Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisor Committee on Reactor Safeguards
Subcommittee on ESBWR

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Friday, September 24, 2010

Work Order No.: NRC-445

Pages 1-184

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

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.

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

SUBCOMMITTEE ON ESBWR

+ + + + +

FRIDAY

SEPTEMBER 24, 2010

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

SUBCOMMITTEE MEMBERS:

MICHAEL L. CORRADINI, Chairman

SAID ABDEL-KHALIK, Member

J. SAM ARMIJO, Member

CHARLES H. BROWN, Member

JOHN W. STETKAR, Member

CONSULTANTS:

THOMAS S. KRESS

GRAHAM B. WALLIS

DESIGNATED FEDERAL OFFICIAL:

CHRISTOPHER L. BROWN

NRC STAFF:

JOE ASHCRAFT

AMY CUBBAGE

THOMAS FREDDIE

DENNIS GALVIN

IAN JUNG

HULBERT LI

KHOI NGUYEN

DINESH TANEJA

DEANNA ZHANG

JACK ZHAO

GENERAL ELECTRIC HITACHI:

GARY ANTHONY (via telephone)

J. ALAN BEARD

SKIP BUTLER

PATRICIA CAMPBELL

ROMEO EL DACCACHE

BRAD JOHNSON

RICK KINGSTON

WAYNE MARQUINO

IRA POPPEL

PETER YANDOW

ALSO PRESENT:

WILLIAM BIRD, LOCKHEED MARTIN

KIMBERLY KEITHLINE, NEI

JOHN SMITH, WSC

A G E N D A

P R O C E E D I N G S

(8:30 a.m.)

CHAIRMAN CORRADINI: Okay, so we'll come to order. This is the second day of the ACRS Subcommittee meeting on the ESBWR application. My name is Mike Corradini, Chair of the Committee. We have with us today our consultants, Dr. Tom Kress, and Graham Wallis. Member Sam Armijo soon to be, John Stetkar, myself, Dr. Said Abdel-Khalik, and Charlie Brown. Our Designated Federal Official is Christopher Brown.

I'll skip through all the preliminaries, and simply remind everybody that a transcript of the meeting is being kept. It will be made available on the Federal Register. It's requested that speakers first identify themselves, and speak with sufficient clarity and volume so they can be heard.

Everybody please check your cell phones, pagers, appliances, silence them. All right? We've not received any request from members of the public to make oral statements. Do we have GEH folks on the phone line as we did yesterday?

PARTICIPANT: We do.

CHAIRMAN CORRADINI: Okay. All right. And then we are under the impression, and I'm going to make this clear to the GE presenters, that we're not presenting proprietary information relative to Chapter 7 I&C issues. If we delve into proprietary matters, and we need to close the session, you need to let us know. We can maybe postpone those questions until after break and pick them back up. All right?

Other than that, I am told that the GEH folks have some clarification, or information from what we had as open questions, or just open informational items from yesterday. So, Wayne, are you going to lead us in that?

MR. MARQUINO: Alan Beard is.

CHAIRMAN CORRADINI: Oh, Alan is. Okay, I'm sorry.

MR. BEARD: That's all right. Alan Beard with GE Hitachi. Two issues to follow up from yesterday. The first dealt with the potential for valve misalignment to draining of the suppression pool, or the GDCS pools, the mechanism up through the surge tanks.

CHAIRMAN CORRADINI: Okay.

MR. BEARD: Some information we delve out on that. The lines that connect both the suppression pool and the GDCS are 10 inches in diameter. The suppression pool has safety-related isolation valves on that system; however, they are manually actuated. There is no automatic actuation on those.

CHAIRMAN CORRADINI: Say that again. I'm sorry.

MR. BEARD: The suppression pool suction lines, there are safety-related containment isolation valves on them, that they are motor operated, and they require manual or a signal form the -- via manual operation in the control room. Signals that would be available to the operator to detect that he was having some sort of situation like that would be a decreasing level within the suppression pool, or a rising level within the surge tank of the spent fuel pool, so that there should be plenty of time to do that. With a 10-inch line and approximately 5-1/2 meters of head, we could estimate that the flow would be not tremendous. It would certainly be a significant amount, but not a huge volumetric rate.

As far as the connection to the gravity-driven cooling system pools --

CHAIRMAN CORRADINI: Could I just stop you just for clarification?

MR. BEARD: Yes, you may.

CHAIRMAN CORRADINI: So, the time window for them to see this is based on an annunciator that would show a low level, and they'd have to take action?

MR. BEARD: That would be correct.

CHAIRMAN CORRADINI: Okay. Thank you.

MR. BEARD: Normal operating level in the suppression pool is 5.45 meters, high level if 5.5 meters, low level is 5.4, so you would drain -- if you were operating at the high end of the band, potentially a tenth of a meter from the suppression pool before you would get the alarm that the level was dropping.

CHAIRMAN CORRADINI: Okay.

MR. BEARD: I would expect that if you're doing that, the first alarm that you would get would be the surge tank level going high.

CHAIRMAN CORRADINI: Okay. Thank you. I'm sorry. And then you wanted to go forward with GDCS.

MR. BEARD: Yes. As far as the GDCS pool suction, this was alluded to yesterday by John Gels on the phone from Wilmington. There are a scupper type of arrangement, and you can actually see this pictorially in Figure 9.1-1. The water that has been cooled, and is being returned to the GDCS pools is actually introduced into the center pool, which is labeled B on that drawing, and then it overflows through connections into the A&C pools. And then there are scupper suctions within the A&C pools to take that water, route it to the point. We're not exactly sure what the level of those are, but the scuppers are towards the top of the pool, so that the amount of water that could be lost in there would be fairly minimal.

The other question I was going to respond to was Mr. Stetkar's concern about load handling, and a statement about any radiological release --

CHAIRMAN CORRADINI: Why don't we -- can we hold that until we have him?

MR. BEARD: Yes.

CHAIRMAN CORRADINI: Okay. And we'll find him, and have him later. We'll catch up to you. Is that all right?

MR. BEARD: Yes.

CHAIRMAN CORRADINI: Okay.

MR. BEARD: And then the final thing, to go back, I did make a statement in error yesterday. I said that the rooms that house the FACPS pumps have watertight doors on them. Apparently, at some point I missed a design change. Those rooms actually do not have watertight doors on them, so I need to correct that for the record.

CHAIRMAN CORRADINI: Okay. And we'll wait on the heavy load handling, and the other question, Alan, until all the members are here.

So, Amy, did you want to say anything to lead us off here?

MS. CUBBAGE: No, we're just pleased to be here to continue with the meeting, and get to some challenging issues here on I&C. The Staff and GE have done a lot of work to prepare for this meeting. We're very hopeful that it'll address the Committee's concerns that have been expressed in the past, and look forward to your questions. And, hopefully, we can get them all answered today.

CHAIRMAN CORRADINI: Okay. And of the trio that's up there, who's going to lead us off, is it Skip, or you?

MR. BUTLER: I'll kick it off.

CHAIRMAN CORRADINI: Okay.

MR. BUTLER: And then when we get into portions of the technical material, Ira Poppel, who's the Principle Engineer and Lead Designer for the I&C DCIS will lead those discussions.

CHAIRMAN CORRADINI: Go ahead.

MR. BUTLER: Okay. So, next chart, please. Okay. So, just a brief overview of the agenda. We will highlight changes from Rev. 6 through 7 and 8, briefly. We'll talk about the ACRS letter on DAC on August 9th, 2010. And then we decided in GEH to proactively address some of those concerns after doing an internal assessment, and perhaps not having the content in tier two that was appropriate, so we'll discuss that. We'll present some of the key themes from the letter in our design, and then we'll present a key topic to some of the ACRS Members on logic diagrams. And then, if necessary, we have a number of backup slides that we might ask to go to if there's some additional discussions. Okay, next slide.

So, from Rev. 6 to Rev. 8, when we were here last on the 22nd of October, there's been a number of RAIs, three specifically for Chapter 7. One of them had to do with set point methodology, which is not germane to this particular discussion today, I think. There was one in November on digital devices, and we clarified some ambiguity in our licensing topical reports, that yes, all digital devices that involve software or firmware are covered by our LTRs. And then there was a clarification on GDCS equalizing valves, and some information regarding when they actuate with regards to sustained levels.

MS. CUBBAGE: Skip, if I may just for the

Members' benefit, when he refers to DCD Rev.8, DCD Rev. 8 has not been formally docketed as a whole DCD yet, but GE has docketed recently some change pages to Rev. 8, and they're going to be speaking to those today. The Committee has not received those. They just came in, I believe, yesterday, but we'll be happy to get those to you.

CHAIRMAN CORRADINI: So, just to clarify for the Committee, so Rev. 8 is be the one that is going to be docketed with all the necessary information that allows Staff -- that, essentially, answers the RAIs, and, therefore, closes all the open items.

MR. BEARD: That's right, in addition to these changes that GE has recently made in preparation for this meeting.

CHAIRMAN CORRADINI: Okay. Thank you. Go ahead.

MR. BUTLER: So, as I noted, we were also able to read the letter issued on the 9th of August, which gave us an opportunity to critique Tier 2, and most of this presentation is centered around sort of enhancing the design detail information in Tier 2 to sort of address that letter.

And then we have ECAs and CARs, and there was one change to Chapter 7 I&C related to an ECA. And, actually, that ECA is related to the RAI 62-202. And really all that happened there was we added a forth independent control function and a DPS function for the ICS DPV isolation, so that was a minor change on the I&C side to support that change, engineering change authorization.

And then, as I mentioned, we had some CARs, Corrective Action Requests. The most germane one is the one that we self-identified to add content to Tier 2 that we submitted to the Staff. Okay, next chart.

Okay. Really, the key theme of this paragraph from the letter is really highlighting these key principles of redundancy, independence, determinant data processing, and communication, as well as defense-in-depth and diversity, and the subjective attribute simplicity, and the statement that systems, digital I&C systems can be functionally specified and shown to meet the essential criteria, regardless of what technologies you choose to do your elaboration and implementation. So, we would concur with that. And our goal with the CAR 52743 that we issued to add changes was to really bring together in one portion of Chapter 7.1, and one smaller portion in

7.8 for diversity, 7.1 being "Introductory Material," bring together the design features that do exist to better address the ACRS' concerns.

And I'd like to make a note that we did all that with just a Corrective Action Request. There was no engineering change. There was no fundamental change to our design. We just added further detail. Okay. So, the next chart.

Okay. Here is the theme of the presentation. Independence and determinism were the two themes that we felt most in need of additional material and explanation, so not only did we focus a bit more on these two themes out of the four plus one, but most of this presentation is really going to be about a deep dive into independence and determinism, particularly in one aspect of the safety system, which is SSLC/ESF.

MEMBER BROWN: You're going to talk about it relative to ARC, to the reactor trip system, as well, RTIF?

MR. BUTLER: Yes, RTIF, Reactor Trip and Isolation Function. We have a little bit of material in there on RTIF, yes.

MEMBER BROWN: Okay. Because that was one of my points of interest. They look different, and

I'm going to ask you to explain a little bit of the difference to me, just make sure I understand it --

MR. BUTLER: Sure. Right.

MEMBER BROWN: -- once you get into it. Okay?

MR. BUTLER: Yes, we'll get into it.

MEMBER BROWN: Thank you.

MR. BUTLER: Okay. So, in order to add the additional material in Tier 2, we just wanted to explain briefly how we did that. There are the four key design principles, and we have three diverse platforms on the safety side, so there's RTIF, NMS, there's SSLC/ESF, and there's the independent control platform. So, what we did is for each one of the platforms, we explained how these four design principles are met. Simplicity being more of a subjective attribute, we added a discussion section on that, and then DPS being a RTNSS system, we had a standalone discussion on that. So, that's, essentially, the outline format for how we changed the DCD. And if you go to the next slide.

This in very high-level summary explains the additional sections that were added, and the page count for Tier 2 that they're related to.

MEMBER BROWN: This is in Rev. 8 now.

MR. BUTLER: This is the Rev. 8 in progress that I introduced with, yes. And it was submitted yesterday to the Staff on the letter. So, in overall, there were --

MS. CUBBAGE: I'll send it right now.

MEMBER BROWN: Gimmie a break, why don't you?

(Laughter.)

MEMBER BROWN: I was just wondering how long you all wanted to hold it before you go it out to --

MS. CUBBAGE: Oh, I'll send it right now. I'm just --

MEMBER BROWN: Okay. All right. Thank you.

CHAIRMAN CORRADINI: Amy, I'm sorry. You're going to send what? I'm sorry.

MS. CUBBAGE: The markup pages that GE submitted on the docket yesterday --

CHAIRMAN CORRADINI: Okay, fine. Got it.

MS. CUBBAGE: -- about the Rev. 8 content.

CHAIRMAN CORRADINI: Thank you.

MR. BUTLER: If you would like, there's a binder. Do you want to have this binder for the meeting? It might help.

MEMBER BROWN: You expect me to read all this?

MR. BUTLER: Well, you can thumb through it, as might be appropriate. Some of us might have begun to commit it to memory, so I don't know.

MEMBER BROWN: I can pass lunch, and just do it during lunch. Right?

MR. BUTLER: We're just trying to make sure you don't miss anything.

MEMBER BROWN: No, I appreciate that. Thank you.

MR. BUTLER: Okay. So, next page. Okay. For Tier 1, it was also mentioned in the ACRS' letter that applicant should do a better job identifying design descriptions and features that should be testable, inspectable, so we went ahead and looked through the material that's now, hopefully, better presented in Tier 2, and realized that on some of the key areas that maybe the ACRS is struggling to better understand our design independence and determinism, we would go and add additional ITAACs, both DAC and construction ITAACs, and specifically apply independence and determinism to these three platforms. And, as a result of that, we added a number of additional ITAACS. And that's really the theme here.

Okay?

MEMBER BROWN: Those aren't reflected on this sheet here. So, you're saying in addition to Chapter 7 changes, there are some Tier 1 changes, as well, that go along with these?

MR. BUTLER: Yes. And maybe you'd like to be able to have a copy of that. So --

CHAIRMAN CORRADINI: John, do you want to sit over there?

MEMBER STETKAR: No, that's all right.

MEMBER BROWN: This is too far to the right for him.

CHAIRMAN CORRADINI: Go ahead.

MEMBER STETKAR: It's the evil empire over there.

MR. BUTLER: So, the theme really is independence and determinism. And, as you notice on the upper right, this is Tier 1, so we sort of focus on the key points that were now better presented in Tier 2. For independence and determinism, in our Tier 2, Item 11, in our Tier 1, excuse me, Item 11 is a family of ITAACs that talk about 603 criteria, 5.6 and 6.3, so we added a number of ITAACs there. Determinism is addressed in Item 8, which is new, and Item 17, which we modified by adding content too. And it's these -- this is the outline of the changes that we made in Tier 1. Okay? Next slide.

And here's the count of what was added, and what was the purpose, so we ended up adding 32 DACs and 32 construction ITAACs, for a total of 64. And pretty much, again, they follow this theme of independence and determinism, and the platforms. Now, some of these ITAACs are specific to a platform and a topic, and others for a particular design principle are generic, and apply across all of Table 7, all of Table 15-1, which is where our platforms are presented. All right? So, that's how you combine the two primary tables, Tier 1, 2.2.15-1, and 2.2.15-2 and generate the specific unique ITAACs. That's the count.

MEMBER BROWN: Table 15, you mean Chapter 15?

MR. BUTLER: No, it's Tier 1, and the section is 2.2.15-1 is the table.

MEMBER BROWN: Oh, 2.2.15. Okay.

MR. BUTLER: Yes, sorry.

MEMBER BROWN: No, I've got --

MR. BUTLER: So, 2.2.15-1 is the table which presents the platforms and the specific functional systems that are related to the safety case. That's in the horizontal row. And then in the vertical are all the 603 criteria from Tier 2.

MEMBER BROWN: Okay.

MR. BUTLER: And then the Table 2.2.15-2 is the specific ITAACs, but they're then applied as matrix algebra to the one above, and that's how you generate the unique list of --

MEMBER BROWN: What do you mean by a platform multiplier in that column?

MR. BUTLER: The platform multiplier is how many times this specific ITAAC is applied to RTIF-NMS, or is it applied to SOC, or is it applied to one of the ICPs? So, in that Table 2.2.15-1, the 603 Table, the horizontal rows have letter Rs in them. The R means reference requiring a report, a closure report. So, each one of the ITAACs that are in the 15-2, where there's an R, these tables get applied.

MR. BUTLER: So, there are seven Rs in one line.

MR. BUTLER: There are seven Rs in one line.

MEMBER BROWN: I got it.

MR. BUTLER: So, up until we added the items for 11, those rows were applicable to all platforms. But with independence, we've now presented design features for communication, particularly, which are specific to that implementation, and so to write a good ITAAC, we had to become platform-specific. So, that's why there's a little bit of a jitter, if you will. Okay, next chart, Romeo.

Here's an example for what we added in Tier 1. Okay? So, this is the Item 11A, B, which is the DAC, followed by the construction ITAAC. And this one here is for independence and interactions. And what we're trying to present here in a series of four of these, so there's one of four, two of four, three of four, four of four, is a specific example from the prior table where we've highlighted what is the type of additional material added. Hence, it's blue underlined, So as not to confuse, blue underline means we've added it for Rev. 8 in progress. This is what we submitted yesterday.

DR. WALLIS: That's a very readable slide.

MEMBER BROWN: Well, Mike just pointed out that this is not the Tier 1 thing, this is Tier 2.

MR. BUTLER: These are the change pages. Sorry. I apologize.

MEMBER BROWN: That's fine. Just a real rapid look at this, when I look at one of these design commitments, it talks about intra-divisional input/output, which is within a division. So, from a -- the major independence issue is from division to division, so intra-division, I mean, you've got to be careful that you don't do certain things, also. But the division to division, is there an equivalent?

MR. BUTLER: Yes. So, Romeo, if you -- thank you for being the questioner. This one is on intra-divisional for the VDUs. And if you go to the next one, inter-divisional, so the three of four is the inter-divisional for the SSLC/ESF platform. This is the one where we use a particular implementation of ethernet, so we'll have more discussion that IRA will lead, which will talk --

MEMBER BROWN: Is this the next page? Oh, you went two pages.

MR. BUTLER: Yes, three of four.

MEMBER BROWN: There it is.

MR. BUTLER: So, this is the one that talks about the inter-divisional data communication within safety-related --

MEMBER BROWN: All right. So, you address both areas.

MR. BUTLER: Yes. SSLC/ESF is an interesting one, an interesting platform to discuss with the Staff, because in this case of data communication, there were four themes. There's the intra-divisional for sensors, intra-divisional for the VDUs going to the main control room, or the remote shutdown system, they're intra-divisional. There's inter-divisional, and then there's safety to non-safety. So, the next one, four of four, are a set of very specific criteria related to the safety to non-safety one-way.

MEMBER BROWN: Okay. Now, is there a set of things like this for, I don't mean slides, but ITAACs, and whatever we want to call them, for the RTIF, as well?

MR. BUTLER: Yes.

MEMBER BROWN: Okay.

MR. BUTLER: And that's presented in the table, the Introductory Summary Table, where it's 32 and 32, for a total of 64.

MEMBER BROWN: Okay.

MR. BUTLER: So, these are the new ones added for each platform.

DR. WALLIS: Could you explain what a hash function is?

MR. BUTLER: Ira, you want to jump on that?

MR. POPPEL: A hash function is like a one-way algorithm that, basically, it's like a -- the best way to describe it would be a signature. So, that if the sender writes it, it's a complicated algorithm that the receiver can determine that only the sender --

DR. WALLIS: This is the right person sending it.

MR. POPPEL: Yes.

DR. WALLIS: The right thing is sending it. Okay. Came from the right place.

MR. POPPEL: It's not a corruption thing, it's a signature thing.

DR. WALLIS: Okay. It's a strange name for a signature, though. Some people's signatures look like hash, but --

CHAIRMAN CORRADINI: Well, that would be your doctor.

DR. WALLIS: Okay. Thank you.

MR. POPPEL: Actually, hash function is widely -- I don't want you to think we're designing from Wikipedia, but, for example, you'll certainly find a description of it there. It's a very common name for it.

DR. WALLIS: Thank you very much.

CHAIRMAN CORRADINI: Keep going.

MR. BUTLER: So, the next one is an example of determinism for the new ITAACs. There's two examples here. This one has to do with -- we did note that perhaps we weren't as clear as we should have been in Tier 2 about clearly presenting the fact that for every plant process, there is -- safety-related plant process, there is a timing budget that's determined by the Systems Engineer in Chapter 15, which Wayne leads. And from that plant process timing budget, then any controls on that plant process must complete their complete loop of action, which is sense, command, and execute, or sense, command, and actuate within something less than that plant process control timing budget. So, we explicitly added material in Tier 2 related to the 603 Criteria 4.10 that talks about that, and then we added an ITAAC, which is an ITAAC for all platforms, and all functional systems that says there will be a timing budget, and it will be part of the design basis. And it will insure that the control function and protective action completes in the specified allowable time less than required by the plant process. So, that's what this one is.

It was inferred in Rev. 7 and prior, but it wasn't explicitly stated, so we made it explicit in Chapter 7, Tier 2, and we added this ITAAC into it.

MEMBER BROWN: Okay. Now, in one place, going back to the number where you talk -- and maybe it was the Staff's writeup in the SER, you talked about the determination -- determinism of the processes. While we're operating, you said it was near, because you had to depend on loading of the bus, so you said you had near determinism, which might have been applied to RMUs. I'm not exactly sure where it was. It's just some that's muddled around. Are you going to address program cycle architecture, and its -- forget the RMUs right now, but the stuff that goes directly --

MR. BUTLER: Yes, there's a chart on that.

MEMBER BROWN: Okay.

MR. BUTLER: So, the next one is 17A.2 and 17B.2, the As being the DACs, and the Bs being the construction ITAACs related to inspection, test, and analysis. So, here we address BTP HICB-21, and make specific note that in the safety-related control processors, and application programs, we do not use the methods which are identified, which could be a negative impact to a deterministic behavior. So, the processors that are used in all three platforms, ICP not really have an explicit processor, because it's gate logic, they do not use these specific features, which are not advantageous to insuring deterministic behaviors. So, we made that commitment. Earlier it wasn't clear, so we highlighted it with some change pages in Tier 2, and we've made this new ITAAC, so that it can be assured through design and inspection that we don't do that.

MEMBER BROWN: Okay.

MR. BUTLER: So, there's been, obviously, throughout the process a few changes. This slide is simply a statement of where we are today. The numbers might change a little bit, as all of the resolutions come forward with Rev. 8. And, also, we have ongoing conversations with the construction inspection at Branch, with Patricia Campbell, to make sure that we are all agreeing on which ones are ITAACs and DACs. And this is just something we need to make sure we clarify before everything is finalized, so that we all have the same set of ITAACs. And they have a common unique numbering scheme.

MEMBER BROWN: Based on looking at this one, I'm anticipating with great thrill running up my leg, to coin a phrase, you talk about the features are not used as part of your ITAAC determination. There was no political intent meant by that, just it was a good phrase, that's all. Not used, interrupts in multi-tasking, so I take it that the DCD revision which you make will note or discuss the fact that your program cycles and stuff like that are not interrupt-driven, or if they are, where they are, and why they're not -- and why they don't matter. I'm not saying interrupts aren't useful. In some places they are. This is probably no absolutely interrupt-free prevalent cycle architecture. It's just you don't want them in the main processing.

MR. BUTLER: Right.

MEMBER BROWN: So, I'm anticipating since there's an ITAAC on this, or DAC ITAAC, that's a DAC in that case, that --

MR. BUTLER: Well, A is the DAC, and B is --

MEMBER BROWN: I got -- I even made a note of that, so I won't forget it.

MR. BUTLER: There's a picture coding --

MEMBER BROWN: Okay. So, that — I should expect to see some discussion of that aspect of the --

MR. BUTLER: Yes.

MEMBER BROWN: Okay.

MR. BUTLER: Next one. Okay, so this is sort of a transition to the specific technical material and associated deep dives. And just to orient everybody on the ESBWR architecture, and I won't belabor this, other than to say that it's a very modular and layered level to insure that we meet the 604 Criteria. And when you're at the functional system, and platform level, we've made every effort to make in that area of design and implementation things as simple as they can be, when you're actually implementing at the end of the day an overall digital scheme for a nuclear power plant. But what we've tried to achieve is something that, at the functional level, and the subsystem and system level, that's in a singular type of technology platform, that that work scope is understandable for the engineer, for the implementer, and for the auditor, and, obviously, for the QUIN operator. So, next slide.

So, the first one is on independence, and Ira is going to present the topic on independence, so go to the next one.

MR. POPPEL: Can you go back to the overall one? Okay.

MEMBER BROWN: Let me backtrack for just a second, if I can. I'm trying to -- I want to make you've got the right understanding. For each of the divisions, they have their own dedicated -- I'm talking RTIF right now. They have their own dedicated sensors for each division. You don't share them division to division, but they all feed into a multiplexing system to be fed into their own division processing. Is that correct? For instance, pressure, temperatures, flows, et cetera.

MR. POPPEL: Yes. The multiplexor for Div. 1 handles the Div. 1 sensors, and it only goes to the Div. 1 --

MEMBER BROWN: Right. Okay. My question relative to that is, I almost forgot my point now. Is that addressed relative to the multiplexing function, the timing of that -- in a predictable approach, so that all the data actually gets fed within a certain prescribed time? And if it doesn't, then there's some -- something gets flag to the processor, say I'm not getting the right data, and I don't know what message you use, but is that there to insure that they get everything in every cycle?

MR. BUTLER: Yes.

MEMBER BROWN: And is that discussed any place in --

MR. BUTLER: Yes. In Tier 2, what --

MEMBER BROWN: I don't remember reading it in Rev. 7.

MR. BUTLER: Correct. It was not adequately discussed in Rev. 7 of Tier 2.

MEMBER BROWN: Okay.

MR. BUTLER: So, in looking at Tier 2, Chapter 7 after the letter on August 9th, we realized that we had not done an adequate job presenting that topic, so we wrote a CAR, and we added a significant amount of material to explain through sense, command, and execute through the layers that you go through, including the multiplexor, that there is divisional independence, that there is a timing budget, and that that timing budget will execute in the allowable time, which, obviously, has to be less than what's required for the plant to be safe. So, we took great pains to do that in these 23 pages.

MEMBER BROWN: Okay.

MR. BUTLER: That was the objective.

MEMBER BROWN: Yes. My -- what I'm trying to make sure I understand with all of this is that from sensor input to actuation output, the trip in the -- that there's a predetermined, predictable, repeatable path that is verifiable. And that's what I'm looking -- it looks like you all are going after the attack to show that that is --

MR. BUTLER: Added the description that says that will exist. It will be part of the design bases, and the relevant engineering documents. We will inspect for it as DAC, and we will test to it.

MEMBER BROWN: Okay. Thank you. Sorry to interrupt.

MR. BUTLER: And we did that with no engineering design change. It was just we hadn't adequately described it.

MEMBER BROWN: Well, that's good.

MR. BUTLER: Okay.

MR. POPPEL: This is a good diagram to occasionally refer back to, because you can get lost in exactly where we are in these systems. But overall, on the left side, you can see the four divisions. You can, if you have your glasses on, can see the three platforms in the divisions, the platforms being roughly what you guys would call the reactor trip system, and another one what you would call roughly the ECCS, which is SOC ESF, and the third one is the independent control platforms. And, in general, the whole plant is radial. In other words, the signals that things need, safety and non-safety, come to the processor directly. They do not come through a network. So, we do not use in the safety or non-safety side the network, which I'll put in quotes, to do data transfer. Essentially, our networks are used for monitoring, alarming, et cetera, but if you -- so, the radial thing is the sensors are on the bottom lower left for the safety. They come up through remote multiplexing units. They turn to fiber. They go to the four divisional DCIS rooms in the control building, where roughly the controllers are, and then they go through one-way gateways to the non-safety side. And then those five gray different sized boxes that says GENE network, PIP network, et cetera. Our network is really five individual networks, all of which can run by themselves. So, in other words, first of all, you don't need any of those networks to do anything for safety, and none of those networks can control anything safety. But you can lose any one of them, like our RTNSS network, RTNSS-A and RTNSS-B will continue running. So, it degrades very gracefully, and pretty much everything you see there is redundant in terms of communication paths. There's a few that aren't, and I'll tell you.

On the right side is the non-safety, and I could say pretty much the same thing about it. The RTNSS stuff is separate from what you would call the power generation stuff, and the plant computer stuff. And then, essentially, the main control room, various displays, monitors, recording devices in the upper left plug into those networks. Okay?

So, one of the other things about the design is, if you lost the main control room, the plant controllers continue to operate autonomously. The only thing you need the main control room for is monitoring, and to send operator commands down to them, but if, for example, you stop sending commands for reactor water level, the reactor level controller will control water level at the last known command, et cetera. So, that's pretty much the overview of our system. And most of this discussion is going to concentrate on the lower left, and most of that will concentrate on SSLC/ESF, because that's probably the networks that you will find most interesting.

MEMBER BROWN: Question. You said the sensors enter from the bottom. Right?

MR. POPPEL: Yes.

MEMBER BROWN: On this diagram.

MR. POPPEL: Yes.

MEMBER BROWN: I can't read it, so -- and then I see these things -- those three little units right above in the pink area, those three right there. What are those?

MR. POPPEL: Those are the remote multiplexing units.

MEMBER BROWN: They are the multiplexing units. Okay. And then the processing units are up here in the gray area, the blue, light gray?

MR. POPPEL: Yes.

MEMBER BROWN: And then I see this thing off multiplexing, called low drivers. What do those feed?

MR. POPPEL: For the RPS system, the load drivers are the things that actually interrupt current to the scram solenoids. They are --

MEMBER BROWN: Say that again.

MR. POPPEL: The low drivers are the things that interrupt currents to the scram solenoids. And they are intelligent, which I can describe a little bit about.

MEMBER BROWN: Well, before you get to the intelligent part, they look like they come right off the RMUs, and they don't care about the RTIF, so before the RMUs feed data up to the RTIF, where, presumably, the processing is done.

MR. POPPEL: Well, the load -- okay.

MEMBER BROWN: I'm trying to figure how --

MR. POPPEL: Well, what we should have made clear is an RMU --

MEMBER BROWN: -- two of the four

channels.

MR. POPPEL: An RMU is a two-way device. There's outputs, and those inputs. Okay? So, when a controller makes a decision -- one other thing. Our control processors for almost everything are located in the control building. Almost all the signals of safety interest are located in the reactor building. There's a few in the control building. So, hence, the remote multiplexors. So, basically, outputs occur in the reactor building, and inputs occur from the reactor building. And the generic term for the boxes in the reactor building is remote multiplexor units, whether they house inputs to measure pressure, temperature, or whether they house outputs to drive loads.

MEMBER BROWN: You have separate RMUs for output, or are you using the same RMU to process plant data, that then goes to the RTIF, then it goes back down to the RMU and gets fed out to the scram breaker?

MR. POPPEL: In the case of RTIF, it happens that the boxes are separate, but for the SSLC/ESF, they are mixed. They do inputs and outputs.

MEMBER BROWN: How come there are no load sensors devices in Divisions 3 and 4?

MR. POPPEL: Okay. This has been a subject of a lot of interest in the electrical area, but -- we're sort of out of -- okay. A load driver in the reactor building, if you look at it in a broad block diagram level, you'll see four fibers going into it coming from the four divisions. And the load driver is an intelligent device that when it gets a signal from two out of those four fibers, it will interrupt the current. The current being interrupted is in Division 1, or the Division 1 solenoids on the hydraulic control units.

There's another cabinet, similar arrangement, except there the current being interrupted is in Division 2. And then just like all BWRs, you have to drop out both the Division 1 and the Division 2 scram solenoids to get a scram. So, electricity is in two divisions, logically it's four divisions.

MEMBER BROWN: Okay. That's fine, but why aren't there little wires going over here to the load drivers from Divisions 3 and 4 then?

MR. POPPEL: There are -- well, the right answer to that is it's a simple broad block diagram.

MEMBER BROWN: That's the point.

MR. POPPEL: Okay.

MEMBER BROWN: That's the difficulty of

understanding.

MR. POPPEL: Yes.

MEMBER BROWN: That gave me some difficulty the first time I went through this trying to figure out how anything from 3 and 4 got over to 1. That's why I asked, since you, obviously, knew what you were talking about.

MR. POPPEL: Okay. The --

MR. BUTLER: Was that enough to answer the question?

MEMBER BROWN: I'm not sure.

MEMBER STETKAR: Let me ask. You mentioned something very quickly that it's given you interest among your electrical folks. This means that not all electrical divisions in this design are created equal, because Division 1 -- if I fail power, Divisions 1 and 2, I get a different type of plant response than Division 1 and Division 3, or Division 2 and Division 3. I know this is beyond single failure design space, but I just want to make sure that I understand that it's not a fully symmetric plant.

MR. POPPEL: Yes.

MEMBER STETKAR: There are some other subtleties because of what powers, like the remote shutdown panels, things like that.

MR. POPPEL: Well, this came about in the electrical area because of the batteries.

MEMBER STETKAR: Yes.

MR. POPPEL: Everybody thought that look, Division 1 and 2 are different, and, therefore -- however, if you think about it, the scram solenoids are energized normally, so the division, if you will, is powering the solenoids. Almost every scenario you can think about results in a reactor scram, which means the power goes away.

MEMBER STETKAR: Going to unload this.

MR. POPPEL: So, now all four divisions are pretty much the same, because they dropped off 4,500 watts of scram solenoids.

MEMBER STETKAR: The remote shutdown panels are also just Division 1 and 2. Right?

MR. POPPEL: Yes. But the loads we're talking about there are --

MEMBER STETKAR: Yes. Get back to the other stuff that you were going to do. I just wanted to make sure I understood sort of that level. Thanks.

MR. POPPEL: Okay. And, incidentally, when you say it's beyond design basis, it's beyond design basis squared, because it should never be forgotten that each of our divisions is redundantly powered.

So, in other words, it's possible in tech spec land to talk about losing power for -- losing a division. Okay? It takes a lot more to lose a division in this plant than it does in any other plant.

MEMBER STETKAR: On the other hand, in tech spec land you can have one division out of service indefinitely.

MR. POPPEL: Yes. But we didn't go into the -- one power, half a division's power out, that would drive everybody crazy. You know, you can three and a half divisions running, that would -- that doesn't work. Anyway --

MEMBER STETKAR: Back to I&C.

MR. POPPEL: Back to I&C.

MEMBER STETKAR: I just wanted -- you just happened to give me the lead by saying there's concern for your electrical folks, and I want to make sure that --

MR. POPPEL: Okay. Next one, Romeo.

DR. WALLIS: This is off their subject all together. You show this wide display panel.

MR. POPPEL: Yes.

DR. WALLIS: Is that really a huge screen up there that dwarfs everything else?

MR. POPPEL: The technology for that is

evolving incredibly fast, but, essentially, it could be done with composite amount of LED displays. And nowadays, there are people who are making them almost with the right resolution for LED --

MEMBER STETKAR: I think he's answered a much higher question. The answer is yes, it's like the size of that wall behind you.

MR. POPPEL: Yes.

DR. WALLIS: This is the thing that sort of displays the state of the plant.

MR. POPPEL: Yes. It's a main --

DR. WALLIS: It dwarfs everything else. If you want to see any details, then you've got to look at these little screens down below. Is that --

CHAIRMAN CORRADINI: Or you could focus in. This is -- I mean, the fact that I know this scares me. If you go to a combined cycle natural gas plant now, that's how the CCGTs run. So, it's the same thing.

DR. WALLIS: But it just seems so enormous compared with the other --

MR. POPPEL: Well, it's always --

DR. WALLIS: So, that's the thing they look at really.

MEMBER STETKAR: It's what the operators

normally use --

(Simultaneous speech.)

MR. POPPEL: In ABWR, and our intention is to put everything up there that would be a control parameter for the operator to handle emergencies, and to gain a very quick understanding of the plant status.

DR. WALLIS: That's right. There's an awful lot of information, according -- the picture shows an awful lot of stuff up there.

MR. POPPEL: Yes.

MR. BUTLER: Well, there's a section of the wide display panel which is, essentially, a strip at the very top which is meant to be upon final HFE design and analysis, is meant to be a means by which alarms by system, which the plant engineers and operators are very aligned with, if there's any condition that needs to be interrogated, there will be an annunciator that comes up as a light, and then they'll be able to go into the appropriate monitors in the main console to look at it. So, you won't -- the objective is not to get lost in all the information, but to have one place, which is the top strip, that if there is really something that needs to be interrogated, it'll be annunciated.

DR. WALLIS: And it's all there. All the focus is on that one thing most of the time.

MR. POPPEL: Yes. They don't want the operators to develop tunnel vision looking at two displays. They want them to have a broad overview of the plant status.

DR. WALLIS: I just wonder if they ever look at the other displays.

MR. POPPEL: Although, of course, our plant would never had an alarm. If it did, then they would look down at the other displays.

DR. WALLIS: Look down at the other displays. Okay.

MR. POPPEL: And, of course, you would also operate the systems. That mimic is not an operations thing, so you would call up the display to operate the feedwater system.

DR. WALLIS: You would.

MR. POPPEL: Yes.

DR. WALLIS: Thank you.

MR. POPPEL: Slide 2. Okay. So, now a different view of the same thing. We're talking about independence now, so we're concentrating -- I mean, this slide isn't very profound, except to say our four divisions are electrically separate. There are no conductive paths between divisions. Our four divisions are physically separate, both in the control building, and in the reactor building where it's set up by quadrants. So, in other words, the Division 1 RMU and the Division 1 instrument rack is in whatever quadrant it's in, and then it goes back via its own fiber separate path than the other divisions to the room in the control building that houses the controllers. So, physically and electrically we have the independence that everybody wants. And those boxes that say gateways, not only do we have no conductive paths between divisions, we don't have any conductive paths between divisions and non-divisions. So, we hope to blow off the electrical and the physical, and just get and discuss mostly data isolation. Okay? Which is most people's concern. We did want to get across that we did the other things, too.

Oh, and the other thing I should say is, every one of those divisions is separately and redundantly powered, so no safety powers non-safety, no safety Div. 1 powers anything in Div. 2, et cetera, et cetera, et cetera.

MEMBER BROWN: When you say redundant, you mean if you lose one of the two, then the other one can fully support the operation of that one division?

MR. POPPEL: Yes.

MEMBER BROWN: So, there's no load sharing. I mean, they may share a load when they're in parallel, but effectively drop one, the other one can supply --

MR. POPPEL: Yes. The only difference is --

MEMBER BROWN: You don't have to elaborate, if you don't want to.

MR. POPPEL: Yes, is the answer.

MEMBER BROWN: Yes.

MR. POPPEL: Okay. So, it sounded like you wanted to talk more about RPS, so maybe I should just say one thing about RPS does not have any inter-divisional networks. RPS -- all of the divisional platforms have several communication paths. One communication path is --

MR. BUTLER: There's a chart on that we can talk to.

MR. POPPEL: Okay.

MR. BUTLER: So, I suggest that we just try to get through all the material, just go through the charts. And I assure you that there is one that we can talk to on RTIF. Is that okay?

MR. POPPEL: Okay. All right. So, the

controllers in question are, if you will, not shown here, but they're underneath the bottom row. And the -- what you're looking at for SSLC/ESF is the four divisions. And each of the divisions has four CIMs or communication cards. Okay? And, basically, the communication cards are ports to the various networks.

One of the networks is two out of four, one of the networks is the display units, one of the networks is to non-safety. Those are different networks, different cards, and all redundant. Okay? So, the network operate in -- not only can they take a single failure proof within the network because of the redundancy, for example, you can lose their links to the non-safety, and it has nothing to do with the two out of four, et cetera. So, it's not like there's one box which communicates everything, separate, individual things. And you can see the communication cards talk to, they're called CIMs there, but they are mildly smart switches, ethernet switches, and you can see that they're arranged one, two, three, four in one path, and one, three, two, four in the other path. I'll explain to you why, but --

MEMBER BROWN: I totally lost what you were saying. I apologize.

MR. POPPEL: Okay.

MEMBER BROWN: I mean, I'm --

MR. BUTLER: Why don't we just get to the next slide.

MR. POPPEL: Okay.

MR. BUTLER: We have a series of slides that sort of break it down.

MR. POPPEL: Okay.

MEMBER BROWN: It gets worse. I already looked at those quickly to see if it clarifies. I'm just trying to look at the simple picture here for a minute.

MR. POPPEL: Okay.

MEMBER BROWN: The four lower -- you've got four divisions of four boxes each down at the bottom.

MR. POPPEL: Yes.

MEMBER BROWN: And where are those getting -- this is in the SSLC?

MR. POPPEL: Yes. They're getting their information from the controllers that are not shown there. This just the communication network.

MEMBER BROWN: This is not gateways and stuff going out to the plant.

MR. POPPEL: No.

MEMBER BROWN: This is within --

MR. POPPEL: This is just one network for

SSLC four inter-divisional communication that's dedicated.

MEMBER BROWN: Okay.

MR. POPPEL: That's the only thing this network does.

MEMBER BROWN: Okay. So, these -- the bottom four are just feeding data into the two networks that are above it.

MR. POPPEL: Yes. And taking data from it.

MEMBER BROWN: Yes. Well, there's no -- okay. I see the bidirectional arrows. The lower network shows a path except it doesn't always go -- I guess it's always bidirectional. Is this a dual fiber --

MR. POPPEL: I will show you in the next slide, but yes.

MEMBER BROWN: Okay. The upper network doesn't look like it operates the same way. It's one and three, and two and four are connected.

MR. POPPEL: Yes. And we will explain that, also.

MEMBER BROWN: All right.

MR. POPPEL: Okay. Maybe the next slide will make it clearer.

MEMBER BROWN: Simplicity was the thought process.

MR. BUTLER: It is when you get to the layer that works.

MEMBER BROWN: Okay.

MR. POPPEL: First of all, if Romeo flips between this slide and the next one just back and forth, you can see the two networks, and you can see the two different communication cards. Okay? That's just meant to show that there are two cards, two networks, two sets of switches. They're completely redundant to one another, and they're completely independent of one another, so that, in other words, we can take N minus 2 failures in the system and still get the information we need to get a two out of four decision for ECCS initiation, and isolation decisions.

The way those switches work is, assume like Division 1 says I have some information. I have to write a message to Division 2 to say my trip status. I am in trip. And the reason it's sending that to Division 2, as well as all the other divisions are sending the Division 2, is so that Division 2 can make a decision two out of four to do a trip. So, the networks are common, so these messages are floating around on the network together. Okay? So, periodically, there's a Division 1 message to Division

2, periodically, to Division 3, to Division 4, and same thing is happening with Division 2, Division 3, and Division 4. So, the data path is the communication card takes the information, puts it onto the network which is the switch, and the switch's rules are let's send the data around through the other switches, and you can see it's a loop, and it comes back to the original switch. So, if it comes back, that means the network is in tact. So, the response of the switch is to say all is well, and take the message off the network. That always happens.

If, in fact, the message doesn't come back, all is not well. Something has happened to interfere with the message. So, the switch's response to that is to send the data around in the other direction. Okay? So, for example, if you break the top network between red and green, so red tries to send -- Div. 1 tries to send to Div. 2, and the link is broken, so it sends the message around the other way to Div. 2. So, this is to demonstrate that if you actually have a fiber break, the data still gets to all three divisions, all three other divisions. And this is one of the redundant networks, so the other division is in tact, and still working, but the intent is to show that it's self-healing. Okay? If it goes down, and the other thing that happens is, if the switch reverses direction, a set of alarm contacts close to let the operator know that there has been a communication failure. Okay? So, that's how the fiber breaks are handled.

The next thing is, those switches, and those communication cards, and the division, in general, are actively powered. So, if you want to send a message from Div. 1 to Div. 3, it goes through the Div. 2 switch. Okay? So, what happens if the Div. 2 has gone bye-bye? It's broken, or has no power.

Well, first of all, the same rules hold, it goes around in the other direction. Okay? So, for individual divisional failures, we are completely N minus one. Okay? But we have told you we're an N minus two plant. So, for example, if I take out on this drawing Division 4, and Division 2, then you could properly tell me that the data never gets to Division 3. And, therefore, I will not be able to make a two out of four decision.

Now, you go to the next network, and you can see if I had taken out -- I forgot which ones --

MR. BUTLER: Two and four.

MR. POPPEL: Two and four, that now I can get data to the division that previous was isolated. So, in other words, I can handle two fiber breaks, two divisional failures, and still get the data. Okay? So, we believe this is properly under the independence section, so that somebody would say are you -- is data getting around dependent on other divisions? And the answer is, we are N minus two proof against that. Okay? So, there's that. Next slide.

MEMBER BROWN: So, effectively, all you do is reverse the positions to Division 3 --

MR. POPPEL: Yes, that's why they went through different paths.

MEMBER BROWN: -- and 4, and their location --

MR. BUTLER: Yes, the topology on the ring for the nodes is different, so that you can be assured that the message will always go through.

MEMBER BROWN: Okay.

MR. POPPEL: Okay. This is what's actually going on in the individual divisional processors and communication cards. Okay? So, first of all, what you guys would call a controller, main application modular processor, is the top box. Okay? And the architecture is such that we have an application controller on the far left. The application controller is that controller that's actually running the logic for --

MEMBER BROWN: Before you go to that, if I'm looking at your big diagram, this is the three lines, RTIF-NMS, and SSLC, it's the box that's labeled SSLC/ESF.

