCD description, and the description in Tier 1? If they follow within Appendix B type of QA requirements, are they going to get to the outcome, which is a safe and sound design?

And their answer has been yes pretty much since last year, and additional detail came in. Yes, it's good. So, I just want to have ACRS consider that there's some point that the design details maybe warrant getting into a realm that it may actually have impact on our review. Sometimes, when we look for additional details, actually we started getting additional RAIs.

So, that's why the staff had to make some

decisions, and given the ITAAC availability for verification inspection by the staff, and they're working on the process to ensure beyond the licensing stage, the agency still has enforcement and oversight responsibility. We're going to work through that.

So, I believe -- I think the staff are very comfortable with that decision that they're making. So, I just want to share the information with the staff.

MEMBER STETKAR: I appreciate that, and I also appreciate the desire and need to keep the DCD for the FSAR a tractable document, and it's well on its way to violating that criterion already. But I think that what I'm asking for, at least in my opinion, is not more detail. It's intermediate information because indeed in the DCD right now, there is excruciating detail for commitments to follow criteria, and those are -- those are well defined.

Those are auditable by inspectors certainly, so inspectors can know how to do their job. You've left very well the inspector confusion or judgment. You tried to do a very good job to try to pull that out of the inspection process.

The thing that I'm struggling with is that you don't really rely on inspectors to think about the

fundamental implementation of safety functions. Their job as inspectors is to make sure that the licensee said they were going to build it in this particular way, and in fact it was built in that way, and there's traceable documentation to show that indeed that process was followed, but at a fairly small level of detail, and it's an audit function. It's not a design review function.

MS. CUBBAGE: Let me just clarify. When DAC are involved, it's not going to be a random inspector that doesn't know I&C out in the field. This is going to be a very detailed process.

MEMBER STETKAR: That gets out into the other part of the DAC issue I think that Mike brought up earlier that I don't particularly want to bring up because it's not just the ESBWR.

CHAIR CORRADINI: If I might just interject? I'll let you guys converse some more. I think Amy's -- what I'm hearing is Amy's answer is you're uncomfortable -- your lack of comfort -- you should be -- you should be comforted by the fact that the inspection will do it in a disciplined, consistent, organized fashion that won't be class-specific nor region specific. It'll be coordinated. That's what I thought you -- I guess my only -- my

only -- if I get to the staff, I think where John is coming from is, at least what I'm hearing him say is that if you took the 500 pages and you replaced them with 200 pages of detail, you might be better off all the way around.

MEMBER STETKAR: Well, no. I'm sensitive to the fact that because it is DAC/ITAAC, and because the inspectors who are -- still I come back to the point that the only thing that I've heard the inspectors will be performing is a design implementation audit function, not a design review. Inspectors will not be producing a safety evaluation report of the I&C design. That -- there will be no safety evaluation report of the I&C design, other than what we are discussing today.

MS. CUBBAGE: But I believe the committee has heard some recent discussions that I haven't been part to about the ITAAC and DAC closure process, and there is a possibility that there could be topical reports in for review that would then be later relied upon to resolve DAC, but that's --

MEMBER STETKAR: If I were more comfortable about that processing, I wouldn't be so uncomfortable right here today. And that's a reason for my discomfort.

Let me -- let me pull back from the process a bit and ask a couple of specific questions, because unfortunately on the committee, we're not privy to all of the discussions between the staff and the applicant.

I heard Rick say that there -- and you said also, Amy, that -- that there was a process where the staff looked at the DCD verbiage, tables, verbiage whatever, and looked at the Revision 5 functional logic diagrams, and compared them to say, indeed, do these functional logic diagrams do what the words in this 500-page document seem to say the functions should be done?

That's a good process. I'm glad -- I'm glad you did that. Were there any RAIs issued as a part of that process, or is it -- or is that process not subject to RAIs because --

MS. CUBBAGE: Absolutely we would use that process to inform RAIs if you needed to, but I can't speak to whether there were any specific RAIs that came out of that region.

CHAIR CORRADINI: Back to Dennis.

MR. GALVIN: There was no RAIs. They did the -- the staff didn't generate any RAIs in that process.

MEMBER STETKAR: Okay, that's a bit surprising that something that complex that -- that it's implemented perfectly, and there weren't any questions when you looked at those diagrams because the diagrams are pretty involved.

Also, did you -- did you ever get a functional logic diagram of the leak detection and isolation system? I couldn't find out, which is a pretty pervasive system that closes valves and opens things.

MR. LI: They have a typical one in the 1711.

CHAIR CORRADINI: I'm sorry?

MR. LI: Typical isolation in the type John was asking --

MEMBER STETKAR: No, I meant in these -- in these -- the drawings that are on the docket that I've seen; that was one of the functions that I didn't stumble across.

MS. CUBBAGE: GE, do you recall if -- if your simplified logic package included any leakage detection?

MEMBER STETKAR: LDIS.

MS. CUBBAGE: LDIS.

MEMBER STETKAR: I couldn't find it, but

again, the only thing I have is what I pulled -- I think what you sent to our staff.

MR. BUTLER: Off the top of my head, I don't think we can -- Skip Butler. Off the top of my head, I can't recall.

MEMBER STETKAR: The thing that I'm trying to do here is get a sense of what level of examination was done by the staff relative to those drawings, and if -- if there were any questions that evolved out of them, and if there was any sense of completeness of those drawings, or whether they're just simple for information only?

You said they're filed on part of the docket, but they're not -- they're not part of the DCD. So, therefore, they're treated somewhat differently.

MR. LI: Yes, we just added basis. We do not go through every one to verify. I think we concentrate on these DCD warnings.

MEMBER STETKAR: Understand.

MS. CUBBAGE: And that's similar to the process. Again, I'll come back to the mechanical systems side. We don't go out and look at every drawing that GE produces. We sample.

MEMBER STETKAR: But in the DCD, I think

for most of the mechanical systems there are at least simplified PNIDs that indeed show all of the valves, things like pumps and pipes and valves. I didn't have too much difficulty understanding how the mechanical systems worked from simply the information that was in the DCD.

MS. CUBBAGE: We do have PNIDs that we also looked at.

MEMBER STETKAR: They go beyond.

MS. CUBBAGE: Yes, they go beyond the DCD.

MEMBER STETKAR: They go beyond those, but the information in the DCD is --

CHAIR CORRADINI: John, I don't know if you have another question.

MEMBER STETKAR: No, I don't.

CHAIR CORRADINI: Okay, I at least want to summarize the give and take here as I understand it, since I'm not as adept at this. So, what I'm hearing at least from you, John, is that -- that what Rick's point was about the using the -- I'll call them the intermediate diagrams as a point for auditing actually is a good step, at least in looking at if the design criteria were being followed.

MEMBER STETKAR: Yes.

CHAIR CORRADINI: Okay, and there's more

there than I'm expecting you're going to tell me.

MEMBER STETKAR: The thing -- the thing that bothers me is that there does not seem to be any active use of those. In other words, I'm hearing that the staff used those drawings as a way to verify the words, which is good. I mean that's sort of step one.

The second part of the step is a critical examination of that logic to see whether there are any -- I don't know what the right term is, the politically correct term. Areas where there might be division -- I don't want to use the word deficiency because the problems is that you can follow all of the design criteria and implement those criteria, and put -- potholes is a good word.

You can even look at those criteria in perhaps six different ways. Perhaps four of those ways may be clearly deficient. It might not -- it might not be clear which is the better way to implement the design. Now, you say, well, it's not the proper --

MS. CUBBAGE: It's not for us to say what's --

MEMBER STETKAR: That's right. And recognize it is not the staff's design, and it is certainly not the ACRS' function to design --

CHAIR CORRADINI: However much we try to?

MEMBER STETKAR: No.

CHAIR CORRADINI: Okay.

MEMBER STETKAR: It is, however, I think, a function to look at the design and ask questions, critical questions, to say, why did you do it? Why would you implement it this way? And there might be a perfectly good answer.

MS. CUBBAGE: At the end of the day, we're not going to have -- we don't have a function of looking at everything the applicant does. We rely on process. We rely on Appendix B. We've looked at their process. We've seen some of their outputs, and that's where we make our conclusions.

MR. JUNG: John, from -- BTP-19 describes a lifecycle. Even though intention was for software, it also includes hardware outputs. You might've seen BTP-9 lifecycle table. For GEH, ESBWR design over perspective, there are some there in the requirements. Depending on which discipline you look at, some are planning requirements. You can look at the simplified logic diagram being one of the outputs. It's in the design stage of lifecycle.

So, the staff relies on -- the reason that whole lifecycle, structured detailed lifecycle came

along, was partially because of the very complex process involved in software design, associated hardware design.

So, in the BTP-19, staff makes it clear to have a good output. The degree of structure and rigor of the process is something that staff relies on to make a safety decision.

So, when. John, you're asking for certain output that we, the staff, believes that it's going to come along down the road, when COL applicants are really serious, and they're going to spend money on. And outputs, we believe it's going to be there, and we put a -- so, you're asking something. You believe it has to be -- it's now available. It should be here.

The fact of the matter is without it -- first, the staff believes we can make a reasonable-assurance finding. That's one. If that information is available now, whether we find additional safety issues of significant that can impact the reasonable-assurance finding, we're not sure unless we look at the final single-logic diagrams and go through one at a time. But you're getting into a situation, and certainly NRC is doing an independent design review.

That's not our role. Our role is clearly to license the facility, and beyond the licensing, we

have a role of oversight, inspection and enforcement that we believe Part 52 framework clearly lays out and differentiates licensing functions and the inspection functions through ITAAC and DAC.

So, we relied on those -- both licensing framework, and the structured process that is going to come along, and we feel comfortable at this point. The degree of oversight that we put on, if those concerns are significant concerns, then we could put additional resources to inspect those areas. Yet, I believe that the structure they put up in a 603 -- the Tier 1 and 603 requirements that amounts to more than 600 DAC items, plus several hundred more ITAAC items, I believe the agency has put up significant restrictions, and oversight that if those are implemented and verified through inspection, I think we'd feel comfortable.

John, you are looking for -- my belief is you're asking for something. Yes, more -- additional confidence, and you're looking for something missing. I'm not sure. There might be, but you're almost getting to the situation where we're looking at almost a perfect review that given the resources we have, we may not be able to achieve it at this point.

MEMBER STETKAR: No, I don't think I'm

asking for a perfect review. It's my opinion. I think my fundamental concern is that indeed we are in a situation now where we are relying on a process at this stage in the design review.