MR. POPPEL: Yes. Correct.

MEMBER BROWN: Okay.

CHAIRMAN CORRADINI: So, you had your correct. So, the Committee was all given, essentially, the response that now updates the information they had just told us about at the beginning of the presentation. So, we have what they've given to Staff. Thank you. Go ahead.

MR. POPPEL: So, the application processor is the one Mr. Brown is so interested in, in terms of its determinancy, and all the good design rules, et cetera. That application processor is programmed, and then the programming is not changeable unless you have access to a bunch of equipment, and key locks, and door locks, and access that is not available to the average person. That application runs continuously, and uninterruptedly, and it has -- that application processor has its very own communication processor. And you can see the shared memory between them. So, in other words, that's the way we say hey, when we have data for you, we are not going to interrupt you. We are just going to put communications data into the shared memory, and then the application process will access it, so it has no -- memory location 3 is reactor trip -- level trip status from Div. 2. No idea how it got there, but it just accesses it at the cycle rate of the processor to use in its calculations. So, the shared memory and separate communication processor concept is one of the things that supports the lack of interrupts on the main application processor.

Now, you've also heard us say that each of our divisions for SSLC/ESF is triply redundant within the division. Okay? So, there are three of these purple boxes per division. Okay? And the reason for this is because our SSLC depressurizes the reactor, we don't want to do that inadvertently. That's why we have the triple redundancy to avoid that. Okay?

So, in the background of all of this, there's a lot of two out of three voting going on, which we're not going to describe, but each of the processors gets the data in the way that I'm about to describe to you.

So, the blue line --

MEMBER BROWN: You said purple. Am I color blind, or is that -- which I may be.

MR. POPPEL: That is red.

MEMBER BROWN: Slightly red, more like --

MEMBER STETKAR: It's the upper rectangle.

CHAIRMAN CORRADINI: It's rose.

MEMBER STETKAR: The top one.

MEMBER BROWN: Rose, that's fine.

DR. WALLIS: It's a different color on the handout, too.

MEMBER BROWN: I just wanted to make sure -- I didn't think I was missing anything here, or that I'm going color blind. I need to see the doctor again.

MR. POPPEL: The blue

MEMBER BROWN: Let me --

MR. POPPEL: Oh, I'm sorry.

MEMBER BROWN: I want to clarify something. I understand your box. I understand what you're talking about here. I'm going to look at the little controller application processor A. And you've got all of your application code is in there.

MR. POPPEL: Yes.

MEMBER BROWN: I presume it's in PROM?

MR. POPPEL: No, this is programmable.

MEMBER BROWN: That's what I said.

MR. POPPEL: Yes.

MEMBER BROWN: It's programmable read on the memory, probably e-squared PROM, I guess, or something, whatever, so you can change it outside within the controls that you have.

MR. POPPEL: Yes.

MEMBER BROWN: I understand that part. So, that if you had, I'll just pick a number, okay, ten applications, functions that you needed to process, ten little subroutines that it cycles through, starts Subroutine A, finishes Subroutine A with whatever data has come via the shared memory, goes to B, C, D, E, right on up until it's through number ten. When it finishes, it comes back, starts over at A, and it doesn't stop anywhere in-between. It doesn't stop A, to start B, stop A to start --

MR. POPPEL: No.

MEMBER BROWN: Based on some priority assignment or anything like that. It's a straight main -- what I kind of call a main operating loop --

MR. POPPEL: Yes.

MEMBER BROWN: -- run, where you take -- I'm just saying in my words, you take data that's in a data bus or data buffers, you read it, you use it as you go through, and that's it.

MR. POPPEL: Yes.

MEMBER BROWN: Okay.

MR. POPPEL: The only thing I would add to that is, it starts to loop again after checking in with the watchdog timer.

MEMBER BROWN: Yes. And it tells the watchdog timer after all of them are done, it says don't tell the system that I'm broke.

MR. POPPEL: Yes.

MEMBER BROWN: Okay.

MR. POPPEL: This portion was already in Rev. 7.

MEMBER BROWN: Not clear, but that's okay. It's tough for me, okay? Give me a break.

MR. POPPEL: So, the blue/middle, the T-shaped box is an internal triply redundant communication bus to support the triply redundant control application processors. And that bus goes to the two communication cards that you'd seen on the previous slide. Okay? So, the orange and the yellowish --

CHAIRMAN CORRADINI: Just watch the pointer.

MR. POPPEL: Yes.

MEMBER BROWN: The other one is taupe.

MR. POPPEL: Yes.

MEMBER BROWN: I have no idea, that's --

MR. POPPEL: Those represent -- they're the same physical type cards, but they're two physically separate cards. Okay? So, you can see that there is a shared memory in the communication processors of the main processor, and a shared memory read and write in the communication card. Okay? So, for example, as you'll see later, if you disable read and write, you can control information flow, but the intention is that the communication card has its own processor, and what that processor does for a living is mainly authentication, which we'll describe. So, as you go horizontally, and then down to the white boxes, you can see the connections to the two networks. Excuse me. The left one is one network, the other one is the other network. The cards have two ports on them, so one is the VDU network, and one is the two out of four network. They're kept completely independently. Okay? And the reason we show that is because they're safety, they have no connection to non-safety.

So, essentially, data comes -- the buffer is where ethernet data are stored both when you write to the network, and when you read from the network.

So, if we investigate data coming in, so data comes in from the network. It's completely asynchronous to the main processor, and it's completely asynchronous to the communication card, because other divisions are sending it, and other divisions are not time synchronized in any way with this division, except that they're all running at approximately say 10 times a second. Okay?

So, data comes in. The communication processor looks at it. We'll describe some of the authentication, and decides whether or not it's good data. And then puts it onto the shared memory. If the -- well, that's enough to say for this one. Let's go to the next slide.

MEMBER BROWN: Before you do that, this is one -- I'm trying to -- this is the TRICON stuff. Right? And that's the triply redundant, so this in each division, if I understand what I read before, there are three of these pink modules, CPU processing units per division.

MR. POPPEL: Yes.

MEMBER BROWN: Now, each division, obviously, has to get some voting information from the other divisions in order to make a two out of four determination. They each also have three, let me call them A, B, and C. In terms of the intra-divisional -- I may be ahead, but let me ask the question, then you can tell me you're going to elaborate later, but I've got to get it in my head. In order to do the voting in each of the processors in one division, does Division 2's A feed Division 1's A, and only A, or does it also feed A, B, and C?

MR. POPPEL: What happens is the communication card is just like an IO device. So, the communication -- it's a bus, so each communication card has access to all three of the processors. So, the three processors saying here's my trip decision, so each communication card does its own internal two out of three. And it says this is the information I'm going to put on the bus. And, of course, if the three don't agree, you get an alarm, but the communication card does that. Each communication card makes that two out of three decision from the three processors.

So, in other words, there's a Communication Card A, Div. 1 trip status put out, and there's a Communication Card B, Div. 1 trip status put out, but you don't put out Div. 1 main processor A, Div. 1 main processor B, Div. 1 main processor C trip status.

MEMBER BROWN: Go to your pink thing, go to the next slide, that one. It says "Main application module A, B and C not shown." So, I presume those are the other two processors.

MR. POPPEL: Yes.

MEMBER BROWN: And it says, "Communication Bus A, B, and C not shown." Where do they vote between those three? You're telling me there's another -- okay, no. Let me phrase that differently. Each of these three units comes up and say gets a trip. They each communicate that trip to their -- to safety communications cards.

MR. POPPEL: Yes.

MEMBER BROWN: All of them go to the buffer.

MR. POPPEL: No.

MEMBER BROWN: Well, within their own communication card they have a buffer.

MR. POPPEL: Yes, but what happens is, you can see -- what's shown there is the connection to the communication bus of main processor A. You can also see four other empty boxes not showing the communication bus --

MEMBER BROWN: Okay. So, this is -- where is the voting done in this brown box?

MR. POPPEL: Done in the communication

processor.

MEMBER BROWN: Okay. So, you do get the stuff from B and C via these other shared memory units.

MR. POPPEL: Yes.

MEMBER BROWN: And the voting is done down here, so that'll pick up a two out of three in this division.

MR. POPPEL: Yes.

MEMBER BROWN: And then that division trip is sent to the other voting logic.

MR. POPPEL: In the other divisions, yes.

MEMBER BROWN: Okay. How does -- that's not shown on here. Right?

MR. POPPEL: Not yet, but the connection is having --

MEMBER BROWN: Put it on the ethernet switch. It goes to the ethernet switch.

MR. POPPEL: Yes. It goes from the communication card to that switch.

MEMBER BROWN: Okay. So, that puts one trip signal on that switch for that channel, that division.

MR. POPPEL: Yes.

MEMBER BROWN: So, now where does it go

after that? It goes back to the -- it comes back -- it goes to Division B or 2. Right?

MR. POPPEL: So, if you remember the loop, every division has two communication cards, and one of the communication cards is for Network One, one is for Network Two. Two out of four Network One, two out of four Network Two. Okay? So, that Div. 1 trip decision is set out to Network One through its communication card and its switch, and Div. 1 trip status is set out to Network Two through a separate communication card and separate switch. So, it's now circulating on the network following the switch rules which say send it around, and if I don't get it back, that's all that business of reversing direction, picking up alarms, et cetera. But what's happening is, so a Div. 1 message to Div. 3, for example, will pass through the Div. 2 switch. The Div. 2 switch isn't that smart, it'll send it to — every division sees all the messages. This is where the authentication comes in. Okay?

So, the switches don't have any intelligence, other than what I described to you about reverse --

MEMBER BROWN: Not voting.

MR. POPPEL: No. They're not voting at

all.

MEMBER BROWN: Where is the voting done?

MR. POPPEL: Okay.

MR. BUTLER: That's why I said keep going. Ira, just --

MR. POPPEL: Okay, but let's go back to the -- okay. We describe how it got out, now let's describe how it gets in. Okay? So, the Div. 1 -- if this is Div. 1, Div. 2, 3 and 4 messages are circulating around on the two networks. Okay? So, the communication card sees it, it gets pulls into the buffer, and it goes to the communication processor. So, the communication processor is now making a decision, is this a good message? One of the things about that is, is it addressed to me, as opposed to one of the other divisions. Okay? But I'll describe authentication in a second. But, basically, it goes into the communication processor in two cards, two networks, so each communication processor says is this a good message? And I'm going to put it in the shared memory so that it can go on the communication bus to the communication processor on the main processor card, control application processors, where it gets taken in and used for the logic.

MEMBER BROWN: Where is the logic? That's still --

MR. POPPEL: The logic is in the --

MEMBER BROWN: Processor A.

MR. POPPEL: Yes. It's in the left box. All the logic for the division is in the three controller application processors associated with that division. So, all of this scheme that you see here is, basically, a way of getting that data into the control application processor. So, in the end, the control application processor, this is what you'll see in the next slide, but in the end, the control application processor has trip statuses from four divisions, its own internal, and then the other three, and it has that times two, because it gets it from each communication card. So, in other words, I have a Network One trip status from Div. 2, I have a Network Two trip status from Div. 2. And now let's go to the next slide.

MEMBER BROWN: No, not yet.

MR. POPPEL: Oh, I'm sorry.

MEMBER BROWN: So, if I get a -- you said these are not smart switches, and you haven't talked about authentication yet, which is of interest to talk about, because, effectively, you're saying to me that a piece -- let's assume a piece of corrupt data got through whatever it is, kind of like when you're playing with your PC or your laptop, or your desktop at home, and all of a sudden your mouse pointer doesn't move, so everything stops and your only choice is to reboot. So, something stopped the microprocessor from operating. And so I'm taking any one division's trip unit, trip signals being circulated, and they're being fed to everybody. And if there's a piece -- and every one sees every piece of data.

MR. POPPEL: Yes.

MEMBER BROWN: So, that means if the corrupt piece of information got to the processor and would lock up -- wanted to lock all of them --

MR. POPPEL: Assume that --

MEMBER BROWN: Even if they're operating asynchronously, I'm making that assumption, it's like assuming --

MR. POPPEL: Assuming that a corrupt data could interrupt the processor, and assuming it go to authentication, you're correct.

MEMBER BROWN: I understand that. So, it would lock up every one of them.

MR. POPPEL: Yes.

MEMBER BROWN: And that, in my own mind, is a point of weakness, if you're depending on authentication modes for insuring that all that data is always correct, and will always be detected. I mean, fundamentally, you've got a niche. There's a little -- no, a chink, excuse me, in the armor, in that you have to do -- you're potentially sharing corrupt data from division voting logic, to division voting logic, to division voting logic, and you can lock them -- you could lock them up. And you're depending upon authentication to insure that that doesn't happen in some way, shape, or form.

MR. POPPEL: Even though this is a network, what you said is, essentially, no different for the point-to-point communication for the reactor trip system.

MEMBER BROWN: Well, that's another problem.

MR. POPPEL: Yes. But, I mean, the authentication is easier, because it's point-to-point, so you assume that if it was set up right, that it would --

MEMBER BROWN: I haven't gotten to ask you about the trip logic unit switch. What you're telling me is I'm going to see the same thing --

MR. BUTLER: But there's always a chink in the armor, because they'll all use some form of authentication.

MEMBER BROWN: If you design the system such that you don't have a processor doing your voting, and you send nothing but analog data, you can isolate it, and you don't have to worry about one piece of trip logic unit corrupting, or stopping a three, two of four analog voting unit.

CHAIRMAN CORRADINI: So, couldn't a relay stick analog?

MEMBER BROWN: It's okay if a relay sticks. You get one set of contacts, but it doesn't corrupt the other three relays. It can't. That's why they have electrical isolation and contact isolation. So, I'm not -- all I'm pointing out is that any time you use microprocessors as voting units, and you have them all doing -- you have them all getting all the data, that's why I asked the question about do you just go to A to A, B to B, C to C, and each of those is kept separate, and they voted separately, then you could argue that hey, I'm not mixing things; therefore, I can't have one corrupt data from one processor contaminating all the voting logic in all the processors, and not have to depend on authentication. Authentication doesn't always work theoretically.

MR. POPPEL: You're right; however, it works --

MEMBER BROWN: Most of the time.

MR. POPPEL: Yes.

MEMBER BROWN: Well, most of the time is very long.

MR. POPPEL: I agree.

MEMBER BROWN: I'm just saying it's most of the time.

MR. POPPEL: Okay.

MEMBER BROWN: So, architecturally, you've made -- a good discussion. I appreciate this. You've made it very, very clear, but, I mean, architecturally, the system is not -- I call it not architecturally independent. You have to depend on something else, another belt of armor, in order to -- and it's software-related, an authentication methodology that will always insure that you don't have a corrupt set of data that can lock everything up.

MR. POPPEL: There's a difference between corruption and locking everything up. Okay? The application processor is instructed to look by its own program, which isn't changeable in normal operation, look to this memory location. Okay? That's the only place it looks. Okay? And there's no question that the data, however unlikely, in that memory location could be corrupt. But it's hard to understand how that will stop the processor from continuing its program work.

CHAIRMAN CORRADINI: Can I ask a question, since I don't understand half of what you've been asking, are you trying to say that there's something goofy, there's a goofy piece of information in the central box, and that goofy piece of information is taken in the voting, and that stops the voting? And everything comes to a grinding halt?

MEMBER BROWN: Yes.

CHAIRMAN CORRADINI: Okay.

MEMBER BROWN: Bad information, corrupt information can lock up microprocessors. Does it all the time. That's what happens when your -- that's why you go to -- that's why you turn it off, and turn it back on.

CHAIRMAN CORRADINI: That's a PC, it never happens to me.

MEMBER BROWN: Well, that's because you're an Apple, right?

CHAIRMAN CORRADINI: You betcha.

MEMBER BROWN: With a stem. And I'm not

saying -- there may be other pieces of armor, architecturally, that provide a backstop to this, and maybe the watchdog timer is depending on how they operate, may be a way of overcoming this particular chink. And I understand your point, but to say it can't happen, while you can really say is, it's unlikely that it will happen.

MR. POPPEL: We will try to be cautious in that direction in the future, for unlikely.

MEMBER BROWN: But you've got what you've got right now.

MR. POPPEL: However, unlike other plants, for example -- let's do two things. Let's assume what you say just happened, okay? Unlike other plants, we have DPS, didn't happen there.

MEMBER BROWN: You're depending on the diverse protection system.

MR. POPPEL: We're depending on the diverse protection system after a chain of events that is borderline incredible.

MEMBER BROWN: One event.

MR. POPPEL: No, not one event.

MEMBER BROWN: Oh, yes, a corrupt set of data that stops them all. It's a single failure.

MR. POPPEL: Okay. I have -- yes. The

other thing is, having "stopped that," is the vast majority -- the ECCS isn't controlling anything in terms of reactor operation. So, for example, what -- you've heard us mention the tech spec monitor. We're not going to go into in great detail --

MEMBER BROWN: But what you said, it applies to the RTIF, as well.

MR. POPPEL: Yes. But --

MR. BUTLER: Your point is a generic point.

MR. POPPEL: Yes, it's a generic point.

MR. BUTLER: Yes, so that's why we can move on, Ira.

MR. POPPEL: But I just want to say one other thing. That whatever else is true, it can't happen silently, because one of the things that's going on, for example, is the ECCS processors through the N-DCIS data link, are sending out, for example, a square away to the tech spec monitor. So, your failure would have to be it locks up the processors, stops them from operating, and yet continues to send the square away. I will now say that that's incredible squared. So, in other words, there is no question that the operator will know that these processors have locked up in the unlikely event --

MEMBER BROWN: But you have to assume the failure occurs when I'm having some other casualty, and it doesn't matter whether he knows, or not.

MR. POPPEL: The idea --

MEMBER BROWN: The whole intent of the single failure approach to doing business is you can have a single failure, and not stop the system from operating. I'm not saying there's not something else in here that's okay. I'm just saying this -- depending upon an authentication like that, which can mess up, they are not impervious.

CHAIRMAN CORRADINI: So, can I say in simpler lingo for me. What you're saying, it's not 100 percent -- there's not a zero chance of failure.

MEMBER BROWN: There's not single -- this, architecturally, it is not single failure proof, architecturally.

MEMBER STETKAR: For certain types of failure.

MEMBER BROWN: For certain --

MEMBER STETKAR: For certain failure modes.

MEMBER BROWN: For certain failure modes. And all I did was -- all I'm trying to --

MEMBER STETKAR: I think it's important to --

MEMBER BROWN: Yes. No, it's very

important. There's a lot of other failure modes, is totally satisfactory. It's just the particular circumstance of trading data, trip data and voting in microprocessors results in fundamental -- unless you do the architecture properly, results in it. I don't want to say this is not -- I'm just saying do it in a certain way, you run into this potential problem of having something lock up those voting logic units, all of them.

CHAIRMAN CORRADINI: So, just for my understanding, again. His response to you for reactor trip would make it even smaller there, but this whole method of control is everywhere, so if I go away --

MEMBER BROWN: This is very generic.

CHAIRMAN CORRADINI: I understand, but just let me ask you before you answer. So, before I go -- if I go away from reactor trip, I don't have the backup system. I have the system as described here for other things, depressurization, I don't know, but that's a good one. They want to depressurize the plant. It would go through the same sort of voting logic, et cetera.

MR. POPPEL: Yes.

CHAIRMAN CORRADINI: Okay. Fine. All right. Thanks.

MR. POPPEL: Okay. The next sheet is, we're going to touch on the authentication process. Okay? But what you're looking at is a truth table that's being run by the control application processor. And the truth table has to deal with I'm getting an authentic message from Network One, or not. And I am getting a trip message from Network One, or not. And same thing in Network Two. And this is for a single divisional message coming in, so there'll be three truth tables like this for each of the divisional messages coming in. So, basically, what happens, since this is not a failsafe system, if the message isn't authenticated, it doesn't trip. If one of the divisions is authenticated, then it accepts the data as valid, trip or not trip.

MEMBER ARMIJO: Ira, your note says it does some sort of a corruption check.

MR. POPPEL: Yes.

MEMBER ARMIJO: Now, Charlie made the point that corrupt data can get through it.

MEMBER BROWN: Well, this is CRC check. That's --

MEMBER ARMIJO: I just don't know what -- you know, I imagine there's all kinds of corruption, and the question is, is there -- this is a very narrow corruption check, so why --

MEMBER BROWN: It's a data transmission check. All it does is say if I've got corrupt data in, and I calculate the CRC based on that corrupt data, and it receives that corrupt data on the other end, it looks at the CRC at the other end, computes it separate. They got a match, if they don't, it rejects the data. All that does is say the bad data started out bad, and it ends up, and I'll pass it on, it checks out fine, it goes on to the thing. That's CRC, it's very effective to make sure data doesn't get corrupted in transmission.

MEMBER ARMIJO: But if it started out --

MEMBER BROWN: If it started out bad, and you assigned a CRC based on the bad data, then it's going to get to the other and say okay, that data is just fine, and go on in. So, that's the difficulty. It doesn't mean it's not useful, but --

CHAIRMAN CORRADINI: Ira, did you want to say something?

MR. POPPEL: Yes. Authentication is not just corruption, so imagine you have a message that says -- my message is one or zero --

MR. BUTLER: Ira, just a second. If you look at the bottom of the chart, we'll try and explain some of the techniques to mitigate Charlie Brown's concern. Okay?

MEMBER ARMIJO: Yes. That was the root of my question.

(Simultaneous speech.)

MR. BUTLER: It's more than just corruption preventer.

MEMBER ARMIJO: That's what I was --

MR. BUTLER: Yes, so what we're trying to explain here to the best of our ability is that it's not just one thing that would allow the corruption Charlie's concerned about to get through the triply redundant processors per division. Rather, there is a defense-in-depth layered approach here that we're trying to explain in the bottom of this chart. It doesn't eliminate it 100 percent, but what it does is it dramatically mitigates it to a nearly highly unlikely situation.

MR. POPPEL: The authentication process is probably two orders of magnitude larger than the data being sent. The data is one or zero, trip, no trip. So, the first thing that happens in the communication card is it says I'm going to put my sending address on it, so it has the address of Div. 1, won't be saying Div. 1, it'll be a numerical address and saying I have a message for Div. 2. So, it has a sending address and a receiving address. Okay? That's how the cards know who the data is for.

In addition, it has a sequence number. So, the sequence number is Div. 1 sends a message to Div. 2. Okay? Let's say the sequence number is one. Okay? Div. 2 gets it, and Div. 2 acknowledges back. Okay? If Div. 1 gets an acknowledgment back, it changes the sequence number to two, and the receiving division changes its number to two. So, in other words, the next message that's sent better have a sequence number of two, or it won't be authentic from that division.

DR. WALLIS: Much more complicated than having a wire that connects A to B.

MR. POPPEL: Yes.

DR. WALLIS: Just go directly. You don't have to ask where it came from, or where it's going, or who sent it.

MR. POPPEL: Yes. So, the -- and, incidentally, these messages are going on at the cyclic rate of the processors, which is ten times a second. So, the idea of somebody pulling the fiber and reconnecting it fast enough, and spoofing the sequence number is unlikely. Okay? So, next comes the hash function, which is a -- you know how like with your computer you have pretty good privacy.

MR. BUTLER: It's a signature.

MR. POPPEL: It's a signature. It basically says I'm adding my Div. 1 hash function on to this message so that something downstream can determine that. It's not just Div. 1 because of the sending address, it's Div. 1 because the hash function can be decoded by Div. 2, and knows it's from Div. 1. And then the cyclic redundancy check, which is, basically, let's add up all of these bits, ones and zeroes that we just laid on top of the message. Okay? Divide them in this case by 64, get a remainder, and put the remainder into the message. So, the message gets received, and the remainder is there, the receiving processor calculates what -- its own cyclic redundancy.

DR. WALLIS: You think of discussions between people were like this.

MR. POPPEL: So, basically, it's not impossible, but it's highly unlikely, but the net result of all of this is the communication card says it's a good message, and I'm going to put that one or zero trip into the shared memory of the communication card, which then goes to the communication processor all the way back to the application. Okay? So, authentication is a very complicated process, but it does -- it goes a long way to assure that it's going on.

MEMBER ARMIJO: But it doesn't check for the type of corruption that Charlie is talking about.

MR. POPPEL: No, if the sending division -- but remember, what we're sending is a one or a zero, so, in other words, we're not expecting some huge complicated message. What we're sending is, we want to see a one or a zero in this shared memory location of the application processor. That's the only place it's told to look.

DR. WALLIS: I want to tell you, all your message here are not authentic, because there's no page number on the slide. So, I cannot make notes on different slide numbers in my notes.

MR. POPPEL: Okay.

DR. WALLIS: I was disappointed. You have to number your slides. It really helps us very much.

MR. BUTLER: Okay, point taken. We'll take this as an opportunity to ask for permission to resubmit with various things that we capture, page numbering might be one of them.

MEMBER ARMIJO: I really want to get to

this thing. If it is just simply a zero or one, why is Charlie concerned that this --

MEMBER BROWN: Because it doesn't eliminate --

MEMBER ARMIJO: How can a zero or a one --

MEMBER BROWN: You have to postulate because you're sending digital data from Point A to Point B, that you could be in a situation, regardless of how you get there, that the data is not going to be what you want. So, it's a -- and if you ask anybody that goes and does it, they'll tell you no, we can't guarantee, but we're pretty sure it's going to be okay. That's all.

MR. BUTLER: So, you're right. You're right, and the techniques that we're trying to present here are those techniques which dramatically mitigate your concern, so that there's a very, very high probability that the message that gets through for trip status, bypass status is authentic, and is actionable for the safety of the plant. That's the technique, and we're doing it digitally, and that's the way it is.

MEMBER BROWN: I got it.

CHAIRMAN CORRADINI: I'm doing a time check. Are we like on track here?

MR. BUTLER: Sure. We can forward at a higher rate, hopefully.

CHAIRMAN CORRADINI: So --

MS. CUBBAGE: But I will say it's very important that we bring these issues to resolution today, so take whatever time is necessary for that to happen.

MEMBER BROWN: We will proceed on. I mean, this is fine.

CHAIRMAN CORRADINI: Okay. Let's go.

MR. POPPEL: So, now you've gone through that truth table authentication for three divisions in the receiving processor, and, of course, it knows its own internal status for trip. And now you see the messages combined in the two out of four logic with the bypass status. So, each of the three control processors is doing what you see in the yellow upper box, which is fairly straightforward two out of four stuff you've seen all over the place.

In addition, the bottom box shows that if the data are different on Networks One and Two, and authentic, you get a data alarm. If you have an authentication problem, it shows up as a communication alarm. Okay? And remember these are all -- the control application processor is different from its own communication processor, which is different from the communication processor in the card. Okay? So, that -- and all of these cards are expecting to talk to one another. So, for example -- again, I'll go back to, it's very hard to have this problem happen silently. You'll get alarms all over the place.

Okay. The reason we discussed this under independence is because we have several networks, but the two out of four network is one of the -- because it's between four divisions challenges independence, and there's another network which is to say communicating to non-safety, which also challenges independence. Okay? There's networks inside the division, but they just show up as single divisional failure-type things. These are the ones that challenge independence.

So, now if you look at this slide, and the one next to it, go to the I Chart flipping back and forth, you can see we have redundant separate networks. So, in other words, we're now on a different communication card, and on a different network than is doing the two out of four. So, none of this data that we're seeing here shows up on the two out of four network.

MEMBER BROWN: Where is this on your big

diagram?

MR. POPPEL: Okay.

MEMBER BROWN: Which network is this?

MR. POPPEL: That's the one that goes to the gateway, the vertical line up to the gateway from -- yes. From the SSLC/ESF. So, basically, what we're doing is we're -- the goal of this is to try and make this network one-way, and because we want to insure the statement that no non-safety can control safety. And, in fact, we want to make it such that the existence, or anything on this network will have nothing whatever to do with the safety function of SSLC/ESF. So, this is a convenience network for alarming, showing things on the non-safety displays, et cetera, et cetera, but not to control. Okay?

MEMBER BROWN: So, if it's one-way, why did you make the statement at the beginning that it challenges the independence of the SSLC/ESF? Is that because it's not one-way?

MR. POPPEL: Yes. Because you've taught me never to say never. But let me explain it, and see if I can get the point across. Okay? You'll see in a second. But the important thing is that -- I just want to get across it's a separate network, it's redundant, and it does this function, and doesn't do the other functions. Okay?

So, now we have the familiar main processor card times three in the upper box. We have the familiar communication network, and now we're talking to two different communication cards, different ones than the ones that were on the two out of four. But you can see they look exactly the same. Okay? So, this is what happens in the card, the communication card is disableable by which we're saying that you can see there's an X through the right shared memory. So, in other words, what we're saying is for data on this network, the communication card is not capable of writing back to the application processor. That's program in. Okay? I want to talk a little bit more about that in a second.

MEMBER BROWN: Yes, that's -- my question is, you say it's programmed in. So, in other words, you've sent a bit in to say disable that line.

MR. POPPEL: Yes.

MEMBER BROWN: Or do you hard bus that line so that it cannot be programmed digitally?

MR. POPPEL: No.

MEMBER BROWN: So, in fact, you still have a path of failure then.

MR. POPPEL: Yes, but as --

MEMBER BROWN: If that digital signal somehow gets flips --

MR. POPPEL: Silently, of course.

MEMBER BROWN: It probably is silent. Okay?

MR. POPPEL: It probably isn't.

MEMBER BROWN: Okay. Now, you have the capability of having information transmitted back the other way through that particular port.

MR. POPPEL: Yes. But there's more to say about that.

MEMBER BROWN: Yes, but why didn't you just lock it down? That's what I used to do? We used to tie them to ground so they couldn't do that.

MR. POPPEL: It's the technology we have.

MR. BUTLER: That's a technique, but we're using a different technique.

MEMBER BROWN: I know you are.

MR. BUTLER: Okay. There's two different techniques. This technique, which we'll elaborate a little bit more on, will achieve the objective.

DR. WALLIS: I think you ought to tell us the modes of failure instead of having Charlie have to tell us.

MR. POPPEL: Okay.

MR. BUTLER: We're trying.

MEMBER BROWN: I'm getting ahead of the game probably.

MR. POPPEL: Okay. But the point is, in normal operation, the communication card won't write to the main controllers.

DR. WALLIS: But if something bad gets in there and turns all those things so they can write, then --

MR. POPPEL: That's a programmable thing which, incidentally, is not programmable by a little switch in front of the card. You have to turn a key, make the division in op, and et cetera, et cetera, et cetera to change the program.

MR. BUTLER: You have to have special equipment to come in and change the program. That can't happen during normal operations.

MR. POPPEL: Unless, as you say, it flips. But, of course, it would have to flip in two processors, because the minute you get two processors sending different information, you'll get an alarm, two communication cards.

DR. WALLIS: Couldn't you get a lightning strike or something that -- although you filtered everything out, it sends some piece of information in through this thing that reverses all those no write instructions?

MR. POPPEL: We have learned a bunch of lessons about lightning and voltage surges from recent operating experience, and although I could tell you about it, I'm not sure we want to go in that direction.

MR. BUTLER: No, we're not going to go into that. We're not going to do that in a public session.

MR. POPPEL: Yes, it's not going to happen on the fiber optics. It would have to happen in the division. Okay? But let's continue on with the path a little bit.

So, all -- the application program in the processor on the left side that we write, this is what we want the SSLC/ESF to do for a living. Okay? One of the things you have to do is say I need data from the outside world, or I have to write data to the outside world. You have to declare that as a read/write or both variable in your program, which is, therefore, then after under change control. So, what that's really saying is, I ain't even going to read the shared memory unless it's written -- the variable is written as a write variable. So, in other words, all the MDCIS data coming in, even if it got through the X of the closed right port, and somehow got to the main processor, and somehow got put in the shared memory, it still would not be used under the control of the application that we wrote.

DR. WALLIS: If the write function is disabled, why is it even there?

MR. POPPEL: Because it wasn't disabled on the other -- in other words, we want --

MR. BUTLER: So, the reason why it's still there is because we try to design these things from an industrially practical perspective, so that there's available technology and products on the market that don't require everything to be fully custom designed from scratch. So, these are implementation techniques with technology and products that are available on the market today that can be applied with appropriate techniques and Appendix B controls to present a layered defense approach to whether or not that kind of failure could occur. And in this case, you have to go through several processor failures, or application programming failures, through several shared memory buffers in order to be able to present the wrong data there. And these are industrial techniques for secure communication in industrial controllers. They are well known in the industrial field.

MEMBER STETKAR: What kind of industries?

MR. BUTLER: Process industries, oil and marine industries.

MEMBER STETKAR: Ware industries, yet?

MR. BUTLER: There is a particular platform that has an LTR in which these techniques are presented.

MEMBER BROWN: LTR?

MR. BUTLER: Licensing Topical Report, which is an approved LTR.

MEMBER BROWN: Okay.

MR. BUTLER: And these techniques are on that LTR.

MEMBER BROWN: This is -- they might be approved, but I'm still going to ask the question.

MR. BUTLER: No, that's fine. I'm just saying that --

MEMBER BROWN: I understand what you're talking about.

MR. BUTLER: Okay.

MEMBER BROWN: I just wanted to make sure. I just -- you're going through the stork dance on the things --

MR. BUTLER: But it's important --

MEMBER BROWN: In fact, you don't have to have lightning or surges. I mean, we -- in my past, we actually found that bits got flipped by simple gamma radiation. We lost -- the program changed in certain places just due to gamma radiation that was around, which was not a very happy circumstance. So, what did we do? We now have protected data such that we can -- we refresh the PROMs that we use just to make sure we maintain the program authentically for what it does. And that's outside the -- it doesn't happen -- it's very infrequent. Let me use Ira's words, it's very infrequent, but it's happened.

MR. BUTLER: But just to emphasize again, that not only is this presented in a layered approach through the communication card into the communication processors environment into the shared memory, but this pink bar at the top is triply redundant, so even if you had this gamma radiation that affected one thing, there would still be a TMR two out of three vote. So, now you're talking about the same kind of gamma --

MEMBER BROWN: No, no, no, no. I'm not trying to go there.

MR. BUTLER: Okay.

MEMBER BROWN: I'm just telling you that --

MR. BUTLER: Because that would be highly -

-

MEMBER BROWN: That's just a fact, that's all I'm saying. That's all I'm saying. And I understand the need to use common hardware to minimize cost using conventional techniques. I'm not arguing about that.

MR. BUTLER: Okay.

MEMBER BROWN: I'm just pointing out that there's better ways with the common card to make sure that doesn't happen by grounding the port.

CHAIRMAN CORRADINI: Are you guys done with independence, because I'm going to vote for a break.

MR. BUTLER: We're done with dependence, independence. We're going to go --

CHAIRMAN CORRADINI: So, I just wanted to know, if we're done with independence -- if you're going to start a new topic, determinism, could we like take 10 minutes for those that are --

MR. BUTLER: Sure.

MEMBER BROWN: Biologically impaired.

CHAIRMAN CORRADINI: Okay. We'll take a break for 10 minutes. We'll be back at 10:25.

(Whereupon, the proceedings went off the record at 10:15:10 a.m., and went back on the record at 10:27:11 a.m.)

CHAIRMAN CORRADINI: Okay, let's come back into session.

We're going to have -- we wanted to have another piece of information from yesterday brought to the Committee's attention. Alan, go ahead. I'm sorry.

MR. BEARD: Again, Alan Beard with GE Hitachi, and Gary Anthony should be in the room in Wilmington, and he'll be able to correct me if I state anything wrong, or enhance anything that -- the statements I'm going to make now.

In regards to the loading handling issue that came up yesterday, Mr. Stetkar was referring to Section 9.1.5.6 of the DCD that referred to the potential for a drop of the heavy load, and we had a statement that it created no radiological hazards. He was worried about load handling events in the turbine building. We'd like to point out that all Section 9.1.5 is confined to discussions of heavy load handling from the reactor building, and the fuel building, and, thus, that any radiological statement is confined to load handling accidents that occur in that building.

Now, in regards to control of the heavy loads within the turbine building, couple of issues that we would like to point out. Number one, the operating deck of the turbine building is a very robust structure. Any heavy loads that we're handling in that building we're keeping as low to the floor as we can, such that if you were to drop it, we would certainly expect that the floor would prevent propagation of that load to lower elevations.

During operation, access to what we would call the south end of the building, which is the end where the high-pressure turbine is, and the moisture separator reheaters is restricted because of the shielding that's in place to prevent that. Gary Anthony, I'm going to ask you to verify this, but the moisture separator reheaters are actually located below the operating deck. Is that correct?

MR. ANTHONY: No, they are on the operating deck, but they're fully shielded in cubicles, including shine shields over the turbines so you couldn't drop anything on them.

MEMBER STETKAR: Gary, this is John Stetkar. The shielding -- just to make sure I'm clear on this, the shielding extends up above the tops of the main turbine enclosures?

MR. ANTHONY: The main turbine is under a set of shine shields.

MEMBER STETKAR: Okay.

MR. ANTHONY: And the MSRs are completely in like bunker-type cubicles that are completely enclosed.

MEMBER STETKAR: Okay. So, if you were to move something on the turbine building crane over those enclosures, the shield walls and the enclosures would provide protection for both the steam lines and the MSRs?

MR. ANTHONY: Yes. Actually, the main steam lines do not appear on the operating deck. They are on the lower deck below, underneath.

MEMBER STETKAR: I tend to generically assign the HP to LP and MSR crossover lines are up above. Right?

MR. ANTHONY: They're completely shielded, also.

MEMBER STETKAR: Okay. Great. Thank you.

MR. BEARD: Okay. And then continuing to build on that, any heavy load handling that might be -- pre-staging of heavy components for an upcoming outage would largely be limited to the north end of the building where we don't have any of the steam piping that you're worried about.

MEMBER STETKAR: Great.

MR. BEARD: Okay?

MEMBER STETKAR: Yes. And that information pretty well satisfies my concerns. Thank you.

MR. BEARD: Okay.

CHAIRMAN CORRADINI: Thank you. Go ahead.

MR. BUTLER: Okay. So, just a few introductory remarks. We're back to talk about determinism as part of the four plus one. And this section -- so this section will focus mainly on the processors related to RTIF-NMS, and SSLC/ESF, because, in fact, in the ICP there isn't formally a processor. It's a series of hard logic gates. So, this discussion will primarily focus on RTIF and NMS. Ira.

MR. POPPEL: Okay. Basically, this is one of the new sections that's been added to Rev. 8, was on the list way back at the beginning of this talk. So, the three platforms, in our case the two platforms, we'll discuss the four principles. And this is the determinant principle, so here's where you'll find it in the new DCD. And, basically, what we're saying is that we recognize that as a design basis for these platforms, that you must have a time budget. It must be traceable to some requirements, which will be mainly Wayne's, that these events happen at these times in the accident sequences. And that we must then take that that time budget and insure that the systems meet it consistently, and in that time or less, so both. And we must, further, take the time budget for the system, and if we have individual components in the system, like sensors, RMUs, et cetera, et cetera, et cetera, whole bunch of out of service for the system that we must assign, breakdown the time budget further, and assign it to those individual communication links, and to the individual processing that's going on all through the system, so that in the end in a demonstrable way traceable back to a specific requirement we can show that the systems are deterministic and will work.

DR. WALLIS: Is determinism just timing, or is it -- it completes an operation in an adequate time with no errors, because if it gets near the end of not being able to quite meet the time, does it introduce errors? Isn't errors introduced into this somehow, or is it only time you worry about?

MR. POPPEL: So far, we're only worried about time, because if, in fact, there were errors introduced, we would interpret that as a single divisional failure.

DR. WALLIS: Well, a person, they were trying to conduct something, complete an operation in a given time, is more likely to screw up if it's almost hasn't got quite enough time. So, you don't worry about that at all?

MR. POPPEL: We worry about it, but what you said is, especially, a human -- anything an operator does is so long in time frame compared to the process that we're talking about.

DR. WALLIS: It's all relative. So, determinism is only a matter of time in your view.

MR. POPPEL: Yes.

DR. WALLIS: Okay. That's all I'm getting at.

MR. POPPEL: But --

MEMBER BROWN: Repeatable and predictable.

DR. WALLIS: That's also part of it, isn't it? Predictable is key. It's not just time. So, his view is like my view, so it's repeatable and predictable. But your's is just time?

MR. BUTLER: It's repeatable and predictable within the specific time allowed.

DR. WALLIS: Yes, but the other two are important criteria.

MR. BUTLER: Yes.

DR. WALLIS: Thank you. It's not just time you're worried about.

MR. BUTLER: Yes.

DR. WALLIS: Otherwise, I can just put in for my ACRS hours and not care about what I did.

CHAIRMAN CORRADINI: We won't go there.

MR. BUTLER: Next chart.

CHAIRMAN CORRADINI: Yes, let's avoid that.

MR. POPPEL: Okay. So, this gets down to okay, having decided we needed a time budget, and having decided we need to design using it, then how do we design the various systems, what techniques do we use for the design to insure that we can get the repeatable deterministic, predictable response. And it's silly just to read it, but, basically, we have to consider well known programming techniques that are used to do this.

So, for example, we are clock-driven. So, in other words, we're going to look at reactor water level every 20 milliseconds no matter what. We don't care about a reactor water level event. We're just going to keep on looking at that rate no matter what, so that we are totally independent of the events. Okay. So, we're not going to use those techniques. And, as Skip said earlier, you'll find a listing of the techniques that we're not using in the ITAACs. That was one of the changes in Tier 1, so it can be verified that we're not using these techniques. Next slide.

Okay. We skipped to this one earlier, but, basically, the idea is that we're just going to have a large programming loop that's going to do everything that that chassis or that system uses, and it steps through the various functions continuously all the time, and nobody says stop what you're doing, and listen to me. It just keeps on going, and then loops around. So, we have to design the IO systems, the measurements that the process needs, and the communications that the process needs so that it doesn't interrupt that main loop. And, in fact, we do those programming techniques so that we don't interrupt the main loop.

The advantage of having the main loop run all the time is so that in a predictable way, so you can have a watchdog timer to say it didn't run, and you can tell when it stopped built into the actual application. Next.

Okay. So, this is RTIF, and this is --

MEMBER BROWN: Let me backtrack to that for just a second. I presume this timing cycle also includes all -- since you've got the voting logic in the processor, this includes all those functions.

They're not done as a separate --

MR. POPPEL: Correct.

MEMBER BROWN: So, this is straight through. You do it all, so regardless of what happens with all these other microprocessors, data coming in and out, you're just receiving data from other divisions, from parameters, whatever, telling you, and you just look at that, and you determine whether you've got two out of four trips, et cetera.

MR. POPPEL: Yes.

MEMBER BROWN: Or two out of three, whatever they are. Okay.

MR. POPPEL: Emphasizing the parameters, again, are just trip and bypass.

MEMBER BROWN: I understand that.

MR. POPPEL: So, there's lots of pieces in say the RPS system that have to be deterministic. We're going to look at one piece, and we're going to look at the piece that says let's talk about the two out of four logic used to support the reactor scrams. Okay? And Skip filled in the dotted blue line, which wasn't on the main thing, but that's the line by which the RTIF processors have to talk to one another. Now, let's go to the next slide.

In reality, that isn't a network. It

isn't a bus, it's point-to-point. So, here is a box in Div. 1, and it has three ports on it. One port goes to Div. 2, one goes to Div. 3, and one goes to Div. 4. Okay? And, again, the only information on those links is authentication, and trip and bypass status. And I should also say per parameter, so it's like a pressure trip, a level trip, et cetera, because the ultimate two out of four logic is any two like parameters that aren't bypassed exceeding their values will cause the scram. So, as it happens, this is described in the DCD, and we don't have to do it here, because it's a communication thing, we actually have two two out of four votes in the RPS system. One is at the sensor level, so it's basically saying if I -- I can bypass one of these divisions, so it says, basically, don't consider the Div. 1 pressure sensor in your two out of four calculation. And there is a joystick-type switch to make sure you can only do that one division at a time. Okay? And the switch is enforced by logic that says despite that, if more than two divisions are in bypass, then no divisions are in bypass. Okay?

Another thing associated with -- and then following that, we have a logic trip, so we've made a trip, Div. 1 that says there's a two out of four trip, and communicates that to all four divisions. And then we have another vote, again, to see whether the four divisions, there's two out of four divisions that agree, and that causes the ultimate reactor scram. That causes a logic trip. Too much detail for here, but --

MEMBER BROWN: Just a minute. Back that up a minute. I want to ask two questions. One on the bypass thing. You're talking about an operator thing bypass.

MR. POPPEL: Yes.

MEMBER BROWN: Okay. So, that's -- I just wanted to make sure I understood that point. The -- each division has its own two out of four voting function.

MR. POPPEL: Yes.

MEMBER BROWN: And then you made the next statement, said there's another, if I understood you correctly, another two out of four. In other words, you've got to have two out of four divisions all coming to that two out of four decision.

MR. POPPEL: Yes.

MEMBER BROWN: Now, where is that voting done, in the same processors?

MR. POPPEL: You can see on this thing

here, the flow across the yellow boxes is the remote multiplexing unit in the field talking to, we'll talk about that later, to the DTM, which is the box that says the parameter has exceeded its value. And then you can see the two out of four links going to the other divisions, so that each division communicates a per parameter trip decision. And then the DTM reports and says that Div. 1 has determined that there is a two out four pressure trip. Okay?

It gets transmitted to the box called TLU, Trip Logic Unit, which, basically, has another two out of four vote at the, for want of a better term, load driver level. So, when I told you that here's a load driver that has four fibers connected to it, and when two out of the four fibers say you should interrupt the current to this thing, if I bypass it, it says to the load drivers don't pay attention to that division in your decision. Okay? And just like the first bypass switch, there is a joystick and logic to insure that only one division at a time can be bypassed.

MEMBER BROWN: So, the second voting logic is not done in the processors, it's done at the load driver --

MR. POPPEL: It's done at what's called the output logic unit. Okay? But it is done in a processor. I shouldn't mislead you. It is absolutely done in a processor. The processor is in a different chassis than the first processor. The first processor being the VTM one, and the second being the TLU one.

MEMBER STETKAR: Ira, quick while he's looking for a reference. Is it physically possible, or legally allowed to place, for example, is Division 1 sensor has been bypassed, and Division 2 logic, if I can call it --

MR. POPPEL: Yes.

MEMBER STETKAR: -- in bypass simultaneously.

MR. POPPEL: Yes.

MEMBER STETKAR: Both physically possible, and there's two separate joysticks, one of sensors, and one for whatever it's called, logic.

MR. POPPEL: Maybe the most assuring statement to say is, no matter what the operator does with those joystick switches in the main control room --

MEMBER STETKAR: You still have two left.

MR. POPPEL: -- will not degrade you to below two like parameters exceeding their parameters, not bypassed will cause a trip.

MEMBER STETKAR: But you can, actually --

MR. POPPEL: Yes.

MEMBER STETKAR: Yes, do that. Okay.

MR. POPPEL: And what it, basically, boils down to is what boxes you want to do maintenance on.

MEMBER STETKAR: Yes.

MR. POPPEL: Okay. The reason you have to do -- well, you don't have to, because it's two out of four. You can always work on one while it's quote. But if you disable anything in the system, if the boxes don't talk to one another, et cetera, being a fail-safe design, it just goes to trip. So, for example, those two out of four links, one of the reasons they're not redundant is -- says I'm telling you about the trip status of all my measurements, and if you don't get it, you just assume that I'm all tripped, unless I have a signal that says that division is in bypass.

MEMBER STETKAR: In bypass.

MR. POPPEL: I should also say that the -- I'm sorry, Charlie.

MEMBER STETKAR: I'm assuming he's ready.

MEMBER BROWN: Yes. I'm waiting for him.

MEMBER STETKAR: No, I'm done. I've got enough.

MEMBER BROWN: Okay.

MEMBER STETKAR: Thanks.

MEMBER BROWN: Don't ever assume I'm ready for anything, John.

MEMBER STETKAR: You look prepared.

MEMBER BROWN: I'm looking at your figure here, which I saw in the Rev. 7 stuff, also. And I see the TLU. Then when I go look at Figure 7.2-1 in the DCD, it shows the output of the TLU going to an RPS output logic unit, which is not shown on here that I can see.

MR. POPPEL: Right. There's another figure in the --

MR. BUTLER: I think those figures are all in backup.

MEMBER BROWN: Well, I don't know. I haven't gone through your entire presentation. But, I mean, it's Figure 7.2-1, shows that, and it goes -- so, is the output logic unit -- why does it have to be a microprocessor? All it's doing is getting a division output unit singing a one or a zero off to -- or something, whatever you're sending. It's kind of maybe a load -- but it goes off to a load driver down where you have all the scram solenoids.

MR. POPPEL: Just in case I misunderstood you, the DTM and the TLU are processor-driven devices.

MEMBER BROWN: Yes.

MR. POPPEL: You asked -- that's what I thought you were asking.

MEMBER BROWN: No, I said each division --

MR. POPPEL: The OLU, not only does it not have to be, it is --

MEMBER BROWN: Yes. Okay. That's what I thought. The DTM, though, I mean just the processing, the TLU is a separate processor, that's where the voting is done.

MR. POPPEL: Yes.

MEMBER BROWN: Okay. You confused me for a minute. You have to be careful with old guys.

MR. POPPEL: The only reason we concentrate on the first slide is because that's where the two out of four point-to-point lines are shown.

MEMBER BROWN: Yes, from all the DTMs and all the other type stuff.

MR. POPPEL: Right.

MR. BUTLER: That's where the inter-divisional communication --

MEMBER BROWN: I got that. But for the two out of four division level trip, the actual trip that gets sent out, I mean, does something, actuates the final control device, is a matter of how the load devices are arranged. Is that correct?

MR. POPPEL: Yes.

MEMBER BROWN: So, they get a division trip signal, and then they're the final two out of four, any two out of four the division trips will trigger the load device, will trigger the scram breakers.

MR. POPPEL: Yes. We discussed that, that they only existed physically in Div. 1 and Div. 2 because that's the power they were switching. So, where it says LD, that means Load Driver.

MEMBER BROWN: Okay.

MR. BUTLER: That's in backup. It's Figure 7.2-11b from the DCD Rev. 6, and 7, and 8.

MEMBER BROWN: I have that one, also, which is readable. Okay. All right. This is just an expansion of this in here. Okay.

MR. POPPEL: Now, if you go back to --

MR. BUTLER: Okay, you're fine. Let's stay on track. So, let's keep going.

MR. POPPEL: Before we leave this one, just to say that the two out of four is point-to-point, it's fiber, of course, and its coding is such that in a simpleminded way it can tell that there is no communication, and it can also determine something about each division's clock, technical Manchester coding. But the bottom line is, it's set up so that to support the failsafe nature of the communication and the isolated nature of the communication.

When the communication occurs, it gets dumped into a shared memory. Okay? And then it's pretty much like we had our discussion before. So, the application program, which in this case is a burnt in, accesses the shared memory to see what was brought in by that point-to-point link.

MR. BUTLER: Okay. Let's go to SSLC.

MR. POPPEL: Okay. SSLC has the same line, but in this case, it's the bus that you saw before. So, the SSLC is, in fact, the network. So, unlike the point-to-point communication, which is 100 megabits a second at 30 feet of fiber, which is, essentially, instantaneous in terms of our time budgets, anything that's ethernet is not instantaneous, and on the face of it may not appear deterministic because of the way ethernet works. Okay? So, we had to think about that carefully.

So, we have the buses that you saw before. So, this is a little example of our communications that are going on. So, in other words, this is a calculation to say well, how loaded is that bus? So, in other words, if I'm sending a Div. 1 message that's

1,024 bytes long, which is -- and I don't know whether there's 1,024 bytes to send one or a zero with all that authentication stuff on it, so I have Div. 1 doing that roughly 10 times a second, and acknowledging to the four divisions, so Div. 1 is doing that times four, times two because of the acknowledgment, and so is Div. 2, and Div. 3, and Div. 4 all on the same network.

DR. WALLIS: This is all to send a one or a zero.

MR. POPPEL: Yes, all to send a one or a zero. So, in other words, if you say okay, it's 1,024 bytes and it's 100 megabyte a second link, exactly how much do we fill out that link, just assuming it's just random, and we'll talk about the randomness stuff. And the bottom line is, we're filling up the link about zero percent, .6 percent. Okay? So, it's a very, very lightly loaded network. Okay?

Now, the other thing we did is said, okay, well that's how long the message is in time, but how about the transport of the message? Okay. The next calculation is the bottom one, said well, okay, speed of light in the fiber, the distance of the DCIS rooms, et cetera, et cetera, so the bottom line is, our message is about 82 microseconds in length, and the transmission time is about .15 microseconds. Okay? That's a fairly straightforward calculation, so what we have to do about determinism is say what does that mean given the way that ethernet works? But the takeaway is, transport time is almost negligible. The network is extremely lightly loaded, and the messages are not long in time. So, this is what happens with ethernet to make it, perhaps, non-deterministic, and we say functionally deterministic.

So, I draw your attention to the yellow box, and that box across the top is 100 milliseconds. So, in other words, it may or may not have been obvious by now but the ESBWR is a very slow beast in terms of ECCS. Not much has to happen fast, there's a long time to do stuff. We don't have to get diesels started in 10 seconds, et cetera, et cetera. So, nominally, we don't know yet, but we're saying we'll probably be running the SSLC/ESF, that cyclic program that we talked about at maybe two to four times a second, but we wrote down 10 times a second. So, in other words, the top yellow bar is 100 milliseconds in time, and we say that's how often the loop is going to repeat. Okay? So, we want to make sure that our two out of four messages get to the microprocessors in a timely way to support their two out of four decisions.

So, we set a criterion of one millisecond. That's that little red sliver that Romeo is pointing to there. That's what we're saying is success. If we can get our message in a reliable way in one millisecond, we'll be fine.

And then we expanded that one millisecond and said by the way, the green that you're seeing there is the length of the message. That's the 82 microseconds we talked about before. So, somehow we have to make sure that all four divisions using the same network doing this stuff can get the information in a timely way. So, here's the way that ethernet works. And this isn't unique to GE, this is just the way ethernet works.

So, the first thing that happens is that all the divisions typical of ethernet, but all four divisions are looking at the network. Is there anything on it? Okay. Well, in general, 99.4 percent of the time there's nothing on it. Okay? There's random, but in general, 99.4 percent of the time there's nothing on it, so it sends a message. It's an 80 microsecond message, it takes .15 microsecond, all is well. Okay?

So, the next thing that happens is well, wait a minute, suppose I go look at the network, more or less the remaining .6 percent of the time, and there's something on it? Okay. Because everything is common, they're not synchronized in any way, so it says there's something on it. Okay? So, I'm not going to try to transmit. I'm going to wait. How long do you have to wait? You have to wait 82 microseconds for the message to clear, plus another .15 microseconds for the message to get through the fibers. That's how long you've got to wait, and then the division that's sitting there waiting says my turn, so then it sends its message. So, now what you've done is you've sent the message, if you will, 82 microseconds late, which more than meets our one milliseconds criteria for getting the message there in a timely way.

So, that's the situation that's going to happen essentially all the time, but there is a possibility of data collisions. Okay? The way this comes about is, Div. 1 is using the network. Okay? And as it happens, just randomly, Div. 2 and Div. 3 have a message to go. Okay? So, Div. 2 and Div. 3 are looking, they wait for the Div. 1 to clear, and then Div. 2 and Div. 3 simultaneously, because they don't talk to one another, they say my turn, and they both put data on the ring. Collision. Okay? So, what ethernet does about that is they say everybody backs off, and we're going to -- this is heavy inside baseball, we're going to wait some random slot time, which is like 5 microseconds for 100 megabyte ring, we're going to wait like -- each division makes a random calculation. I'm going to wait an X multiple of 5 microseconds, and then I'm going to try again. Okay? And they do that independently. So, in general, one division goes and gets it, and then the third division waits. And now, if you will, you lost 80 microseconds, 80 microseconds, and the third one goes 164 microseconds late, which is still okay for our one millisecond.

But suppose just at random both divisions said I'm going to wait the same random amount of time and try again? So, they have another collision. Okay? Then ethernet says okay, I'm going to back off a different random time that has bigger numbers, so before I could have just had a random two slot times to four slot times, the second time it'll be like four slot times to a slot time. But the bottom line is, they keep trying. Okay? And each time they're trying there's a longer delay, but each time they're trying the chances of this event happening are becoming less, and less, and less, because, in general, there's nothing on the network.

So, you can actually take a calculation that says here's the ethernet rules. Okay? So, what are the chances of getting a message through in -- next slide. Yes. What are the chances of getting a message through in our -- so, here's our criteria. We said we want to get the message through in 100-year period in one millisecond with a certain probability.

DR. WALLIS: These are probabilities per 100 years. They're not probabilities per message.

MR. POPPEL: No, it's actually probability of it happening in 100 years per message. So, this is happening at 10 times a second per division, but each one is an individual chance. So, in other words, what chance do I have of getting my message through on this "network?" So, you can see, I mean, we included a lot of stuff there, but our thing which says 1,024 and 100 megabit a second network, and dead time of one millisecond, et cetera, et cetera, and you can see the probability calculated, and we're like seven nines.

DR. WALLIS: And your X axis on the right there is a zero percent that should be message rate. The X axis is message rate, it's not network load.

CHAIRMAN CORRADINI: What are you looking at, Graham? I didn't understand.

DR. WALLIS: The X axis in the probability of success, the upper graph there shouldn't be zero percent for every spot, it should be -- it's per message rate, if you look at the table.

MR. POPPEL: Oh, no. The reason for that is, you can see that all of those varying loadings that we calculated, the network is all, essentially, zero percent --

DR. WALLIS: The variable is message rate. The independent variable is message rate, zero, five, ten, fifteen, twenty, twenty-five.

MR. POPPEL: Okay. I see what you're seeing. Yes.

CHAIRMAN CORRADINI: Plotted the wrong X variable with Excel.

MEMBER ARMIJO: That's right.

MR. POPPEL: So, all I'm trying to say out of this is that it's unlikely that the message won't get through, and the probability is enormous. And it's like -- and, remember, the success criteria is getting it through in one millisecond.

DR. WALLIS: Well, the probability of something else going wrong must be bigger.

MR. POPPEL: Yes.

MR. BUTLER: That's it, that's the point.

Let's go.

MEMBER BROWN: What did he say? I didn't --

MR. BUTLER: He said the probability of something else going wrong is bigger.

MEMBER BROWN: Yes.

MR. BUTLER: Yes. Okay. So, let's go on to the next chart.

MR. POPPEL: Universal agreement having been obtained.

MR. BUTLER: All right. We won't spend too much time on redundancy, simply because I don't think there's too many concerns about that. So, what we did here was just present the highlights, no different than from the 22nd of October, no different than what's been in the DCD since Rev. 6, or earlier. Okay?

We wanted to make a specific point, again. We are trying to highlight an area of concern around ethernet networks within SSLC/ESF, so here is the explanation, again, very briefly, Ira, which we kind of discussed before, what happens with a fiber break in the dual rotating rings. So, I don't think there's any -- okay, next chart. All right. Diversity. We're highly diverse. Okay? Any questions about this?

MR. POPPEL: By definition, the three platforms are highly diverse.

MR. BUTLER: Okay. So, the next one. All right. So, this is just another graphic to show how it lays out in an architectural format, so go the next one.

MEMBER ARMIJO: Going back to that diversity chart.

MR. BUTLER: Yes.

MEMBER ARMIJO: You point out that you use this approach or design from the ABWR Lungmen Project, and was it also part of the design, or the same thing in the Japanese ABWR?

MR. POPPEL: No, the Japanese ABWR was different. What happened at Lungmen is, we separated out ECCS and reactor trip, two different platforms, and we maintain that with ESBWR, and added the diverse protection system.

MEMBER ARMIJO: Okay. But that plant has yet to operate. Right? It's almost ready, it's almost built.

MR. BUTLER: Architecturally, with the exception of DPS, the approach to having different platforms for RTIF-NMS and SSLC/ESF was what we learned from that project to address concerns in digital systems. Let's go to the next one. Simplicity.

MR. POPPEL: We're, basically, as simple as possible given the complexity of the design. But, I mean, there were some active decisions that we took about how to configure all of this DCIS. Okay? And one of the things we did is, we split it up into lots of different functions, so that -- in other words, a Mark VI controller, or a DTM processor is capable of doing lots and lots of things, far more than we're asking it to do, but we didn't put those things in it. So, we made it so this controller controls reactor pressure, it doesn't control reactor level. So, the bottom line is, removes the concerns about the failure of the platform. It also means that when it comes time to specify design and test the software, it's a lot simpler when it only has one or a few functions to do, permutation combinations, and all of that.

Another one that we did is no closed loop control over a shared network. So, basically, here's the reactor pressure system controller. Okay? Obviously, it has to measure reactor pressure, and it measures its own reactor pressure, and it measures its own reactor pressure with its own sensors that it controls, and it poles, and doesn't depend on anybody else's reactor pressure sensors to do it.

So, similarly, all our controllers that have functions to do are not using that big network to pass data back and forth because it's convenient. If they need it, they measure it themselves. Okay? And that allows us to make the statement that -- the reason for the control room is monitoring, alarming, and all the rest of it. If you lost all of those links, the controllers continue on autonomously controlling their processes, both safety and non-safety can say that.

MEMBER BROWN: In each division, let me just pick the RTIF, again, doesn't matter which, pressure, each division has its own pressure sensor.

MR. POPPEL: Yes.

MEMBER BROWN: Other than trip functions, or like functions, which that data, once it gets tripped, sent from division to division, do you do any data evaluation? For example, do you take your say Division 1 pressure and then somehow Division 2, 3, and 4 get over there, and you say oh, look at all of these, and I'm going to reject this, because it differs from an average of the other three, or the four, blah, blah. Do you do any --

MR. POPPEL: I did that, Charlie. You shish kabobbed me.

MR. BUTLER: So, we have a chart on that.

MEMBER BROWN: That's why I asked the question.

MR. BUTLER: We say absolutely not, and the chart is in there.

MEMBER BROWN: Okay. That's fine.

MR. BUTLER: Yes. So, that's it, we don't.

MEMBER BROWN: Yes, we don't have to go -- we can go on.

MR. BUTLER: We don't have to go any further, yes.

MR. POPPEL: I, also, just wanted to say that the pressure sensor in SSLC/ESF is different than the pressure sensor in RTIF. They're not the same even within the division.

MR. BUTLER: And they're different for DPS.

MEMBER BROWN: Yes. I mean, you've got independent sensors for each function.

MR. BUTLER: Do have independence.

MEMBER BROWN: Yes. Thank you.

MR. POPPEL: The other thing is a big issue nowadays with DCIS is cyber security. We have -- it's hard to say about that. Basically, we said we're going to choose communication protocols that make it highly resistant to spoofing, et cetera, and we're going to use all kinds of smart switches to prevent all kinds of bad things from happening. And even our non-safety controllers can't be programmed externally.

So, for example, if they need data, I mean, the application in the non-safety program basically says I'm going to listen to this. I have to be programmed for it. I'm going to send this out, but nobody can say to me stop and do it.

MEMBER BROWN: Okay. So, go backwards to the shared memory, the communication via -- with the writes being X'd. The only way that can be done is at the cabinet?

MR. BUTLER: Yes.

MEMBER BROWN: You have to come down, open the cabinet --

MR. BUTLER: With a special device.

MEMBER BROWN: Yes, whatever, lap -- whatever the thing is you use, but it cannot be done --

MR. BUTLER: You cannot do that through the network.

MEMBER BROWN: -- from the main control room.

MR. BUTLER: It cannot be done. Only with a separate piece of equipment --

MEMBER BROWN: At the --

MR. BUTLER: -- at the actual chassis.

MEMBER BROWN: Okay. All right. I just want to clarify.

MR. BUTLER: Okay.

MR. POPPEL: Main control room can't program anything.

MR. BUTLER: Anything. And nothing can be programmed from outside of the cabinets, themselves, in the Q-DCIS room. And, in fact, all of the information that we shared with you about the design, to get to data isolation and data independence, are the similar techniques that one uses to create a cyber secured digital environment. So, that's why if you embrace 603, and do it is in this modular, segmented, and layered way making the functional level simple, and building up from there, that creates a cyber secure design from a data perspective. That's why they're synergistic.

MR. POPPEL: Just a few more simplicity things. Our remote shutdown panel is basically an auxiliary control room with less screens. So, it's not a limited function, you can only do this, that, or the other thing. It's, basically, the operator controls the plant in the same way with the same screen formats that you will control from the main control room, and only loses functionality depending on power and all the rest of the stuff. But he doesn't have -- there's no new human factors, or different human factors associated with that. So, you can pretty much operate the plant completely from the remote shutdown panels.

This is sort of a duh. I mean, we use -- even where we don't have to, we use optical fiber.

MEMBER BROWN: Let me go back to the other question, again. Is that captured in the DCD? That's a configuration management issue. Is that -- your remote programming.

MR. BUTLER: We have made it very clear with the Rev. 8 that we've submitted, yes.

MEMBER BROWN: Okay. Yes, I didn't see any --

MR. BUTLER: It was implicit before in some of the way we stated things, we made it very clear.

MEMBER BROWN: Okay. All right. Thank you.

MR. POPPEL: Okay. Next.

MR. BUTLER: Next.

MR. POPPEL: This is sort of like a major simplicity. Absolutely, we do not have non-safety talking to safety, or controlling it, or any possibility of it. I shouldn't say any, very low possibility of it, and we do not have any -- very low possibility of any division controlling any other division. To control a division, you have to go to the VDU associated with that division. That is the only way operator commands can get to the things in that division. Absolutely, so we never have any box saying who should I listen to?

MR. BUTLER: There's a question.

MEMBER STETKAR: Ira, what do you do in some -- some systems have both non-safety and safety functions. Pick fuel auxiliary pool cooling system, for example, it's a normally operating non-safety system, provides cooling, some pools can be aligned to the suppression pool. It has a safety function in a sense that it has containment isolation valves that need to close from a safety signal. How do you interface the non-safety signals? For example, if I, as the operator, through the non-safety system want to during normal operation align the fuel and auxiliary pool's cooling system for cooling the suppression pool, I need to open those isolation valves. And, yet, if an accident happens, the leak detection and isolation system has to come in and tell those valves to close, even thought they might have an open demand signal from my non-safety controls.

MR. POPPEL: You said it correctly. The operator has to do that. What the operator has to do is, he has to step over to the safety VDU.

MEMBER STETKAR: Okay. So, those valves are only controlled through safety.

MR. POPPEL: Yes.

MEMBER STETKAR: Okay. Thanks.

MR. POPPEL: It makes it simpler to do the design that way.

MEMBER STETKAR: The thing with RWCU and, yes, all that kind of --

MR. BUTLER: They're all done that way.

MEMBER STETKAR: Okay. Good. That wasn't completely clear.

MR. POPPEL: Even with the plant automation system, can't control anything except safety. Okay. Oh, logic. I'm sorry. Let's go to the next one.

MEMBER BROWN: You really want to say that?

MR. POPPEL: Which?

MEMBER BROWN: Not required.

CHAIRMAN CORRADINI: Well, they're just

stating facts.

MEMBER BROWN: I know. I know. I'm just --

MR. POPPEL: It's a factual statement.

MEMBER BROWN: You've got to have --

MR. BUTLER: So, yes, we want to say that. They're not required by regulation. Second bullet, Ira.

MR. POPPEL: You mean notwithstanding.

MEMBER STETKAR: The correct term is that the regulations do not require that you submit that. It's not that the regulations preclude you from submitting them. Is that correct?

MR. BUTLER: Yes.

MEMBER STETKAR: Okay.

MEMBER BROWN: Thank you, John. I like that.

MR. BUTLER: You want us to change the statement on the chart?

MEMBER STETKAR: No, it's fine.

MR. BUTLER: Okay. But your clarification is correct. Bullet two.

MR. POPPEL: Okay. The original logic diagrams that had been submitted were called simplified logic diagrams, and they were, basically, to demonstrate statements in the DCD. They were in no way, shape, or form a description of the entire system, or all the things that were in them. Okay? So, it's sort of a dead-end path. Okay? But, as you've seen with our software management LTRs, we have a very detailed development process to making software, and putting into those controllers. And part of that is to make logic diagrams, in this case functional logic block diagrams, as an input to the software design process, to say this is some of the stuff we want you to incorporate in the software requirement specification.

So, we just wanted to leave, I guess, with the warm fuzzy that there will be logic diagrams. They will be viewable. And in the ITAAC process, coupled with the software LTRs, you may remember there was something called a Baseline Review Process, we have phases of the software design, and at the end of the phase, we say have this Baseline Review Process, in part to look at all the documentation associated with that phase, to give approval before you can go on to the next phase. And part of that will be the review of the logic diagrams that were created to support that phase. So, they will exist, they will be viewable.

MR. BUTLER: Available for audit.

MR. POPPEL: Available for audit, is the --

MEMBER ARMIJO: Who does the baseline review, is that a GE function?

MR. BUTLER: So, the baseline review is convened by the design organization. It's chaired by an independent group. And for those things identified as software critical, there's an independent -- a group that does not report to Design Engineering, that does the assessment and the approval of those artifacts, which include the logic diagrams.

MEMBER ARMIJO: Well, it's equivalent to an independent design review --

MR. BUTLER: It's equivalent to an independent design review, yes.

MEMBER ARMIJO: Within GEH?

MR. BUTLER: Yes. It is within -- for the LTRs, it is within GEH, but it is — ultimate approval to go forward is by an independent body. And that's the role of SQA, and that's why there's a whole separate SQA LTR. There are three LTRs. There's one that describes the overall systems engineering process. There's the one for SQA, which is the independent auditor, not in Design Engineering, and then there's one for cyber security. And they all integrate together, and they all have a role in these six phases. Just a typical example of a block diagram from Rev. 5. There's many of them. Go to the next. Okay. I'll do this one.

What this shows from Rev. 8 that was submitted yesterday is the RTIF software plan example, and what you see here is, for each phase -- let me draw it. So, for each phase, here's the planning phase. The logic diagrams are explicitly identified in the LTRs as being input and output requirements for every design phase. There is an ITAAC for each one of the platform to go through and say it exists, and it's adequate. It's done again in the requirements phase, the design phase. Implementation is where the initial coding is done, test phase, installation phase. All of these have an independent assessment, and they all have the requirement that the logic diagram, or any of the other input/output requirements have been independently assessed, fit for use, and meet their intended safety function purpose. Go to the next.

MEMBER BROWN: Go back up to that for a second. I guess you're still there.

MR. BUTLER: Yes.

MEMBER BROWN: I read through a whole bunch of these, 2As through whatever. They were in Rev. 7. And, I guess, I have to admit, I walked away a little bit -- I mean, they are very, very, very, very general. I mean, it effectively says our design phase says we'll design it, and the acceptance criteria is that there is a report that says we designed it in accordance with our requirements, which --

MR. BUTLER: I guess, what I'd like to ask you to consider, Charlie, is that the three LTRs are Tier 2*, and in the three LTRs, they do explain not only the process, but how the voracity of the input/output documents are assessed. So, you can't just read the ITAACs outside of those three LTRs.

MEMBER BROWN: They are Tier 2*.

MR. BUTLER: They are Tier 2*.

MEMBER BROWN: I guess, my point being, I'm just going back to the, I guess, logic diagrams. These are the logic diagrams that are, in my mind, it's not what I've been talking about in terms of architecture and stuff. This is the functional system logic diagrams that says I'm going to take a pressure, and a flow, and a level, and I've got water in the reactor compartment, excuse me, in the reactor building, then certain things happen, and pumps start. That's a logic diagram that describes a safety function, and that's what you're talking about. And some of those, I don't know whether they're simplified or not, but I guess they are, show up. You've given us some of those in the DCD, I think in Tier 2. Yes, Tier 2, Chapter 7, didn't you? I thought I saw some.

CHAIRMAN CORRADINI: The logic diagrams?

MEMBER BROWN: Yes.

CHAIRMAN CORRADINI: I think Ira --

MEMBER BROWN: John, you pointed that out last time, didn't you?

CHAIRMAN CORRADINI: Well, I think just to state it as I remember it, we asked for them, they gave us samples. Ira's point was the samples, you used the word "dead-end," I'd say incomplete. That is, the examples we got were not complete. John found some things when he was looking for completeness, but I think the characterization was we got examples of them, and that was kind of --

MR. BUTLER: Yes, design basis of the plant. Yes.

MEMBER STETKAR: Except even within Rev. 5, there were incomplete is one, errors is another. So, it's not clear what they -- what purpose they were meant to serve, because they were not an accurate logical replication of the plant design. So, it's not clear what they were. I could give you specific examples, but going into specifics is not worth the effort. If you want, go look at GDCS actuation.

MR. BUTLER: Okay.

MEMBER STETKAR: It's wrong.

CHAIRMAN CORRADINI: In the example that was given to us.

MEMBER STETKAR: Yes.

MR. BUTLER: Okay.

MEMBER BROWN: One of my concerns was that, and this is just at this level right now. Okay? Is that I've sat in these meetings where we've taken the various systems, the GDCS, the other -- whatever all the various systems that go into the safety, the ESF-type functions, what have you, and we get excruciating detail of pipe lengths, and runs, so that water flows down through the pipes at the right velocity, and the amount of debris that gets caught in the screens, and all this, so it's just -- I mean, it's down to the stainless steel bolts.

CHAIRMAN CORRADINI: That's because that's the important stuff.

MEMBER BROWN: That's the important stuff, right. But, yet, the logic diagram for saying when we actuate these systems is not there. And that's what got me, is that the logic diagram for telling all this stuff to start, and what is the coincidence, what are the things that do this, what are the things -- you didn't follow Mike's request.

(Off the record comment.)

MEMBER BROWN: And we sit here, and we don't have those, and those will be developed later, but the NRC has had no look at whether those cover all the parameters, and are they configured or timed in a safe viewpoint. So, I mean, I think that's what -- one of the -- that was my concern, and it's done later, and that the oversight is not there. But it is for the diameter of the pipe, and all the other type of stuff.

MEMBER STETKAR: I'm going to -- I've been pretty silent so far this morning, by design, because I think the discussion we've had for the last three hours has been exceedingly useful, really, really, really productive, and I don't want to try to interrupt this. And, Charlie, if you're kind of to the end of --

MEMBER BROWN: Yes, I'm kind of to the end.

MEMBER STETKAR: Now, I'm going to pick up the logic diagrams. As they're presented here, the logic diagrams seem to be focused as part of a software development tool, which they are. They should be. They're kind of the architecture of the way that you want that logic to work.

I look at them as something different from an overall plant integrated safety review perspective, in the same way that we have piping and instrumentation drawings that show that water goes from Tank A through Pump B, through Valve C, out into Pipe Connection D, into the reactor vessel, that picture gives me a good way of understanding in a nice, comprehensive format the way that that system works. Now, I might have questions about the pump flow rate, about the opening times on the valves.

We had an example yesterday where I thought about gee, there's a way of getting water from Point A to Point X, where I don't want water in Point X, and I don't see a check valve in this nice little piping diagram to prevent that from happening. So, as a reviewer, as someone who might be concerned about not putting water from Point A to Point X, that little drawing is really, really helpful for me, because I can ask gee, can you get water from those two points, and should there be a check valve in that line. That might be a safety concern.

I don't have similar diagrams right now in the DCD to allow me to look at the integrated reactor protection, safeguards actuation, and control functions that, basically, orchestrate how everything in the plant works. So, as a reviewer, I have a difficult time standing back and getting that integrated perspective. That's just a statement.

Because of that, I believe that the Staff, and the Staff has done a tremendous amount of work, as you're well aware, the Staff has been relegated to spending, essentially, all of their time trying to insure that every single possible design requirement, and standard, and technical position shall be satisfied in words, such that later there is some assurance that the design can be audited, inspected, reviewed, and I'm not going to use any one of those three words in preference to the other, to gain some confidence that, indeed, the design is going to do what we want it to do; in other words, keep the plant safe.

My impression is they've spent a lot more time doing that sort of stuff, than they've spent looking at the real design, because there are only 24-hours in a day, and so many human beings in the world, and they've had to spend their time looking at things that look like the slide in front of us, which are tiers of numbers of requirements of things.

Now, that's just a monologue. Let me ask some questions. I wanted to ask a kind of example question, kind of bring this point across. And I, honestly, don't know the answer. I really tried to figure out the answer, and I don't know. And I hope we've got the talent from GEH here that I need to get the answer to this question.

Suppose the plant is operating at 100 percent power. I normally have three feedwater pumps running, and one feedwater pump in standby. Suppose that feedwater pump that was in standby is out of service for maintenance. It's allowed, it can be. And now suppose that one of my three running feedwater pumps trips, so that now my feedwater flow reduces. What happens to the plant?

CHAIRMAN CORRADINI: Somebody has a hand up out there.

MEMBER STETKAR: Anyone.

MR. MARQUINO: Wayne, here.

MR. POPPEL: I know, but, I mean, the -- well, I'll let -- the proper answer is it has to be in the system design spec for the feedwater system, but the answer to your question is, I think, first we have an auto start of the feed pump, which would be disabled, and then we would have a select rod insert to reduce power.

MEMBER STETKAR: And, theoretically, the plant should stabilize at a reduced power with -- the pumps are nominally 33 percent pumps, so let's give them 40 percent.

MR. POPPEL: Twenty-five percent.

MEMBER STETKAR: Okay. So, the plant is going to stabilize at maybe 80 percent power, 90 percent power, somewhere in there. But the key is that the plant automation system will initiate select rod insert?

MR. POPPEL: Yes.

MEMBER STETKAR: Okay. Is that true?

MR. POPPEL: Well, the --

MEMBER STETKAR: Everybody is shaking their heads.

(Simultaneous speech.)

MEMBER STETKAR: This is a key point here, so I want to make sure that GEH agrees to this, because I couldn't find that anywhere in the design certification documents, so this is, honestly, a question. And I want to make sure that that's what will happen.

MR. MARQUINO: Yes. This is Wayne Marquino. I believe you brought this question up at a previous meeting we had --

MEMBER STETKAR: I don't remember, Wayne. I actually don't.

MR. MARQUINO: All right.

CHAIRMAN CORRADINI: I think you did.

MR. MARQUINO: But we should be clear on what functions are documented in the DCD versus what GE internally expects to put in the design, eventually, because I believe you're right in stating that there's no description of an SRI function, or SCRRI SRI function.

MEMBER STETKAR: SCRRI and SRI is all on --

MR. MARQUINO: That triggers on --

MEMBER STETKAR: It's all on ATWS in feedwater temperature in the DCD.

MR. MARQUINO: Right.

MEMBER STETKAR: I'm trying to understand the real plant in the real world, though.

MR. MARQUINO: Right. Now, going forward in the detailed design, Ira and I have had discussions about what we expect to put in the design as requirements as we get into detailed design, and that's what Ira is telling you.

MEMBER STETKAR: So, right now, best available information would be, if I'm in this configuration, if I have one feedwater pump out of service, and I trip one of the three running feedwater pumps, I would expect what I generically call a plant run-back, SCRRI, ER, whatever that is. And I'd stabilize at some reduced power level. Is that a reasonable presumption?

MR. MARQUINO: That's a reasonable presumption.

MEMBER STETKAR: Okay.

MR. MARQUINO: In terms of the actual survival of the plant, if you -- you said I tripped the feedwater pump, and the standby pump, which is intended to mitigate that event is out of service, so maybe the plant will scram, maybe it won't.

MEMBER STETKAR: I'm just thinking --

MR. MARQUINO: Because it's a challenge. I mean, it's a challenge to start with, and then you said I'm disabling this --

MEMBER STETKAR: I'm trying to understand the plant design and operation. I'm not trying to second guess stuff. Don't try to secondguess me yet, you'll get a chance to answer specific questions in a moment. I just wanted to make sure that I -- I didn't know how the plant automation system, because there's very little information, would work. And I just wanted to make sure that I wasn't presuming something different before I walk into this.

Now, in the reactor protection logic, there is a reactor trip from loss of voltage at two power generation buses, and that's called an anticipatory loss of feedwater trip. Why do I have that trip?

MR. POPPEL: If -- okay. The original concern was loss of all feedwater flow. We, actually, lost all feedwater flow, and we did not want that transient to get down to Level One, and turn on the safety systems. Okay? If we had done nothing about it, we're getting very close to that with the traditional Level Three scram. So, the talk turned to can we do something anticipatorily. Okay?

So, how would you measure loss of all feedwater flow? And we don't have any safety-related instrumentation on the feedwater nozzles, but for various other reasons on the independent -- anyway, we can monitor bus voltages pretty well. So if, in fact, we lose the 13.8 KV buses, we will certainly lose all feedwater flow. Okay? Absolutely. The reason it was -- that was chosen was because it's anticipatory, but if even just one feed pump remains on line, that's why it has to be all feedwater flow, one feed pump with 45 percent capacity will avoid the Level One concern.

Okay? So, that was the reasoning behind it.

MEMBER STETKAR: Ira, is the logic loss of four power generation buses, or is it loss of any two power generation buses?

MR. POPPEL: As of now, it's any two.

MEMBER STETKAR: Ahh, that's, basically, what I read in the words. I couldn't confirm that in the nice logic diagrams, except it looked from the logic diagrams, so the logic diagrams were sort of nice, because they were kind of consistent with the words. But that doesn't seem to be consistent with the plant design, because if I trip two feedwater pumps, I don't get this nice anticipatory loss of feedwater thing, but if I trip two electrical buses, I do?

MR. POPPEL: If you trip two feedwater pumps, by definition, you have at least one remaining.

MEMBER STETKAR: I had two in my example. I had two feedwater pumps remaining. I tripped one, and one was out of service.

MR. POPPEL: Okay.

MEMBER STETKAR: I reduced feedwater flow to 70 percent, you said 90 percent of what it was before this feedwater pump tripped. If I trip the electrical bus for the feedwater pump that was out of service, and any one of the three remaining electrical buses, the plant doesn't know the difference in terms of feedwater flow. It doesn't know the difference.

Why in one case do I scram the reactor as an anticipatory loss of feedwater flow from loss of power to two, and only two feedwater pumps, and in the other case, the plant actually just remains operating at power per the plant design. Why does that happen? It seems inconsistent to me.

If I were a reviewer, I would be asking questions about, is the plant protection design consistent with the integrated plant control system, consistent with the design criteria for what you're trying to protect against, which you mentioned is a loss of all feedwater flow, not just a 10 or 15 percent reduction in feedwater flow. I don't see any review questions being asked right now at that level. You get those review questions when you have that integrated logic in front of you, and you can start thinking about coincidences between protection controls, and safeguards actuation.

So, if you have a good explanation of why losing the electric power to the same two feedwater pumps I decided to trip because of a mechanical problem in maintenance, why those give you wildly different plant responses, I'm interested in learning about.

MR. MARQUINO: I can answer the first part of your question. The reason the safety logic has this feature is to allow us to credit a scram in the design basis accident scenario where we're required to assume that we lose offsite power, and we lose feedwater.

MEMBER STETKAR: Okay.

MR. MARQUINO: So, then we looked at -- we want to be able to credit a scram in that event, but we don't want to scram if we lose a feedwater pump in normal operation. So, that's the reason the statements in the DCD are what they are.

MEMBER STETKAR: So, it's in the -- I'm going to be silent.

CHAIRMAN CORRADINI: I guess I heard your answer. Can you say it again, because I don't think I appreciated the answer. John may have got it, but can you try it again one more time.

MR. MARQUINO: So, the feature that's in the safety system to initiate a scram, if you have a loss of two out of four bus power to the feedwater system is to allow us to credit that in the design basis logo. In that event, you would get the scram, and the reason it's two out of four is to prevent the scram from occurring if we have an operational event, which we can survive.

CHAIRMAN CORRADINI: Okay. Thank you.

MEMBER STETKAR: But you can survive the operational event with loss of only two buses. Unless there was something originally I -- you can't, with the current logic, you can't --

MR. MARQUINO: Okay. What you're saying is, if we have 90 percent feedwater capacity, and I think Ira will back me up on this math, and then we have a SCRRI that reduces, a SCRRI SRI that reduces power to around 50 or 60 percent, at least, we could probably survive -- we could survive this event you're postulating, which is when one pump is out of service, and --

MEMBER STETKAR: Reduction of feedwater flow to two pumps, basically, however you get there. However you get there.

MR. MARQUINO: So, yes, maybe we --

MEMBER STETKAR: Part of this is simply, I don't have a particular concern about this one. In fact, it was just something that I thought about that would integrate the normal plant control system, whatever you call it, the plant automation system, and the protection and safeguards system where everybody thinks about that in the context of design basis licensing accidents. Your answer was you needed to take credit for that scram, because you have to assume a loss of power for your design basis accident analysis.

Putting scram signals into a plant that might not actually protect you against the things you want to protect against, or that might introduce inadvertent scrams for conditions that you don't need to scram, simply because they're a convenient way of meeting design basis licensing analysis requirements might be questioned in a review. For example, you mentioned well, you could monitor bus voltage easily, you didn't want to put safety-related flow sensors in the feedwater lines. Safety-related flow sensors in the feedwater lines would give me an unambiguous indication of the fact I don't have enough feedwater flow that's survivable, so I'd better scram the reactor in anticipation of not reaching Level One, or something like that. But you didn't want to put the levels in, the flow sensors in. From a review, you might want to ask is that alternative a better protection?

I had difficulty even dreaming up this

little exercise. The logic diagrams that we haven't officially seen help me, but I didn't even have the logic diagrams to show me the plant automation system, or even the general architecture, what it might do, so that's why I had to ask the question first about the run-back stuff.

MR. MARQUINO: So, your point --

MEMBER STETKAR: I'm not -- my point being --

CHAIRMAN CORRADINI: I think I get your point. Let me say it a different way. Your point is that you think the logic diagrams give you an insight into how control, safety, and safeguard interact, even though they might be meeting the criteria, if I had that there I might ask penetrating questions about how I'm meeting the criteria, and how I might be generating, let's say in this case, unnecessary scrams.

MEMBER STETKAR: This seems to generate an unnecessary scram.

CHAIRMAN CORRADINI: That's what I wanted to make sure.

MEMBER STETKAR: And it doesn't, necessarily, always protect you against the loss of feedwater flow. Eventually, the Level Three scram will get you, if you don't have enough feedwater flow. But it's not clear what the loss of two, and only two buses, loss of three buses, loss of four buses might satisfy everything.

CHAIRMAN CORRADINI: Okay.

MEMBER STETKAR: You follow me? It was simply an example to show -- I've been a strong advocate, as you all know, of getting the logic diagrams into the DCD, and that -- the purpose of that is allow reviewers to have that information available at that level, at the same level as a PNID, a piping diagram that shows check valves and normally open motor-operated valves, and so forth, so that you can look at that in an integrated perspective, and at least think about it, rather than down to minutia of compliance with specific elements of a design standard, like this thing. That's all I'm going to say.

CHAIRMAN CORRADINI: Okay. Charles?

MEMBER BROWN: I have one other question that I forgot to ask, if that's okay. It's not a long question. The watchdog timers that you showed in your cycle, program cycle architecture layout, there's a -- for the reactor trip and nuclear monitoring system, you point out that those watchdog timers, if they time out, process a channel trip, and an alarm while the processor or logic function is resetting. So, I presume what they're doing is they're sending a boot-up again signal to the processor at the same time it's initiating a single trip out of four. And that that information would be sent to all the other three divisions, like any other trip signal. Is that correct? What is the time associate with a restart, a reboot, reset, whatever you want to call it on one of the processors?

MR. POPPEL: We'll have to take the question.

MR. BUTLER: We can get an answer for that. We don't have that --

CHAIRMAN CORRADINI: Say it again, so I capture it. I'm sorry.

MEMBER BROWN: Okay. Well, the watchdog timers that you saw in that program cycle architecture -- oh, they got it back. If you exceed the time and the timer trips for the RTIF and NMS, the Nuclear Monitoring System, those timers go back and they reset that logic processor. In other words, it sends a pulse, whatever you want to call it, says start -- it's like rebooting your computer. And, at the same time, it issues a channel trip, and an alarm. Correct me if I say something wrong, because I'm -- now, I guess my question was, how long does it take to bring a processor back?

CHAIRMAN CORRADINI: They'll come back and give us an answer.

MEMBER BROWN: And they'll get back to that. And the reason for my question is, if you want to know why am I asking this nitwit question, is -- I mean, everybody is familiar with when you hit a reboot on your computer, it takes five minutes before you can do anything. I picked a number, three minutes.

DR. WALLIS: It depends on the computer.

MEMBER BROWN: Exactly, it depends.

(Off the record comment.)

MEMBER BROWN: And one of the points a long time ago when we first doing this stuff in our program, 22 years ago, as a matter -- no, 32 years ago, excuse me, was what do you do if you have a processor all of a sudden blurp, and it needs to restart, how long before operators see anything? And when you started watching screens come up, and it took three or four minutes, you decided very rapidly that wasn't very good for operators. This was on display-type stuff. The point being is, it ought to be quick, and that's just what I'm -- there's a second part to this.

CHAIRMAN CORRADINI: Okay.

MEMBER BROWN: The second part to this is in the very unlikely based on our earlier conversation of corrupting all the --

MR. BUTLER: Those layers.

MEMBER BROWN: All those voting functions at the same time, now I have 16 processors all going into the reset mode. What is -- and I'm now getting all my things -- there's no trip logic, because it's not functional because the processors aren't processing, so the plant just sits there during this period, I would presume. You get the alarms, but that's it. So, would the reactor actually scram in that period of time while they're -- that's the other point is how long they take to reboot. Would it actually scram in that period of time, or would it not?

MR. POPPEL: Yes. It's like -- because you use the statement all of the processors and stuff like that -- if you do it the way -- for example, if a two out of four processor in DTM broke, and all the DTM broke, there's no particular reason that would affect anything downstream.

MEMBER BROWN: Well, the TLU is in there, also. Right? Okay.

MR. POPPEL: But it's a different set of two out of four stuff.

MEMBER BROWN: Yes.

MR. POPPEL: But my point was -- and it's a different watchdog timer. So, the first thing that'll happen is for any of these events that -- any of these incredible events that might be credible is, it will scram. Okay? Because if you have four DTMs out, or four TLUs out, and anything downstream was still functioning, it'll scram.

The second thing is we're -- the reset of those processors per 603 is not allowed to reset the scram. The scram is there. The operator has to --

MEMBER BROWN: No, that's the operable.

MR. POPPEL: The operator has to reset the scram.

MEMBER BROWN: That's fine. This just says it issues a channel trip. A channel trip can reset, but a scram -- if they all -- there is no vote in this case, so my point being is if you issued the -- it issues a channel trip, but what does it issue it to? I mean, is that a -- I guess I lost the bubble when we were looking at one of the previous diagrams. The DTM is a processor, and the TLU is a separate processor in that --

MR. POPPEL: Yes, and a separate chassis.