We are, as an agency, relying on adherence to a process to give us confidence that the final design indeed will -- will meet the ultimate objective. Certainly, you must have a process. Certainly, someone must adhere to a process for that to be achieved. That's a necessary function.

Is it a sufficient function? I don't know. That's the issue. The -- the discomfort that I have is that we seem to be relying on a process, and then immediately auditing compliance with very, very specific, very, very fine structure criteria. And we're developing a perspective that says, well, as long as things are specified very broadly at a high level, as long as we have a defined process and as long as we audit a few specific details, then by definition the designs shall be acceptable.

We've removed that thought process from looking at somewhere in between, and say, does the design act as it will be implemented? And I don't mean implemented in detail by chip sets or lines of code again. As it will be implemented in the

fundamental logic, is there anything there? Have we critically looked at that part of the process to ask ourselves does anything in that intermediate level of the information strike our attention to say, we should at least question it, or perhaps something might be changed?

And now is the time to change it when it's all on paper. It's not the time to change it when things are actually being constructed.

CHAIR CORRADINI: If I might -- I didn't mean to stop you, but on the other hand, I think we've gone back and forth now, and we understand the position. Just to paraphrase to end it, if it's all right --

MEMBER STETKAR: That's fine.

CHAIR CORRADINI: -- is that what I'm hearing from Ian is that they have looked at this intermediate area between high level and detail, and have tested it, and they feel comfortable. You have -- you still have a bit of discomfort because in the testing, you would expect to see -- I don't know what. I can't get into details, but you're looking for more.

So, I think -- I don't know if we can get much more out of this at this point. Yes, Graham?

CONSULTANT WALLIS: I think I'm going to support what John Stetkar is saying. But by looking back at what we're been doing on these other two dates, and the process we've gone through there over a period of years, and we're looking at all hydraulic, mechanical-type issues, in this process, we've learned several times that the devil is in the details.

We look at cartoons of a high level, which you've seen many times in DCD and on slides here, and sometimes they mislead because they give the wrong impression. They don't show the details. They don't show that this pipe, which is connected this way, actually has some bends and some things in it. They don't show the details of how these valves operate and so on, and it has taken us, as you know, Mr. Chairman, some time. We're going back maybe two years. We're asking questions to resolve some of these issues.

Without understanding those details, we wouldn't know if the design would work. We wouldn't have the assurance that the design would work. And I don't see how an inspector can ever do that at that sort of level that we've been examining these other systems.

There's no way an inspector is going to look at a piping system for some ECCS, and say, that's

going to work, but it has to work. He can check the details specified at some lower level detail, but you can't look at the whole thing and say, I know it's going to work. That's not his job.

So, I have that sort of concern. I think it's a bit like what John's concern is. This was a long process, and it doesn't seem to be -- there doesn't seem to be a chance to do it here with this issue. Maybe I&C is different.

And then I see that when we do get the details, sometimes the design is going to be specific, much more specific. And then it may be the real punch point. I mean everything else has been decided. This is all DACs and ITAACs, and you've got to get the plant running. All of a sudden, you've got the specific design, which inspectors can't review. There's going to be a real crunch for the staff. What are we going to do?

Well, in the case of previous issues that we have in these other matters, we brought in consultants, and we wouldn't be able to look at the steam dryer response without bringing in an expert when we ought to look at core stability without bringing in an expert.

Are you going to be hiring some experts at

the last minute to look at the specific I&C design, and advise on whether it is a good design or not?

MS. CUBBAGE: I think we want to speak to that.

MS. DUDES: Well, may I? I apologize. I did come in late. I'm Laura Dudes, Deputy Director, Division of Engineering. I just wanted to -- I know we've had some generic conversations regarding DAC, the inspection associated with I&C. The senior management of NRO is very much engaged in what that inspection process will look like in terms of this is not an inspector going out and looking at a chip, or a function, or following a procedure.

This will be a dedicated design inspection team. It's an engineering design verification with headquarters experts, perhaps contractors, and it is not actually going to be done at the last minute, but is actively being planned right now in terms of how we plant a pilot, or first engineering design verification inspection, focusing on I&C.

So, we will actually be able to get some lessons learned within the next year or two on how this is going to work, but I hate to leave the committee with an impression that we think that the DAC inspections are going to be done by field

inspectors with not the right amount of skills and education and design experience to verify some of that implementation.

MEMBER STETKAR: Let me -- I've got ten minutes.

CHAIR CORRADINI: Well, I was hoping that we were at the end of our discussion, unless you have something more to -- if we're going to go back and forth on philosophy, I'm going to take some prerogative here, and say --

MEMBER STETKAR: We are, but I have examples where indeed plants were built -- these are plants that are currently operating. They were built. They satisfied all of the design criteria. They were inspected, and indeed problems were found later, only when people backed up to the level that I'm talking about. Because people never looked at them at that level in those days.

Problems were found. Not problems that violated any safety criteria. Not problems that violated any single failure design criteria. Problems, however, if you had two failures, it would fail everything because nobody ever looked at that. Nobody was ever required.

MS. CUBBAGE: Can you be more specific

about what is it --

MEMBER STETKAR: A particular power plant had three diesel generators --

MS. CUBBAGE: No, no. Not the -- no, no. I'm not asking about the specifics of the issue. I'm asking about the specifics of this intermediate layer that you feel is missing. Is it the simplified logic?

MEMBER STETKAR: Yes. That's exactly it.

MS. CUBBAGE: Okay, because -- because --

MEMBER STETKAR: When we looked --

MS. CUBBAGE: -- you're implying that no one is ever going to produce or look at those, and -- and they are going to be produced. They're one of the outputs, and the staff is going to have the opportunity through the DAC inspection process, with the appropriate expertise, to look at those before equipment is installed.

MEMBER STETKAR: The question is will the people who've looked at that do the type of confirmatory audit that you talked about before, that says, someone designed it that says A and B and C should do this. And yes, indeed A and B and C do those things. So, they said that we would design it this way. They implemented the design that way, and our inspectors confirmed that the design was

implemented that way.

I'm looking for something that says, A and B and C, because of the way that the intermediate level logic, which it's my understanding inspectors will not be inspecting.

MS. CUBBAGE: Well, I think that's a fundamental disconnect.

MEMBER STETKAR: The way that was implemented --

MS. CUBBAGE: There's a fundamental disconnect in your understanding of the DAC process.

MEMBER STETKAR: Because we haven't heard -- this committee has not heard --

CHAIR CORRADINI: No, we haven't. But now I'm going to -- we're back into a process, which I -- this is the second part of the discomfort, which I think is not just this subcommittee. The whole -- all the members have expressed it relative to the ITAAC process.

So, I guess I'd say I think we understand it. I'd like to go into break for going in the closed session, but I think the specifics have -- I think privately you can give the examples of your concern, which leads you to the need to make sure we're clear on this. But I don't know if we're going to get much

more out of this doing this again. One more round of the discussion isn't going to get us there.

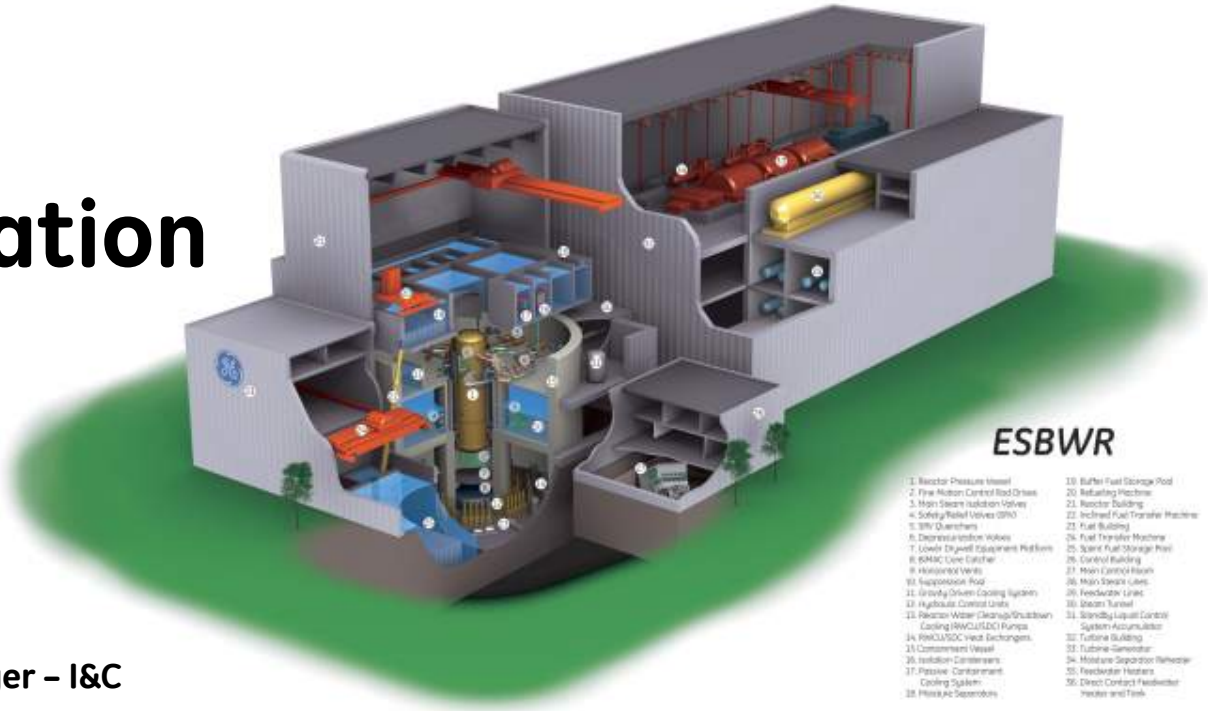
Okay, so at this point, I'm going to thank the staff, thank the members. Take a break until ten of.

(Whereupon, the above-entitled matter went off the record at 10:33 a.m.)