MEMBER BROWN: Okay. I was going back to the even higher level one, where you -- there was a higher level picture, but that's fine. So, they are separate. Okay. So, the TLUs — the DTMs would actually be the relevant -- it would issue a trip to the TLUs. Is that correct?

MR. POPPEL: Yes.

MEMBER BROWN: And I'm not talking about corrupting all the DTMs, because I'm not communicating with those.

MR. POPPEL: They wouldn't issue a trip. The lack of communication would be received as a trip by the receiving thing. So, in other words, we're not saying hey, broken thing, send a trip. The receiving thing is saying I'm not hearing from you. I, therefore, assume you tripped.

MEMBER BROWN: Okay. Now, the DTMs are not exchanging trip data with all the other divisions. It's just the TLUs that's doing that.

MR. POPPEL: No, it's doing it twice.

MEMBER BROWN: Both of those --

MR. POPPEL: That's why we have the TLU level, and it's happening at the DTM level. So, there two two out of four votes going on.

MEMBER BROWN: I'm just looking at Figure 7.2-1, and it does not show any other DTM-to-DTM communication. It only shows DTM-to-TLU communication. Okay? So, that's why --

CHAIRMAN CORRADINI: Is your question answered?

MEMBER BROWN: Well, it's the voting unit issue I'm talking about. Okay? If it got there, and all the voting units went out, there would be no trip issue. If they couldn't process --

MR. POPPEL: Well, when you say all -- okay.

MEMBER BROWN: If they got corrupted, they couldn't process, because that's where the logic function is.

MR. POPPEL: So, when you say that -- so, they got corrupted, but they're still sending no trip.

MEMBER BROWN: I don't know they're sending anything at all.

MR. POPPEL: Then they'll trip, because the next thing downstream --

MEMBER BROWN: So, the watchdog timer would not get struck, and it would do its thing. But where does it send its trip, to the load drivers, to the output logic unit?

MR. POPPEL: The actual -- yes, it's a chain, just like you just said. So, for example, if we go to the -- if you go to the load driver -- well, the backup sheet. Okay. The load driver is a smart switch. Okay? It's receiving four fibers. Okay? And it's expecting to hear that two out of four fibers have said trip. Okay? That's an active communication, it's not a one or a zero. So, the load drivers will say hey, two divisions aren't talking to me, trip. It's failsafe. So, what you have to postulate is this corruption is somehow letting the things go normally, and not tripping when they should trip, as opposed to -- but if they just shut down, you'll scram.

MEMBER BROWN: So, they --

MR. POPPEL: Everything downstream is — upstream of the thing that stopped sending, everything downstream will --

MEMBER BROWN: If the RPS load drivers are not being told to constantly stay on, absence of signal telling them to stay on, they will trip.

MR. POPPEL: Yes.

MEMBER BROWN: Okay. So, that's a reasonable answer that says -- my concern was, even though you're trying to convince me that this whole other scenario is unlikely, that if the TLUs all locked up, which was the basis for my discussion earlier --

MR. BUTLER: The postulated scenario.

MEMBER BROWN: Postulated scenario, the watchdog timer for the TLU would, based on this comment would say channel trip. Okay? And send an alarm, and it would try to reset. Now, you can't reset a scram, but if the TLU is not functioning, what does the watchdog timer tell to trip? Right now, I'm trying to figure out what the -- and it has to go -- somehow it's communicating with the load drivers, I guess.

MR. POPPEL: The load drivers trip and no trip are both actively transported data. So, in other words, you have to keep saying don't trip, and you send also trip. It's not like a relay where the absence of electricity, both ones and zeroes are actively transported so that no information can be determined, and, therefore, set a trip by whatever the downstream component is, wherever it's located in the chain. If the RMU loses power, then the DTM says every RMU signal is in trip. If the --

MEMBER BROWN: I don't want to work on the

RMU right now.

MR. POPPEL: Okay.

MEMBER BROWN: I'm trying to understand -- the watchdog timer can --

MR. BUTLER: If it infinitely fails to reset itself in the processing loop, what happens?

MEMBER BROWN: You've got a DTM, which is processor, it's got a watchdog timer on it with its program cycle. You've got a TLU with a watchdog timer, it's processor, and it's got its operating cycle. Obviously, they stack together for your overall timing budget, whatever it is. Okay? They're determinant, I'm going to take your word based on your operating loops, the main -- all that kind of stuff. Now, with the DTM, if it fails to process data, it sends out a trip. That trip would go to the TLU, I would presume. And, therefore, it's one out of the four -- it doesn't get anything from the other divisions, but the DTM can be reset, so it's trying to reset. You haven't scrammed, but you've got a momentary trip signal to a TLU in one division. Well, excuse me, the other three divisions, as well, so I'm one out of four in all three divisions. Now, the DTM resets. That will go away. You don't maintain that single trip in that one -- well, I presume it goes away. Is that correct?

MEMBER STETKAR: Manually reset?

MEMBER BROWN: No, it's not manual. I don't know, that's -- you have to reset everything to recover from a scram where all the rods go up, or down, or whichever way they go. So, that part I could envision what was going on. Maybe I'm wrong.

MR. POPPEL: If any one of those chassis restarts, it comes up as a trip, and the operator at the chassis level -- even if you just turn the power off, both powers off --

MEMBER BROWN: I don't want to --

MR. POPPEL: -- then turn it back on --

MEMBER BROWN: That's too hard.

MR. POPPEL: So, it was a trip, but the -- so, it comes up as a trip, and because it's like the operator has to go to the chassis if it's happened at the chassis --

MEMBER BROWN: He's got to go to the cabinet.

MR. POPPEL: Yes.

MEMBER BROWN: So, if a DTM exceeded its program cycle, didn't strobe the watchdog timer in time, the watchdog timer issues a trip. That's what this says, it trips -- issues a channel trip.

MR. POPPEL: Yes.

MEMBER BROWN: I'm working only on the DTM right now. Now, if it resets and it comes back up, that trip will stay there, and it will stay in all four divisions.

MR. POPPEL: Until the operator does something to --

MEMBER BROWN: Resets each division, resets that trip to that one -- to each TLU.

MR. POPPEL: I don't believe has to do it in the other divisions. He has to do it in the originating division.

CHAIRMAN CORRADINI: Charlie, are we -- do you have enough that we can move on?

MEMBER BROWN: No. That's why, if I can finish this. The DTM -- the TLU, if that watchdog timer goes, what does it -- does it function the same way? But what does it -- where does it issue a trip, to whom?

MR. POPPEL: The OLUs.

MEMBER BROWN: To the OLUs from the TLUs.

MR. POPPEL: Yes.

MEMBER BROWN: Okay. Now, the OLUs only get data -- only get information from its own channel, according to your other diagrams.

MR. POPPEL: Okay. Maybe there's too many diagrams, or maybe they're too simplified. This is an accurate representation, and you can see that an OLU gets data from --

MEMBER BROWN: Okay. To pick up with my -- well, I guess, what I'd like to see is an under -- I'd like to understand the operation and execution of watchdog timer timeouts, what they do, how they get reset, whatever, if we could get that.

MR. BUTLER: Okay.

MEMBER BROWN: Is that okay, Mike?

CHAIRMAN CORRADINI: Sure. I want to move on to the Staff before lunch.

MEMBER BROWN: That's fine.

CHAIRMAN CORRADINI: Thank you.

MR. BUTLER: Thank you.

CHAIRMAN CORRADINI: I want to hear the Staff.

MEMBER BROWN: Now, we'll be done when the Staff finishes. Right? Is that correct?

CHAIRMAN CORRADINI: Yes.

MEMBER BROWN: Okay.

(Off the record comment.)

CHAIRMAN CORRADINI: Go.

MR. GALVIN: It's still good morning.

MEMBER STETKAR: A more accurate description is just morning. It's not how good it is.

MR. GALVIN: Mike, we ready to go? Okay. The Staff is here to present their review of Chapter 7, Instrumentation Controls, and we're going to talk about the same topics. Ian, go ahead.

MR. JUNG: Okay. A little introduction remark. I appreciate the Committee for giving us the opportunity today. Staff hopes to fully support the needs of the Committee. My Staff's presentation is intended to address the issues of the Committee's interest expressed during earlier interactions, which we'll focus on four plus one issues.

I'd like to take this opportunity for a couple of minutes to provide the Committee an overview of what Staff efforts was about for Chapter 7. Staff's Chapter 7 SER is a result of the following big picture items, so the Committee understands what it took for the Staff to reach at this point.

It's been almost five years since original Revision 0 has been submitted. I had the -- close to 10 Staff members worked on this project, some of them on and off, some of them close to a full-time, for on and off in some period, but 2006, 7, 8 it was almost full-time for some people.

Looking back, we spent more than 15,000 hours for Chapter 7. It involved the multiple disk DCD revisions from Revision 0 to Revision 7, now we are looking at Revision 8 to make sure it does not impact the SAP finding. Not only that, in between certain revisions, Chapter 7 had the draft revisions in between. Chapter 5, for example -- Revision 5, for example, we have three revisions in draft to make sure the final Revision 6 coming in addressed the Staff concerns.

We issued about 300 RAIs on this project, not including many subsequent supplemental RAIs. We had a number of interactions with GEH through public meetings, closed meetings, and conference calls, significant engagement with other Chapter areas. You realize that we cannot work in silo, we have to work with the Chapter 15 Accident Analysis, and the Chapter 3 EQ, Chapter 6 on ECCS systems, and Chapter 11, 10, Chapter 6 in tech specs, Chapter 18, RTNSS and PRAs insights. We all recognize this area is complex, resource-intensive, and challenging technical discipline from a digital perspective, but also from a traditional reactor review perspective.

Staff's goal is to reach the conclusion

that the design is safe from sensors to actuators for various safety and other important safety systems for the whole facility, and complies with the applicable regulatory requirements, and continues to promote standardization that Part 52 intended. At the licensing basis FSAR level of detail, we concluded that we have reached the goal.

My Staff and I will try to address your questions today to the best we can. If we don't, we'll work with you and respond to you as fast as we can.

With that, I'd like to turn it over to my two senior staff members, Hulbert Li on my far right, and Dinesh Taneja, my senior staff. Okay, Hulbert.

MR. LI: Good morning. My name is Hulbert Li. I'm one of the reviewers for ESBWR I&C design. The staff evaluated safety of the I&C design according to the Commission's regulations by following the standard review plan. And we used the design control document, DCD Tier 1 and Tier 2 information to make our safety determination. And we document our review in SER.

In Chapter 7.1, we addressed some critical issues for the overall safety of the I&C system, that including the conformance to the regulations, the software development activities, the diversity and defense-in-depth, the set for methodology, and data communication, and secure development, and operational environments. And those are the critical issues we addressed and document in 7.1. Next page, please.

Next, 7.2 through 7.8, basically, we follow standard review plan, and addressed every concern, and list in the standard review plan. So, the -- for the time concern, we elect next introduce Dinesh to discuss the evaluation of the I&C design principles. That's the meat of today's discussion.

MR. TANEJA: Thanks, Hulbert. Good morning. My name is Dinesh Taneja, and I'm going to be presenting our evaluation of some of the key technical areas that relate to the I&C system design in the ESBWR.

In general, Staff finds the ESBWR I&C design to be safe. That was our determination. And we found that the I&C design employs the four safe design principles that GE has discussed earlier this morning; namely, the independence, determinism, redundancy, and risk beyond defense-in-depth. And the safety-related I&C systems are designed with the concept of simplicity in many aspects. In the next few slides, I'll go over the basis for our findings in these technical areas.

The Staff also found ESBWR I&C design to be in conformance with all applicable regulations. Next slide, please.

One of the key technical areas of digital I&C deals with the maintaining the data communication independence. And we are very familiar with independence, with the non-traditional, and the traditional I&C systems. The challenge that we face in the digital I&C area is maintaining the independence and data communication area.

The Staff found that the I&C system design provided sufficient independence and compliance with the regulations, specifically, IEEE-603 and GDC-21. The safety-related platforms are organized into four physically separated and electrically isolated divisions. And the communication independence is achieved by multiple different ways. And simple things that we saw that were useful for our decision making process was that the inter-divisional data communication and safety-related system is limited, and it's only limited to the voting logic, bypass and data authentication. And, also, the inter-divisional data communication in the RTIF and NMS platform is point-to-point, unidirectional, and wire optical fibers.

And the point that we were discussing earlier, the faulty or loss of data in communication interpret it as a trip signal, and it carries all the way through. That's what we understood it to be. It's a failsafe design. The inter-divisional data communication in the SSLC and the ESF platform uses redundant ethernet network with two out of four voting logic, networks are doubly buffered to prevent data corruption to adversely impact both networks at the same time. Next slide, please.

The ICP platforms, they do not use any multiplexing or data communication. All the Ios are hard wired, so there was really no concern there for the issues of data communication. And, also, the data communication from the safety to non-safety systems is all unidirectional. So, any failure in a division does not prevent the other redundant safety divisions from performing their intended functions, such supporting that in a concept of taking a single failure and continuing to perform its safety function.

Diverse and independent, diverse protection system is provided as a defense-in-depth feature to cope with the unlikely scenario of a primary system malfunction. Example would be common cause failures of software which are beyond design basis, or multiple independent failures. Next slide, please.

The determinism is the other issue with the digital I&C areas, how deterministic, are we getting our things done? And we reviewed this thing with this definition in mind. Basically, our understanding is, determinism means that a required safety function is always accomplished within the required time period specified by Chapter 15, DB Analysis. That is how we viewed the determinism.

So, based on the following, the Staff found that the real high performance of the safety-related I&C systems deterministic, and its conformance with BTP-21 and IEEE-603. The two DCIS data communication protocols are deterministic. The RTIF-NMS platform performed a cyclic realtime execution. The operating system is clock-driven and not event-driven, and it does not incorporate any interrupts.

Similarly, the SSLC/ESF platform also runs cyclical programs that include both the application and diagnostics, and do not incorporate interrupts. The ICP platforms always -- they do not have any operating system, so that was not the concern there. So, all platforms always react in the same way according to the order of events occurring at the point and time of the plant conditions.

In the areas of redundancies, it's very well understood, I think we saw what GE presented this morning, we have four divisions of RTIF, you have four division SSLCs, we have four divisions ICP. They're physically separated, they're totally redundant, different areas. And even the DPS utilizes two out of four voting logic.

And the other thing that we also found in our review was that each division has its own set of sensors, and no sharing of sensors between safety division is allowed. Next slide, please.

The RTIF-NMS platforms use dual redundant communication, inter-divisional data communication. And the SSLC/ESF platforms use doubly buffered redundant networks for two out of four voting logic. Now, within each SSLC/ESF division, there are DMR controllers used for high reliability. And even the non-safety NDCS platforms use double or triple redundant controllers for high reliability, and availability. So, therefore, less challenges to the safety systems. Next slide, please.

The diversity and defense-in-depth, this review really focused on the basic regulatory requirement of ATWS. The ATWS system, essentially, is diverse from the primary system. The ICS is there, used for the SSLC, standby liquid control, SLC. There are too many acronyms here. The standby liquid -- the boron injection is done by the independent platform. Okay? And then the alternate rod injection is done by the DPS system.

The I&C systems also provide diverse backup for RTIF-NMS, and SSLC/ESF to address software common cause failure concerns. And this is in accordance with the SRM to SECY 93-87.

The LTR on diversity and defense-in-depth that was provided, that whole analysis was done following the guidance of BTP-19, which Staff concurred with. And the diverse protection system is designed based on different technology, different equipment, design personnel, different signal sets, and functional diversities. The diversity is also provided within Q-DCIS. There are three different platforms within Q-DCIS, and externally with non-safety-related DPS system.

The DSP system is classified as RTNSS, and is developed by a rigorous, highly structured process similar to the ones used for safety systems.

In the area of simplicity, I think the key thing that we saw was the ESBWR design was very simple for us to review, because it did not really do a lot of mingling of data communication between this and that. Q-DCIS division is independently monitored and controlled. Each division from its dedicated redundant set of VDUs. We really didn't have the concern about any communication occurring from one to the other.

We found the safety-related components cannot be controlled for any non-safety-related media use. The data communication from safety to non-safety I&C system was unidirectional, and the I&C system design meets independent isolation and separation requirement.

The inter and intra-divisional communication is very limited. We talked about the amount of data that gets transmitted there. And the passive nature of the ESBWR plant has very limited safety-related ESF functions, as compared to the active plants. And the other thing is, the maintenance tool is not continuously connected. You have to open the cabinets, and go and hook up the tools to do any work. They're not left there, so that keeps a simple design very simple.

In the area of the logic diagram, I think this concern, we took back and we looked the DCD, and we found that the DCD contains adequate control logic design information for the Staff to make a reasonable safety assurance finding. Information that's described in the DCD will be used to develop the logic diagrams, so that becomes the design basis for developing the detailed logic diagrams. And the logic diagrams are produced used during the I&C development life cycle process. And we anticipate that they will get finalized as the life cycle process progresses through its various life cycle stages.

So, in conclusion, I guess Staff has really concluded safety of the I&C system design and finds the design to be safe. That's what our evaluation has concluded. And the I&C systems are in conformance with the applicable regulatory requirements, and the I&C implementation DAC and ITAAC that are provided in TRM are acceptable.

We have also looked at the, I guess not in depth, but we have looked at the Rev. 8 material, and so far what we see, it just provides clarity of the I&C design information, has no impact on the I&C design, itself, and has no impact on our safety findings.

MEMBER ADBEL-KHALIK: Were these slides prepared prior to receipt of this new information from the applicant?

MR. TANEJA: These slides were prepared -- the new information that we received was just a couple of days ago.

MEMBER ADBEL-KHALIK: Okay.

MR. TANEJA: So, we had the chance to just browse through it. And our initial review, basically, when we went through the whole thing, it was the information that we already knew. We found within the DCD discussing various different areas, so we concluded that information was better presented in a more concise manner. The ITAACs that they've added, those ITAACs were implied in the DACs and ITAACs that were already there. So, they, essentially, took the ACRS comments, and they tried to enhance that, their DCD material.

MEMBER ADBEL-KHALIK: I'm just trying to get to the bottom of this third bullet in view of the changes that were proposed by the applicant. So, you don't think — the changes provided by the applicant do not add value.

MR. JUNG: I think we've engaged, obviously, this is the ACRS letter and interactions, and the previous transcripts have been communicated to GEH, so we've been engaged the last several weeks with

GEH. But the bottom line is that the information they have provided adds additional clarification; yet, is helpful. It's helpful from the sense of those who are now familiar with -- who are not involved in detailed design review, they could interpret that more clearly. For example, inspectors in the future looking at the ITAAC DAC, when they start inspecting against the DCD, they'll be able to better see oh, this is what it was, compared to Revision 7. It's clearly a plus, we felt this as a clarification, additional clarity. However, it did not pose a new safety question that we need to address in our overall safety finding.

MEMBER ADBEL-KHALIK: Thank you.

MEMBER BROWN: I guess I would -- I'm going to springboard off of Said's comment. I mean, I went back, and I did look at the Rev. 7 Tier 1 document, which was more extensive than what was in Rev. 5, which was what I had previously, or even in Rev. -- I won't speak to Rev. 6. I think it was more than in Rev. 6, as well. And just a very quick look at the examples they gave from the design commitment through the description, and into the acceptance criteria, and I haven't looked at them all yet, which I will go do, since I have Rev. 8 markup stuff here for that. And I presume it includes the Tier 1 information, as well, on the CD. Provides a much more clear -- you say it was implicit in the other ones. You would have had to have been a monk looking at this stuff for 1,000 years to figure out that this stuff was implicit. Okay? I'm saying that with a little bit of tongue in cheek, but we have to be lighthearted at some times.

CHAIRMAN CORRADINI: I enjoyed your stork dance before, too.

MEMBER BROWN: Oh, you did? Well, it's like sucking blood out of rocks sometimes, Mike, to get information, but the information provided here provides a much clearer view of how somebody intends to do something, as opposed to saying a report will be issued that complies with our SQAP, or our blah, blah, blah, whatever other of the Alphabet soup that you throw in there for -- it was all process. Everything was going to be okay because of process, there was no technical information identifying what were the technical design attributes that you were trying to meet that are critical to what I call the four fundamentals of making sure this stuff is satisfactory. So, I would disagree with you, if you said the stuff in Rev. 7 or Rev. 6 was acceptable. I would have answered that no. I haven't looked at all this yet, but it, obviously, provides a lot more technical meat, or at least the examples they pulled out, the example had technical meat in them, and provides a much better feeling that yes, there's something cast in concrete which somebody has to meet, which now gives somebody something to review against, and gives somebody like us, who are looking at it at a certain level, some comfort that there's some real technical design issues that people are going to -- which address things you don't want to do in these systems.

MR. TANEJA: Mr. Brown, I agree with you. I agree with your assessment that it does --

MEMBER BROWN: That's not what was on your slide.

MR. TANEJA: -- present this information in a much clearer fashion. I think what's on my slide is saying that -- see --

MS. CUBBAGE: Well, maybe I could say, I think the slide is reflecting what you said. It's that it does provide clarity. We welcome the change, but it doesn't impact our safety finding.

MEMBER BROWN: No, I don't disagree with that.

MS. CUBBAGE: It didn't introduce any new -- okay.

MEMBER BROWN: I understand your comment on that. It's just that the DAC, which is where a good bit of our concern has been focused, whatever the design is, there was nothing implicit that I could find. I mean, I could drag my way through key word after key word search and couldn't even find a mention of any of these in any of the DAC. It's because they weren't. It was all referencing process documents. We're going to do it in accordance with our process documents, and, therefore, it'll be okay. And that's unsettling in some circumstances, in other words. It's fine.

MR. TANEJA: Regarding --

MEMBER BROWN: I'll stop.

MR. TANEJA: I just want to --

CHAIRMAN CORRADINI: Before we start commenting on each other, I want to make sure I get the Committee to ask others that have questions. John.

MEMBER STETKAR: I would have said something, if I was going to.

CHAIRMAN CORRADINI: All right. I'm sorry, Charlie. I didn't mean to -- did you have a -- there was -- you guys are commenting on your comments, but I want to make sure --

MEMBER BROWN: No, I just wanted to springboard off of Said's comment. I thought that that was a good lead-in, because this was prepared before they got the Rev. 8 stuff.

MS. CUBBAGE: Actually, these slides were prepared last night.

MEMBER BROWN: Oh, they were?

MS. CUBBAGE: Yes. The Staff has been looking at the information in great detail that was provided.

MEMBER BROWN: Okay. It said that based on the Rev. 8 stuff, now we find the Tier 1 stuff acceptable, instead of saying it's implicit. It was all there before when --

CHAIRMAN CORRADINI: Well, I think Amy's --

MS. CUBBAGE: At the end of the day, Rev. 8 is what will be certified, and we are pleased with it.

MEMBER BROWN: Okay.

MR. GALVIN: We've had extensive discussions with GE about how they're going to implement the August 9th letter. I mean, this is -- we weren't surprised what came in Rev. 8. What came in is what we expected to come in, because we've been talking about it for the last month.

MEMBER BROWN: Okay. All right. Thank you.

MR. GALVIN: That's sort of what we meant to say.

CHAIRMAN CORRADINI: So, other questions for this group? Don't go anywhere, but any questions for this group in front of us? I want to turn back. Did you guys get some clarification that we can answer Charlie's question, or are you still in the clarification mode?

MR. BUTLER: If it's okay, this is Skip Butler, if it's okay, we'll get back on Monday, if that's acceptable.

CHAIRMAN CORRADINI: That's fine.

MEMBER BROWN: Monday, Tuesday, Wednesday? I mean, I just -- as long as --

CHAIRMAN CORRADINI: Okay. But I just want to make sure --

MEMBER BROWN: I just wanted a more detailed discussion of what watchdog timers do, and how do they execute the functions they're supposed to be doing.

CHAIRMAN CORRADINI: And the timing part of it, too. You had --

MEMBER BROWN: And the timing part of the execution of the watchdog timers, yes.

CHAIRMAN CORRADINI: Okay.

MR. BUTLER: Right.

CHAIRMAN CORRADINI: Okay. Good. I don't think there's any other more open items that we haven't answered. We've gotten all that, so I will just go through everybody today relative to Chapter 7. Dr. Kress, you enjoyed it immensely, I could tell, but I --

DR. KRESS: I enjoyed it immensely. It's not my area. I have no comments.

CHAIRMAN CORRADINI: Okay.

DR. WALLIS: Yes, I felt I learned a lot, but, again, I defer to the experts like Charlie to ask the real questions.

MEMBER STETKAR: I think that the discussion was very, very useful. Thanks a lot to GEH for the effort you put into the responditory part. I remain personally concerned about a different level of the review. In some sense, it has nothing to do with the fact that this is digital, it could be analog, it could be knife switches, for all I'm concerned. It's more of the level of depth of the review of the functional logic, and how that's integrated into the rest of the plant control system. The example that I mentioned before.

CHAIRMAN CORRADINI: I understand. You're welcome to help me try to capture that, but I think I can capture that.

MEMBER STETKAR: Okay.

MEMBER ADBEL-KHALIK: Again, I'd like to thank GE for really a very informative presentation. Thank you. I have no additional comments.

MEMBER BROWN: Yes, I just wanted to say the same thing. I thought they did a very good job of -- much more thorough than we had seen before in any circumstance. And it answered many, many, many, many questions, and was much appreciated with the level of detail, and your tenacity with putting up with my repeated request for clarifying slightly more. So, thank you.

MR. BUTLER: Well, this is Skip speaking. We'd like to thank the Staff and the ACRS, and particularly Charlie for being tenacious.

CHAIRMAN CORRADINI: Okay. Now, that we're thanking everybody. So, let me --

MEMBER BROWN: It sounds like a Congressional committee.

CHAIRMAN CORRADINI: Let me just remind you of the path forward. Yes, we're getting that way. Wait until we get video on site, and then you can be even more eloquacious.

All right. So, I want to thank GE and Staff for doing this. We're kind of at the end. This is our second to last Subcommittee meeting. The last Subcommittee meeting will be on October 6^{th}, where we will be discussing aircraft impact, and the final and enjoyable parts of the PCCS relative to hydrogen control. Okay? Which you all now have a CD, so you can't claim you don't have it. You also all have a CD which is the Tier 1/Tier 2 -- it's in two parts. There's actually two files that you have on that CD that are both Tier 1 and Tier 2. And, unfortunately, Tier 2 is first, and enclosure 2 is Tier 1, but it's there on your CD. So, that's going to be the last Subcommittee meeting.

Let me remind everybody that for that Subcommittee meeting, all members and consultants, if they want to look at the details of the Aircraft Impact Assessment, that will be the day before open by procedures that Kathy and Chris will tell you about, but the day before will be available here, which is August 5^{th}, as we all will be here anyway, because --

MEMBER BROWN: October what?

CHAIRMAN CORRADINI: October 5^{th}. What did I say? I'm sorry, excuse me, October 5^{th}, as we will all be here anyway for AP1000, and the joys of GSI-

191. Okay? So, I think that's the schedule going in, and we're looking forward to trying to produce a --

DR. WALLIS: Is this stuff available?

MEMBER STETKAR: It's available, but only --

CHAIRMAN CORRADINI: Only that day --

MEMBER STETKAR: You have to be physically here.

CHAIRMAN CORRADINI: Physically here. You can talk to Kathy and Chris, and they'll give you the details, the protocol. Thank you.

MEMBER BROWN: Okay.

CHAIRMAN CORRADINI: Other than that, I'll thank everybody again. I truly do think GEH, I think, it was very informative. I think it took me only four years, but I think I got it relative to the differences in, shall we say, views on things, but I think it was very informative relative to the digital I&C.

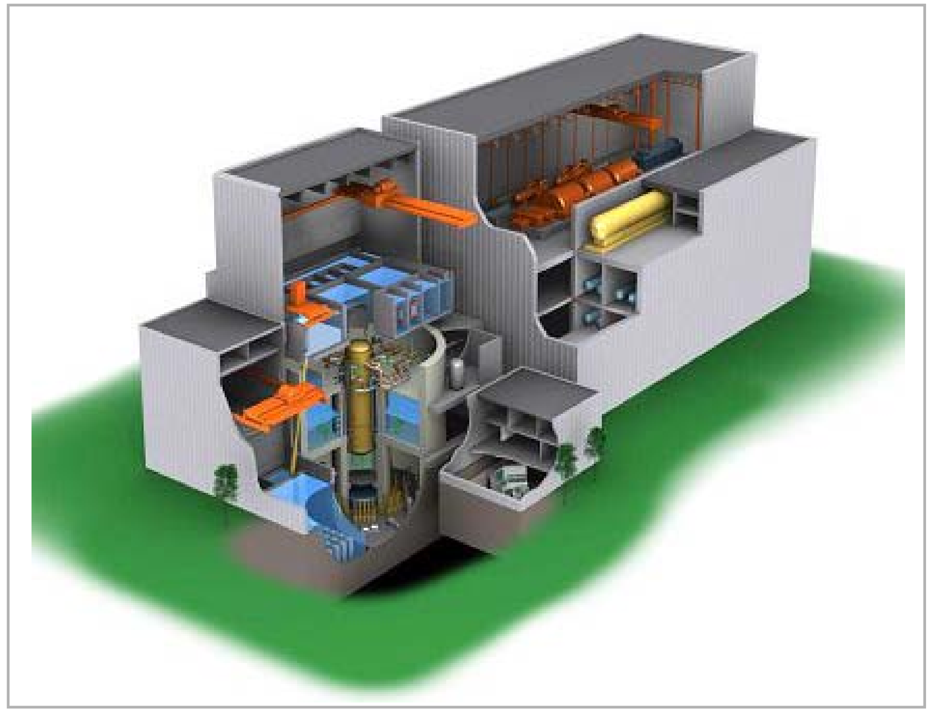
With that, I think we're adjourned.

(Whereupon, the proceedings went off the record at 12:26 p.m.)

GEH Nuclear Energy

ESBWR Design Certification
Chapter 7 I&C

Advisory Committee on Reactor Safeguards



Skip Butler
Ira Poppel
Romeo El Daccache

September 24, 2010

HITACHI

Topics

- **Changes from Rev 6 to Rev 8**
- **ACRS Letter on DAC dated August 9th, 2010**
- **GEH Response to ACRS's Letter**
  - Tier 2 – Additional Design Descriptions
  - Tier 1 – Additional ITAACs
- **"4+1" Design Principles**
  - Independence with Deep Dive into SSLC/ESF
  - Determinism with Deep Dive into SSLC/ESF
  - Redundancy
  - Diversity (D3)
  - Simplicity
- **Logic Diagrams – Implementation Design Artifacts**
- **Backup Slides**

HITACHI

Changes from Rev 6 to Rev 8

	Source	Rev 7	Rev 8	Total	Comment
NRC Driven	**RAIs**	**7**	**1**	**8**	**Included in Rev. 7 and Rev. 8**
	Chapter 7	3	0	3	Setpoint Methodology (7.1-141), Digital Devices in LTRs (7.1-142), and GDCS eq. valves open at RPV Level 0.5 after sustained Level 1 (7.3-18)
	Other Chapters	4	1	5	RAI 6.2-202 S01
	Unresolved	**0**	**1**	**1**	
	ACRS's letter to the NRC dated 9 August 2010 on "Closure of Design Acceptance Criteria for New Reactors"				
GEH Driven	**ECAs**	**10**	**6**	**16**	
	I&C driven	0	0	0	
	I&C impacted	1	3	4	Added 4th ICP function and 1 DPS function for ICS DPV Isolation
	I&C not impacted	9	3	12	
	CARs	**1**	**2**	**3**	Self-Identification; 2 for Consistency, 1 for ACRS Letter

Added one ICP (the 4th)... ICS DPV Isolation Function (IDIF)

No change to overall ESBWR I&C and DCIS architecture and design

ACRS's Letter to NRC dated 9 August 2010...

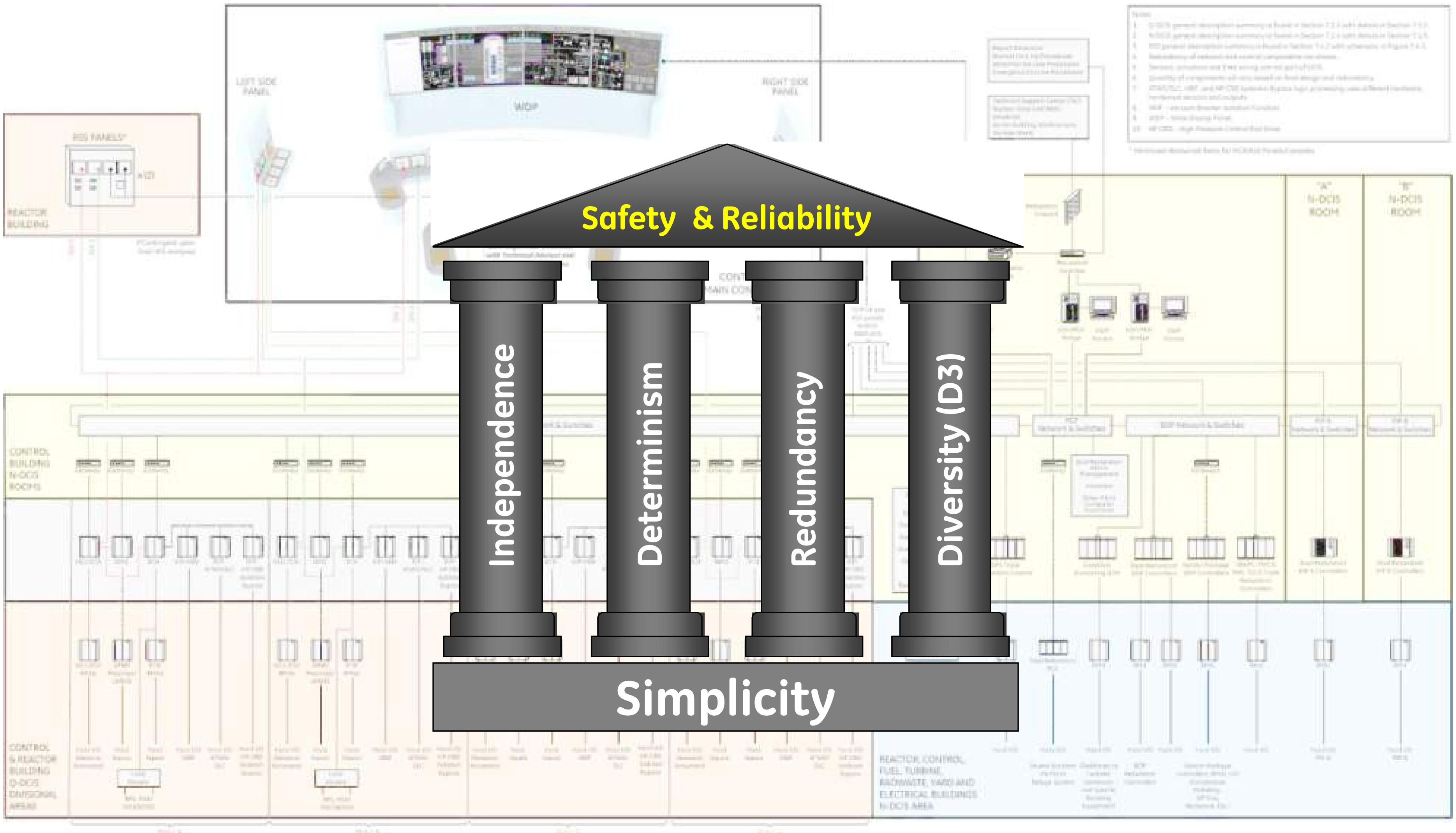
Closure of Design Acceptance Criteria for New Reactors

"The fundamental reliability of DI&C systems is based on four essential objective design principles – **redundancy**, **independence**, **determinant data processing communications**, and **defense-in-depth and diversity** – and one subjective attribute, **simplicity**. The logic and hierarchy of DI&C designs are well established, as are the individuals digital component technologies for implementing these functional system designs. Thus, the design of **DI&C systems can be functionally specified and shown to meet the essential criteria** regardless of the parts technology (digital and analog electronic components) used in developing the designs of the hardware assemblies and sub-assemblies."

ACRS's 4 Design Principles + 1 Attribute of Simplicity ("4+1") represent...
Clear commitment to IEEE Std. 603... "Robust" Engineering philosophy

HITACHI

GEH Responds to ACRS's Letter



Based on IEEE Std 603

Criteria for Safety Systems for Nuclear Power Generating Stations

HITACHI

GEH's Additional Design Descriptions... Tier 2

Align Existing Information plus Additional Features :

- For each of **4 ACRS Design Principles**
  - Independence
  - Determinancy
  - Redundancy
  - Diversity
- Provide features **by Q-DCIS Platform**
  - RTIF-NMS
  - SSLC/ESF
  - ICP
- **Simplicity** (as consolidated discussion)
- **DPS** (as standalone discussion)

Addressed ACRS "4+1" Design Principles with No Design Changes...
ESBWR DI&C is Modular, Robust and Compliant with IEEE Std. 603

GEH's Additional Design Description Specifics… Tier 2

7.1.2.1.1 Independence Design Principle **(~7 Pages added)**
7.1.2.1.1.1 RTIF-NMS Independence Design Principle
7.1.2.1.1.2 SSLC/ESF Independence Design Principle
7.1.2.1.1.3 ICP Independence Design Principle

7.1.2.1.2 "Determinism" Design Principle **(~6 Pages added)**
7.1.2.1.2.1 RTIF-NMS Determinism Design Principle
7.1.2.1.2.2 SSLC/ESF Determinism Design Principle
7.1.2.1.2.3 ICP Determinism Design Principle

7.1.2.1.3 Redundancy Design Principle **(~3 Pages added)**
7.1.2.1.3.1 RTIF-NMS Redundancy Design Principle
7.1.2.1.3.2 SSCL/ESF Redundancy Design Principle
7.1.2.1.3.3 ICP Redundancy Design Principle

7.1.2.1.4 Defense in Depth and Diversity (D3) Design Principle **(~2 Pages added)**
7.1.2.1.4.1 RTIF-NMS D3 Design Principle
7.1.2.1.4.2 SSLC/ESF D3 Design Principle
7.1.2.1.4.3 ICP D3 Design Principle

7.1.2.1.5 Simplicity Design Principle and Subjective Attribute **(~2 Pages added)**

7.8.1 DPS System Description **(~3 Pages added)**

~23 Pages Added – Combination of…
Repackaging Existing plus New Details of Features to support ITAACs

HITACHI

GEH's Additional ITAACs... Tier 1

3 Enhancements to Sec. and Tables 2.2.15 I&C Compliance with IEEE Std. 603 :

INDEPENDENCE (1) :

- **Item 11 (Modified) : Criteria 5.6, Independence and Criteria 6.3, Interactions Between Sense Command Features and Other Systems**

  Note (7) : Data communications between the diverse Q-DCIS platforms is itself diverse. To provide adequate granularity and specificity to the ITAAC descriptions there are ITAACs that are not common across the software projects. ITAACs 11a4, 11a5, 11a6, 11b4, 11b5, and 11b6 are specific to the RTIF-NMS platform. ITAACs 11a7, 11a8, 11a9, 11b7, 11b8, and 11b9 are specific to the SSLC-ESF platform. ITAACs 11a10, 11a1, 11b10, and 11b11 are specific to the ICP platform.

DETERMINISM (2) :

- **Item 8 (New) : Criteria 4.10, The critical points in time or plant conditions... (e.g., overall plant process control timing budget)**

  Remark : New 12th Para. in Design Description, "... included as ITAAC even though it is not included in NUREG 0800, Section 14.3.5, and RG 1.206, Section C.II.1. ..."

- **Item 17 (Modified) : Criteria 6.1 and 7.1, Automatic Control (e.g., sense – command – execute incl. digital processing times)**

  Note (6) : Includes BTP HICB-21 on Design Commitments related to avoiding the use of design practices that lead to non-deterministic timing behaviors.

Focused ITAACs around :

- **Top 2 of "4+1" Design Principles**
  - Independence
  - Determinism
- **Applied to 3 Q-DCIS Platforms**
  - RTIF-NMS
  - SSLC/ESF
  - ICP

HITACHI

Summary of Additional ITAACs... Tier 1

Item Code	Type ITAAC	Description Purpose	Q-DCIS Platform Applicability	T2.2.15-1 Platform Multiplier	DAC ITAAC	Construct ITAAC
8a1	DAC	Determinism	All	7	7	
8b1	Construct	Determinism	All	7		7
11a4	DAC	Independence	RTIF-NMS - Intra I/O	2	2	
11a5	DAC	Independence	RTIF-NMS - Inter VLU	2	2	
11a6	DAC	Independence	RTIF-NMS - SR-to-NSR	2	2	
11a7	DAC	Independence	SSLC/ESF - Intra I/O	1	1	
11a8	DAC	Independence	SSLC/ESF - Intra VDU	1	1	
11a9	DAC	Independence	SSLC/ESF - Inter VLU	1	1	
11a10	DAC	Independence	SSLC/ESF - SR-to-NSR	1	1	
11a11	DAC	Independence	ICP - Intra I/O	4	4	
11a12	DAC	Independence	ICP - Inter VLU	4	4	
11b4	Construct	Independence	RTIF-NMS - Intra I/O	2		2
11b5	Construct	Independence	RTIF-NMS - Inter VLU	2		2
11b6	Construct	Independence	RTIF-NMS - SR-to-NSR	2		2
11b7	Construct	Independence	SSLC/ESF - Intra I/O	1		1
11b8	Construct	Independence	SSLC/ESF - Intra VDU	1		1
11b9	Construct	Independence	SSLC/ESF - Inter VLU	1		1
11b10	Construct	Independence	SSLC/ESF - SR-to-NSR	1		1
11b11	Construct	Independence	ICP - Intra I/O	4		4
11b12	Construct	Independence	ICP - Inter VLU	4		4
17a2	DAC	Determinism	All	7	7	
17a3	Construct	Determinism	All	7		7
Sub-Total					**32**	**32**
TOTAL					**64**	

Target key areas of ACRS concern... Independence and Determinism

Independence ITAACs… SSLC/ESF Networks (1 of 4)

Item 11 a/b 7 : IEEE Std. Criteria 5.6, Independence and 6.3, Interactions…

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11a7. Criteria 5.6, Independence and 6.3, Interactions Between the Sense and Command Features and Other Systems: The SSLC/ESF software project's design base for intra-divisional input/output data communications have the following features: • sensor inputs at the RMUs are measured with triple redundancy; • sensor inputs and outputs sent to and from the RMUs are on a dedicated triply redundant communication backplane bus to triply redundant controller application processors; • data links for sensor inputs from the RMUs are sent via triply redundant optical fibers • actuator outputs from the RMUs are determined using commands from the triply redundant controller application processors; and • data links for actuator commands are sent via triply redundant optical fibers.	Inspection of the software project's design phase summary BRR will be performed to verify that the design for intra-divisional input/output data communications have the following features: • sensor inputs a measured with • sensor inputs a and from the R dedicated tripl communicatio triply redunda application pro • data links for s the RMUs are redundant opti • actuator outpu are determined from the triply controller appl and • data links for a are sent via tri optical fibers. {{Design Acceptance	The software project 'sdesign phase summary BRR show that the design bases for intra-divisional input/output data communications have the following features:

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11b7. Criteria 5.6, Independence and 6.3, Interactions Between the Sense and Command Features and Other Systems: The as-built SSLC/ESF software project's intra-divisional input/output data communications have the following features: • sensor inputs at the RMUs are measured with triple redundancy; • sensor inputs and outputs sent to and from the RMUs are on a dedicated triply redundant communication backplane bus to triply redundant controller application processors; • data links for sensor inputs from the RMUs are sent via triply redundant optical fibers • actuator outputs from the RMUs are determined using commands from the triply redundant controller application processors; and • data links for actuator commands are sent via triply redundant optical fibers.	Inspection of the as-built software project will verify that the intra-divisional input/output data communications design have the following features: • sensor inputs at the RMUs are measured with triple redundancy; • sensor inputs and outputs sent to and from the RMUs are on a dedicated triply redundant communication backplane bus to triply redundant controller application processors; • data links for sensor inputs from the RMUs are sent via triply redundant optical fibers • actuator outputs from the RMUs are determined using commands from the triply redundant controller application processors; and • data links for actuator commands are sent via triply redundant optical fibers.	The intra-divisional input/output data communications have the following features: • sensor inputs at the RMUs are measured with triple redundancy; • sensor inputs and outputs sent to and from the RMUs are on a dedicated triply redundant communication backplane bus to triply redundant controller application processors; • data links for sensor inputs from the RMUs are sent via triply redundant optical fibers • actuator outputs from the RMUs are determined using commands from the triply redundant controller application processors; and • data links for actuator commands are sent via triply redundant optical fibers.

Intra- Divisional Input/Output Data Communications Features

HITACHI

Independence ITAACs… SSLC/ESF Networks (2 of 4)

Item 11 a/b 8 : IEEE Std. Criteria 5.6, Independence and 6.3, Interactions…

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11a8. Criteria 5.6, Independence and 6.3, Interactions Between the Sense and Command Features and Other Systems: The SSLC/ESF software project's design bases for intra-divisional VDU data communications have the following features: • data inputs/outputs are to and from the SSLC/ESF platform; • data inputs are only from RTIF-NMS platform; • data inputs/outputs to and from the safety-related VDUs are via dual, redundant networks; • data links have dedicated communication interface modules; • data links use optical fibers; • message authentication resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.	Inspection of the software project's design phase summary BRR will be performed to verify that the design bases for intra-divisional VDU data communications have the following features: • data inputs/o from the SSL • data inputs a platform; • data inputs/o the safety-rel dual, redund • data links ha communicati modules; • data links use • message auth the receiving • message auth transmitter a identification hash function redundancy c {{Design Acceptan	The software project's design phase summary BRR show that the design bases for intra-divisional VDU data communications have the following features:

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11b8. Criteria 5.6, Independence and 6.3, Interactions Between the Sense and Command Features and Other Systems: The as-built SSLC/ESF software project's intra-divisional VDU data communications have the following features: • data inputs/outputs are to and from the SSLC/ESF platform; • data inputs are only from RTIF-NMS platform; • data inputs/outputs to and from the safety-related VDUs are via dual, redundant networks; • data links have dedicated communication interface modules; • data links use optical fibers; • message authentication resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.	Inspection of the as-built software project will verify that the intra-divisional VDU data communications design have the following features: • data inputs/outputs are to and from the SSLC/ESF platform; • data inputs are from RTIF-NMS platform; • data inputs/outputs to and from the safety-related VDUs are via dual, redundant networks; • data links have dedicated communication interface modules; • data links use optical fibers; • message authentication resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.	The intra-divisional VDU data communications have the following features: • data inputs/outputs are to and from the SSLC/ESF platform; • data inputs are from RTIF-NMS platform; • data inputs/outputs to and from the safety-related VDUs are via dual, redundant networks; • data links have dedicated communication interface modules; • data links use optical fibers; • message authentication resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.

Intra- Divisional VDU Data Communications Features

HITACHI

Independence ITAACs… SSLC/ESF Networks (3 of 4)

Item 11 a/b 9 : IEEE Std. Criteria 5.6, Independence and 6.3, Interactions…

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11a9. Criteria 5.6, Independence and 6.3, Interactions Between the Sense and Command Features and Other Systems: The SSLC/ESF software project's design bases for inter-divisional data communications within safety-related systems have the following features: • data links supporting two-out-of-four voting logic are via dual, redundant networks; • data links have dedicated communication interface modules; • data links use optical fibers; • message authentication resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.	Inspection of the software project's design phase summary BRR will be performed to verify that the design bases for inter-divisional data communications within safety-related systems have the following features: • data links supporting two-out-of-four voting logic are via dual, redundant networks; • data links hav communicatic modules; • data links use • message auth the receiving • message auth transmitter an identification, hash function redundancy c {{Design Acceptanc	The software project's design phase summary BRR show that the design bases for inter-divisional data communications within safety-related systems have the following features: • data links supporting two-out-of-four voting logic are via dual, redundant networks; • data links have dedicated

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11b9. Criteria 5.6, Independence and 6.3, Interactions Between the Sense and Command Features and Other Systems: The as-built SSLC/ESF software project's inter-divisional data communications within safety-related systems have the following features: • data links supporting two-out-of-four voting logic are via dual, redundant networks; • data links have dedicated communication interface modules; • data links use optical fibers; • message authentication resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.	Inspection of the as-built software project will verify that the inter-divisional data communications design within safety-related systems have the following features: • data links supporting two-out-of-four voting logic are via dual, redundant networks; • data links have dedicated communication interface modules; • data links use optical fibers; • message authentication resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.	The inter-divisional data communications within safety-related systems have the following features: • data links supporting two-out-of-four voting logic are via dual, redundant networks; • data links have dedicated communication interface modules; • data links use optical fibers; • message authentication resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.

Inter- Divisional Voting Logic Data Communications Features

HITACHI

Independence ITAACs… SSLC/ESF Networks (4 of 4)

Item 11 a/b 10 : IEEE Std. Criteria 5.6, Independence and 6.3, Interactions…

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11a10. Criteria 5.6, Independence and 6.3, Interactions Between the Sense and Command Features and Other Systems: The SSLC/ESF software project's design bases for N-DCIS data communications between safety-related and nonsafety-related systems have the following features: • data communications are one way out to nonsafety-related components; • data links are via a separate, dedicated, dual, redundant networks; • data links have dedicated communication interface modules • data links use optical fibers; • SSLC/ESF message authentication (for absolute time) resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.	Inspection of the software project's design phase summary BRR will be performed to verify that the design bases for N-DCIS data communications between safety-related and nonsafety-related systems have the following features: • communicatio to nonsafety-r • data links are dedicated, dua networks; • data links hav communicatio • data links use • SSLC/ESF me authentication resides in the r only; and • message authe transmitter an identification, hash functions redundancy cl {{Design Acceptanc	The software project's design phase summary BRR show that the design bases for N-DCIS data communications between safety-related and nonsafety-related systems have the following features:

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11b10. Criteria 5.6, Independence and 6.3, Interactions Between the Sense and Command Features and Other Systems: The as-built SSLC/ESF software project's N-DCIS data communications between safety-related and nonsafety-related systems have the following features: • data communications are one way out to nonsafety-related components; • data links are via a separate, dedicated, dual, redundant networks; • data links have dedicated communication interface modules • data links use optical fibers; • SSLC/ESF message authentication (for absolute time) resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.	Inspection of the as-built software project will verify that the N-DCIS data communications design between safety-related and nonsafety-related systems have the following features: • data communications are one way out to nonsafety-related components; • data links are via a separate, dedicated, dual, redundant networks; • data links have dedicated communication interface modules • data links use optical fibers; • SSLC/ESF message authentication (for absolute time) resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.	The N-DCIS data communications design between safety-related and nonsafety-related systems have the following features: • data communications are one way out to nonsafety-related components; • data links are via a separate, dedicated, dual, redundant networks; • data links have dedicated communication interface modules • data links use optical fibers; • SSLC/ESF message authentication (for absolute time) resides in the receiving division only; and • message authentication includes transmitter and receiver identification, sequence number, hash functions, and cyclic redundancy checks.

Safety –to- NonSafety N-DCIS Data Communications Features

Determinism ITAACs… All Platforms (1 of 2)

Item 8 a/b 1 : IEEE Std. 603 Criteria 4.10

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
8a1. Criterion 4.10. The critical points in time or the plant conditions, after the onset of a design basis event: The software project's design bases ensures that: • a plant process control timing budget (end-to-end sense, command, and execute loop including the associated DCIS components' response times) exists; and • the plant process control timing budget completes its protective action in less than the specified maximum time allowable.	Inspection of the software project's design phase summary BRR will be performed to verify that: • a plant process control timing budget (end-to-end sense, command, and execute loop including the associated DCIS components' response times) exists; and • the plant process control timing budget completes its protective action in less than the specified maximum time allowable. {{Design Acceptance Criteria}}	The software project's design phase summary BRR identifies that: • a plant process control timing budget (end-to-end sense, command, and execute loop including the associated DCIS components' response times) exists; and • the plant process control timing budget completes its protective action in less than the specified maximum time allowable. {{Design Acceptance Criteria}}
8b1. Criterion 4.10. The critical points in time or the plant conditions, after the onset of a design basis event: The as-built software project ensures that: • the plant process control timing budget completes its protective action in less than the specified maximum time allowable.	Tests will be performed to show that the as-built software project complies with: • the plant process control timing budget completes its protective action in less than the specified maximum time allowable.	Tests show that: • the plant process control timing budget completes its protective action in less than the specified maximum time allowable.

Plant Process Control Timing Budget EXISTs
Protective Action Complete in Less that Max. Allowable Time

HITACHI

Determinism ITAACs… All Platforms (2 of 2)

Item 17 a/b 2 : BTP HICB-21 Perspective

Table 2.2.15-2

ITAAC For IEEE Std. 603 Compliance Confirmation

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
17a2. Criteria 6.1 and 7.1, Automatic Control: The software project's design bases show that in normal operation of the end-to-end sense, command, and execute plant process control loops (including the associated DCIS components involved with determinant data processing and communications) the following features are not used: • non-deterministic data communications; • non-deterministic computation; • interrupts; • multi-tasking; • dynamic scheduling; and • event-driven actions.	Inspection of the software project's design phase summary BRR will be performed to verify that the design bases show that in normal operation of the end-to-end sense, command, and execute plant process control loops (including the associated DCIS components involved with determinant data processing and communications) the following features are not used: • non-deterministic data communications; • non-deterministic computation; • interrupts; • multi-tasking; • dynamic scheduling; and • event-driven actions. {{Design Acceptance Criteria}}	The software project's design phase summary BRR shows that the design bases show that in normal operation of the end-to-end sense, command, and execute plant process control loops (including the associated DCIS components involved with determinant data processing and communications) the following features are not used: • non-deterministic data communications; • non-deterministic computation; • interrupts; • multi-tasking; • dynamic scheduling; and • event-driven actions. {{Design Acceptance Criteria}}
17b2. Criteria 6.1 and 7.1, Automatic Control: The as-built software project's normal operation end-to-end sense, command, and execute plant process control loops (including the associated DCIS components involved with determinant data processing and communications) do not use the following features: • non-deterministic data communications; • non-deterministic computation; • interrupts; • multi-tasking; • dynamic scheduling; and • event-driven actions.	Inspection of the as-built software project will verify that in normal plant process control loops (including the associated DCIS components involved with determinant data processing and communications) the following features are not used: • non-deterministic data communications; • non-deterministic computation; • interrupts; • multi-tasking; • dynamic scheduling; and • event-driven actions.	The as-built software project, in normal plant process control loops (including the associated DCIS components involved with determinant data processing and communications), does not use the following features: • non-deterministic data communications; • non-deterministic computation; • interrupts; • multi-tasking; • dynamic scheduling; and • event-driven actions.

Avoid using Non-Deterministic Design Practices
ESBWR Does Not Uses these Features

DCD Rev. 8 In-Prog. ITAAC Count… Tier 1

Tier 1	I&C	Other	Total	% Tot
DAC-ITAAC :	378	24	402	94%
Construct-ITAAC :	428	701	1129	38%
TOTAL ITAAC :	**806**	**725**	**1531**	**53%**

Counting Methodology :

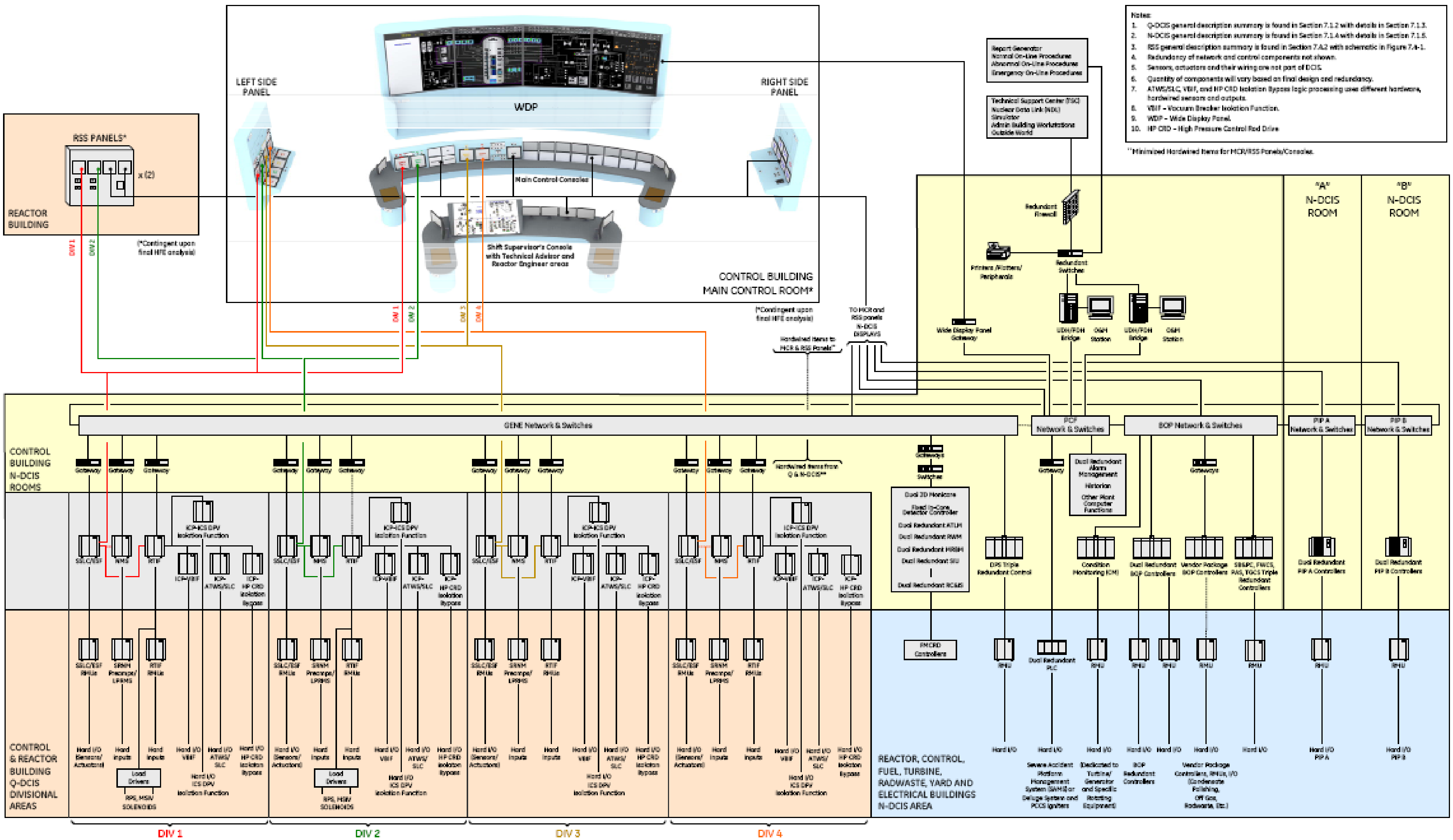
- **Straight Count**
- **Matrix Count**
  - **IEEE Std. 603 Criterion System Applicability Matrix**
    - Every criterion (DAC-ITAAC or Construct-ITAAC) in Table 2.2.15-2 was multiplied by the numbers of 'R' in the corresponding criterion Row of Table 2.2.15-1.
  - **Environmental Qualification (Table 3.8-1)**
    - Every item (DAC or C-ITAAC) in Table 3.8-2 was applied to the corresponding qualification program (e.g. Harsh Mechanical (MH), Harsh Electrical (EH)).

NOTE:

- DCD Rev. 6 DAC,- Construct-, and Total ITAAC count presented at ACRS Meeting on 22 October 2009 was higher (688, 1387, 2075) mainly driven by a reduction in Chapter 7 I&C from (663, 801, 1464) due to correcting an error in the counting methodology applicability rules applied to Table 2.2.15-1 when matrix'ed with Table 2.2.15-2.

Adequate coverage of Digital I&C Design and Process Commitments

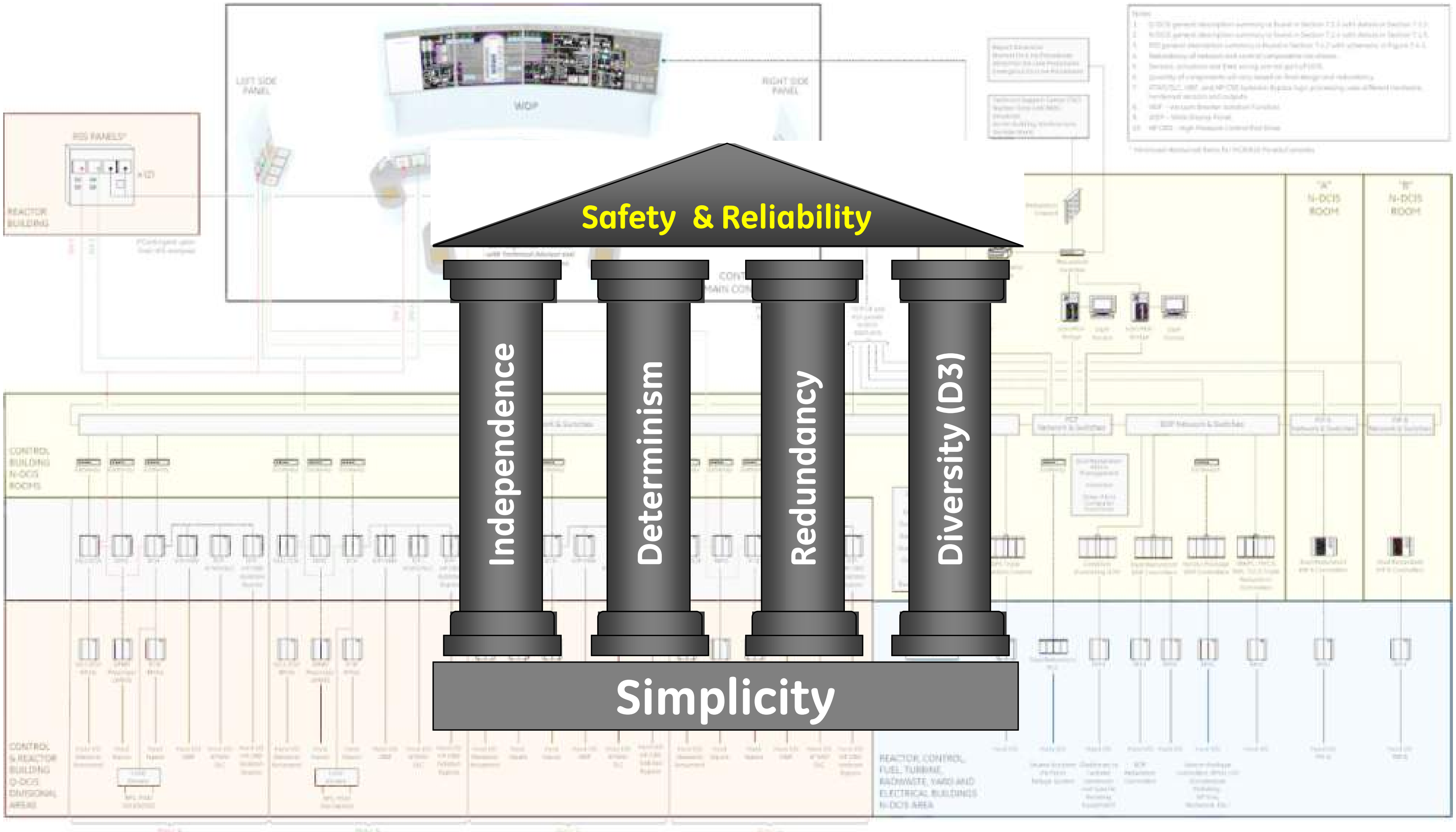
ESBWR DCIS Overview... Simplified Block Diagram



DCD Rev. 8 – Figure 7.1-1

ESBWR Instrumentation and Control DCIS Simplified Network and Functional Block Diagram

"4+1" Design Principles... Independence

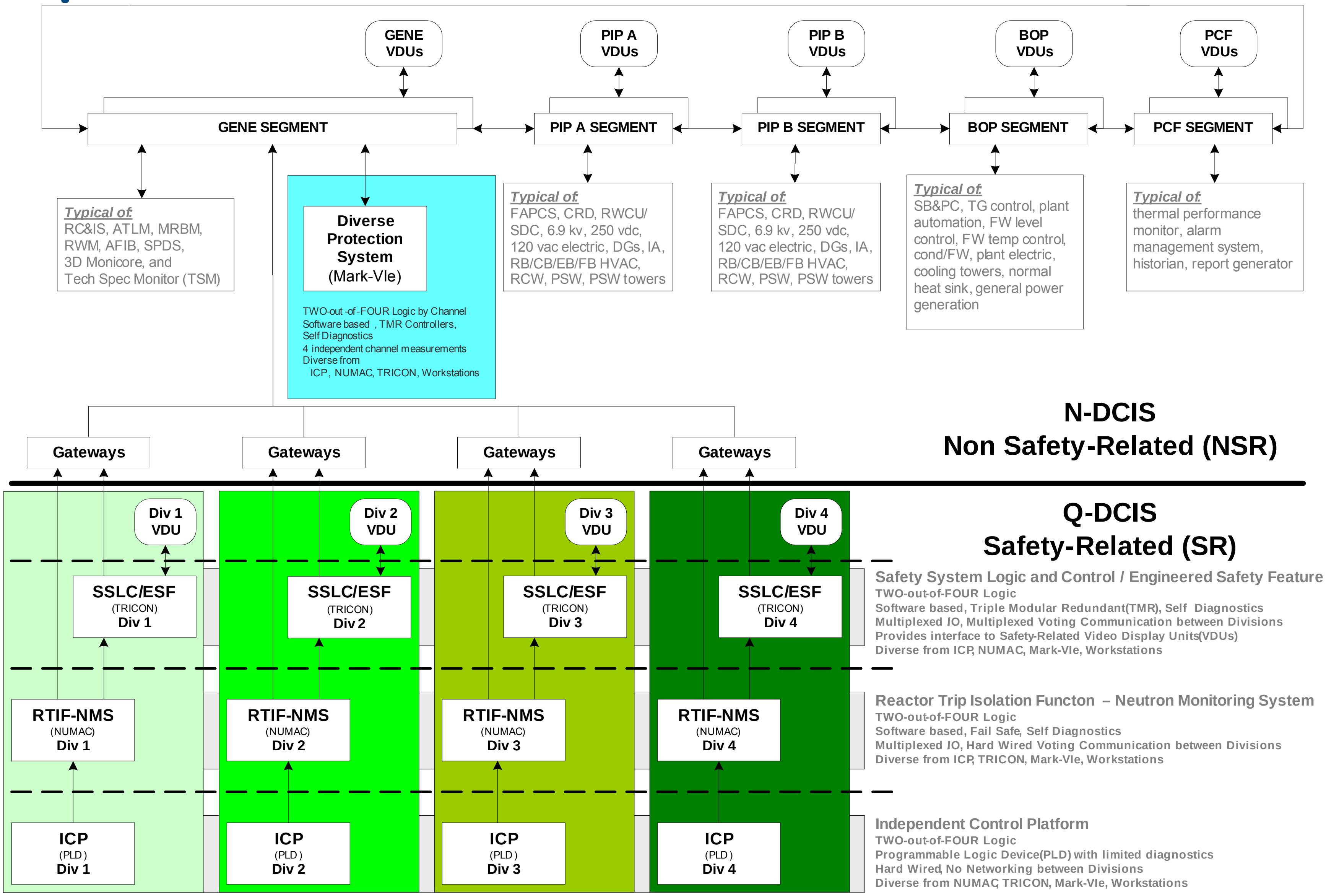


Based on IEEE Std 603

Criteria for Safety Systems for Nuclear Power Generating Stations

HITACHI

Independence... ESBWR DCIS Overall Architecture



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

Platform, Divisional, Network, and Channel INDEPENDENCE

HITACHI

Independence… SSLC/ESF Inter-Divisional Networks

100 Mbits/Sec Ethernet

Inter- Divisional
"2-out-of-4" Voting Logic
Data Communications

Independent and Redundant Inter-Divisional Network

Communication Interface Module (CIM) devices are Safety-Related Equipment

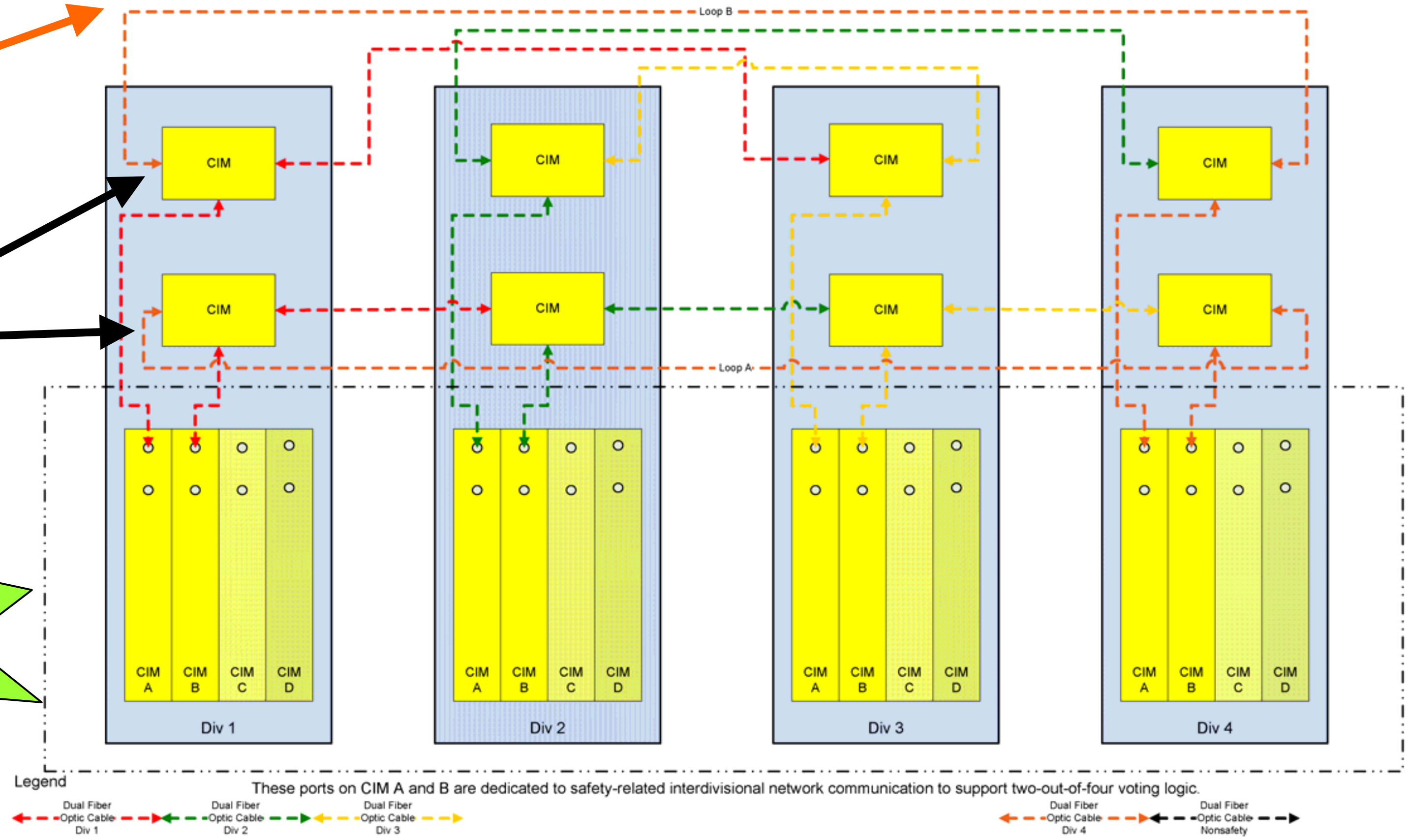


Figure 7.3-8 SSLC/ESF Inter-Divisional Communication Detail

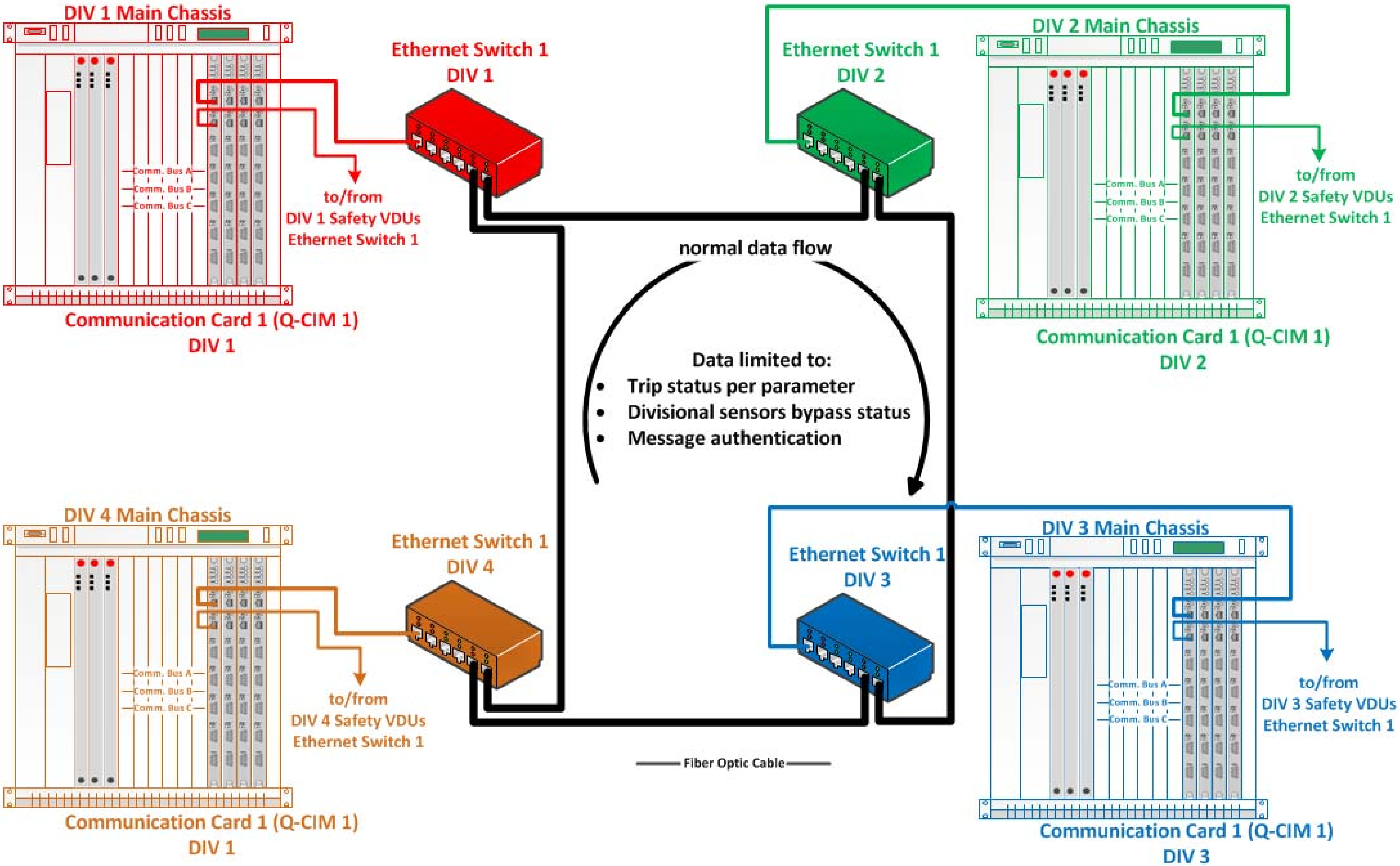
Key Design Features…

- 2 Networks are DUAL
- Each Network is REDUNDANT
- Each Network is DEDICATED
- Messages are "AUTHENTICATED"

HITACHI

Independence... SSLC/ESF Network 1

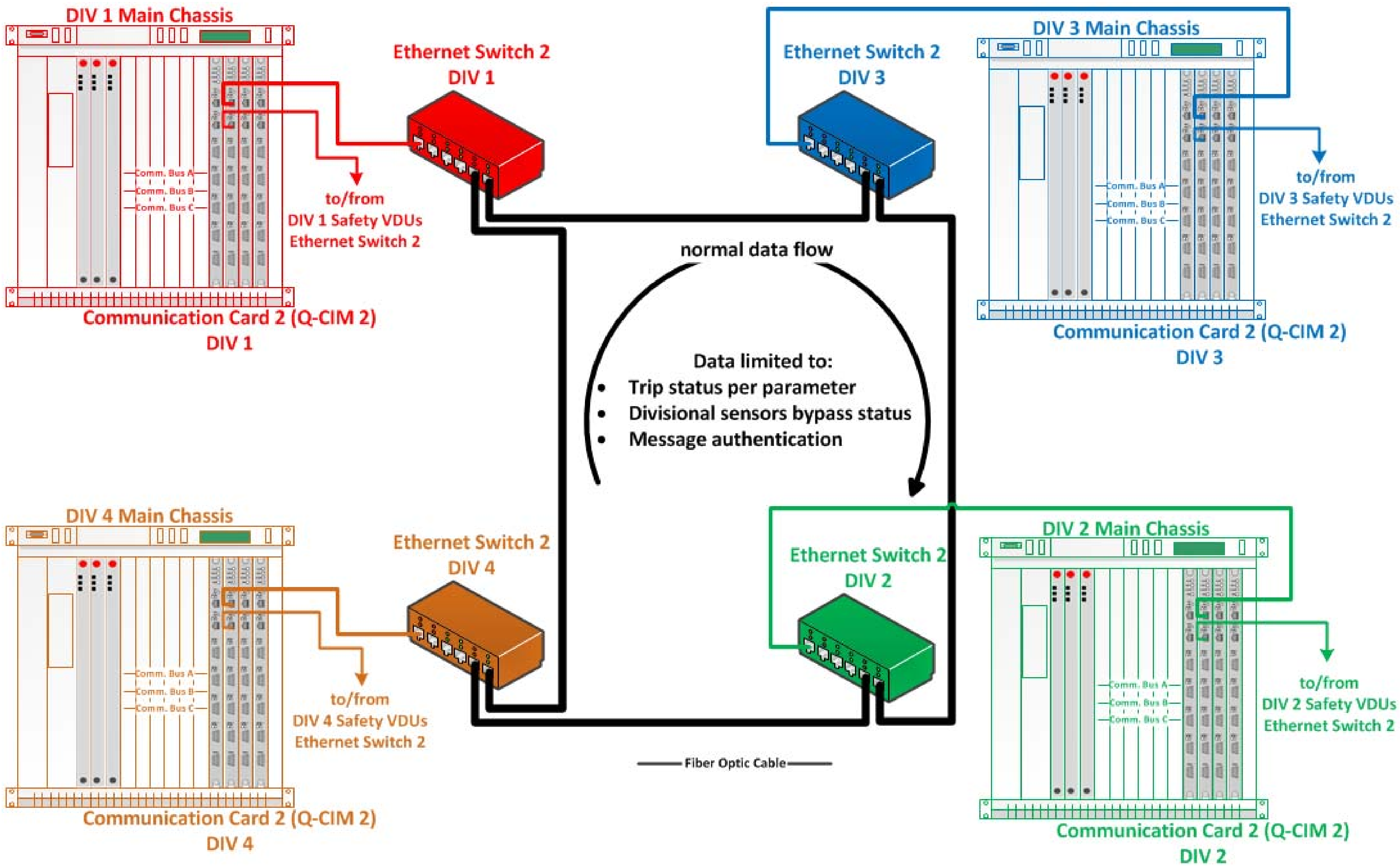
SSLC/ESF "two-out-of-four" Trip Voting Logic Ethernet Network 1 (Inter-Divisional Data Communication)



SSLC/ESF Network 1 is INDEPENDENT... Dedicated, Redundant, and Message Authentication.... Messages travel in either direction

Independence... SSLC/ESF Network 2

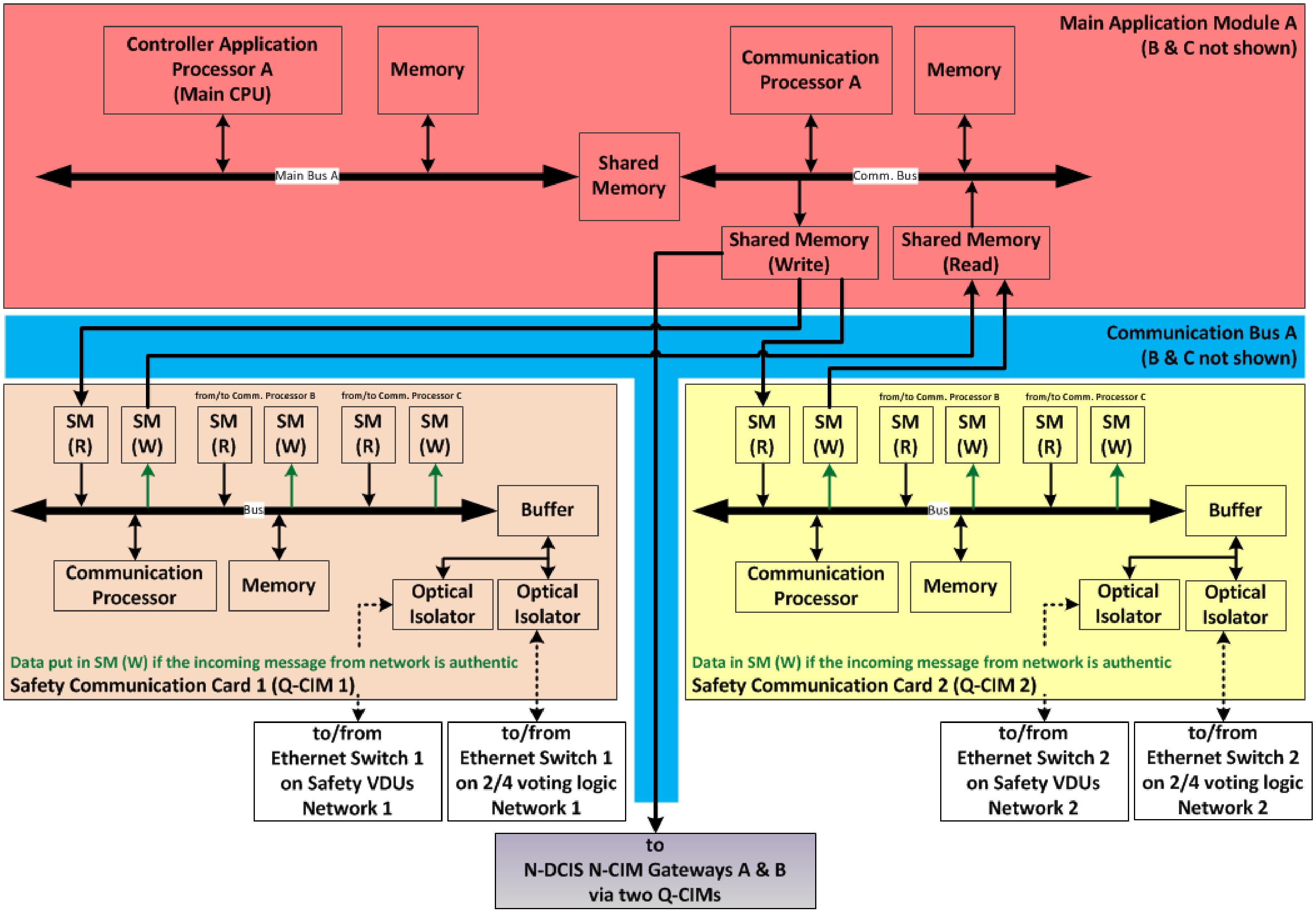
SSLC/ESF "two-out-of-four" Trip Voting Logic Ethernet Network 2 (Inter-Divisional Data Communication)



SSLC/ESF Network 2 is INDEPENDENT... Dedicated, Redundant, and Message Authentication.... Messages travel in either direction

Independence…

SSLC/ESF DIV x Main Chassis
(Inter-Divisional Data Communication)



Main Chassis Backplane Bus supports INDEPENDENCE… Dedicated, Shared Memory, Triply Redundant Channels, and Message Authentication

HITACHI

Independence…

SSLC/ESF Divisional Truth Table for Trip and Bypass Status

Comm. Bus

Shared Memory

DIV x trip status decision truth table in DIV w

DIV x Trip status From Network 1	DIV x Message Authentication status from Network 1	DIV x Trip status From Network 2	DIV x Message Authentication status from Network 2	DIV x Trip status In DIV w
0	0	0	0	0
1	0	0	0	0
0	1	0	0	0
1	1	0	0	1
0	0	1	0	0
1	0	1	0	0
0	1	1	0	0
1	1	1	0	1
0	0	0	1	0
1	0	0	1	0
0	1	0	1	0
1	1	0	1	0
0	0	1	1	1
1	0	1	1	1
0	1	1	1	0
1	1	1	1	1

1 = trip   1 = message is authentic

Note: same truth table applies to the Bypass status

To 2/4 trip voting logic in DIV w

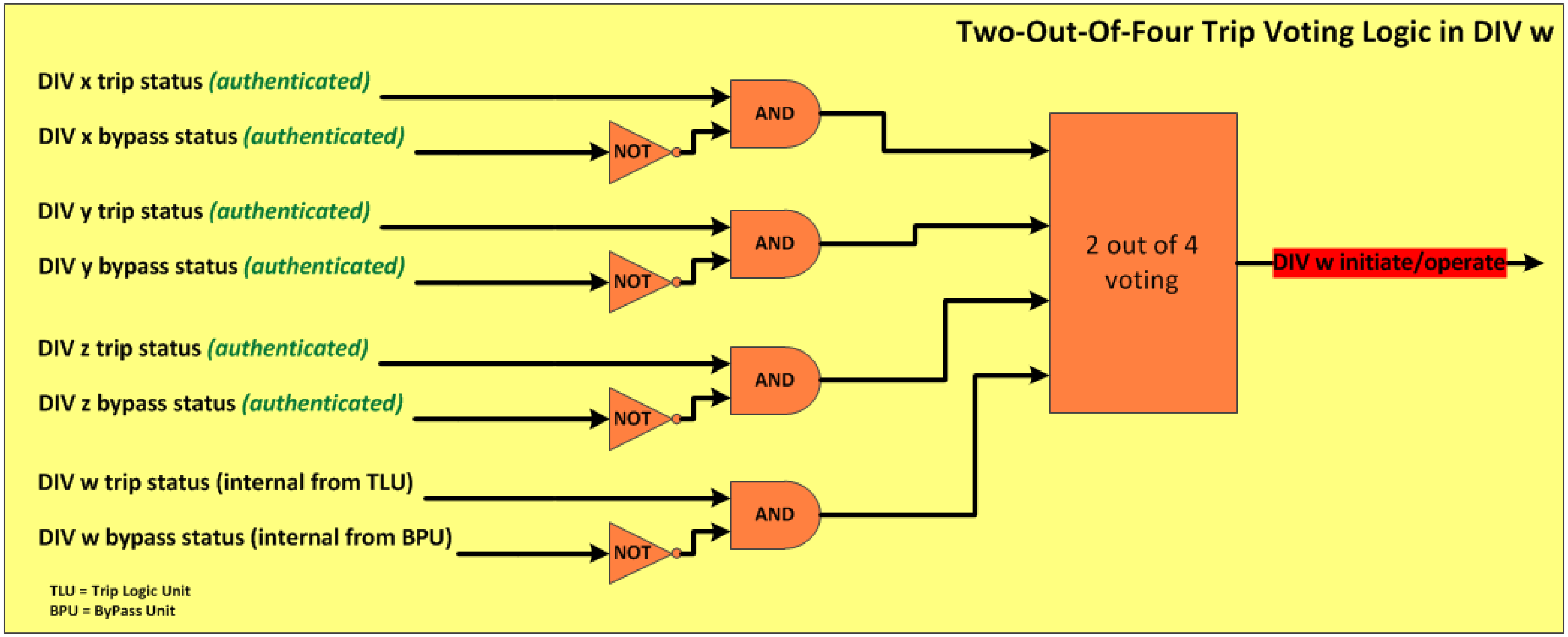
transmitting address is correct (= 1)
receiving address is correct (= 1)
sequence number is correct (= 1)
signature (e.g. hash function) is correct (= 1)
corruption (e.g. CRC) check is correct (1 = no corruption)
messages not too slow (or old) (0 = sequence numbers not changing fast enough or not changing)
messages not too fast (data storm) (0 = sequence numbers changing too fast)

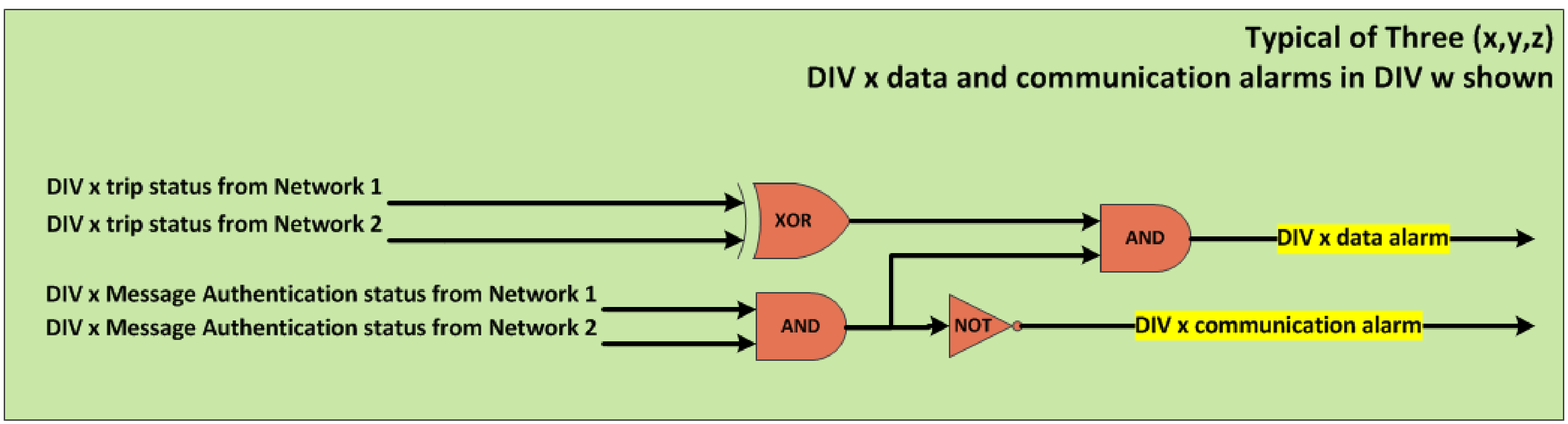
AND → 1 = message is authentic

Achieving Data Independence… Managing Divisional Trip, Bypass, and Message Authentication Status