GEH Nuclear Energy

ACRS Committee Meeting
22 October 2009

ESBWR
Design Certification
Chapter 7 I&C



Skip Butler; GEH ESBWR Engineering Manager – I&C
Ira Poppel; GEH ESBWR Principal Engineer – I&C
Romeo Daccache; GEH ESBWR I&C Lead Engineer
Lloyd Heckle; GEH Software Quality Assurance Manager

HITACHI

Rev. 4 dated 2009-10-20

ESBWR I&C Design Certification Topics

- **Changes to Chapter 7 I&C in Rev 6**
- **ACRS Guidance on I&C based on Rev 5**
  - Design Process and DACs
  - Level of DCIS Design Detail
- **Regulatory Compliance – The Approach**
- **Software Design Process – The LTR Trinity**

  SMPM, SQAPM and CySPP
- **I&C Design Principles – The Overview**
  - Simplicity
  - Independence
  - Redundancy
  - Determinancy
  - Diversity (D3)
- **Questions?**

Changes to Chapter 7 I&C in Rev 6

	Source	Prelim	Final	Total	Comment
NRC Driven	**RAIs**	**~90**	**~4**	**~94**	**Prelim (June) to Final (August)**
	Chapter 7	70	0	70	Conforming changes in support of other disciplines regarding Instrumentation, Control, and Diversity IEEE Std 603 compliance matrices, Cyber Security, Level of DCIS Design Detail
	Other Chapters	20	4	24	S14.3 – Software development process S14.2 – Tier 1 – Description, Arrangements, DAC/ITAAC
	Unresolved			**5**	RAI 7.1-139 - Level of Detail, Setpoint Method (3) RAI 3.11-39 EQ for EMI (Post DCD Rev. 6 - 8 Oct. 09)
GEH Driven	**ECAs**	**6**	**0**	**6**	**No significant impact on I&C design**
	I&C driven	0	0	0	
	I&C impacted	6	0	6	
	I&C not impacted	10	4	14	
	CARs	**1**	**0**	**1**	**Quality Self-Assessment…** Correct LTR consistency w/ itself, Ch7 & Tier 1 SMPM (~250), SQAPM (~350) and CySPP (~200)
	LDRs	**~86**	**~14**	**~100**	**Quality Self-Assessment…** Correct minor issues concerning completeness and consistency of supporting details within Chapter 7, between other Chapters and Tier 1
	IRTs	**0**	**1,210**	**1,210**	**Quality Peer Review…** Mainly correcting minor documentation format issues

Substantial INCREASE in PROCESS and DESIGN DETAIL

ACRS Guidance on I&C based on Rev 5

Extracts from letter dated 22 Dec. 2008 (regarding **ACRS I&C Meeting on 3 Dec. 2008**)

From: William J. Shack; Chairman

To: Mr. Borchardt; Exec. Director Operations

CONCLUSIONS AND RECOMMENDATIONS:

1. The applicant has an acceptable process for developing the Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) for the Initial Plant Test Program as described in Section 14.2 of Chapter 14.
2. **The Design Acceptance Criteria (DAC) for the Distributed Control and Instrumentation System are incomplete. The staff has issued requests for additional information (RAIs) that address the DAC needed to ensure adequacy of the design process.**
3. **The Tier 2 Design Certification Document (DCD) should include additional information on the architecture of the instrumentation and control (I&C) system, and appropriate ITAAC and DAC should be added to the Tier 1 DCD.**
4. We will review the resolution of open items in SER Chapters 7 and 14 during future meetings.

Additions needed to DCD Tier 2 and Tier 1 as well as LTRs to ensure…
Adequacy of DESIGN PROCESS and Level of DESIGN DETAIL

Recommendation – Enhance Design Process and DACs

Tier 2	Ch. 7	Other	Total	Ch.7 % Tot
Chapter count:	1	19	20	5.3%
Page count :	485	~7,515	~8,000	6.1%
Tier 1				
DAC count :	663	25	688	96%
ITAAC count :	801	586	1,387	58%
DAC+ITAAC count :	1,464	611	2,075	71%

ADDITIONAL DETAIL resulted in >80% increase in DACs (and ITAACs)…
Ensures ADEQUACY of I&C SYSTEM and SOFTWARE DESIGN PROCESS

Recommendation – Provide Add'l DCIS Design Detail Example… RAI 7.1-139 – Question 3

NRC Request:

DCD Tier 2 Figure 7.1-1 shows the elements of the Q-DCIS and the N-DCIS with a very high-level functional representation. During the ACRS meeting, GEH presented additional architectural information, including a simplified diagram with a "safety ring." This level of architectural detail needs to be included in the DCD for the safety systems. Add figures with this level of detail to the DCD with corresponding discussion in the text as applicable.

GEH Response:

17 New or Revised Figures provided w/ descriptive text…

New [Qty 8] – (See Backup for copies):

- Figure 7.2-11a, RTIF Functional Block Diagram
- Figure 7.2-11b, RTIF Functional Block Diagram - OLU Detail
- Figure 7.2-12, NMS Functional Block Diagram
- Figure 7.3-6, SSLC/ESF Division 1 Layout
- Figure 7.3-7, SSLC/ESF Functional Block Diagram
- Figure 7.3-8, SSLC/ESF Interdivisional Communication Detail
- Figure 7.3-9, SSLC/ESF Safety-Related VDU Communication Detail
- Figure 7.3-10, SSLC/ESF Nonsafety-Related Communication Detail

Revised [Qty 9]:

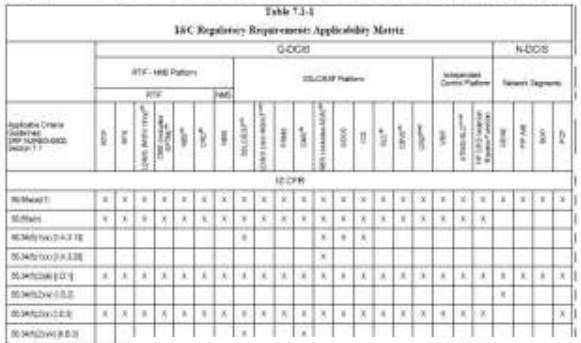
- Figure 7.1-1, Simplified Network/Functional Diagram of DCIS
- Figure 7.2-2, RPS Interfaces and Boundaries Diagram.
- Figure 7.3-1a, SRV Initiation Logics
- Figure 7.3-1b, GDCS and DPV Initiation Logics
- Figure 7.3-2, GDCS Equalizing Valve Initiation Logics
- Figure 7.3-3, LD&IS System Design Configuration
- Figure 7.3-4, SSLC/ESF Functional Block Diagram
- Figure 7.3-5, SSLC/ESF System Interface Diagram
- Figure 7.4-3, Isolation Condenser System Initiation and Actuation

Chapter 7 Rev 6 contains 485 Pages plus Change List with 111 Pages
Significant ADDITIONAL DESIGN DETAIL with block diagrams provided

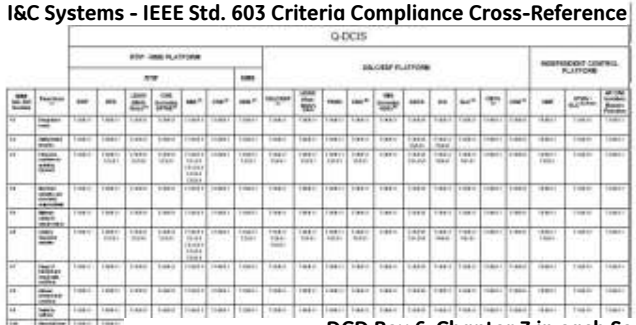
Regulatory Compliance – The Approach

Tier 2

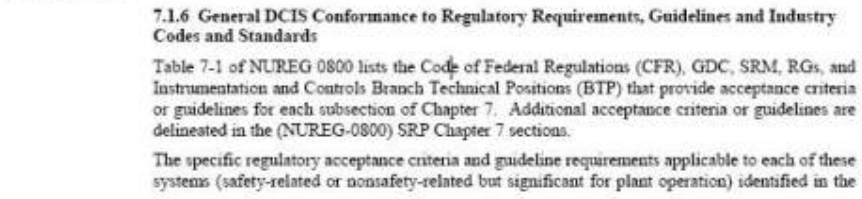
DCD Rev 6 Table 7.1-1
I&C Regulatory Requirements Applicability Matrix



DCD Rev 6 Table 7.1-2
I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference



DCD Rev 6 Chapter 7 in each Section
Conformance Statements to Regulations, Guides, BTPs and Industry Standards



7.1.6 General DCIS Conformance to Regulatory Requirements, Guidelines and Industry Codes and Standards

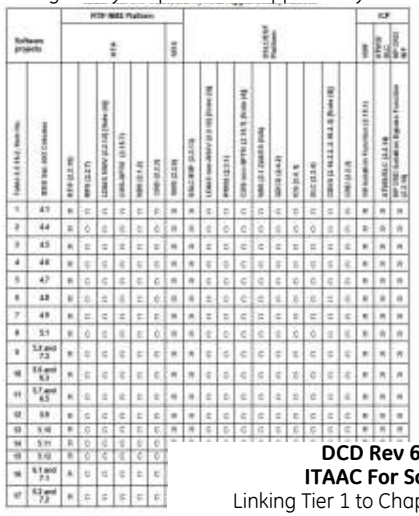
Table 7-1 of NUREG 0800 lists the Code of Federal Regulations (CFR), GDC, SRM, RGs, and Instrumentation and Controls Branch Technical Positions (BTP) that provide acceptance criteria or guidelines for each subsection of Chapter 7. Additional acceptance criteria or guidelines are delineated in the (NUREG-0800) SRP Chapter 7 sections.

The specific regulatory acceptance criteria and guideline requirements applicable to each of these systems (safety-related or nonsafety-related but significant for plant operation) identified in the

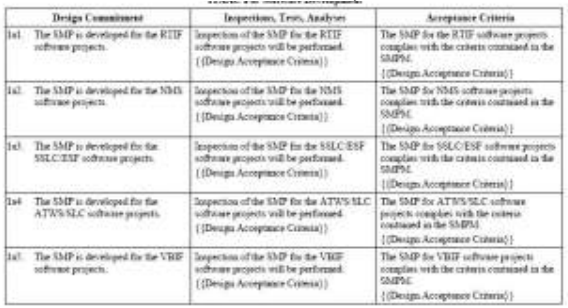
Cross Reference and Traceability Matrix

Tier 1

DCD Rev 6 Tier 1 Table 2.2.15-1
IEEE Std 603 Criterion System Applicability Matrix
linking Tier 1 to Chapter 7 Design Basis and
Table 7.1-1
I&C Regulatory Requirements Applicability Matrix



DCD Rev 6 Tier 1 Table 3.2-1
ITAAC For Software Development
Linking Tier 1 to Chapter 7B Software Development
which refers in the 3 inter-related LTRs
SMPM, SQAPM and CySPP



Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1a1. The SMP is developed for the RTIF software projects.	Inspection of the SMP for the RTIF software projects will be performed. {{Design Acceptance Criteria}}	The SMP for the RTIF software projects complies with the criteria contained in the SMPM. {{Design Acceptance Criteria}}
1a2. The SMP is developed for the NMS software projects.	Inspection of the SMP for the NMS software projects will be performed. {{Design Acceptance Criteria}}	The SMP for NMS software projects complies with the criteria contained in the SMPM. {{Design Acceptance Criteria}}
1a3. The SMP is developed for the SSLC/ESF software projects.	Inspection of the SMP for the SSLC/ESF software projects will be performed. {{Design Acceptance Criteria}}	The SMP for SSLC/ESF software projects complies with the criteria contained in the SMPM. {{Design Acceptance Criteria}}
1a4. The SMP is developed for the ATWS/SLC software projects.	Inspection of the SMP for the ATWS/SLC software projects will be performed. {{Design Acceptance Criteria}}	The SMP for ATWS/SLC software projects complies with the criteria contained in the SMPM. {{Design Acceptance Criteria}}
1a5. The SMP is developed for the VBF software projects.	Inspection of the SMP for the VBF software projects will be performed. {{Design Acceptance Criteria}}	The SMP for VBF software projects complies with the criteria contained in the SMPM. {{Design Acceptance Criteria}}

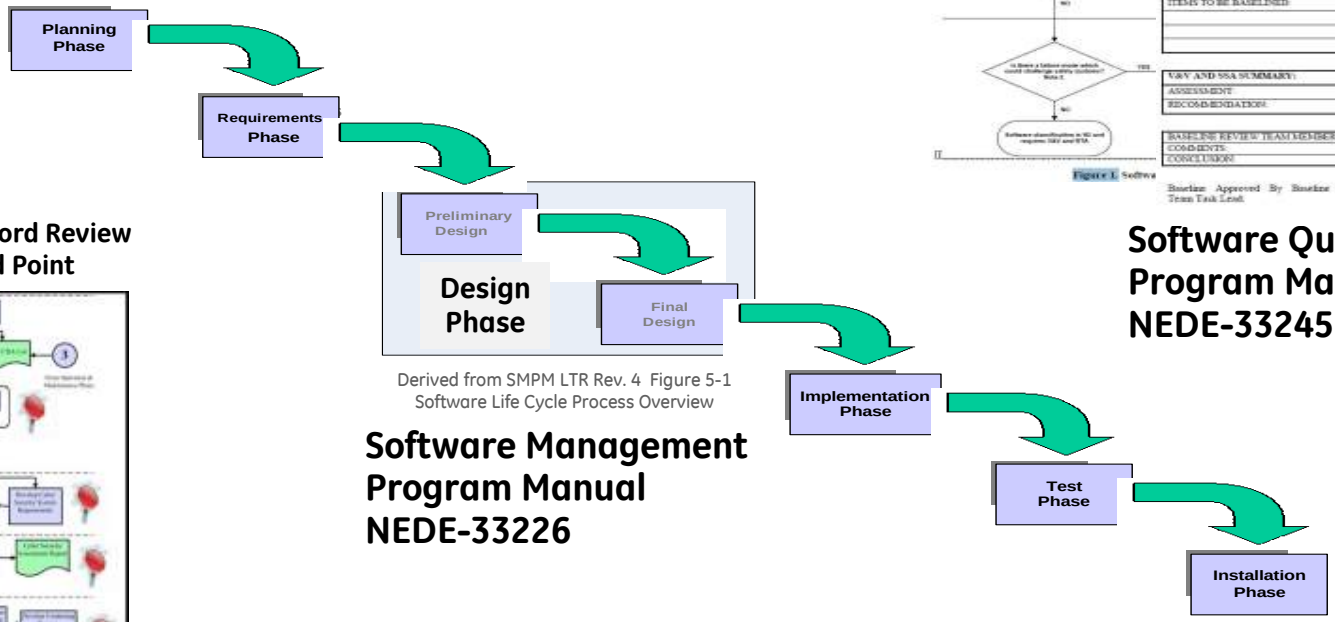
~2,280 Regulatory Conformance Statements

1,464 DAC and ITAAC Commitments

Regulation… Foundation for Quality, Safety and Reliable I&C System DESIGN and Software PROCESS

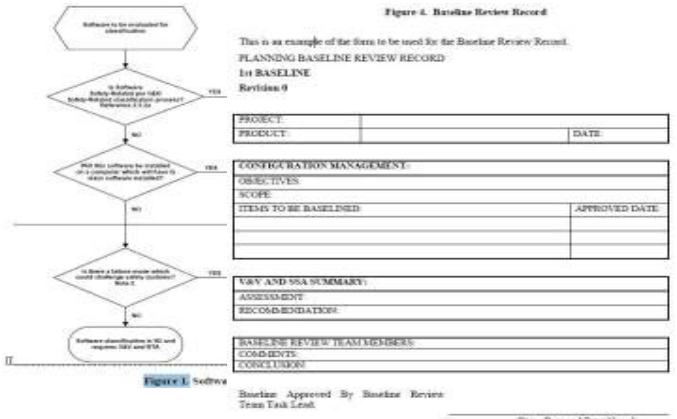
HITACHI

Software Design Process – The LTR Trinity



Derived from SMPM LTR Rev. 4 Figure 5-1
Software Life Cycle Process Overview

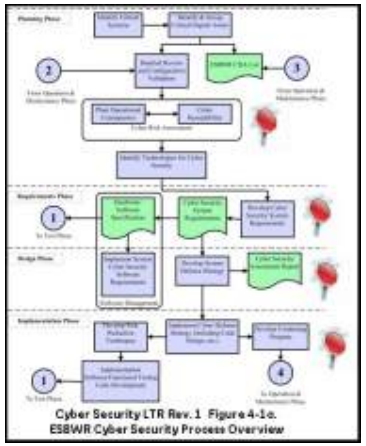
Software Management Program Manual NEDE-33226



Software Quality Assurance Program Manual NEDE-33245

KEY:

Baseline Record Review Audit or Hold Point

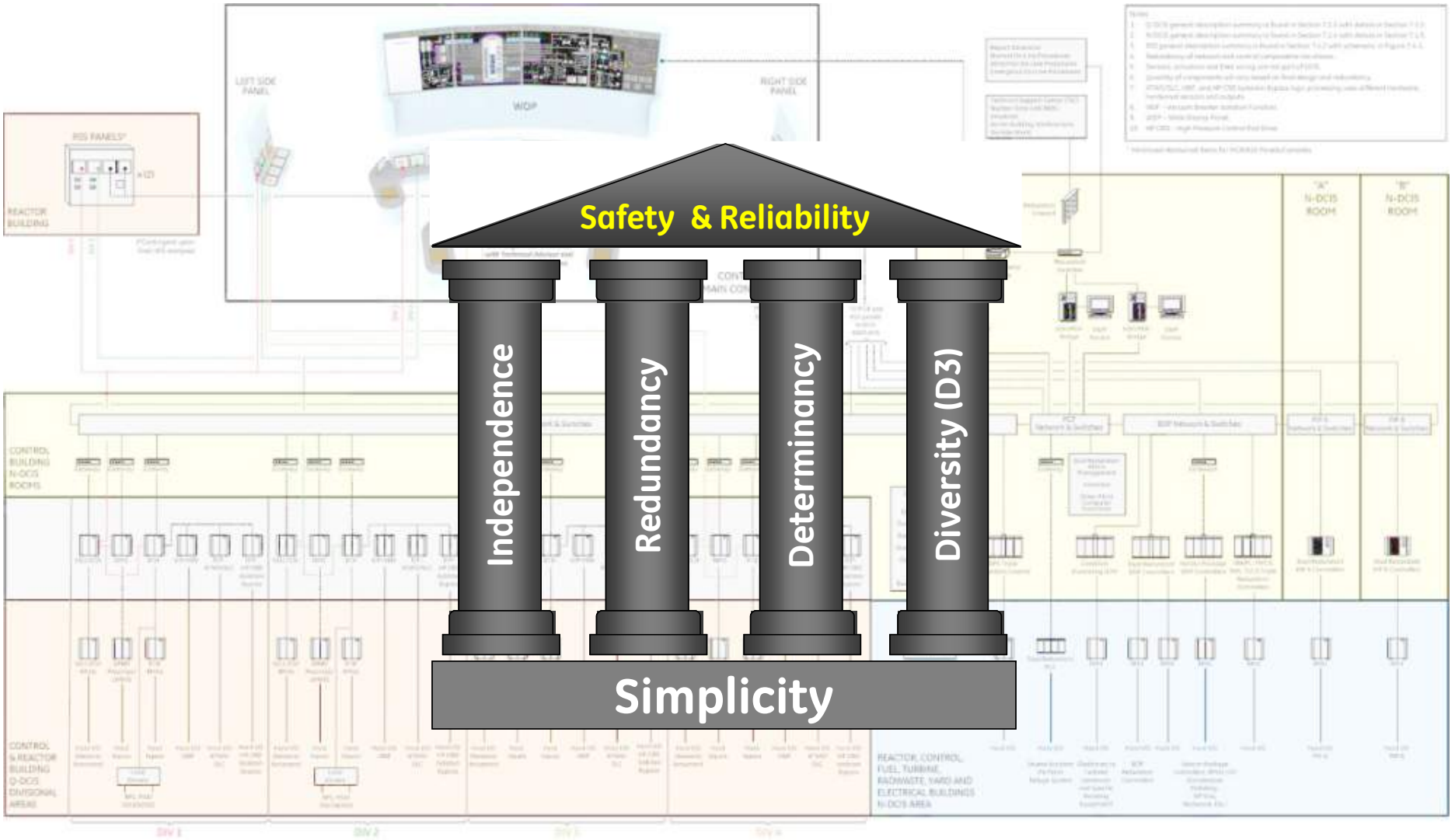


Cyber Security LTR Rev. 1 Figure 4-1c.
ESBWR Cyber Security Process Overview

Cyber-Security Program Plan NEDE-33295

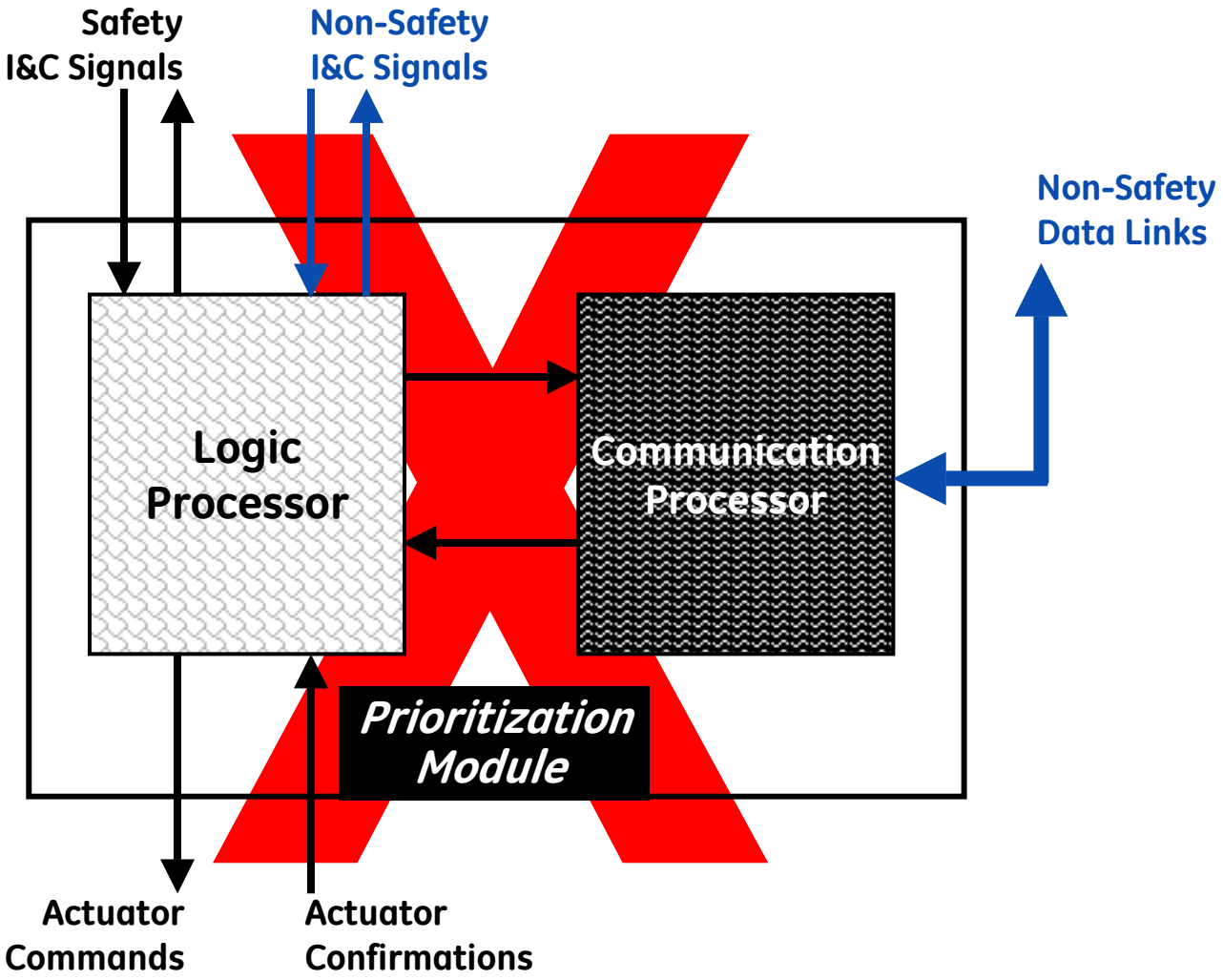
LTRs are detailed, comprehensive and integrated…
Provide structure for System and Software DESIGN PROCESS
Foundation of DAC and ITAAC Closure

I&C Design Principles – The Overview



Based on IEEE Std 603

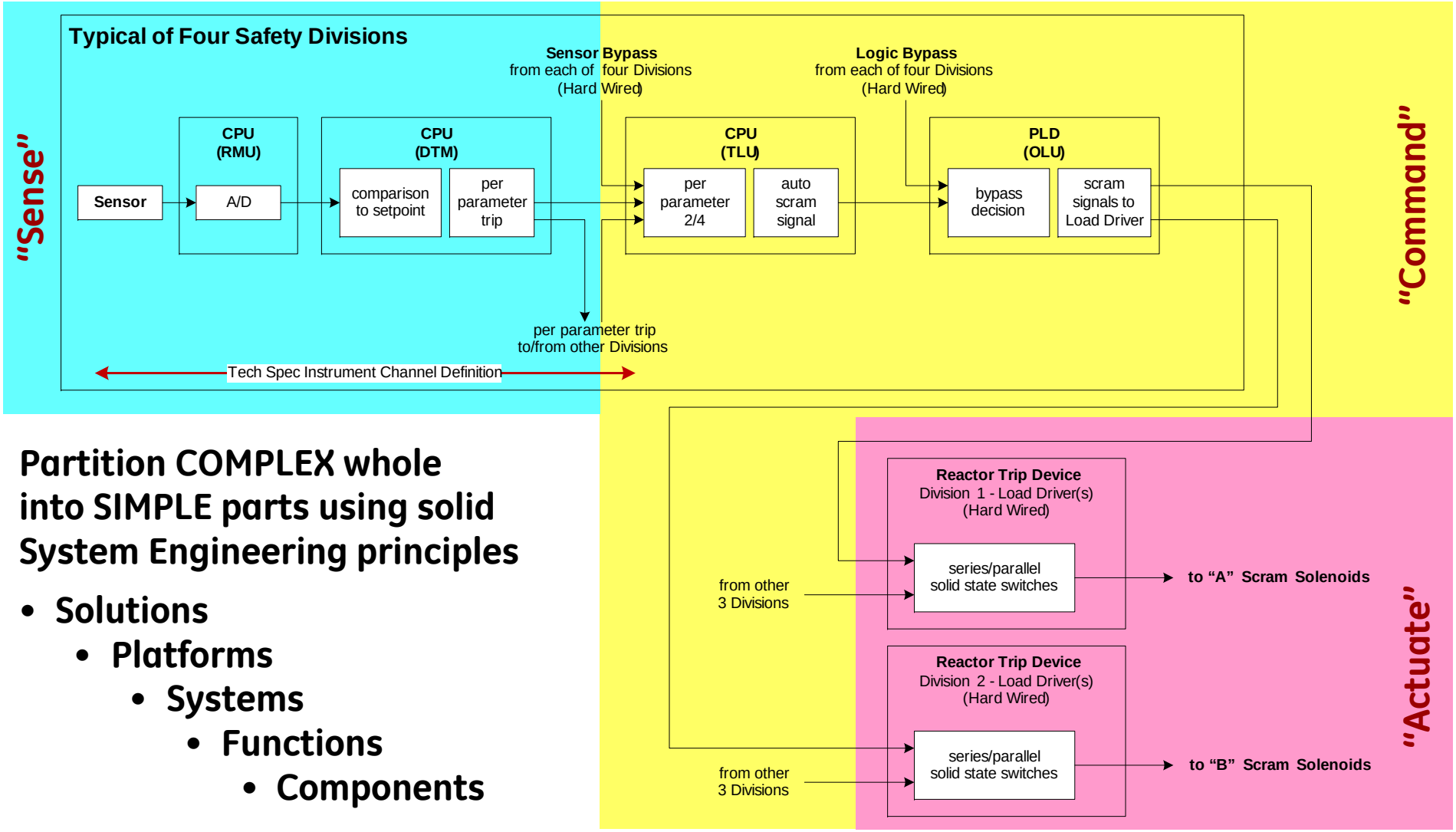
Design Principle – Simplicity



ISG-04 acknowledges possible use of "Prioritization Module" Concept but…
Introduces SOFTWARE COMPLEXITY and IEEE Std 603 compliance challenges

ESBWR DCIS is SIMPLE… Does NOT use "Prioritization Module"

Design Principle – Simplicity… RPS Example



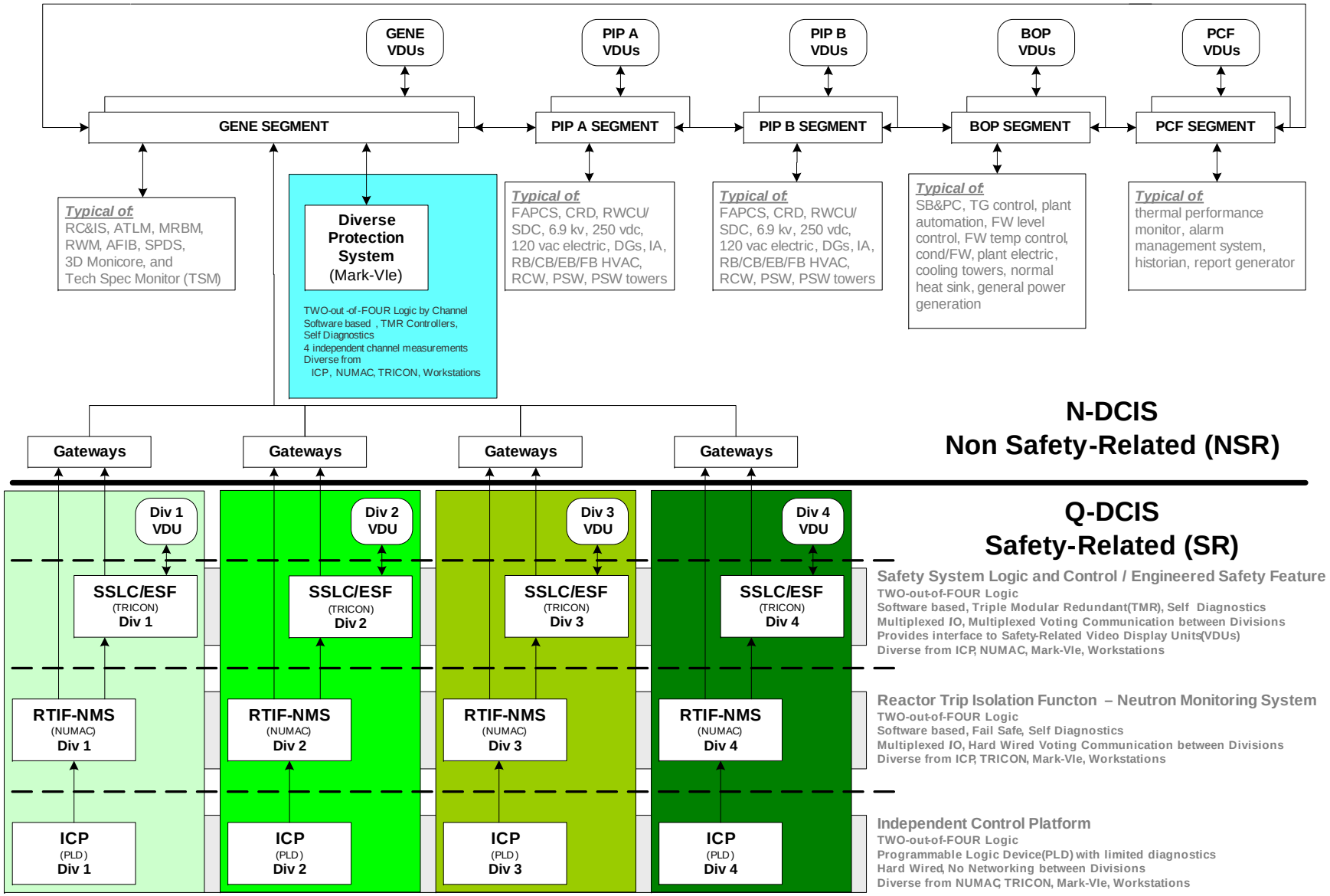
Partition COMPLEX whole into SIMPLE parts using solid System Engineering principles