HITACHI

Independence... SSLC/ESF "2 out of 4" Trip Voting Logic





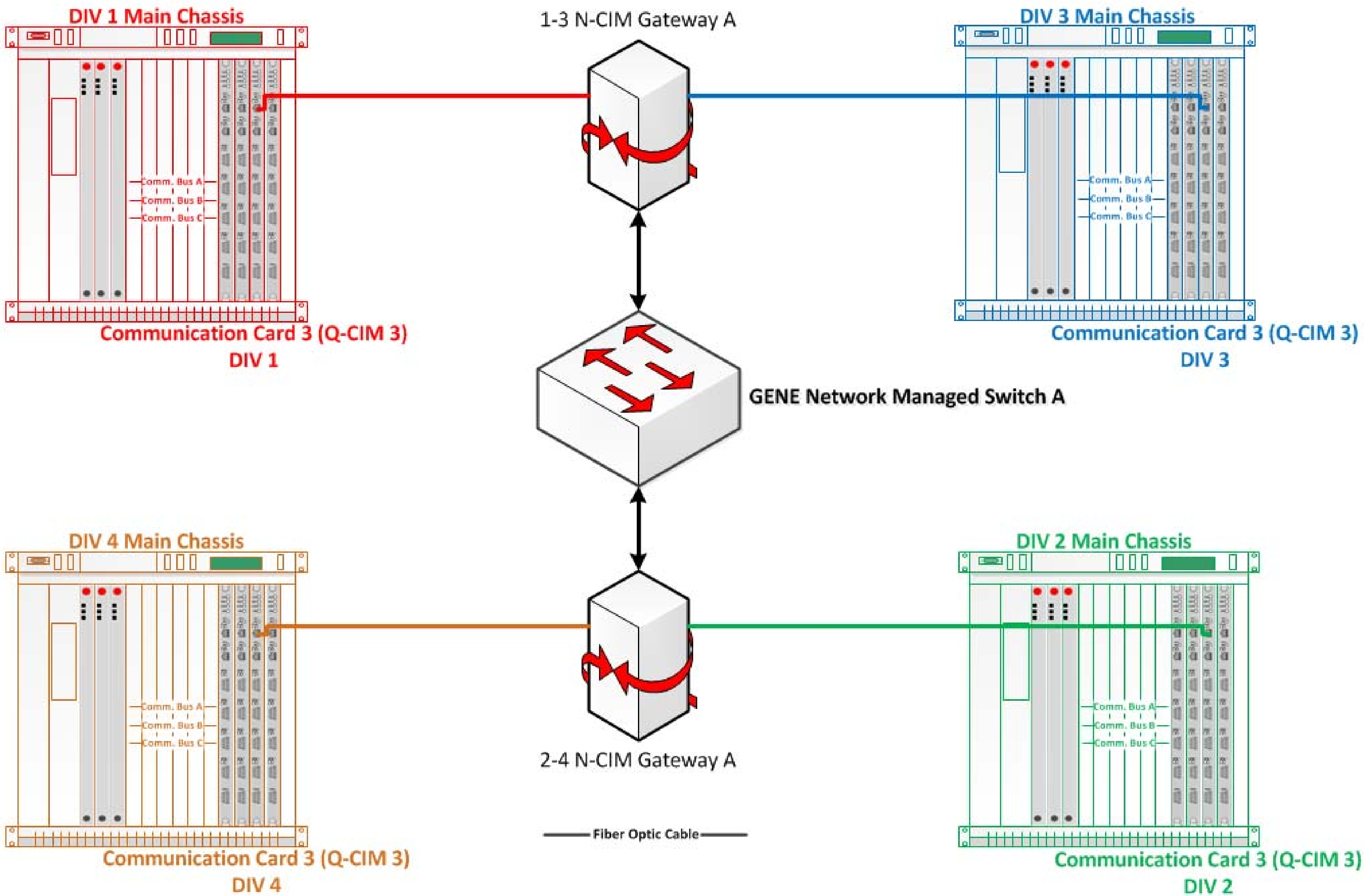
Achieving Data Independence and highly Reliable Initiate/Operate Decision

GE HITACHI

Independence…

SSLC/ESF Network 3

SSLC/ESF Data Communication (A) to N-DCIS

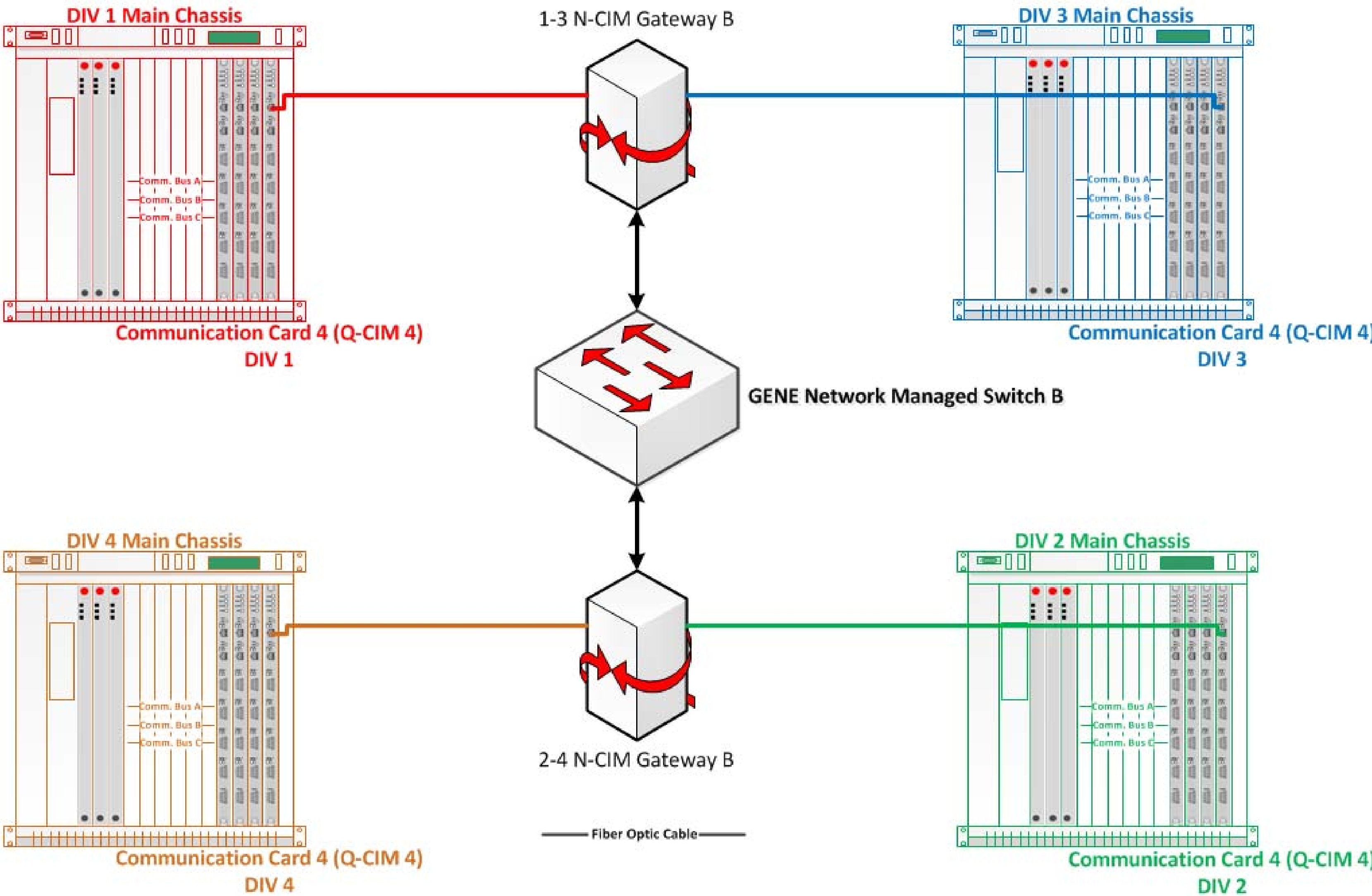


SSLC/ESF Network 3 is INDEPENDENT and SEPARATE from Divisional Trip Voting Logic Network

Independence…

SSLC/ESF Network 4

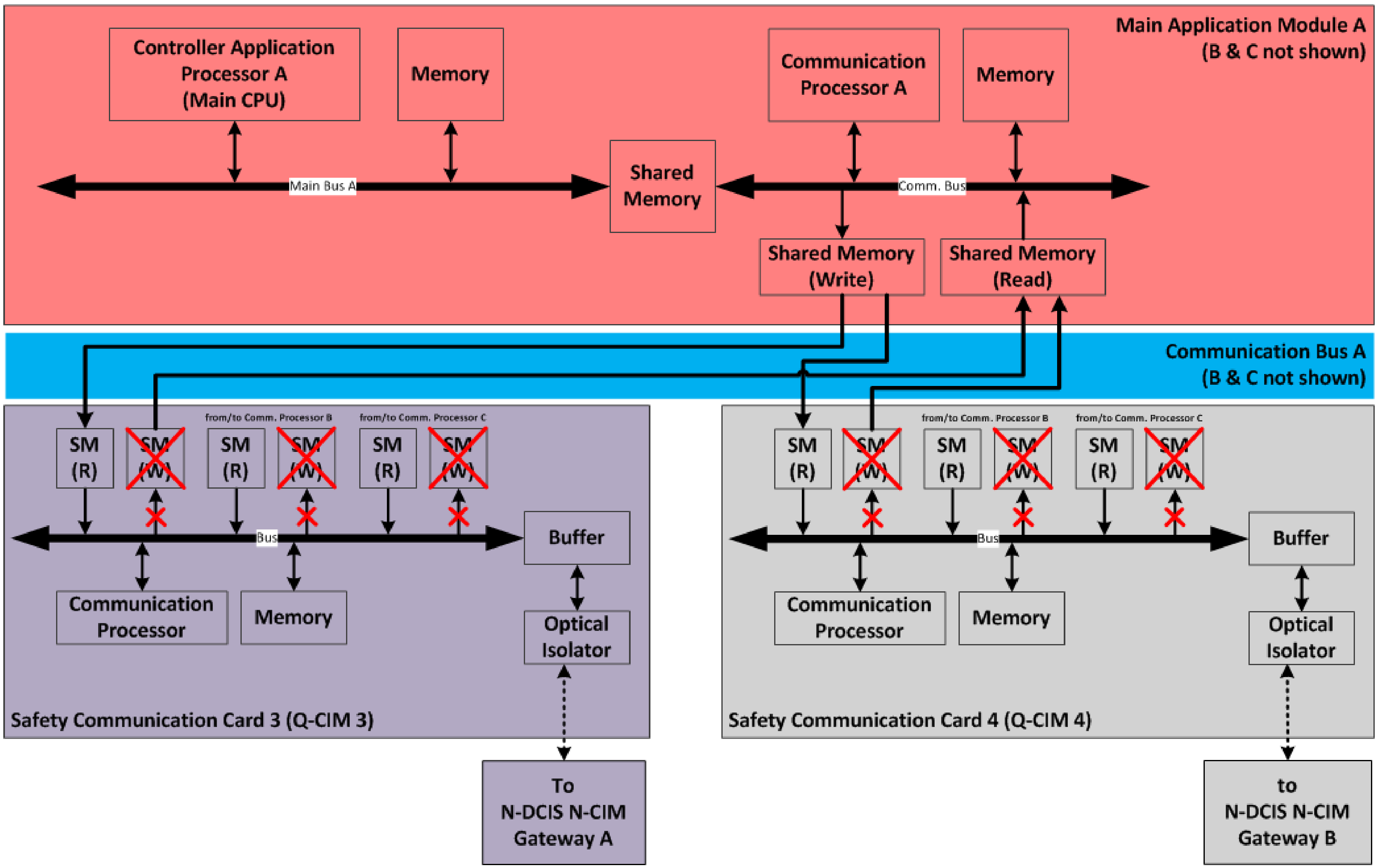
SSLC/ESF Data Communication (B) to N-DCIS



SSLC/ESF Network 4 is INDEPENDENT and SEPARATE from Divisional Trip Voting Logic Network

Independence…

SSLC/ESF DIV x Main Chassis
(Data Communication to N-DCIS)

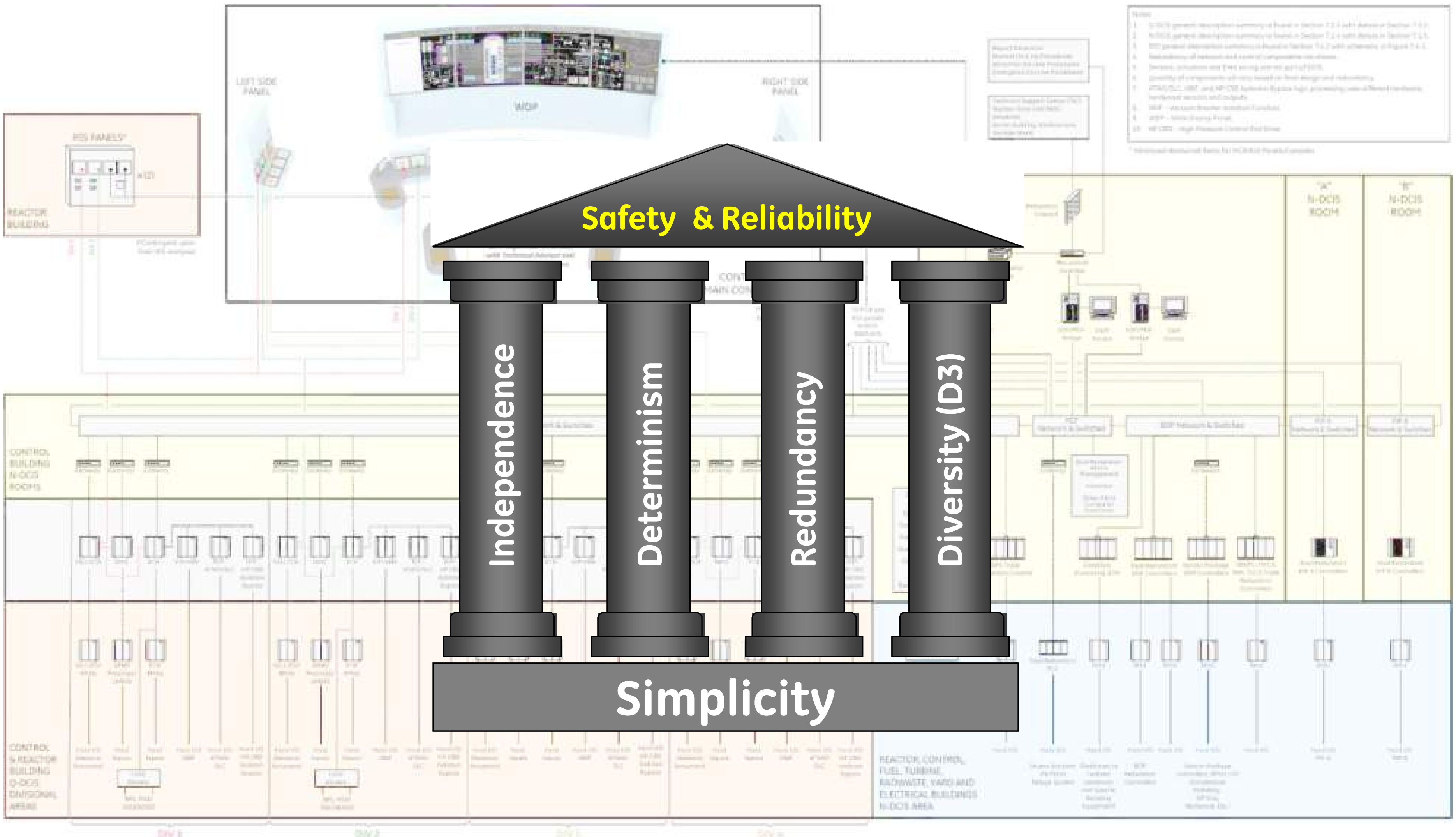


X indicates that the communication card is set "read only"

Main Chassis Backplane Bus supports INDEPENDENCE… Dedicated, Shared Memory, Triply Redundant Channels

HITACHI

"4+1" Design Principles... Determinism



Based on IEEE Std 603

Criteria for Safety Systems for Nuclear Power Generating Stations

Determinism… Timing Budgets

7.1.2.1.2 Determinant Data Processing and Communication (Determinism) Design Principle

Reliability, redundancy and independence in ESBWR DCIS can be achieved separately from timing considerations but **there must be timing criteria that ensure that the DCIS operates fast enough to satisfy the automatic and manual operability goals**. Transients, design basis and beyond design basis events are analyzed in Chapter 15 of the DCD and assume time criteria that the DCIS must meet to make the analyses accurate. The ESBWR DCIS **design bases will use these requirements to determine the speed required of the Q-DCIS (and N-DCIS) controller application programs and required data communication management programs**. Per BTP HICB-21, Q-DCIS computer **timing will be shown to be consistent with the limiting response times** and the characteristics of the computer hardware, software, and data communications systems and ESBWR DCIS design basis documents will describe system timing goals.

Establish timing budget for each plant process to be controlled and Function must always perform in less than allowable time… DETERMINISTIC

Determinism… Processors and Logic Gates

What IS Done…

RTIF-NMS and SSLC/ESF processors, in normal operation, designed using:

- Cyclic real-time executive or operating system with system clock
- Program loop is internally monitored by watch dog timers
- Application processors are buffered from any data communications
- Includes monitoring and diagnostic programs
- Application code implemented differently by Platform:
  - **RTIF-NMS** code is "burnt in" and unchangeable after implementation
  - **SSLC/ESF** code is "blockware" via secure configurator toolkit

ICP is designed using Custom Programmable Logic Devices (CPLDs) that:

- Implement gate logic only for control functions
- Do not use cyclic real-time executive, clock, or run application code for control
- Logic is "burnt in" and unchangeable after implementation

What is NOT Done…

Per BTP HICB-21 Guidance on Digital Computer Real-Time Performance

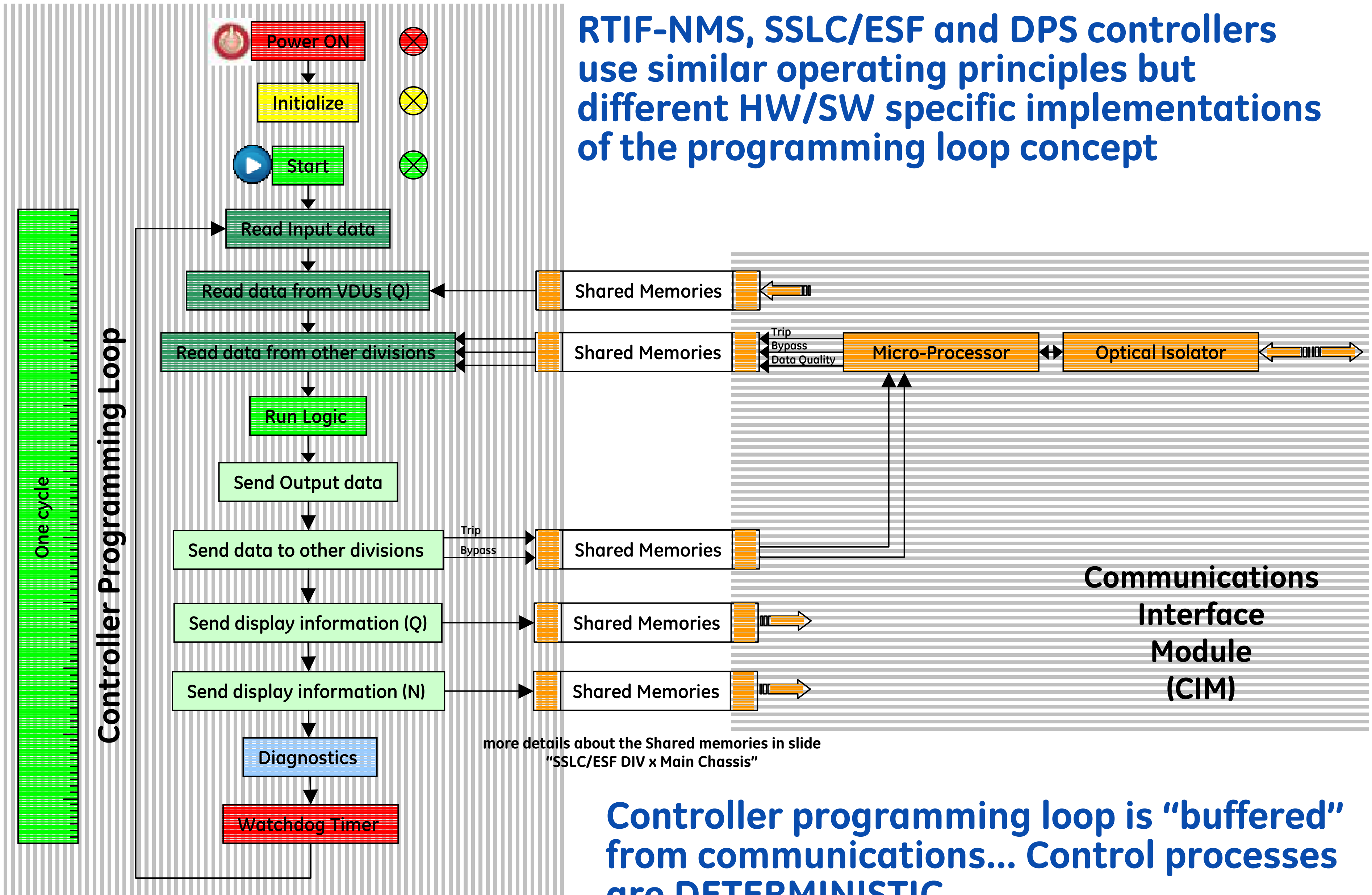
ESBWR Q-DCIS and DPS (specific N-DCIS hardware/software controllers) platforms do not use, in normal operation, the following:

- non-deterministic data communications
- non-deterministic computation
- interrupts
- multi-tasking
- dynamic scheduling
- event-driven methods

Processors and Hard Logic Gates are Functionally DETERMINISTIC

Determinism… Controller Processors

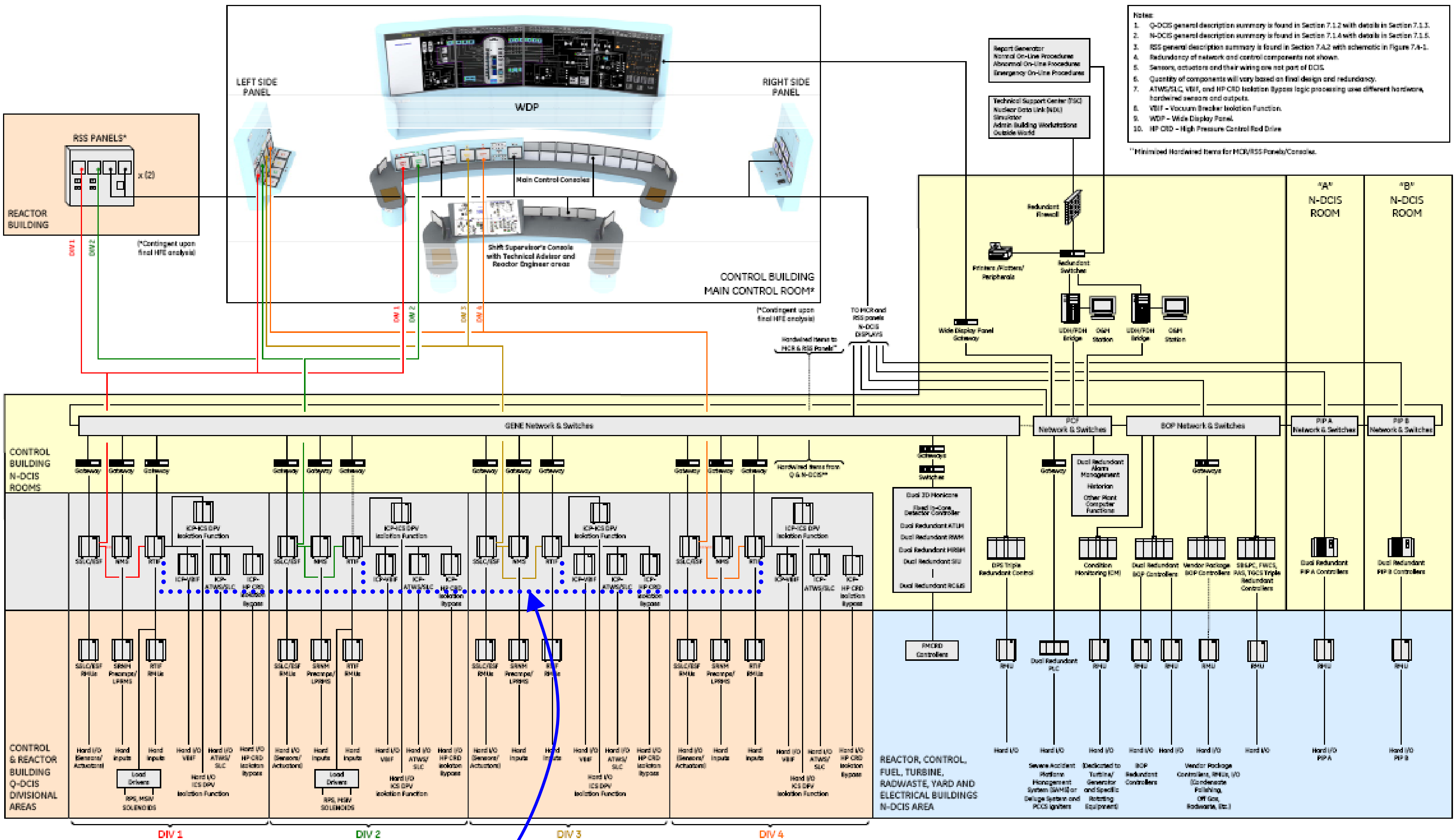
RTIF-NMS, SSLC/ESF and DPS controllers use similar operating principles but different HW/SW specific implementations of the programming loop concept



Controller programming loop is "buffered" from communications… Control processes are DETERMINISTIC

HITACHI

Determinism… RTIF Inter-Div. Data Link Example



RTIF (RPS) "2-out-of-4" Voting Inter-Divisional DEDICATED Point-to-Point Data Communications

Figure 7.1-1

ESBWR Instrumentation and Control DCIS Simplified Network and Functional Block Diagram

HITACHI

Determinism… RTIF Inter-Div.Voting Data Link

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

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

3) One-Way Out
Safety -to- NonSafety

All Communication Interface Module (CIM) devices are Safety-Related Equipment

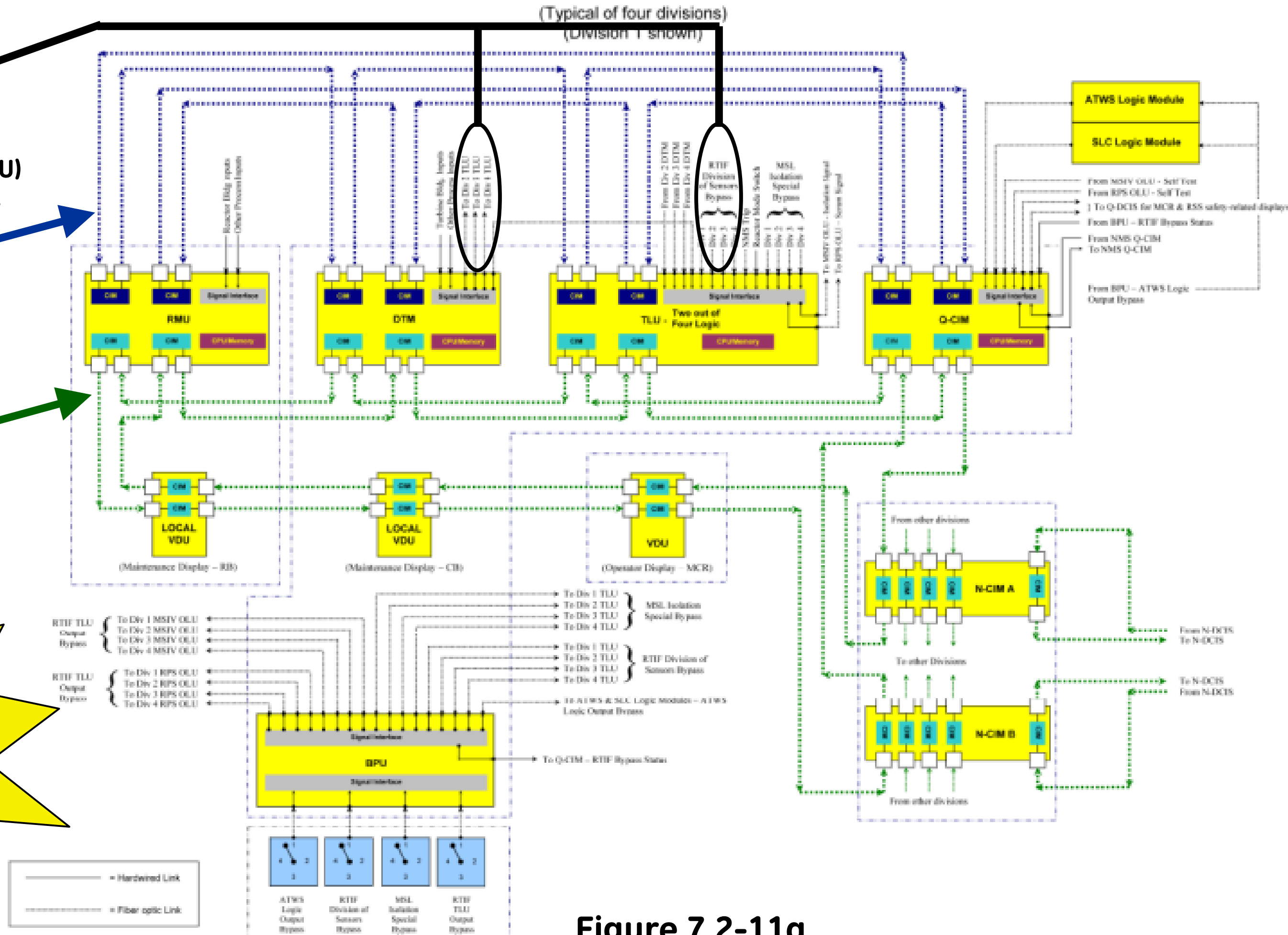


Figure 7.2-11a
Reactor Trip and Isolation Function (RTIF) Simplified Functional Block Diagram

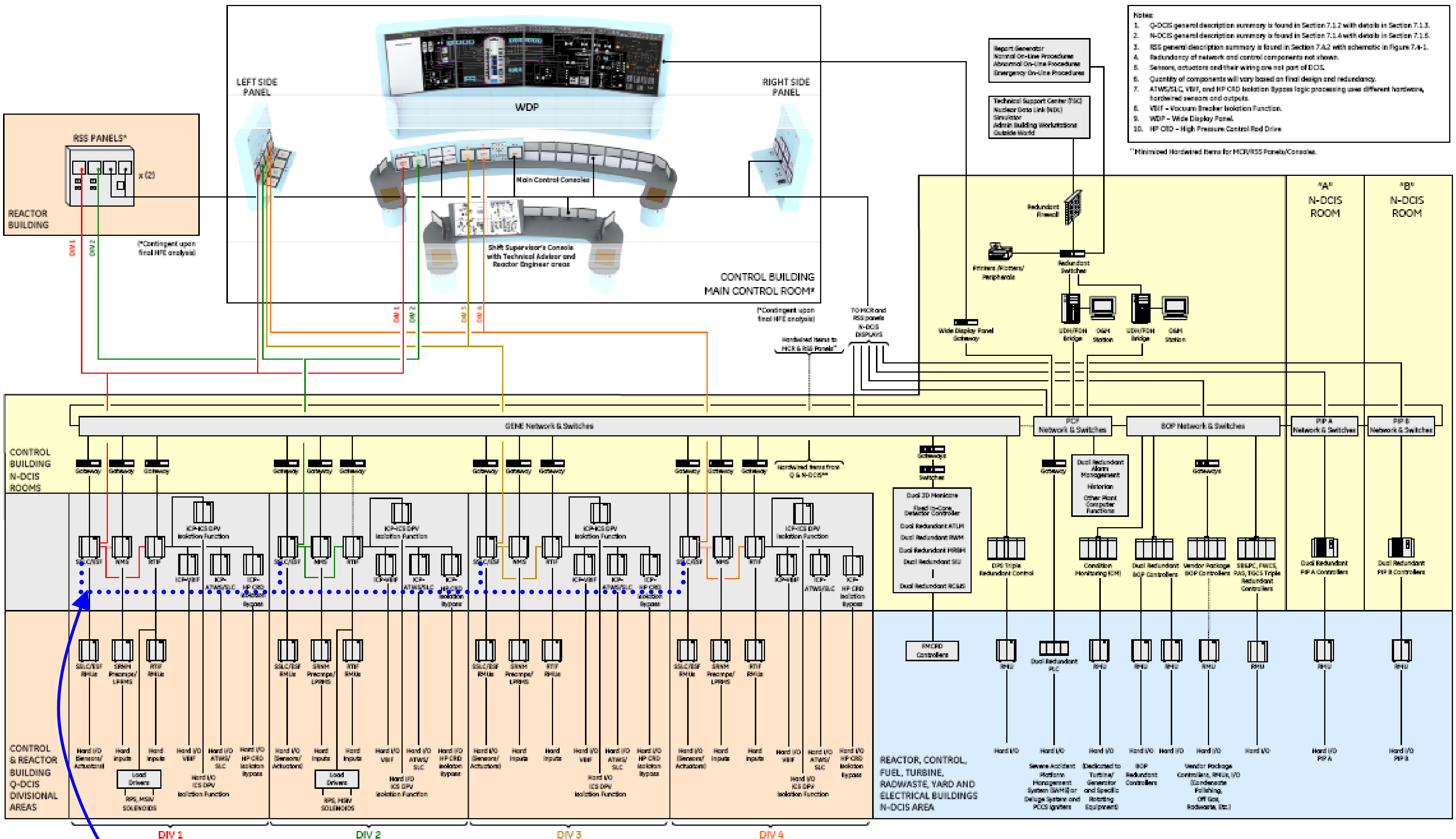
Inter-Div. Pt-to-Pt and Intra-Div. "scramnet" cycle times are… 10's micro-sec.

RPS scram response time is… 10's milli-sec.

Communications are DETERMINISTIC within plant process time budget

HITACHI

Determinism… SSLC/ESF Inter-Div. Network Example



SSLC/ESF "2-out-of-4" Votng Inter-Divisional DEDICATED Ethernet (100 Mbits/Sec) Network

Figure 7.1-1

ESBWR Instrumentation and Control DCIS Simplified Network and Functional Block Diagram

HITACHI

Determinism... SSLC/ESF Inter-Divisional Networks

100 Mbits/Sec Ethernet

Inter- Divisional
"2-out-of-4" Voting Logic
Data Communications

Independent and Redundant Inter-Divisional Network

Communication Interface Module (CIM) devices are Safety-Related Equipment

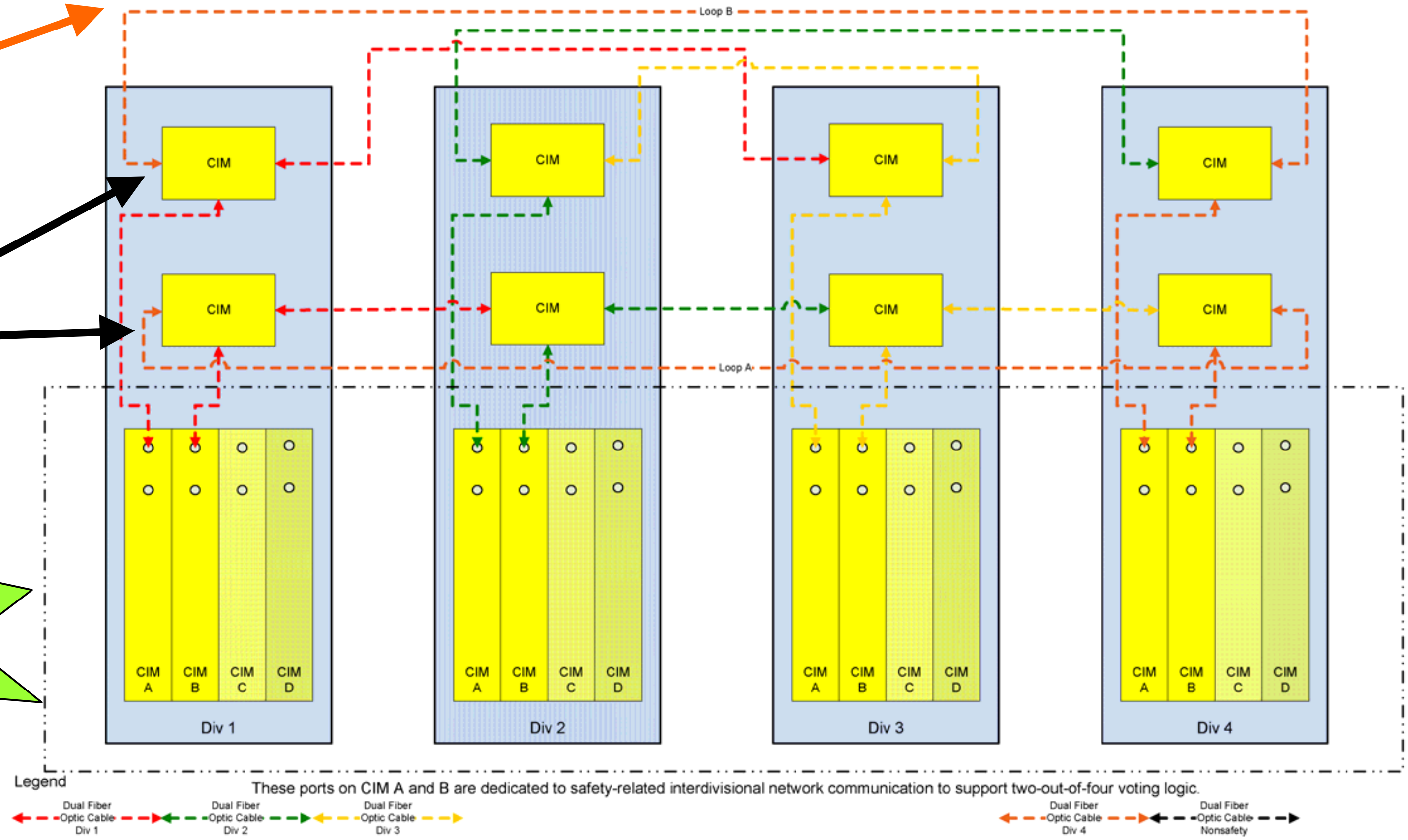


Figure 7.3-8 SSLC/ESF Inter-Divisional Communication Detail

Key Design Features...

- 2 Networks are DUAL
- Each Network is REDUNDANT
- Each Network is DEDICATED
- Messages are "AUTHENTICATED"

HITACHI

Determinism… SSLC/ESF "2-out-of-4"Network Loading
Example - Assumptions

assumption each interdivisional transmittal message on each 2 out of 4 network is: • One bit per Trip status per parameter • One bit for Divisional sensors bypass status • Message authentication	rates and capacities = 1024 bytes (1024 x 8 = 8192 bits)
assumption each division sends message at 10 X per second (conservative for expected 2 to 4 X per second)	= 1024 X 8 X 10 = 81920 bits/sec
each message is acknowledged (assumed same size)	= 81920 X 2 = 163840 bits/sec
there are four divisions (nodes or communication cards) on the network	= 163840 X 4 = 655360 bits/sec on network
network capacity = 100 Mbits/sec therefore network loading	= 655360/100000000 = 0.0066 = .6% (avg no data on network 99.4% of the time)
time "size" of single message on 100 Mbits/sec network	= 1024 X 8 = 8192 bits = = 8192 bits / 100000000 bits/sec = 81.92 microseconds
assumption max distance between divisions for 2 out of 4 communication path	= 30 m
fiber index of refraction	= 1.48
speed of light in fiber	= 300 million m/sec / 1.48 ~ 200 million m/sec
time for message to travel 30 meters	= 30 m / 200000000 m/sec = 0.15 microseconds 0.15 << 81.92 (travel time negligible)

Supporting Assumptions and Math are Industry Practice

HITACHI

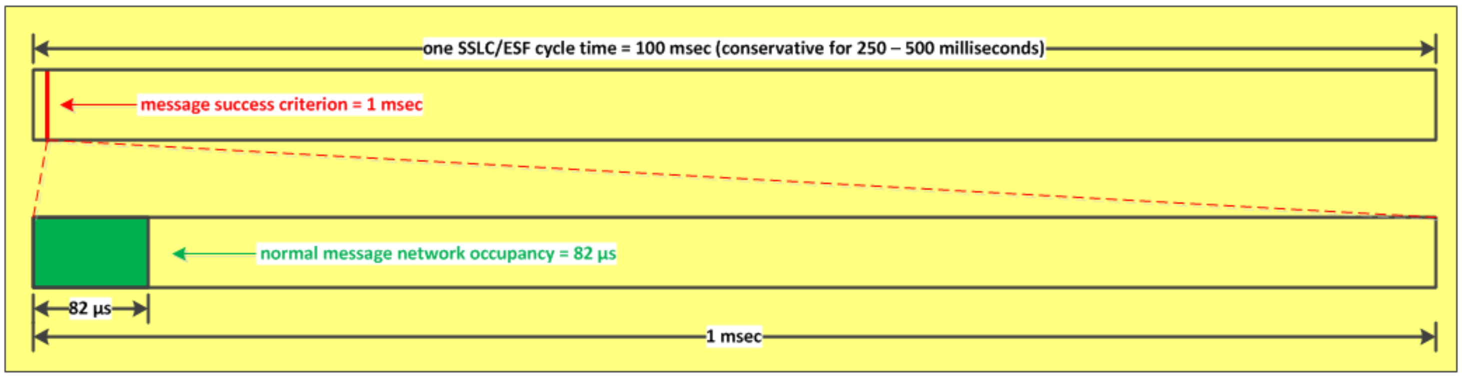
Determinism… SSLC/ESF "2-out-of-4" Network Loading Ethernet Collision Protocol

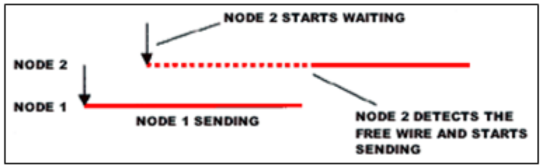
nodes monitor the network for ongoing messages

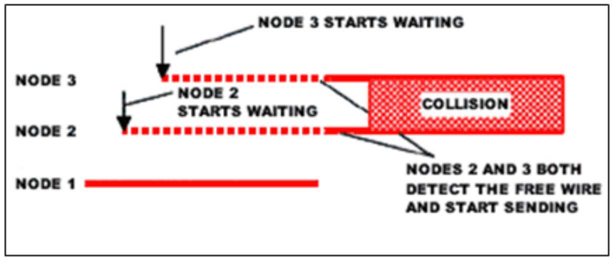
most of the time (99.4% in this example) the network is free and the nodes transmit without delay

if a second node wants the network while data is being transmitted it simply waits for its turn to send – the delay time is the first node's transmission time (81.92 microseconds in this example)

if two nodes try to access the network simultaneously (usually occurs when two nodes are waiting for another node's transmission to clear) they will notice the resulting collision, both nodes will it back off and wait up to two time slots (5.12 microseconds for a 100 Mbits/sec network) before retrying. If the retry fails, the maximum wait time is doubled, and the node waits a random period again. The algorithm continues until the network is acquired – typically 10 attempts (1024 slot delays) and declares an error after 16 attempts. The resulting randomness causes the "deterministic" concern but the probability of not getting a message through or waiting the maximum number of attempts becomes very small as the network speed increases and the message size and number of nodes decrease. For ESBWR the "criteria" for the two-out-of-four messages is (in this example) 10 X second (100 milliseconds) and a one millisecond (i.e. 1000 microseconds) delay is (for this example) is considered acceptable. A probabilistic analysis indicates that the chance of getting a message through in one millisecond on a bus loaded per our example in 100 years of operation is greater than 0.9999999







SSLC/ESF Dedicated and Lightly Loaded Ethernet is DETERMINISTIC

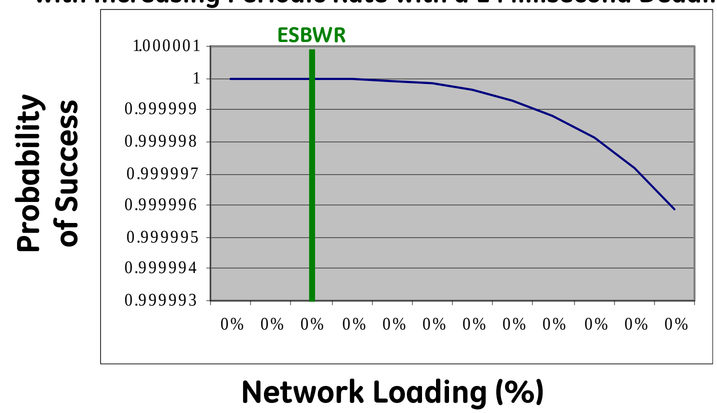
Determinism… Functionally Possible with Ethernet

Developed by Real-Time Innovations, Inc (www.rti.com)

Real-time applications fail when data isn't available on time. This spreadsheet lets you determine the probability you'll never get a program failure (that is, a delay longer than the required deadline) using Ethernet for real-time data delivery of high frequency, periodic data. To calculate the probability for your target environment, enter the network bandwidth, the size of the packets, the rate at which packets are sent (packets per second), and the application life cycle (in years). The results are shown under Network Loading (which tells you how much of the available bandwidth that particular combination is using) and Probability of Success. The tables and graphs that follow illustrate the impact on probability by varying just the message rate and the deadline.

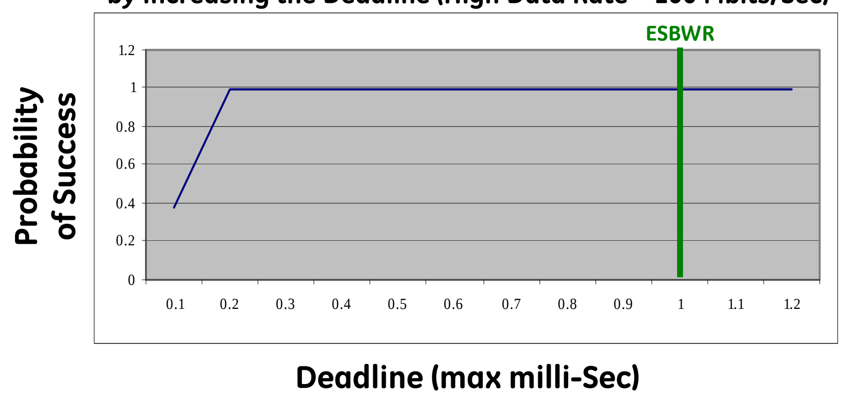
Network Bandwidth (Mbits/Sec)	Packet Size (bytes)	Msg Rate	Deadline (max ms)	Time (Years)	Network Loading	Probability of Success
100	1024	0	1	100	0%	1
100	1024	5	1	100	0%	1
100	**1024**	**10**	**1**	**100**	**0%**	**1**
100	1024	15	1	100	0%	0.99999998
100	1024	20	1	100	0%	0.99999993
100	1024	25	1	100	0%	0.99999982
100	1024	30	1	100	0%	0.99999963
100	1024	35	1	100	0%	0.99999932
100	1024	40	1	100	0%	0.99999884
100	1024	45	1	100	0%	0.99999814
100	1024	50	1	100	0%	0.99999716
100	1024	55	1	100	0%	0.99999585

Impact on Probability of Success
with Increasing Periodic Rate with a 1 Millisecond Deadline



Network Bandwidth (Mbits/Sec)	Packet Size (bytes)	Msg Rate	Deadline (max ms)	Time (Years)	Network Loading	Probability of Success
100	1024	10	0.1	100	0%	0.38190672
100	1024	10	0.2	100	0%	0.99874252
100	1024	10	0.3	100	0%	0.99996187
100	1024	10	0.4	100	0%	0.99996187
100	1024	10	0.5	100	0%	0.99999941
100	1024	10	0.6	100	0%	0.99999941
100	1024	10	0.7	100	0%	0.99999941
100	1024	10	0.8	100	0%	1
100	1024	10	0.9	100	0%	1
100	**1024**	**10**	**1**	**100**	**0%**	**1**
100	1024	10	1.1	100	0%	1
100	1024	10	1.2	100	0%	1

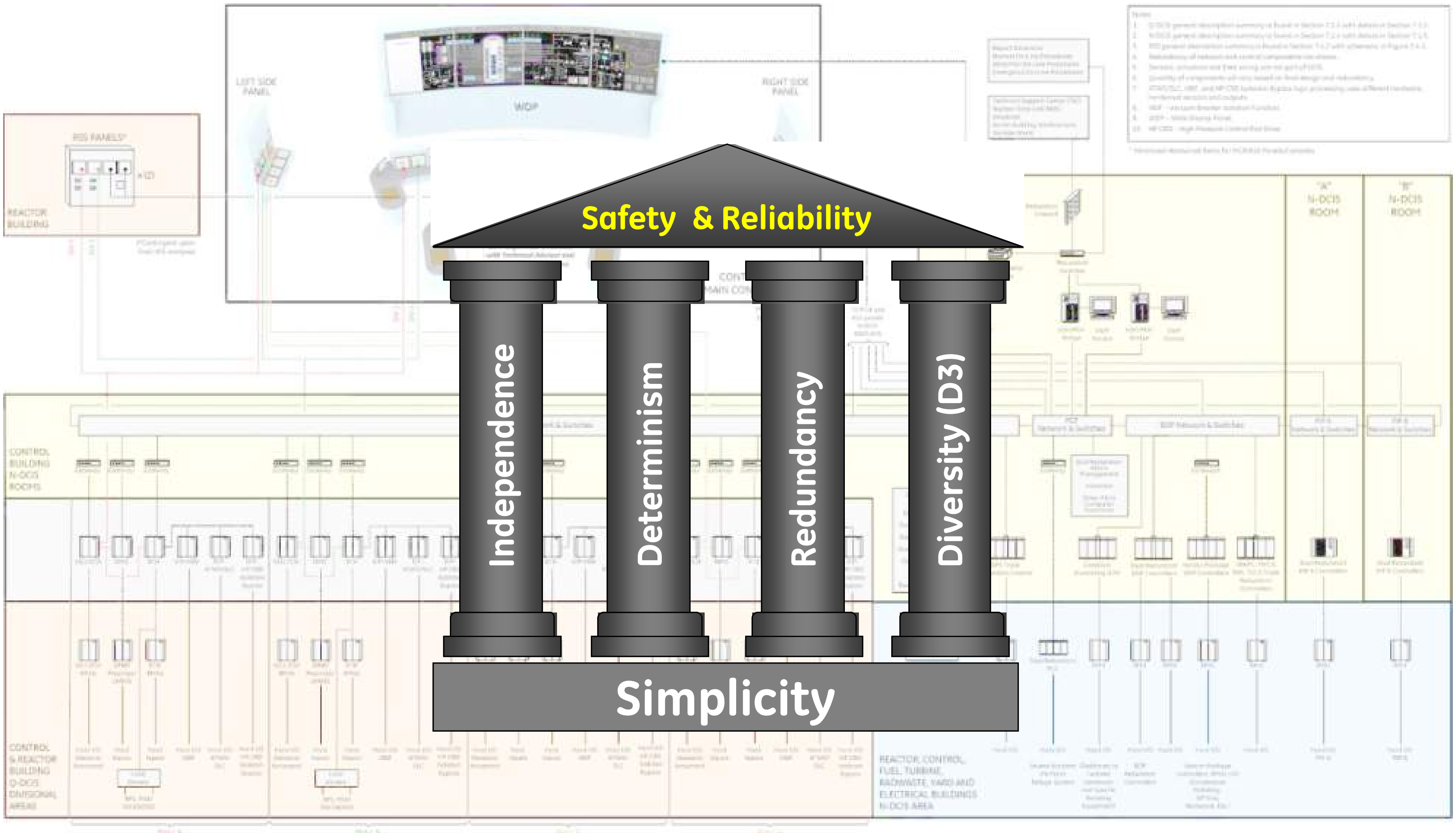
Impact on Probability of Success
by Increasing the Deadline (High Data Rate – 100 Mbits/Sec)



Properly designed and loaded – Probability of message delivery is ~100%
Ethernet is Functionally DETERMINISTIC

HITACHI

"4+1" Design Principles... Redundancy



Based on IEEE Std 603

Criteria for Safety Systems for Nuclear Power Generating Stations

HITACHI

Redundancy… Highlights

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:

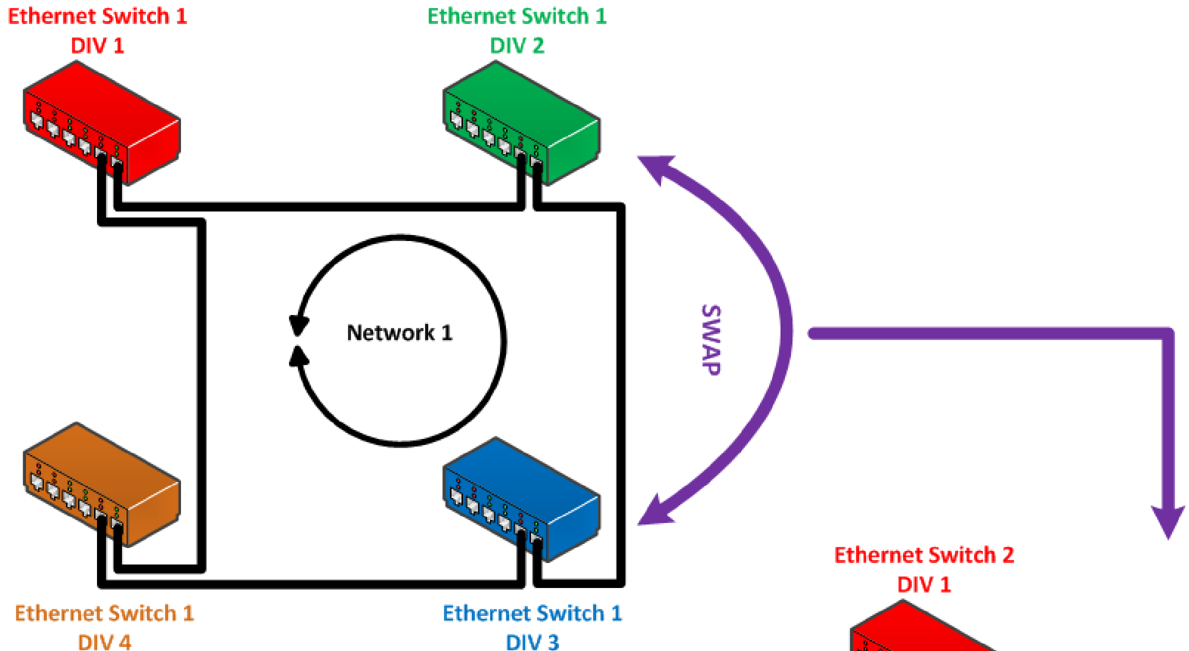
- Sensors, Controllers and Actuators

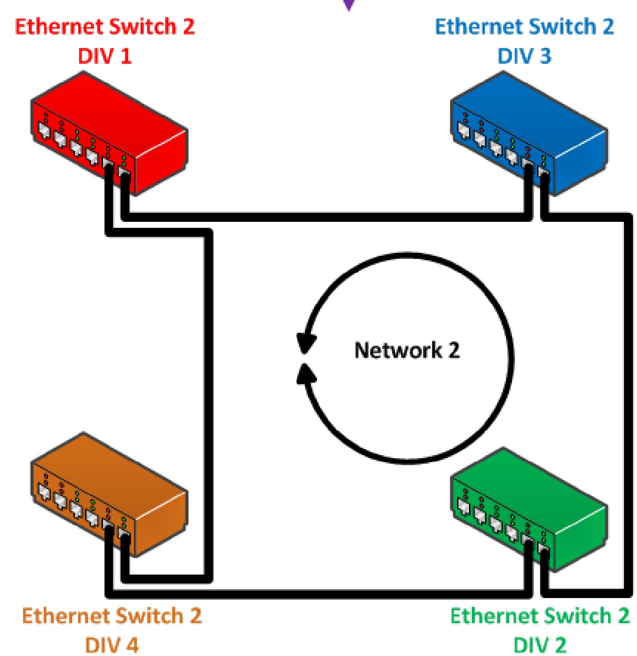
As required for plant availability including single failure proofing

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

ESBWR DCIS meets or exceeds requirements for REDUNDANCY

Redundancy… SSLC/ESF Ethernet Networks





Normal data flow in Network 1 and Network 2 are clockwise

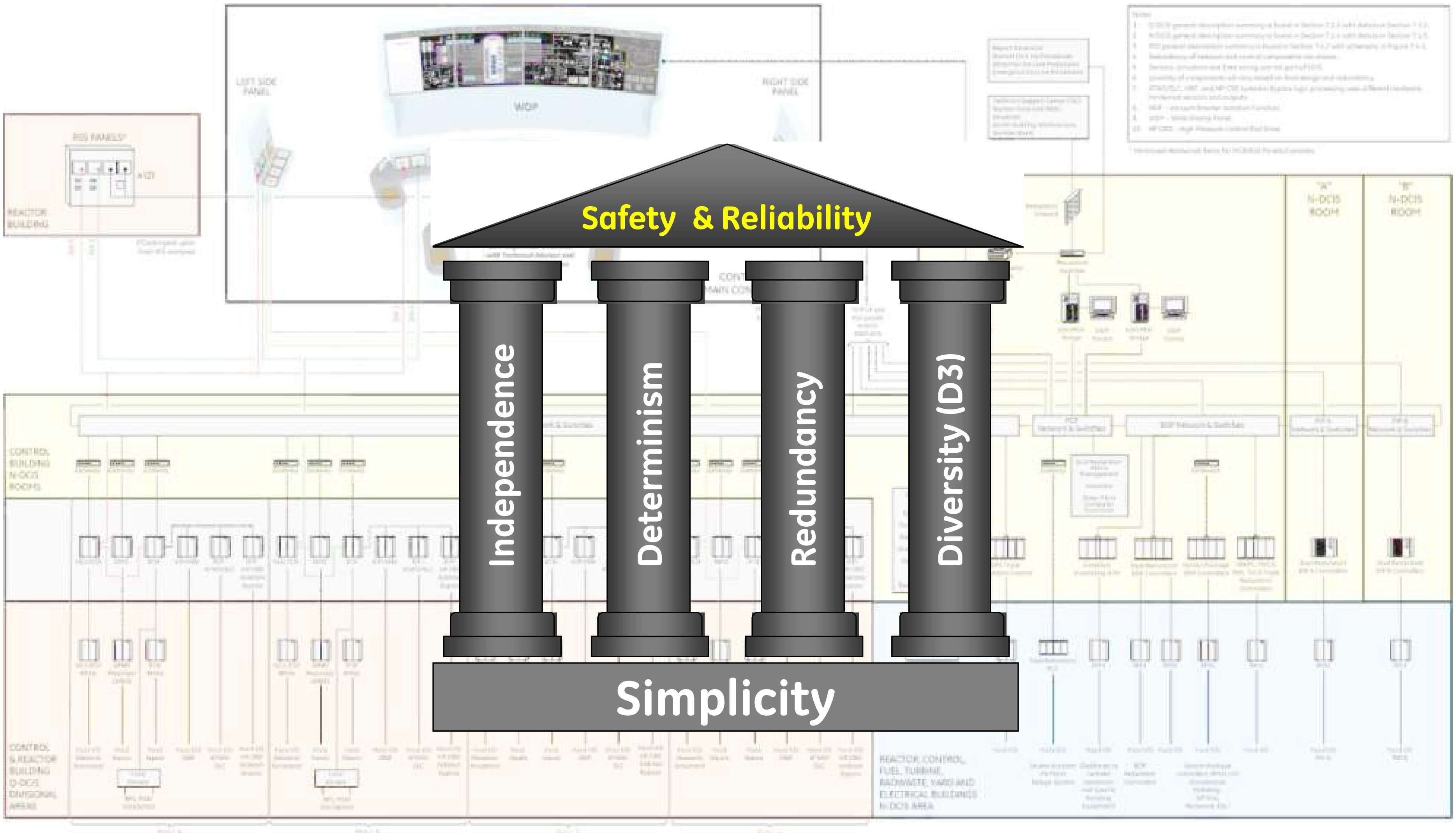
Each division sends its message (trip status, bypass status, message authentication) , on each network, using the normal data flow (clockwise) and expects to receive its message back from the other side in a specific amount of time. If the message does not return around the ring, the same division sends the same message again in the other direction (counter-clockwise) and an alarm is given

The configuration of Network 1 and Network 2 accommodate any one (N-1) or two (N-2) divisional failures

Fiber optic cable breaks will prevent any message from any division to return around the ring clockwise but will not prevent the message from reaching other divisions on the counter-clockwise path

Configuration of 2 Networks is N-2… 3 Failures to Cease Functioning

"4+1" Design Principles... Diversity



Based on IEEE Std 603

Criteria for Safety Systems for Nuclear Power Generating Stations

HITACHI

Diversity…

DCIS Platform Design

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)

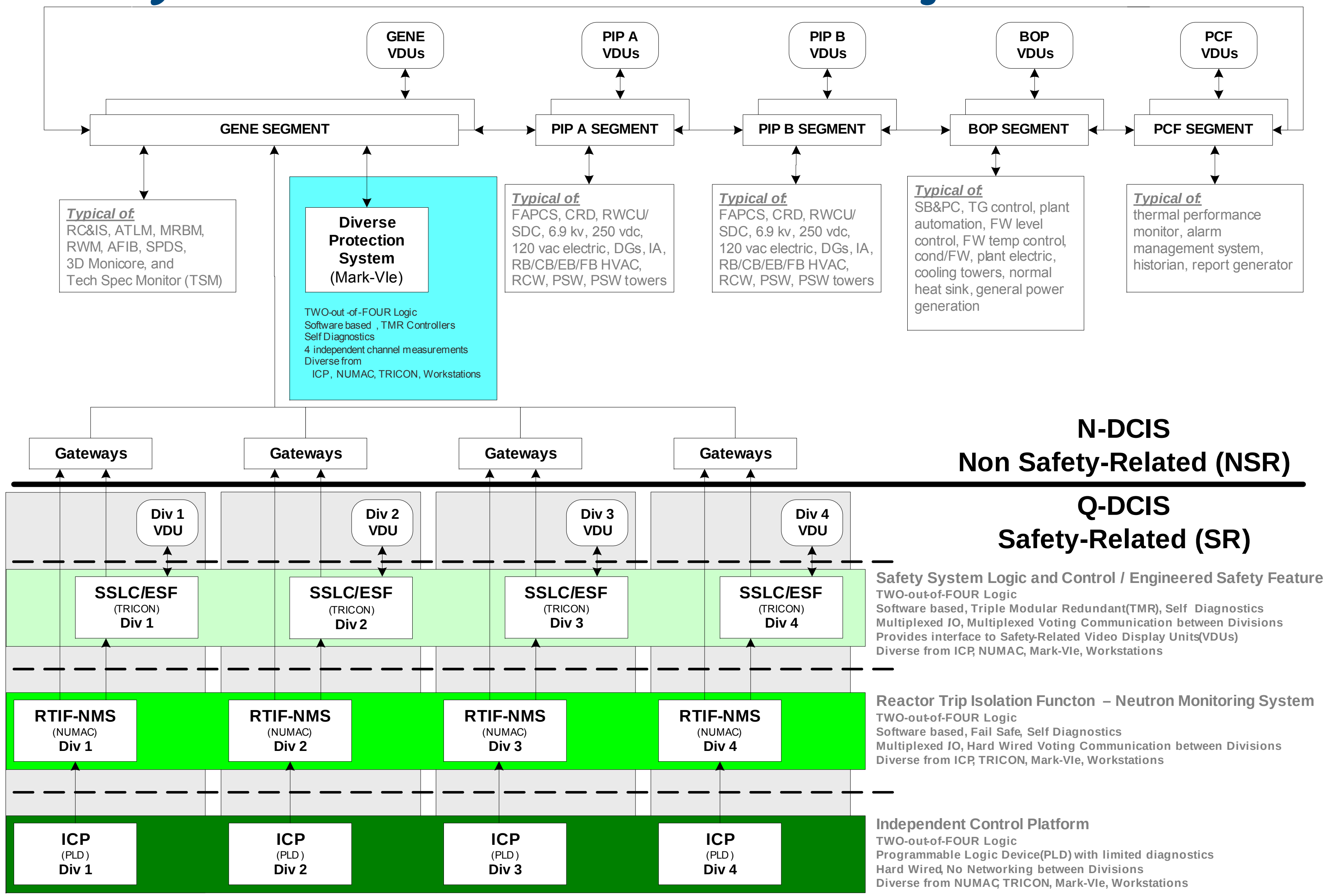
NOTE: Crosshatching denotes different platforms or networks.

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

ESBWR Hardware/Software (Architecture) Diversity Diagram

Essentially Unchanged Throughout ~5 Year Design Certification Process ESBWR inheritance from ABWR (Lungmen Project)

Diversity... 4 Major DCIS Platforms

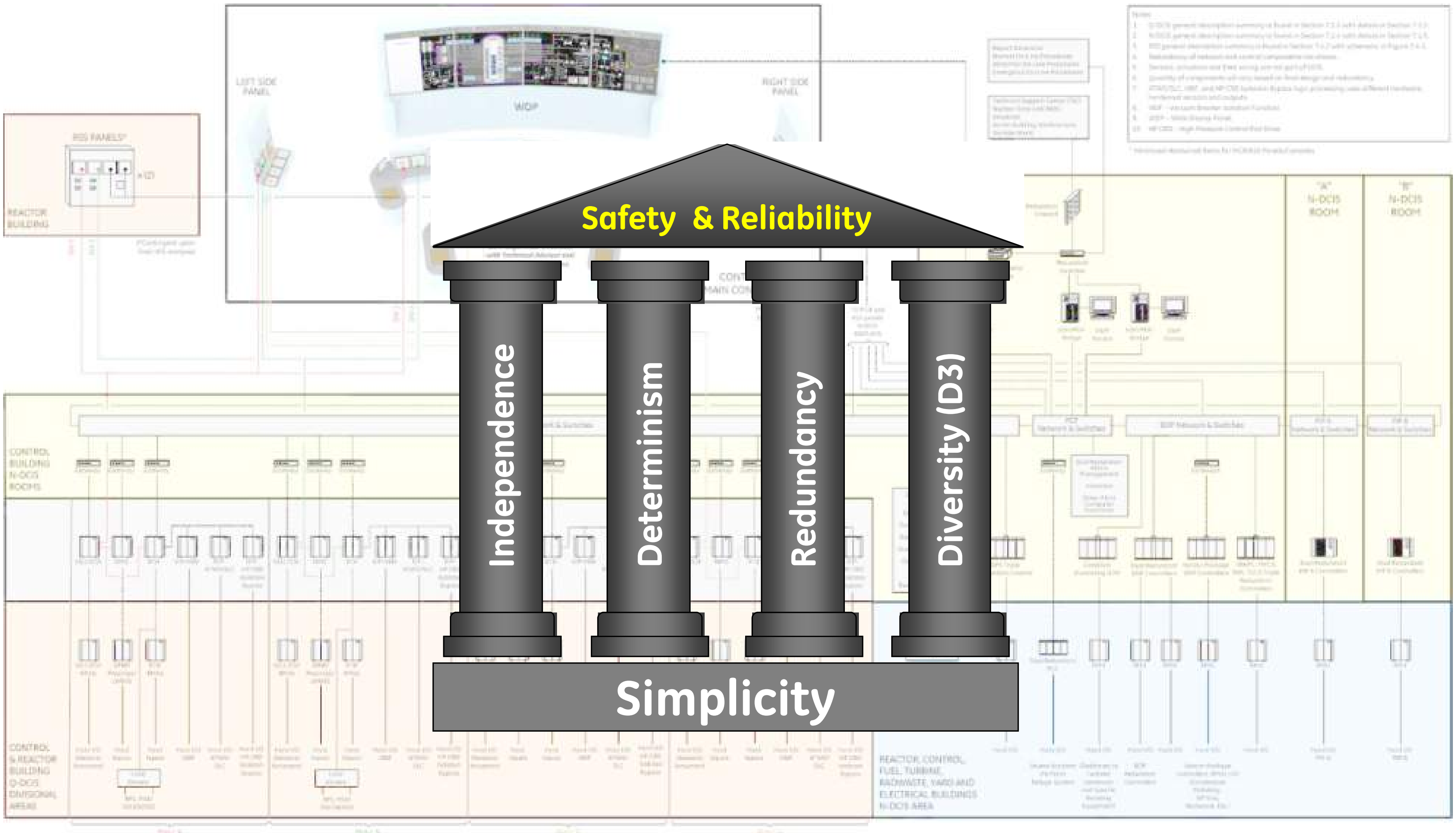


Derived from DCD Rev. 6 Figure 7.1-1 ESBWR Instrumentation and Control DCIS Simplified Network and Functional Block Diagram

3 Safety-Related and 1 DPS (RTNSS) in 4 DIVERSE Platforms

HITACHI

"4+1" Design Principles... Simplicity



Based on IEEE Std 603

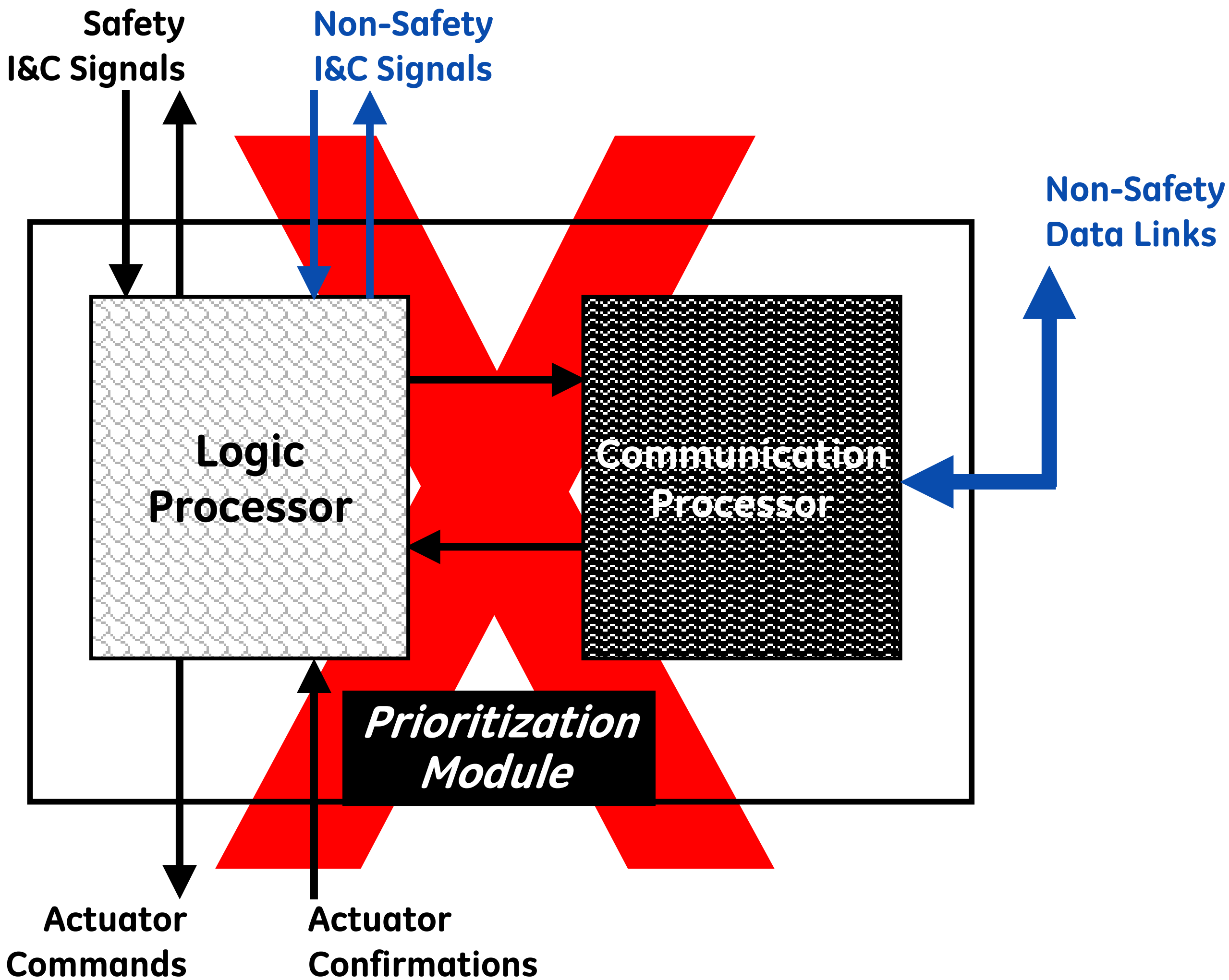
Criteria for Safety Systems for Nuclear Power Generating Stations

Simplicity… ESBWR's DCIS Approach

- DCIS functions are modularized and segmented to simplify requirements management, specification, design and testing
- Few plant process control functions per controller application to simplify requirements management, specification, design and testing
- No closed loop control over a shared network
- Design Certification cyber security is "designed in" to most systems and components rather than added on
- Remote Shutdown System (RSS) is designed as an auxiliary control room
- Use of optical fiber and remote multiplexing maximized to simplify fire protection analysis and design of cable trays, conduit, and raceways

Given nuclear regulations and cyber security requirements…
ESBWR's DCIS architecture and design is as "SIMPLE" as possible

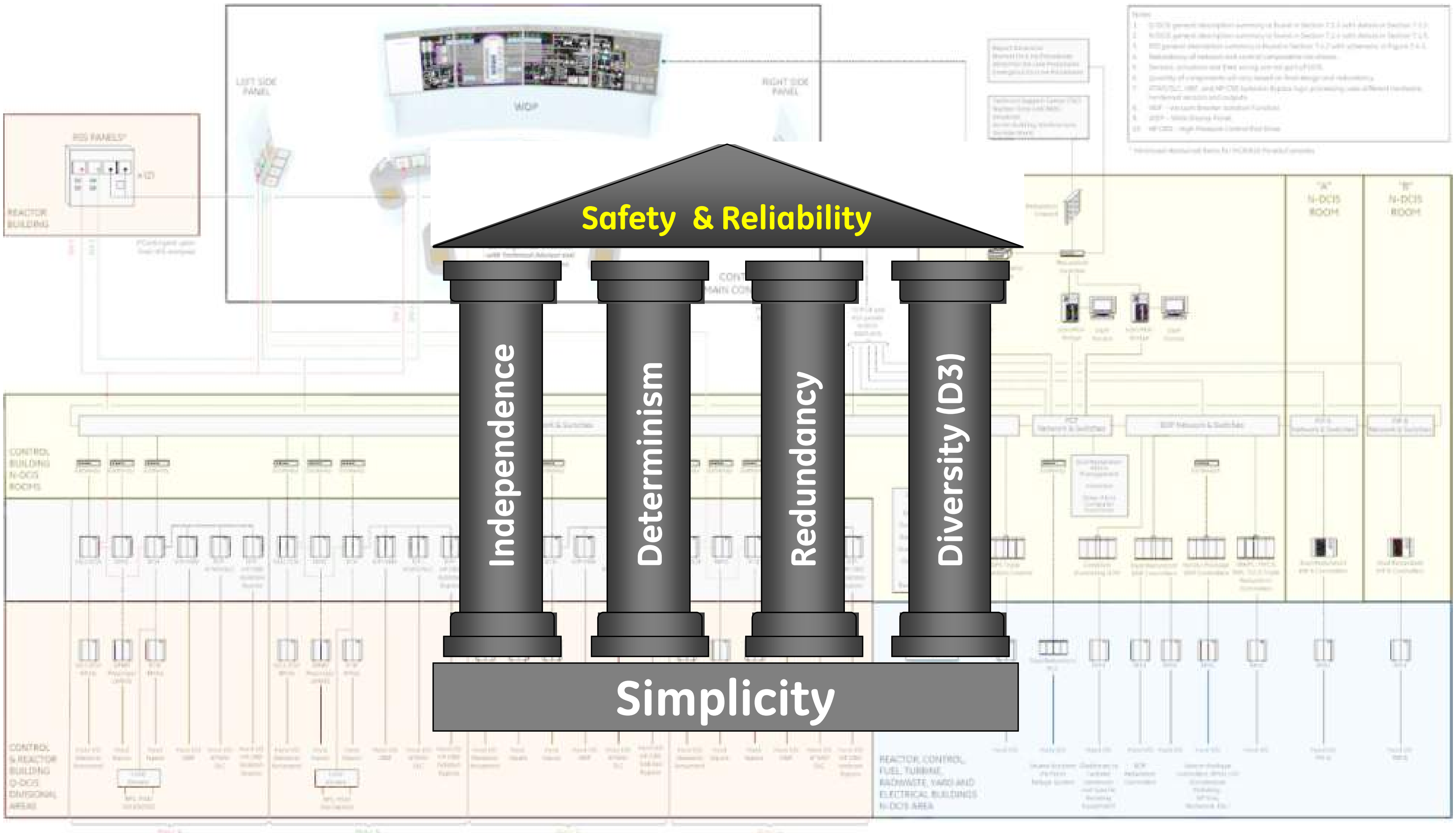
Simplicity… ESBWR Does NOT Use Prioritization Module



ISG-04 acknowledges possible use of "Prioritization Module" but…
Introduces COMPLEXITY and IEEE Std 603 Compliance challenges and…
May require challenging combinatorial tests to demonstrate conformance

HITACHI

Implementation Design Artifacts… Logic Diagrams



Based on IEEE Std 603

Criteria for Safety Systems for Nuclear Power Generating Stations

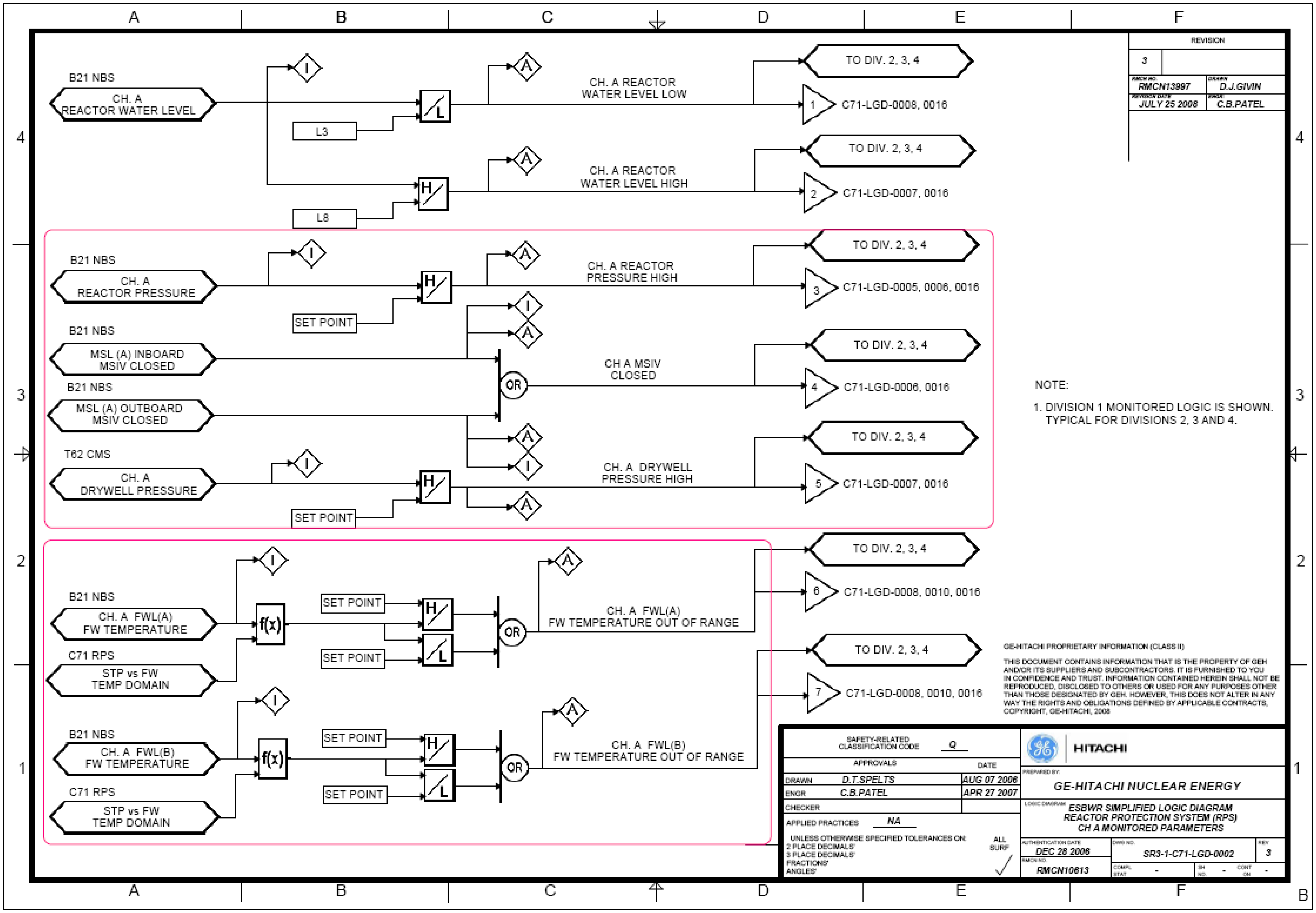
HITACHI

Implementation Design Artifacts… Logic Diagrams

- **Logic Diagrams NOT required to be submitted by regulation for Design Certification**
- **GEH provided "typical" Logic Diagrams based on DCD Rev. 5**
  - Purpose was to substantiate high level design approaches
- **Logic Diagrams are part of the Detailed Design Process… governed by Software Development Life Cycle (SDLC) per 3 Tier 2* LTRs (i.e., SMPM, SQAPM, CySPP)**
  - Created as Functional Logic Block Diagrams (FLBDs) during Planning Phase
  - Iterates under configuration management into Detailed Logic Diagrams (DLDs) as overall plant design matures
  - Iterations controlled via plant system (MPL) Design Reviews and Controls specific Baseline Review Records (BRRs)
  - Configuration management thru 6 Phases…
    Planning, Rqmts, Design, Implementation, Test, and Installation
  - BRRs are foundation for ITAAC Closure Reports

Logic Diagrams do and will exist… Key deliverables of Detailed Design

Logic Diagrams… RPS Monitored Parameters Example



Typical or "simplified" Logic Diagrams provided for DCD Rev. 5

HITACHI

Logic Diagrams in ITAACs…

RTIF Example

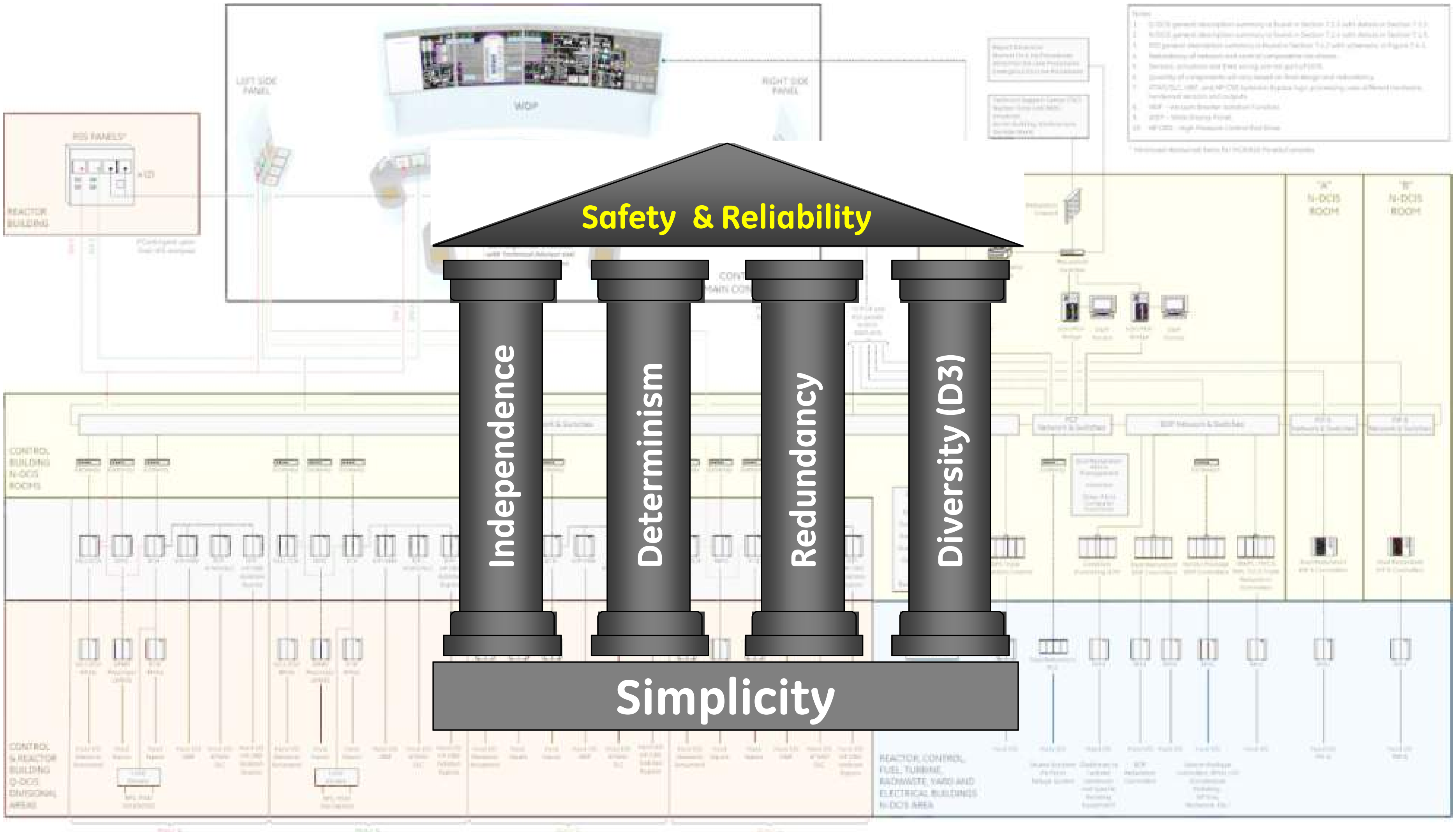
Sec. 3.2 Software Development,Table 3.2-1 2 a/b 1

2a1.	The planning phase activities detailed in the RTIF software plans	The planning phase outputs are inspected and analyzed for the RTIF software	Planning Phase Summary BRR(s) exist and conclude that the RTIF software projects
2b1.	The requirements phase activities detailed in the RTIF software plans	The requirements phase outputs are inspected and analyzed for the RTIF	Requirements Phase Summary BRR(s) exist and conclude that the RTIF software
2c2.	The design phase activities detailed in the NMS software plans and CySP	The design phase outputs are inspected and analyzed for the NMS software projects.	Design Phase Summary BRR(s) exist and conclude that the NMS software projects
2d1.	The implementation phase activities detailed in the RTIF software plans	The implementation phase outputs are inspected and analyzed for the RTIF	~~Implementation Phase Summary BRR(s) exist and conclude that the~~ RTIF software
2e1.	The test phase activities detailed in the RTIF software plans and CySP	The test phase outputs are inspected and analyzed for the RTIF software projects.	~~Test Phase Summary BRR(s) exist and conclude that the~~ RTIF software projects
3a1.	The installation phase activities detailed in the RTIF software plans and CySP are completed for the RTIF software projects.	The installation phase outputs for the RTIF software projects, including RTIF FAT and RTIF Cyber Security FAT, are inspected and analyzed .	~~Installation Phase Summary BRR(s) exist and conclude that the~~ RTIF software projects installation phase activities were performed in compliance with the RTIF software plans and CySP as derived from SMPM, SQAPM, and CySPP.
3a2.	The RTIF software projects performs as designed.	FAT is performed on the RTIF software projects.	~~RTIF FAT report(s) exist and concludes that the~~ RTIF software projects is in compliance with the RTIF software plans as derived from the SMPM, SQAPM, and CySPP.
3a3.	The RTIF software projects is cyber secure.	A cyber security FAT will be performed for the RTIF software projects.	~~RTIF cyber security FAT report(s) exist and conclude that the~~ RTIF software projects is in compliance with the RTIF
3j1.	The RTIF software projects performs as designed.	A RTIF software projects SAT is performed.	~~RTIF cyber security SAT report(s) exist and conclude that t~~The RTIF software projects is in compliance with the RTIF CySP as derived from the SMPM, SQAPM, and CySPP.
3j2.	The RTIF software projects is cyber secure.	A RTIF software projects cyber security SAT is performed.	~~RTIF cyber security SAT report(s) exist and conclude that the~~ RTIF software
3i.	The complete ESBWR instrumentation and control systems with sensors and actuators is capable of operating as designed.	An overlapping and encompassing SAT is performed on the as-built platforms and network segments.	~~The Installation Phase Summary BRR for the complete ESBWR instrumentation and control system SAT exists and concludes that t~~The complete ESBWR instrumentation and control system with sensors and actuators is capable of operating as designed and is in compliance with the software projects plans and CySP as derived from the SMPM, SQAPM and CySPP.

Logic Diagrams Configuration Managed Throughout…

HITACHI

Questions?



Based on IEEE Std 603

Criteria for Safety Systems for Nuclear Power Generating Stations

HITACHI

Back-Up

What is the Independent Control Platform (ICP)?

The ICP platform is fundamentally and technologically diverse from the other two safety-related Q-DCIS hardware/software technology platforms; RTIF-NMS and SSLC/ESF. The ICP digital hardware platform is implemented in a system composed of custom programmable logic devices (CPLDs). The ICP safety-related function is not changeable after initial configuration and setup. The ICP implementation that performs its safety-related control function does not execute, run, or use a cyclic real-time executive or operating system or any associated controller application program to perform its safety function. The ICP implementation that performs its safety-related control function does not include a system clock as there is no cyclic real-time executive. The overall ICP platform does include monitoring and diagnostics programs but these programs are independent from the implementation that performs the safety-related control function. The ICP implementation that performs the safety-related control functions are implemented in CPLDs and are relatively simple functions. The ICP functions are only required after the complete failure of RTIF-NMS or SSLC/ESF functions.