- Solutions
  - Platforms
    - Systems
      - Functions
        - Components

Derived from DCD Rev. 6 Figure 7.2-1 RPS Simplified Functional Block Diagram

SIMPLE… Functions are Separate, Isolated and INDEPENDENT

Design Principle – Independence… DCIS Platforms



Derived from DCD Rev. 6 Figure 7.1-1 ESBWR Instrumentation and Control DCIS Simplified Network and Functional Block Diagram

Strict IEEE Std 603 Compliance… Channel and Divisional INDEPENDENCE

Design Principle – Redundancy

All Safety DCIS (as required by IEEE Std 603) is REDUNDANT for:

- Sensors, Controllers and Actuators

SSLC/ESF DCIS:

- Controllers and Actuator outputs are triply redundant (TMR) within Division to avoid inadvertent actuation

All Safety DCIS design is Single Failure Proof for:

- Safety transient analysis events including inadvertent actuation
- Non Safety normal operations
- DCIS is not a credible transient "initiator"

All DCIS is REDUNDANTLY powered (primary and cabinet)

- Safety DCIS is REDUNDANT with its Division

Non Safety DCIS may use REDUNDANT:

- Sensors, Controllers and Actuators

As required for plant availability including single failure proofing

All DCIS Networks (except Point-to-Point) are REDUNDANT

ESBWR DCIS meets or exceeds requirements for REDUNDANCY

Definition of… Determinancy

In computer science, a deterministic algorithm is an algorithm which, **in informal terms, behaves predictably**.

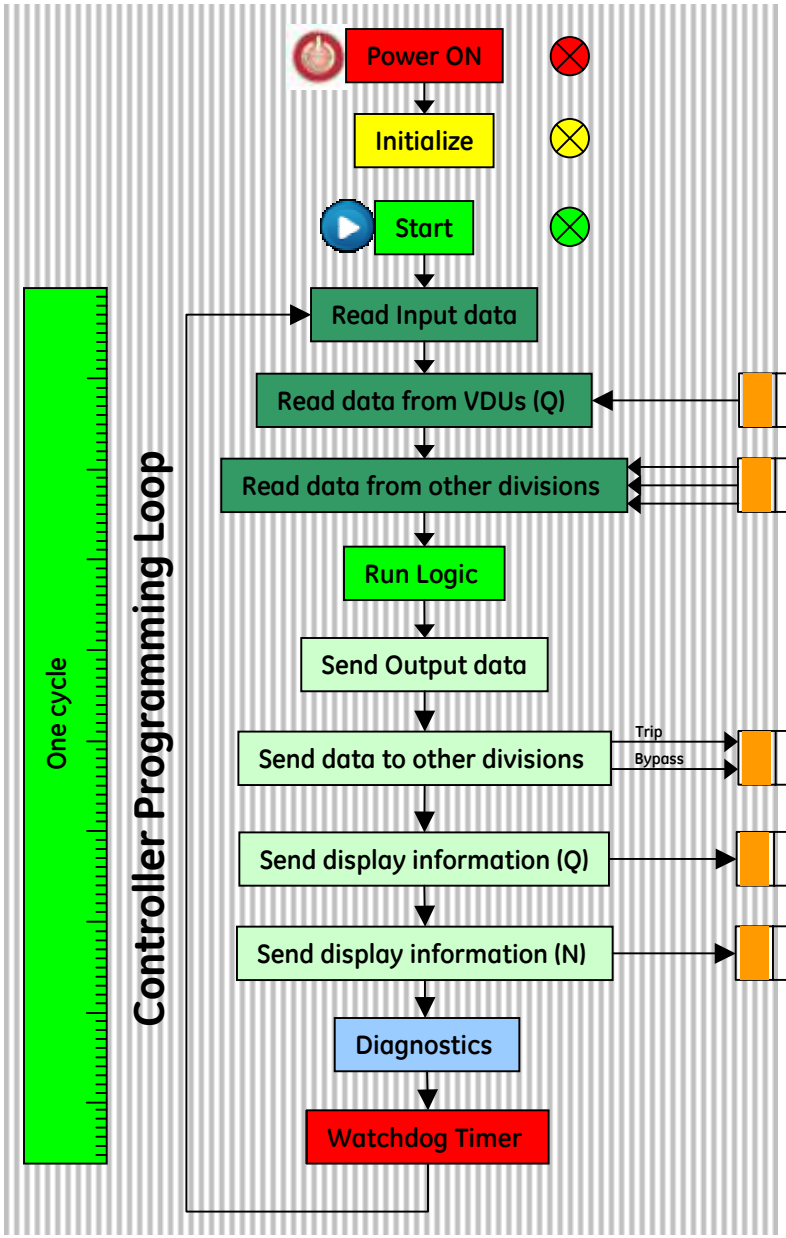
Given a particular input, … output, and the underlying … of states. Determi… algo… m…

DETERMINANCY achieved when…
known PRECONDITIONS and INPUTS provided then…
OUTPUT is PREDICTABLE in time frame of interest

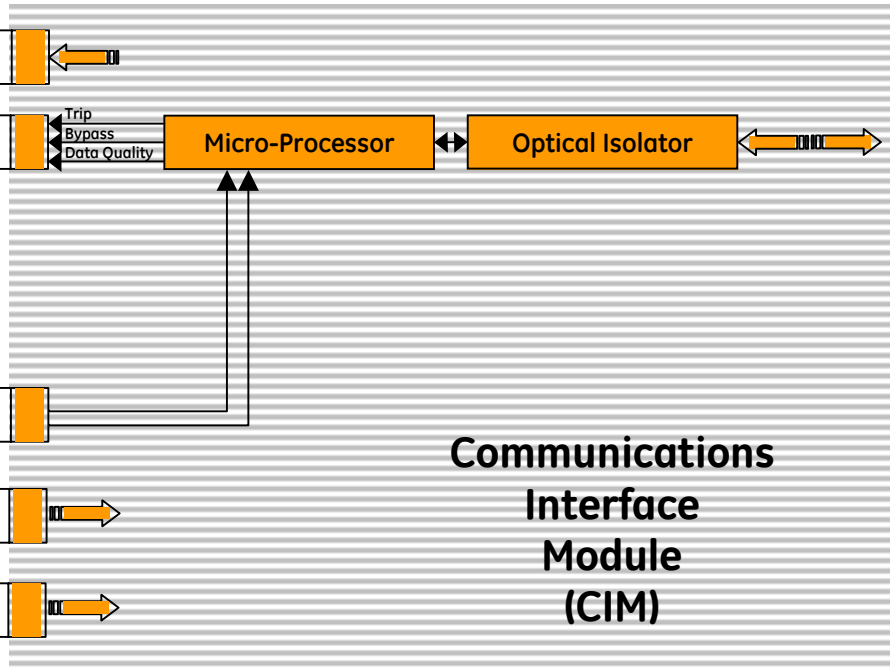
All controllers have I/O dedicated to their functions…
Networks are NOT used for Closed Loop Control
supports design wherein
Control is DETERMINISTIC

Le… chan… **same way … …ring at its input channels**. … input I1 and event E2 occurs at T2 > T1 at the input I2, the consequence of E1 should be seen at the outer limit of the system before the consequence of E2. Here a time out can be considered also as an external event. In order to react in this way, all the events have to be "serialised" in a "scheduler" before their consequence is processed and seen in the corresponding output channel.

Design Principle – Determinancy… Controllers



RTIF-NMS, SSLC/ESF and DPS controllers use similar operating principles but different HW/SW specific implementations of the programming loop concept



Executes DETERMINISTICALLY…
Buffered from data communications

Design Principle – Determinancy… Communications Example (1/2)… RTIF – 2 Types

Safety-to-Safety Communications

Inter-Divisional
"2-out-of-4" Trip Logic Unit (TLU) is on Point-to-Point data links on DEDICATED Optical Fiber

Intra-Divisional
communication uses Shared Reflective Memory (SRM) Bus or ("Scramnet")

Safety-to- Non Safety

All CIM devices are Safety-Related Equipment

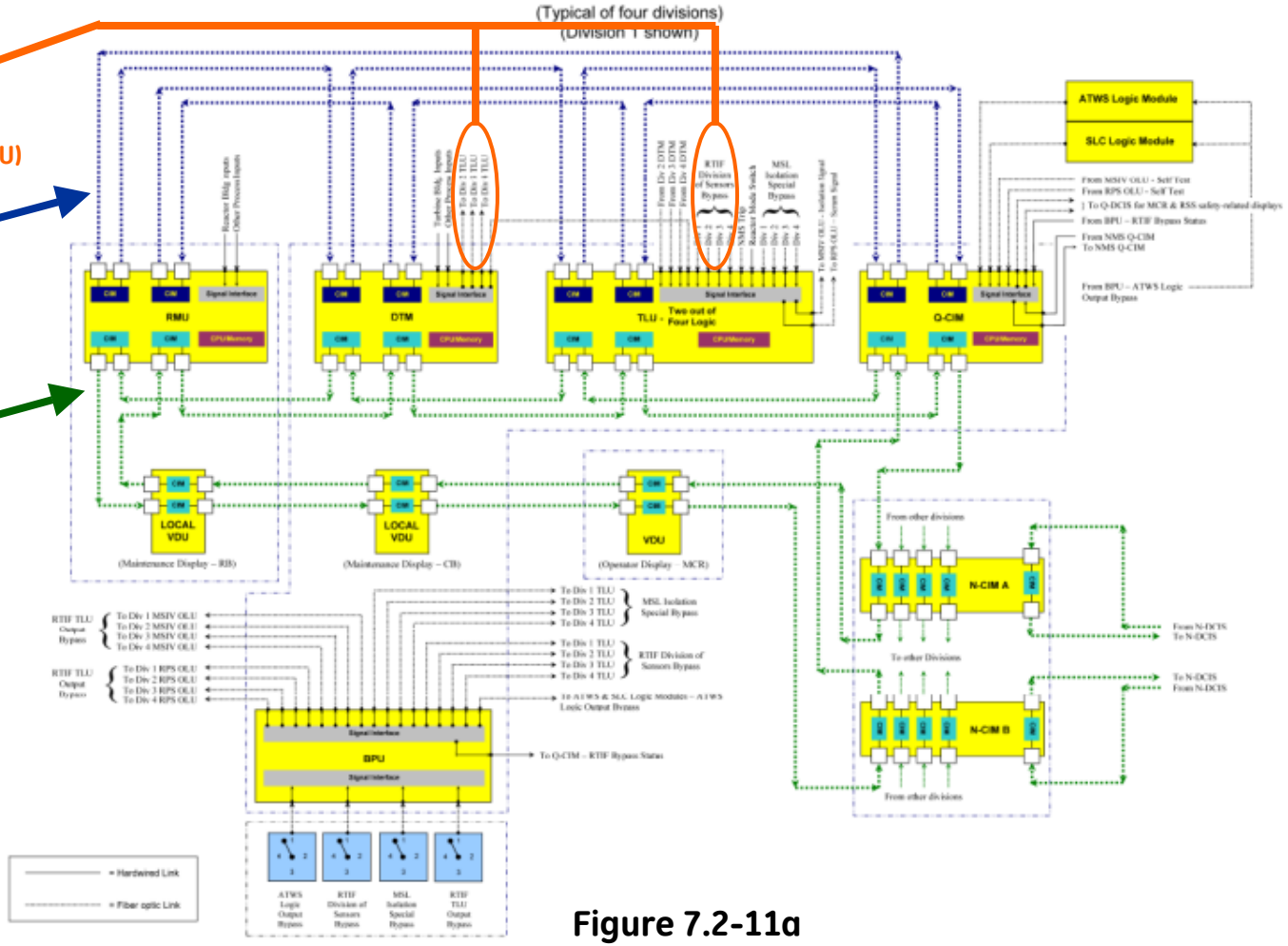


Figure 7.2-11a
Reactor Trip and Isolation Function (RTIF) Simplified Functional Block Diagram

Point-to-Point and Shared Reflective Memory cycle time is 10's micro-sec.
Required reactor scram response time in 10's milli-sec.
Communications are DETERMINISTIC

Design Principle – Determinancy… Communications Example (2/2)… SSLC/ESF Inter-Divisional – Ethernet

"2-out-of-4" voting trip logic on DEDICATED network…
Extremely lightly loaded 100 Mbits/Sec Ethernet

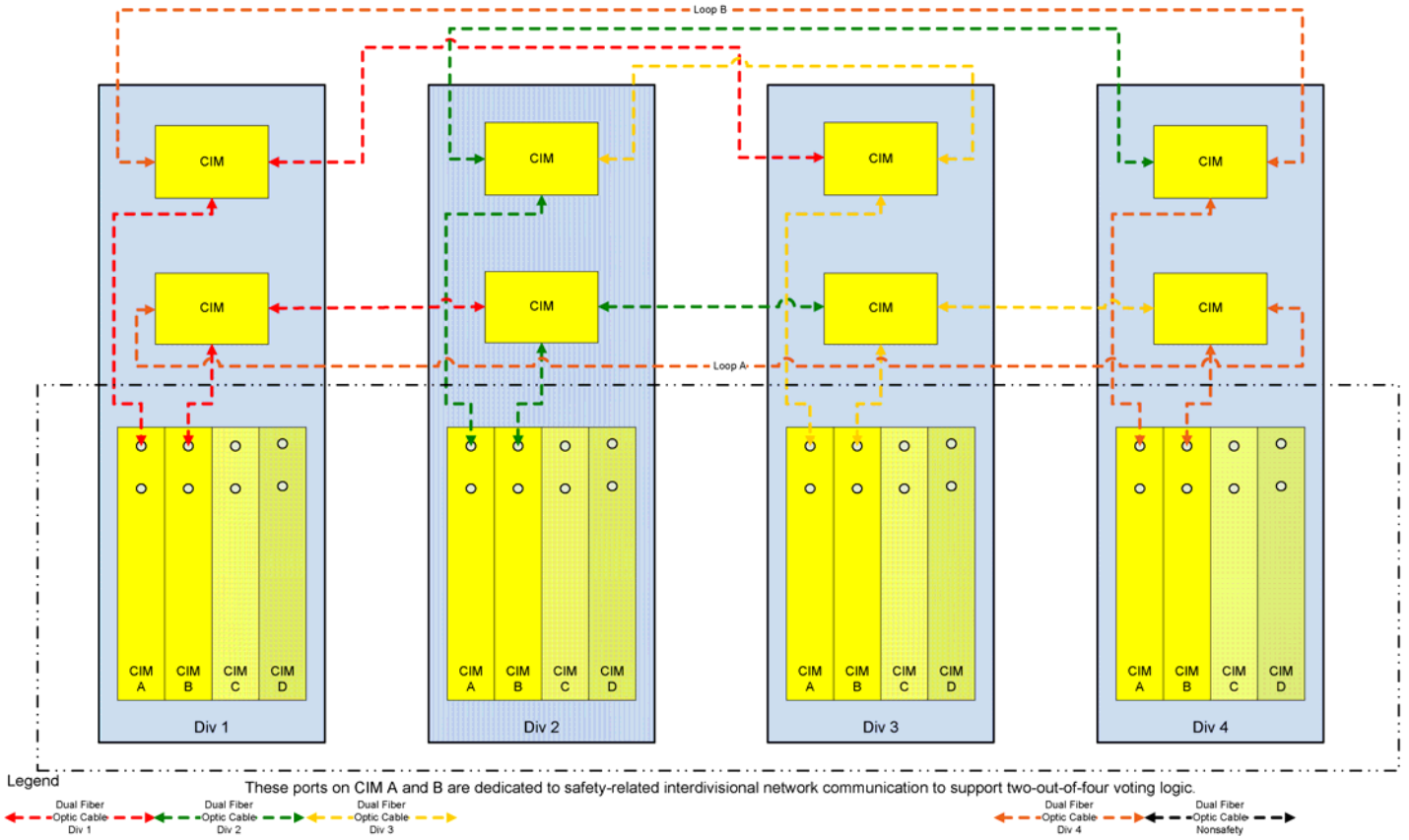
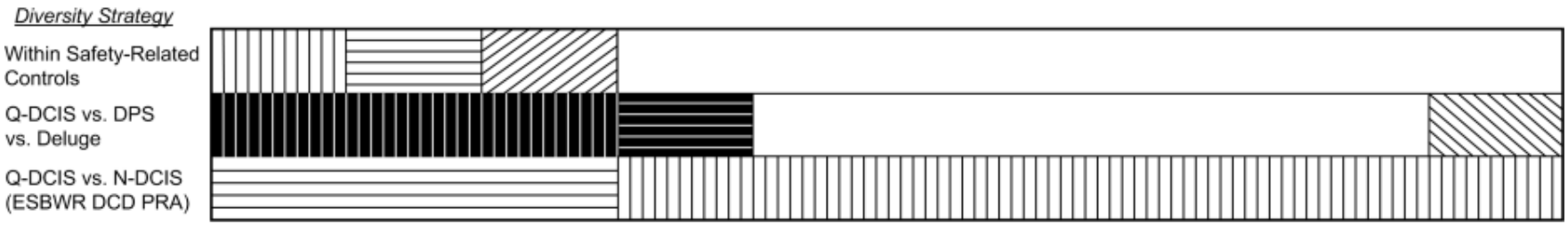


Figure 7.3-8
SSLC/ESF Inter-Divisional Communication Detail

Key design parameters… Bandwidth, Packet Size and Transmit Rate Communications are DETERMINISTIC

Design Principle – Diversity… The DCIS Platform Concept

Safety Category	Safety-Related			Nonsafety-Related						
	Q-DCIS			N-DCIS						
Platform/Network Segment	RTIF NMS	SSLC/ESF	Independent Control Platform	GENE		PIP A/B	BOP		PCF	
Architecture	Divisional	Divisional	Divisional	Triple Redundant (DPS)	Dual Redundant	Dual Redundant	Triple Redundant	Dual Redundant	Workstations	PLC (Deluge)

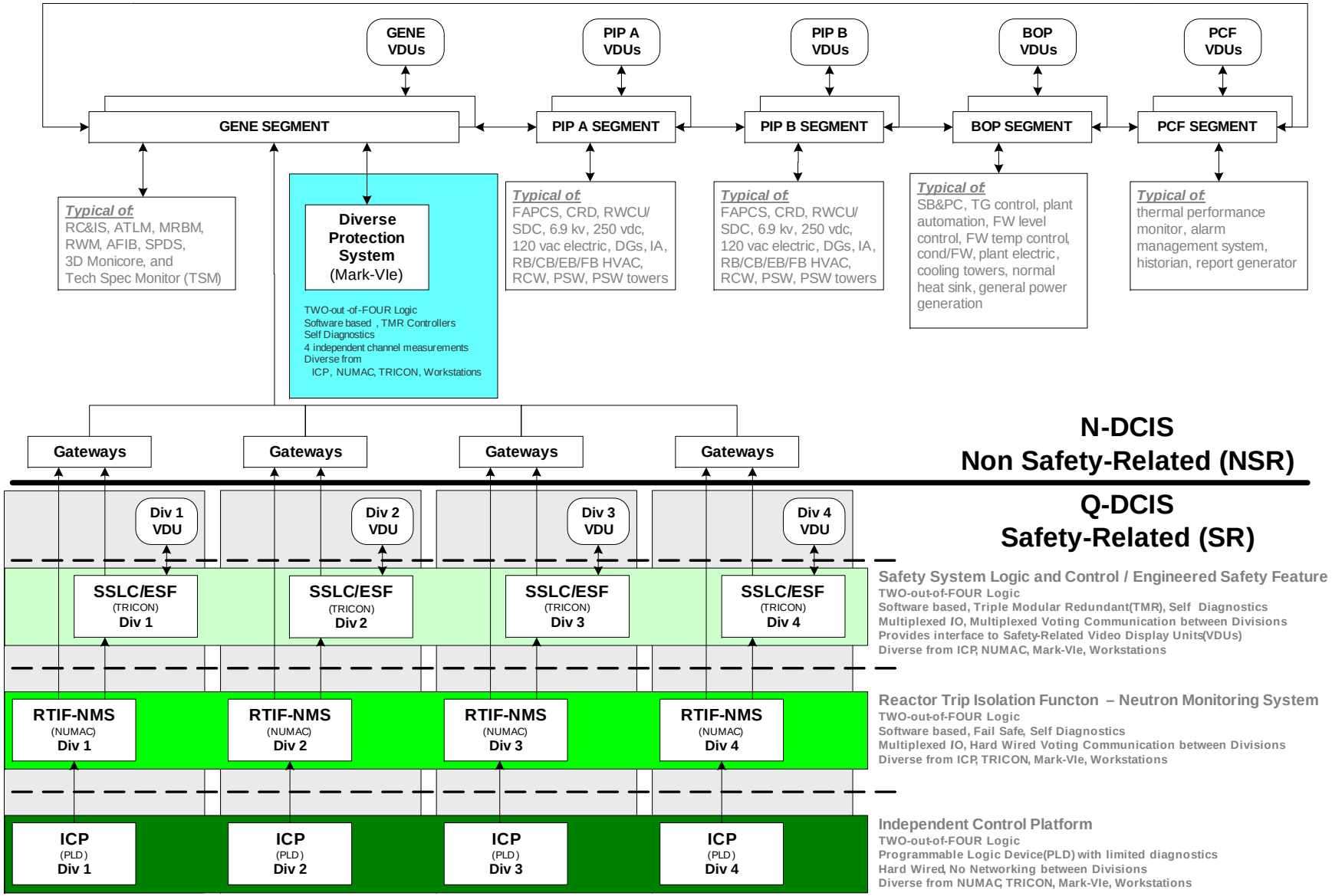


NOTE: Crosshatching denotes different platforms or networks.

DCD Rev 6 Figure 7.1-4 and D3 LTR Figure 1.1

ESBWR Hardware/Software (Architecture) Diversity Diagram

Design Principle – Diversity… The 4 DCIS Platforms

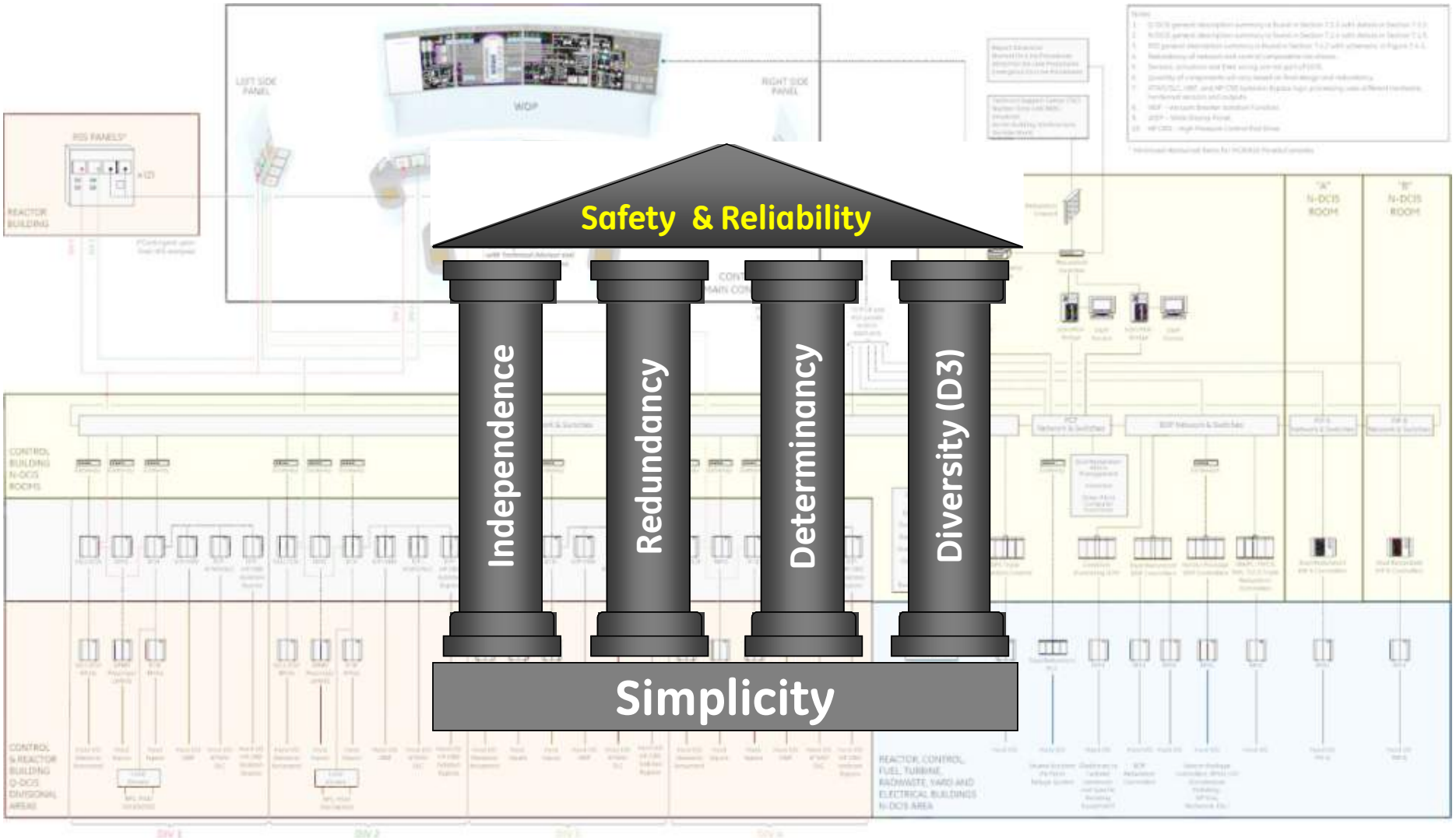


Derived from DCD Rev. 6 Figure 7.1-1 ESBWR Instrumentation and Control DCIS Simplified Network and Functional Block Diagram

3 Safety Systems and 1 DPS in 4 Platforms provides… DIVERSITY

HITACHI

Questions?



Regulatory Compliance + Software Process + Design Principles

Presentation to the ACRS Subcommittee

ESBWR Design Certification Review

Chapter 7, “Instrumentation and Controls”

October 22, 2009

Purpose

- Brief the Subcommittee on the staff's resolutions from earlier ACRS Chapter 7 interactions from December 2008
- Provide staff's perspective on the four pillars plus one design principles
- Request advice from the subcommittee

Chapter 7 Review Team

- Project Manager
  - Dennis Galvin

- Technical Reviewers
  - Hulbert Li, Lead
  - Leroy Hardin
  - Joseph Ashcraft

Timeline

- ACRS meeting (Dec 2008)
- ACRS letter (Dec 2008)
- Staff's response (Jan 2009)
- Staff request for additional information
  - ACRS recommendation and transcript
- DCD Revision 6
  - reflects RAI responses

Resolution of Specific ACRS Comments

1. Cross-reference between Tier 1 and Tier 2

GEH Action: DCD Revision 6 (Tables 7.1-2 and 14.3-1a) provided cross reference

The staff finds the cross references accurate and useful and, therefore, acceptable

Resolution of Specific ACRS Comments

2. The Design Acceptance Criteria (DAC) for the Distributed Control and Instrumentation System are incomplete. The staff has issued RAIs.

   GEH Action: DCD Revision 6 (Tier 1 Section 2.2.15) provides detailed ITAAC to cover the requirements of IEEE Std. 603 for all safety-related I&C systems. Section 3.2 provides detailed ITAAC for verification of life cycle implementation of all I&C platforms

   The staff finds the I&C DAC in the updated DCD acceptable

Resolution of Specific ACRS Comments

3. The Tier 2 DCD should include additional information on the architecture of the I&C system and appropriate ITAAC and DAC should be added to the Tier 1 documentation.

GEH Action: DCD Revision 6 added additional description and functional block diagrams in Sections 7.1, 7.2, 7.3, and 7.4. Provided enhanced ITAAC for verification.

The staff finds the additional architecture information in the updated DCD acceptable

Resolution of Specific ACRS Comments

4. The current Tier 2 documentation does not contain integrated functional logic diagrams at a level of detail showing input signals, protection and actuation logic, output signals, and basic dependencies such as power supplies.

GEH Action: GEH provided a set of functional logic diagrams for staff information. A copy of these logic diagrams were also provided to ACRS.

The staff's review of the diagrams determined that they were consistent with the description in relevant DCD revisions. The staff understood that the diagrams reflected of the ESBWR I&C design and would be refined as the detailed design is implemented. The staff will inspect the diagrams during ITAAC resolution stage. .

Staff Conclusion

- The staff requested additional information from GEH on architecture of I&C and other level of detail questions based on ACRS recommendations and meeting transcripts
- In DCD Revision 6, GEH provided additional information in Tier 2 that includes more detailed functional block diagrams and descriptions in Tier 2, Sections 7.1, 7.2, 7.3, and 7.4
- In DCD Revision 6, GEH provided ITAAC for verification of all IEEE Std. 603 requirements for all safety-related I&C systems and ITAAC for verification of life cycle implementation of all platforms
- The staff concludes that the GEH's substantive I&C design information in DCD including the DAC and ITAAC conforms to the regulatory requirements under part 52 and provides reasonable assurance of safety. The implementation of DAC and ITAAC will be inspected by the staff to ensure the appropriate design implementation and as-built design.

Redundancy

- All safety-related platforms are organized into four physically and electrically isolated divisions
- FMEA will be used to confirm that the safety-related I&C systems satisfy single failure criterion
- Nonsafety-related network segments are triple/double redundant
- The staff finds the ESBWR I&C design meets redundancy design principle

Independence

- The staff's review of independence design principle is based on DCD design information and the DAC/ITAAC verification process
* The only inter-divisional data (trip or bypass) is sent for the "2-out-of-4" voting
- The RTIF-NMS and ICP platforms use "point-to-point" data link. The SSLC/ESF platform uses communication interface modules (CIM)
- The staff's careful review of the DCD information which include statements of communication independence finds that the ESBWR I&C design meets the communication independence principle

Determinism

- DCD states that Q-DCIS internal and external protocols are deterministic
- Determinism means a specific function always be accomplished within the required time period specified
- The deterministic character will be inspected during ITAAC resolution process

Defense-in-Depth and Diversity (D3)

- The license topical report provided D3 analysis following SRP BTP 7-19 guidance
- The diverse protection system design is documented in DCD Tier 2, Section 7.8, and the associated ITAAC is documented in DCD Tier 1, Section 2.2.14.
- The staff has reviewed the ESBWR D3 design and finds acceptable

Simplicity

- ESBWR design is to follow “Sense – Command – Actuate” approach
- ESBWR design meets “Independence – Isolation – Separation” requirements
- Inter-divisional communication is limited
- The staff finds that the ESBWR design follows “Simplicity” principle

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Committee Questions

Discussion/Committee Questions