The design objective with ICP implementation is to configure them to be nearly 100% testable. The currently available CPLD logic and associated digital circuit engineering design and configuration tools are software based. There is a possibility that system level or functional logic and control requirement errors exist or that the engineering design and configuration tools used to implement the CPLDs contain a latent defect. Identifying, dispositioning, and remediating both of these types of errors are addressed by the rigorous and structured system and software development lifecycle (SDLC) as described in Section 7B. SOFTWARE DEVELOPMENT. The ICP platform does not execute, run, or use any active software to perform its safety-related control function, the functions implemented are simple, and it is designed to be nearly 100% testable. Therefore, the ICP digital hardware platform is highly immune to common-cause failure (CCF) with respect to its own software based engineering design and configuration tool, itself, as well as the other two Q-DCIS hardware/software technology platforms as well as the systems and functions implemented on them.

ICP is highly IMMUNE to CCFs and is DIVERSE from RTIF-NMS and SSLC/ESF

DCD Tier 2 Ch 7 I&C – Uses of… "deterministic"

7.1 Introduction

7.1.3.2.7 Data Communication Systems

The DCIS data communication functions are embedded within the Q-DCIS and the N-DCIS architectures. Safety-related Q-DCIS internal and external communication protocols are **deterministic**.

7.1.6.4 Regulatory Guides

A discussion of the general conformance of the I&C equipment to RGs is provided below.

The following sections are noted in IEEE Std. 7-4.3.2 as specifically addressed by the NRC in RG 1.152:

- Annex F, "Computer reliability." The NRC states that quantitative reliability goals are not the only means, and does not endorse this method as the sole means of meeting the regulations for reliability of digital computers. The NRC acceptance is based on **deterministic** criteria.

7.1.6.6.1.17 Automatic Control (IEEE Std. 603, Sections 6.1 and 7.1)

The RTIF-NMS, and ATWS/SLC logic automatically initiates reactor trip and the RTIF for LD&IS (non-MSIV), SSLC/ESF and VBIF logic automatically actuates the ESF that mitigate the consequences of DBEs. These automatic protection actions are implemented through two-out-of-four voting logic whenever one or more process variables reach their actuation setpoint. Variables are monitored and measured by each of the RTIF - NMS, ATWS/SLC, SSLC/ESF, and VBIF divisions.

Plant-specific setpoint analyses determine the protection systems' instrument setpoints using the methodology described in Reference 7.1-9. The GEH setpoint methodology uses plant-specific setpoint analyses to ensure that the combination of characteristics of the instruments such as range, accuracy and resolution provide the required high probability that the analytical limits in Chapter 15 analyses are not exceeded for the safety-related control system components and systems of the safety-related I&C. The response times of the I&C systems are assumed in the safety-related analyses and verified by plant specific surveillance testing or system analyses. The Q-DCIS application software, hardware processing rates, and internal and external communication system design ensures that the real-time performance of the safety-related control systems is **deterministic**.

7.2 Reactor Trip System

7.2.1.3.5 Branch Technical Positions

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The real-time performance of RPS in meeting the requirements for safety-related system trip and initiation response conforms to BTP HICB-21. The real-time performance of the safety-related control system is **deterministic** based on the Q-DCIS internal and external communication system design and the RPS logic design. Timing signals are neither exchanged between divisions of independent equipment nor between logics within a division.

7.3 Engineered Safety Features Systems

7.3.5.3.5 Branch Technical Positions

BTP HICB-21, Guidance on Digital Computer Real-Time Performance:

- Conformance: The real-time performance of SSLC/ESF in meeting the requirements for safety-related system trip and initiation response conforms to BTP HICB-21. Each SSLC/ESF controller operates independently and asynchronously with respect to other controllers. The real-time performance of the safety-related control system is **deterministic** based on the Q-DCIS internal and external communication system design and the SSLC/ESF controller design. Timing signals are not exchanged – neither between divisions of independent equipment, nor between controllers within a division.

Logic, Controllers, and Communications are by design DETERMINISTIC

DCD Tier 2 Ch 7 I&C – Uses of… "error"

7.1.3.4 Q-DCIS Testing and Inspection Requirements

2nd Para.:

The Q-DCIS uses three diverse safety-related platforms: RTIF-NMS (RPS, NMS, and the MSIV isolation function) and SSLC/ESF, and ICP. The RTIF-NMS and SSLC/ESF platforms are accessible for testing purposes. Their continuous automatic on-line diagnostics detect data transmission **errors** and hardware failures at the replaceable card or module level. On-line diagnostics for RTIF-NMS and SSLC/ESF are qualified as safety-related in conjunction with functional software qualification, and also meet the self-diagnostic characteristics for digital computer based protection systems recommended by IEEE Std. 7-4.3.2.

7th Para.:

The ICP is similar to the RTIF-NMS and SSLC/ESF platforms in that it contains self-diagnostic capabilities to ensure that the platform is functioning properly. The ICP self-diagnostics possess the capability to:

- Detect data transmission **errors**,
- Detect hardware failures, and
- Check platform operability.

7.1.6.6.1.8 Capability for Testing and Calibration (IEEE Std. 603, Section 5.7)

1st Para., 5th Sentence:

The I&C equipment has built-in self-diagnostic functions to identify critical failures such as loss of power and data **errors**. The Q-DCIS meets the requirements outlined in this section. Refer to Subsections 7.1.3.3.6, 7.1.3.3.7, 7.1.3.4 and 7.1.3.5.

7.3.5.4 Testing and Inspection Requirements

2nd Para.:

The self-testing includes continuous error checking of transmitted and received data on the serial data links of each SSLC/ESF controller; for example, **error** checking by parity check, checksum, or Cyclic Redundancy Checking (CRC) techniques. Self-test failures are indicated to the operator at the MCR console and recorded in a log maintained by the PCF of the N-DCIS.

7.8.2.1 Design Techniques for Optimizing Safety-Related Hardware and Software

1st Para., 8th Bullet, 3rd sub-bullet:

Code is segmented by system and function:

- Fixed message formats are used for plant sensor data, equipment activation data, and diagnostic data. Thus, corrupted messages are detected by **error**-detecting software in each digital instrument;

7.8.2.2.1 System Level Defenses

1st Para., 2nd Bullet:

Operational defenses include:

- Automatic **error** checking on all multiplexed transmission paths. Only the last valid data is used for logic processing. If a permanent fault is detected, the channel alarms and a trip is initiated for the RPS and MSIV isolation functions;

2nd Para.:

Functional defenses include:

- Automatic **error** detection. This permits early safe shutdown or bypass before common mode effects occur. Instantaneous, simultaneous, and undetected failure on a common mode **error** is unlikely; and

"Errors" are detected and mitigated…

Control and Communications are DETERMINISTIC

DCD Tier 2 Ch 7 I&C – Uses of… "checksum"

7.1.3.4 Q-DCIS Testing and Inspection Requirements

6th Para.:

Both RTIF-NMS and SSLC/ESF are cyclically tested from the sensor input point to logic contact output. The self-diagnostic capabilities include power supply checks, microprocessor checks, system initialization, watchdog timers, memory integrity checks, I/O data integrity checks, communication bus interfaces checks, and checks on the application program (**checksum**). Cyclically monitored items include:

- inputs to the I/O for unacceptably high/low levels;
- Proper execution of application code/checksum verification of code integrity;
- Internal clocks;
- Functionality of input cards/modules, and their main processor communication;
- Main processor communication with the output contact (SSLC/ESF platform);
- Inter-divisional communication between RPS and NMS logic processors or logic functions (RTIF-NMS platform);
- Functionality of the output contact by momentarily reversing its state and confirming readiness to change state on demand (SSLC/ESF platform); and
- Power supplies.

7th Para.:

Subsequent to verification and validation (V&V) of software during factory and preoperational testing in accordance with approved test procedures, there is no mechanism for the RTIF-NMS or SSLC/ESF code, response time, or coded trip setpoints to inadvertently change. For user adjustable parameters a new **checksum** is calculated at the time acceptable changes are implemented. The new checksum is used from that point forward to validate the application software.

7.3.5.4 Testing and Inspection Requirements

3rd Para.:

The self-testing includes continuous error checking of transmitted and received data on the serial data links of each SSLC/ESF controller; for example, error checking by parity check, **checksum**, or Cyclic Redundancy Checking (CRC) techniques. Self-test failures are indicated to the operator at the MCR console and recorded in a log maintained by the PCF of the N-DCIS.

"Checksums" used to identify and mitigate them…
Control and Communications are DETERMINISTIC

DCD Tier Ch 7 I&C – Uses of… “interrupt” & “query”

7.1.3.3.2 Communication Pathways (CIMs, Fiber-Optic Cable, Datalinks, and Nonsafety-Related Gateways)

4th Para.:

Safety-related software is as simple as possible so that Q-DCIS components have neither **interrupts** from nonsafety-related devices nor do they respond to nonsafety-related component **queries** for information. The Q-DCIS components simply put information on the safety-related (Q-DCIS) networks in a known format so that other safety-related devices can retrieve what is needed for their function. Self-diagnostics information is also put on the DCIS networks.

7.1.3.3.3 Nonsafety-Related Gateways

1st Para.:

The nonsafety-related gateways translate the information sent between the Q-DCIS (through the required isolation, via datalinks and fiber-optic cable) and the N-DCIS into a format that the other portion of the DCIS (either N-DCIS or Q-DCIS) can apply. The N-DCIS gateways package the safety-related information into the necessary message packets to support specific N-DCIS components for monitoring and alarm management purposes. The N-DCIS gateways also respond to **interrupts** and **queries**. Safety-related to nonsafety-related communication pathways that do not involve nonsafety-related gateways use safety-related fiber-optic CIMs (which provide the safety-related isolation), datalinks, and fiber-optic cable.

7.1.4.5 N-DCIS Testing and Inspection Requirements Summary

2nd Para.:

The N-DCIS controllers, displays, monitoring and input and output communication interfaces function continuously during normal power operation. Abnormal operation of these components can be detected during plant operation. In addition, the controllers are equipped with on-line diagnostic capabilities to identify and isolate failure of I/O signals, buses, power supplies, processors, and inter-processor communications. These on-line diagnostics can be performed without **interrupting** the normal operation of the N-DCIS.

“Interrupts” and “Queries” are not used in or recognized by safety systems…

Control and Communications are DETERMINISTIC

HITACHI

DCD Tier 2 Ch 7 I&C – Uses of… “watchdog timer”

7.1.2.5 Q-DCIS Testing and Inspection Requirements Summary

1sh Para.:

The Q-DCIS integrated hardware and software functions, including the network parameters and data status, are checked and tested together. The Analog-to-Digital (A/D) converters in the RMUs are the only components requiring periodic calibration checks. Key diagnostics include:

- The central processing unit (CPU) status check,
- Parity checks, **watchdog timer** status,
- Voltage level in controllers,
- Data path integrity and data validation checks,
- Data cycling time, and
- Processor clock time.

7.1.3.4 Q-DCIS Testing and Inspection Requirements

4th Para.:

The RTIF-NMS hardware has **watchdog timers** for various logic processors and logic functions that monitor the execution of the software. If the software stops executing (suspending the self-diagnostics), its watchdog timer resets the affected logic processor or logic function. This results in a channel trip and alarm while the logic processor or logic function is resetting..

5th Para.:

The SSLC/ESF platform is a Triple Modular Redundant (TMR) system, with three main processors. The main processors are monitored by **individual watchdog timers** that reset or fail a main processor depending on the severity of the problem. A single or double main processor failure causes alarms, but the division continues to function to provide the required automatic protective actions.

6th Para.:

Both RTIF-NMS and SSLC/ESF are cyclically tested from the sensor input point to logic contact output. The self-diagnostic capabilities include power supply checks, microprocessor checks, system initialization, **watchdog timers**, memory integrity checks, I/O data integrity checks, communication bus interfaces checks, and checks on the application program (checksum). Cyclically monitored items include:

6th Para., 4th Heading – Response Time Test:

The response time test is performed by a series of sequential, overlapping, or total steps to measure the entire response time. The logic processor or logic function self-diagnostics and the TSM support the performance of the response time test for the safety-related platforms. **Watchdog timers** monitor logic processor or logic function internal clocks and alarms for out-of-limit conditions and the completion of application code per logic processor or logic function cycle. Since the clocks set the response time, there is no mechanism for the response time to change without alarm or trip. All time delays incorporated into system logics are performed by software and the values are set during factory and preoperational testing in accordance with approved test procedures. Subsequent to final V&V of the code, there is no mechanism for the time delay values to inadvertently change. The response time tests for the remaining portions (i.e. sensors [except neutron radiation detectors] and final control elements/actuators) are performed separately from self-diagnostics and the TSM.

7.8.2.1 Design Techniques for Optimizing Safety-Related Hardware and Software

1st Para., 9th Bullet:

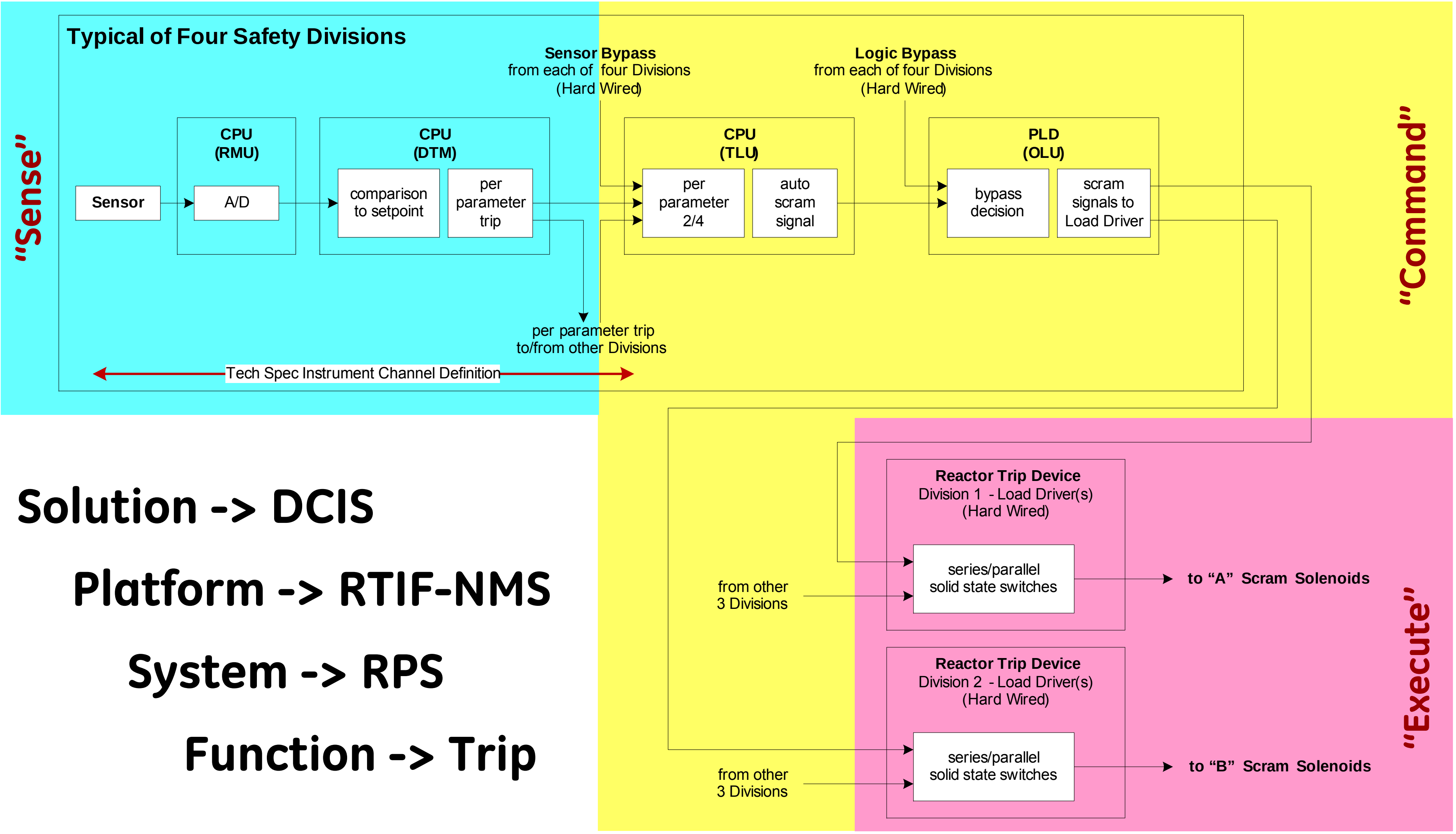
In addition to the DPS, other techniques ensure safety-related system reliability by minimizing both random and common mode failure probabilities.

- Software design uses recognized defensive programming techniques, backed up by self-diagnostic software and hardware **watchdog timers**;.

“Watchdog Timers” monitor software – Enable completion of protective action…

Control and Communications are DETERMINISTIC

Simplicity... A Typical Example - RPS



Solution -> DCIS

Platform -> RTIF-NMS

System -> RPS

Function -> Trip

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

Decompose COMPLEX into SIMPLE elements... Systems Engineering

Each Control Function partitioned into Sense – Command - Execute

Logic Diagrams… RPS Monitored Parameters Example

Software Management Program Manual (SMPM) NEDE-33226 (Tier 2*)

Software Quality Assurance Program Manual (SQAPM) NEDE-33245 (Tier 2*)

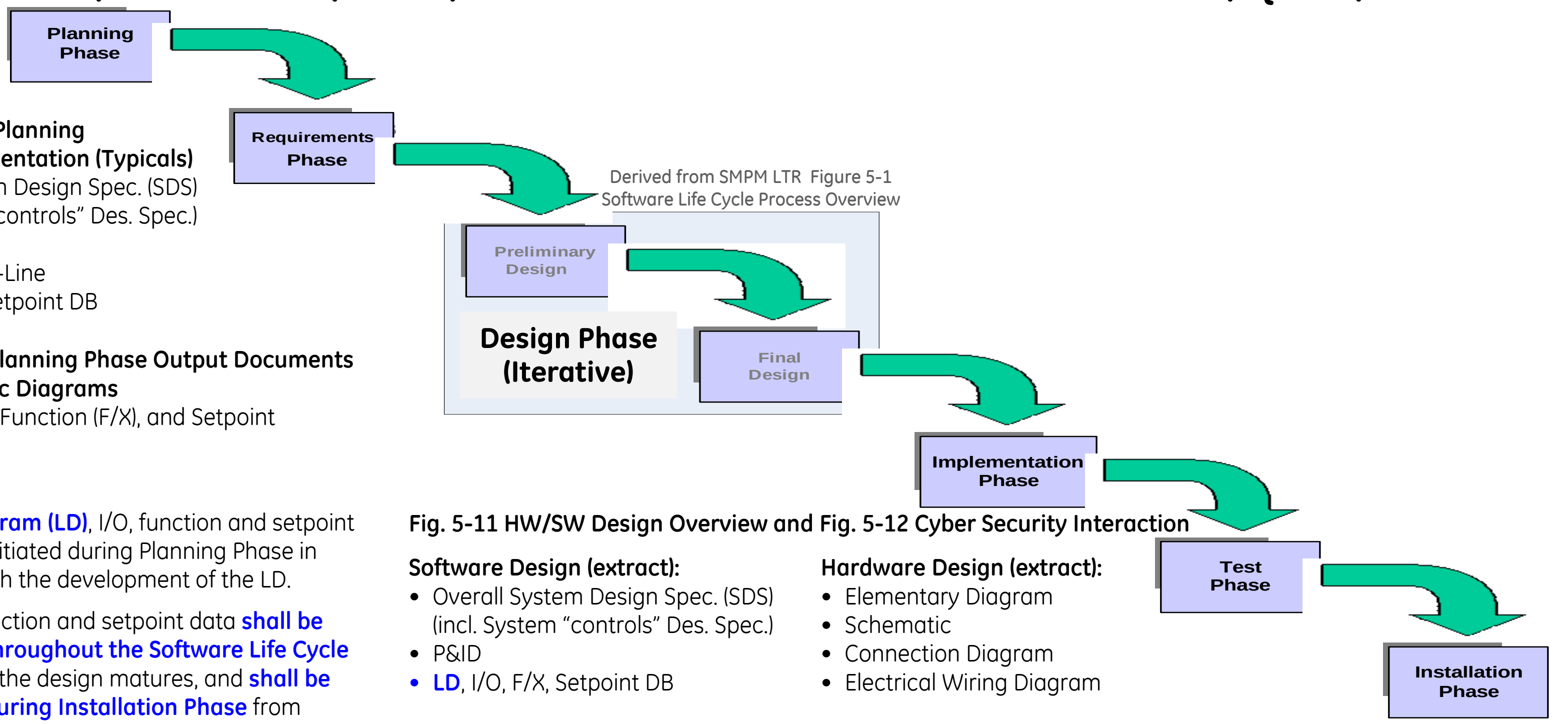


Fig. 5-2 SDLC – Planning Concept Documentation (Typicals)

- Overall System Design Spec. (SDS) (incl. System "controls" Des. Spec.)
- P&ID
- Electrical One-Line
- LD, I/O, F/X, Setpoint DB

Table 5.6-1 Planning Phase Output Documents
Item 6 – Logic Diagrams
(includes I/O, Function (F/X), and Setpoint Database)
Note (*) :

Logic Diagram (LD), I/O, function and setpoint data are initiated during Planning Phase in parallel with the development of the LD.

LD, I/O, function and setpoint data **shall be updated throughout the Software Life Cycle phases** as the design matures, and **shall be finalized during Installation Phase** from which **"As Built" DLDs** and **SLDs** are produced.

Remark::
Generally, design process begins with a Functional Logic Block Diagram (FLBD) or equivalent and matures into a final Detailed Logic Diagram (DLD). Simplified Logic Diagrams (SLDs) are developed from the "As Built" DLDs and are a customer deliverable.

Fig. 5-11 HW/SW Design Overview and Fig. 5-12 Cyber Security Interaction

Software Design (extract):

- Overall System Design Spec. (SDS) (incl. System "controls" Des. Spec.)
- P&ID
- LD, I/O, F/X, Setpoint DB

Hardware Design (extract):

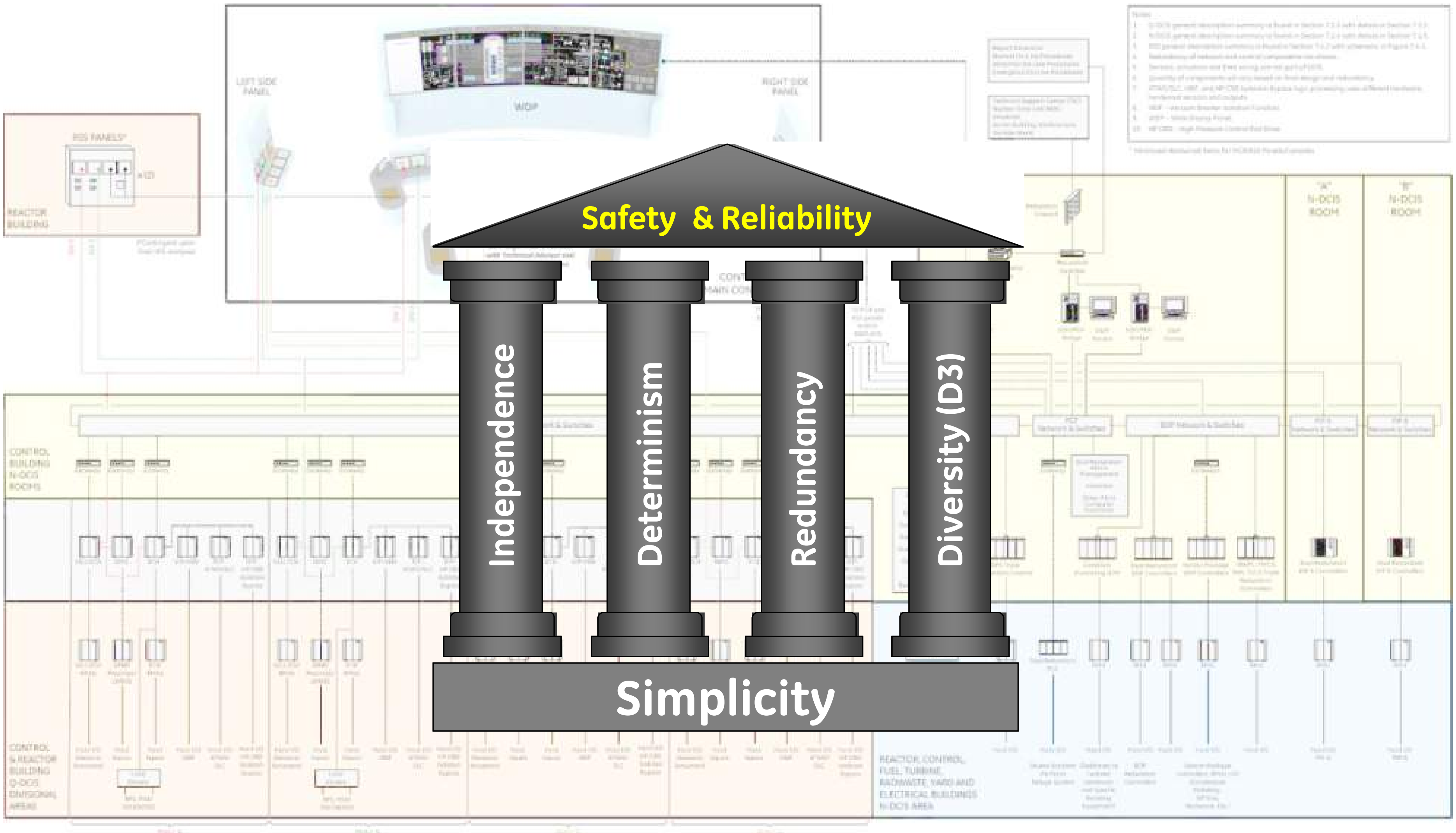
- Elementary Diagram
- Schematic
- Connection Diagram
- Electrical Wiring Diagram

Cyber Security Program Plan (CySPP) NEDE-33295 (Tier 2*)

Logic concepts proposed early in overall System SDLC as FLBDs…
Matures under configuration management into DLDs
Iterations controlled via design reviews (DRs) or baseline reviews (BRs)
Design basis records (BRR) foundation of all ITAAC closure reports

HITACHI

Regulatory Compliance Approach… Governing LTRs



Based on IEEE Std 603

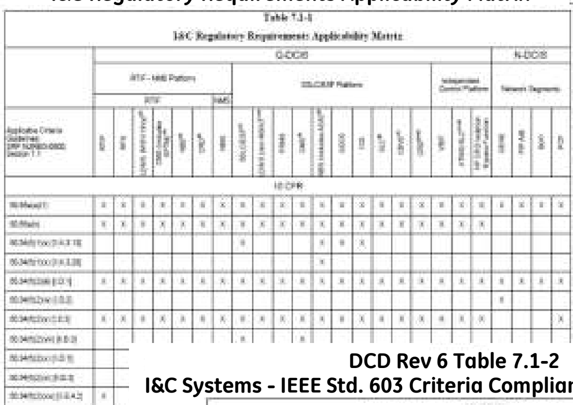
Criteria for Safety Systems for Nuclear Power Generating Stations

HITACHI

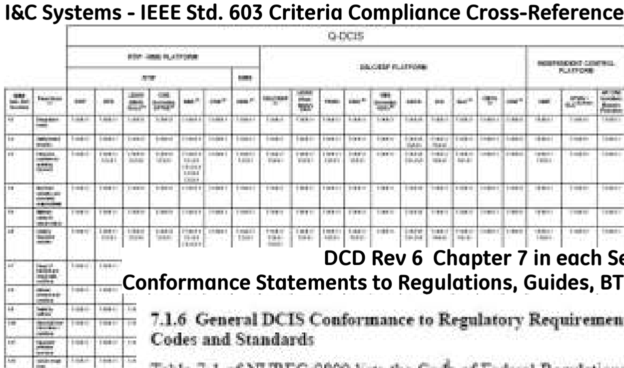
Regulatory Compliance… The Approach

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

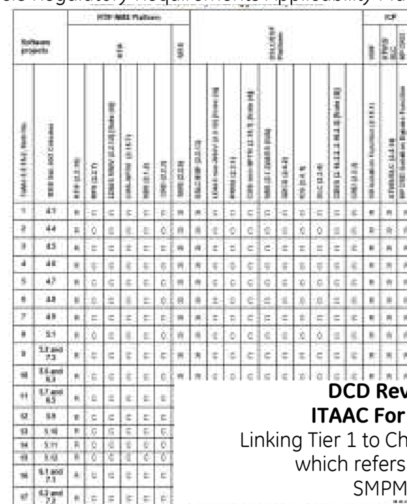
Table 7-1 of NUREG 0800 lists the Code of Federal Regulations (CFR), GDC, SRM, RGs, and Instrumentation and Controls Branch Technical Positions (BTP) that provide acceptance criteria or guidelines for each subsection of Chapter 7. Additional acceptance criteria or guidelines are delineated in the (NUREG-0800) 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 the 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 VBIF software projects.	Inspection of the SMP for the VBIF software projects will be performed. {{Design Acceptance Criteria}}	The SMP for the VBIF software projects complies with the criteria contained in the SMPM. {{Design Acceptance Criteria}}

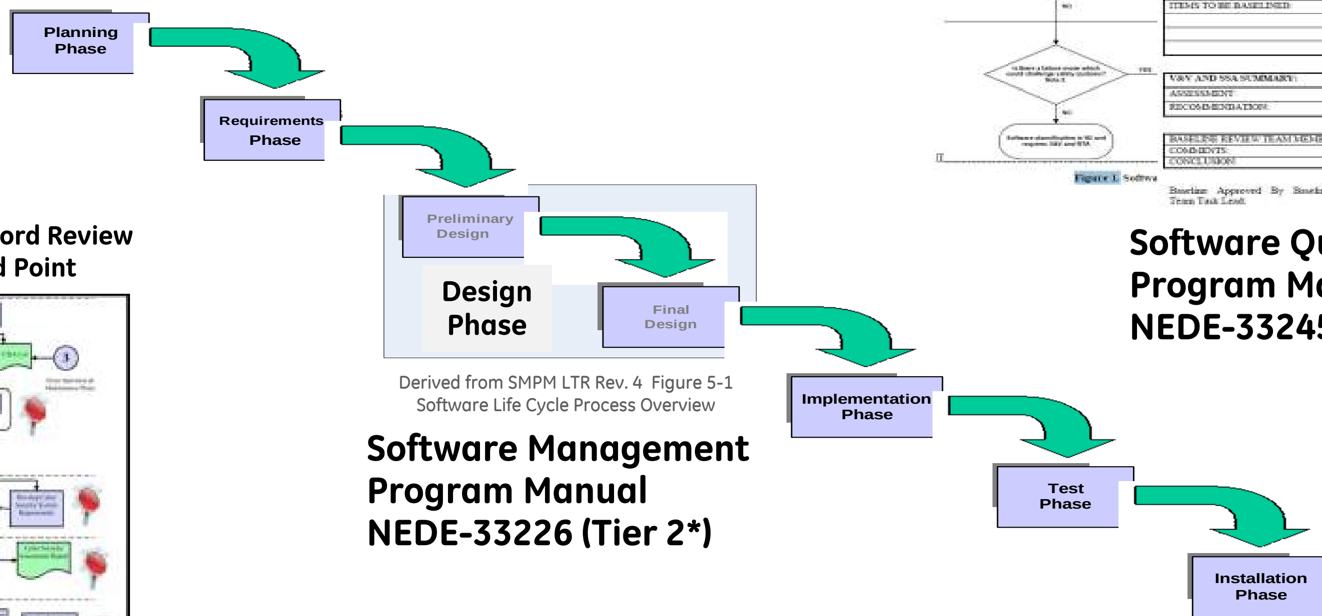
~2,280 Regulatory Conformance Statements

~806 ITAACs (including ~378 DACs) Commitments

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

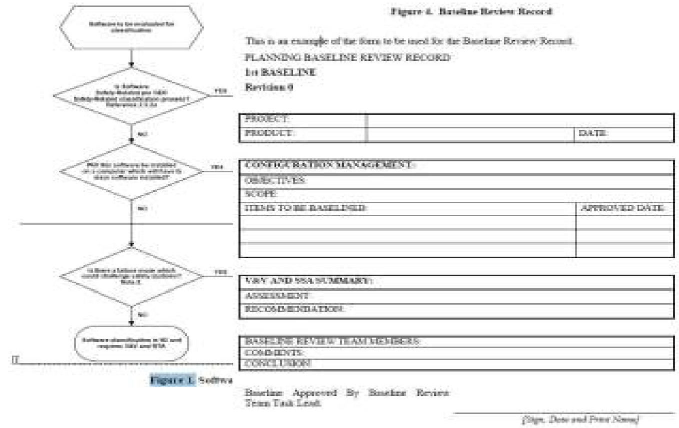
HITACHI

System and Software Design Process... LTR Triad



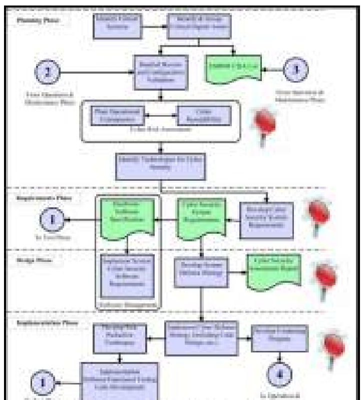
Derived from SMPM LTR Rev. 4 Figure 5-1
Software Life Cycle Process Overview

Software Management Program Manual NEDE-33226 (Tier 2*)



Software Quality Assurance Program Manual NEDE-33245 (Tier 2*)

KEY:
Baseline Record Review Audit or Hold Point



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

Cyber-Security Program Plan NEDE-33295 (Tier 2*)

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

HITACHI

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

Add'l Design Detail – New Fig. (1/8)… Figure 7.2-11a From: RAI 7.1-139 – Question 3

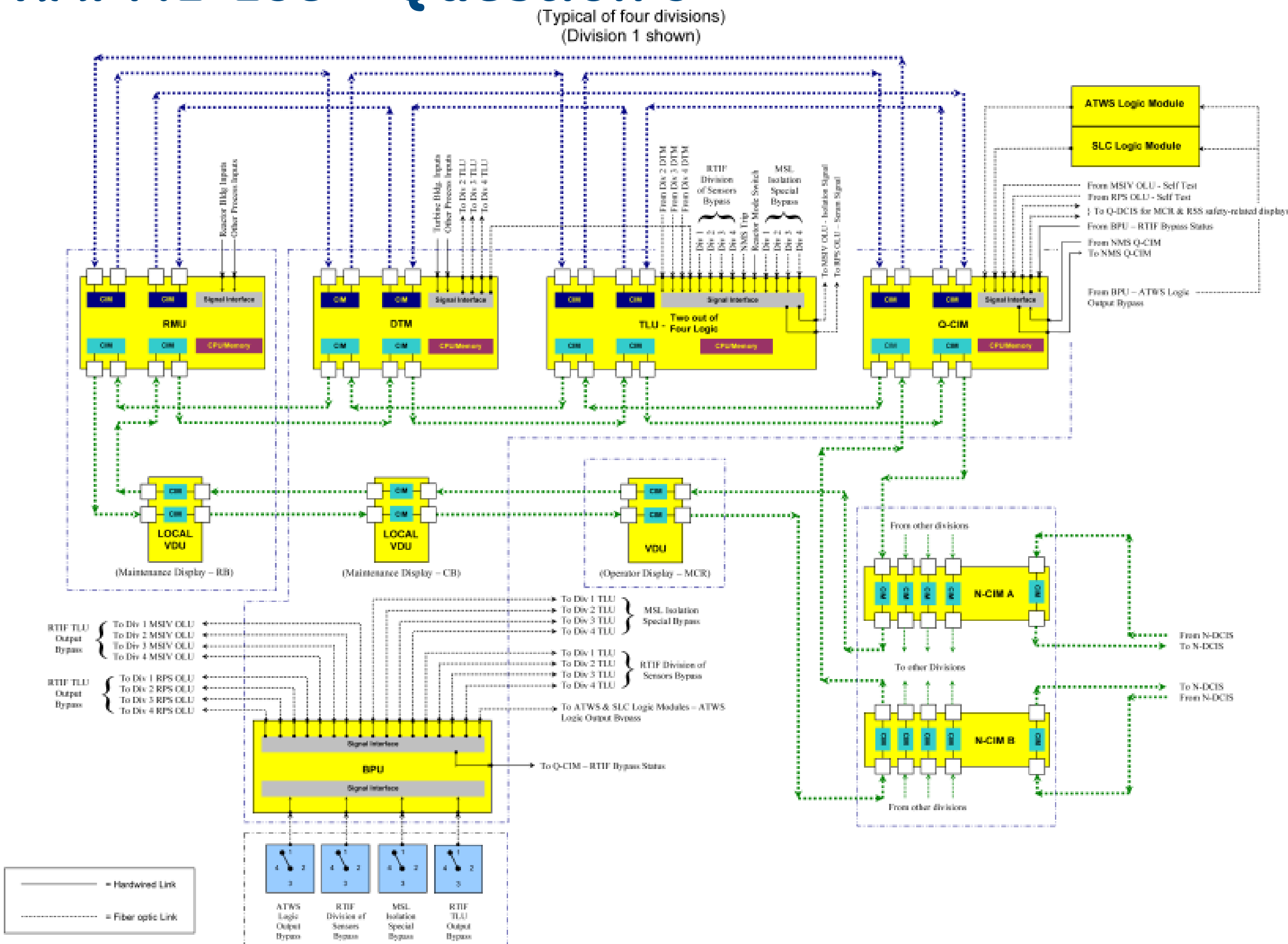


Figure 7.2-11a

Reactor Trip and Isolation Function (RTIF) Simplified Functional Block Diagram

Add'l Design Detail – New Fig. (2/8)... Figure 7.2-11b From: RAI 7.1-139 – Question 3

(Four Divisions Shown)

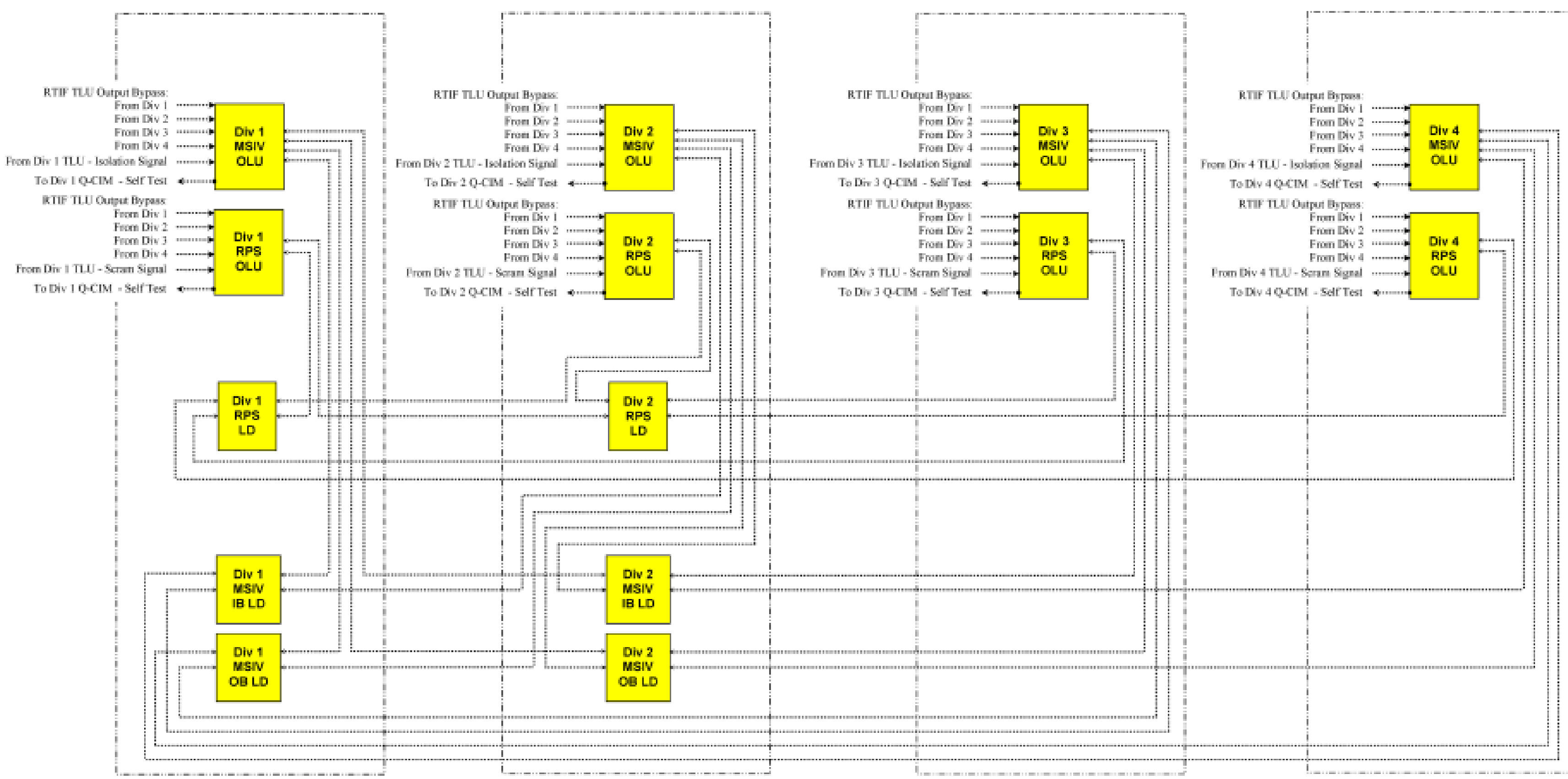


Figure 7.2-11b

Reactor Trip and Isolation Function (RTIF) Simplified Functional Block Diagram – Output Logic Unit Detail

HITACHI

Add'l Design Detail – New Fig. (3/8)… Figure 7.2-12
From: RAI 7.1-139 – Question 3

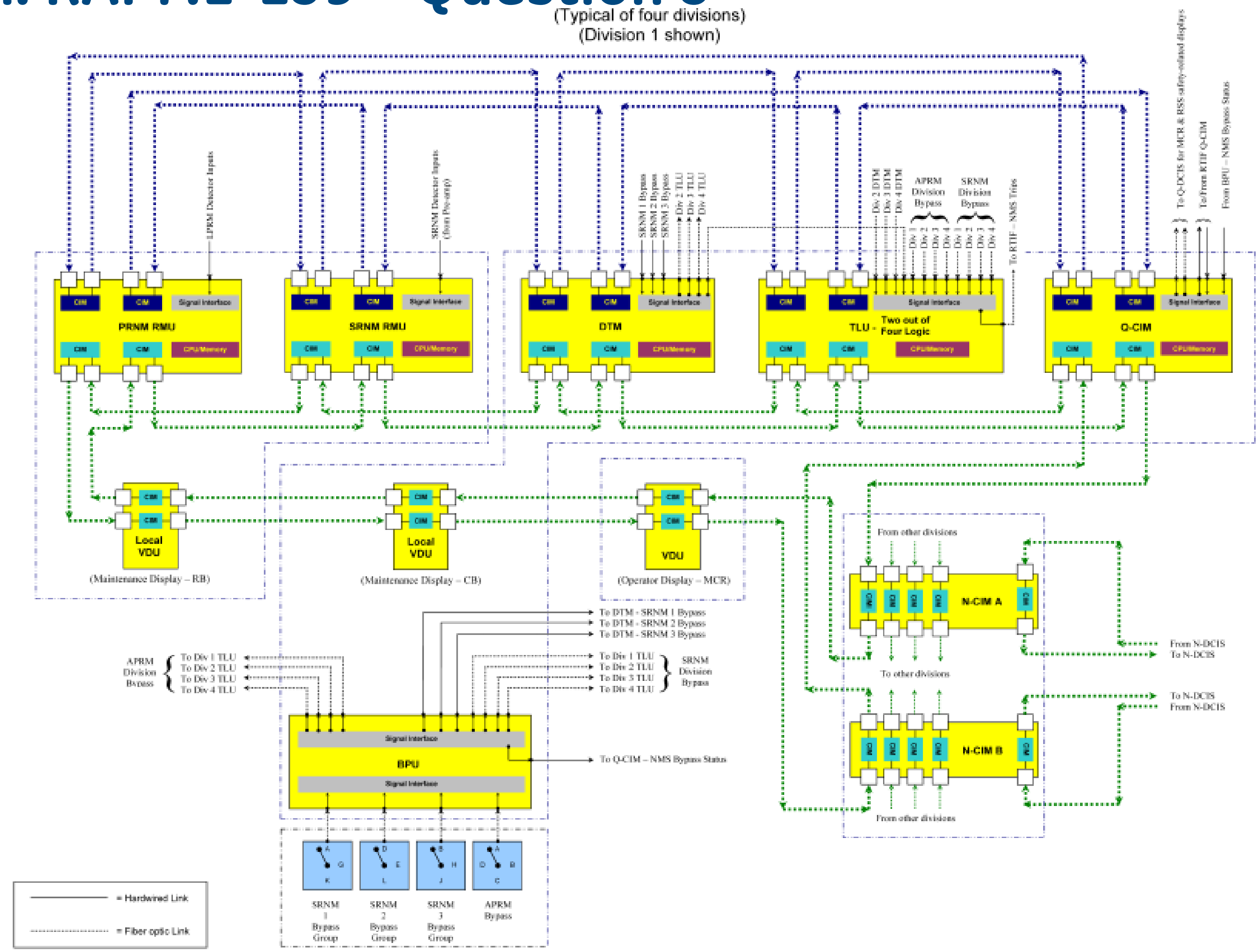


Figure 7.2-12

Neutron Monitoring System (NMS) Simplified Functional Block Diagram

HITACHI

Add'l Design Detail – New Fig. (4/8)… Figure 7.3-6
From: RAI 7.1-139 – Question 3

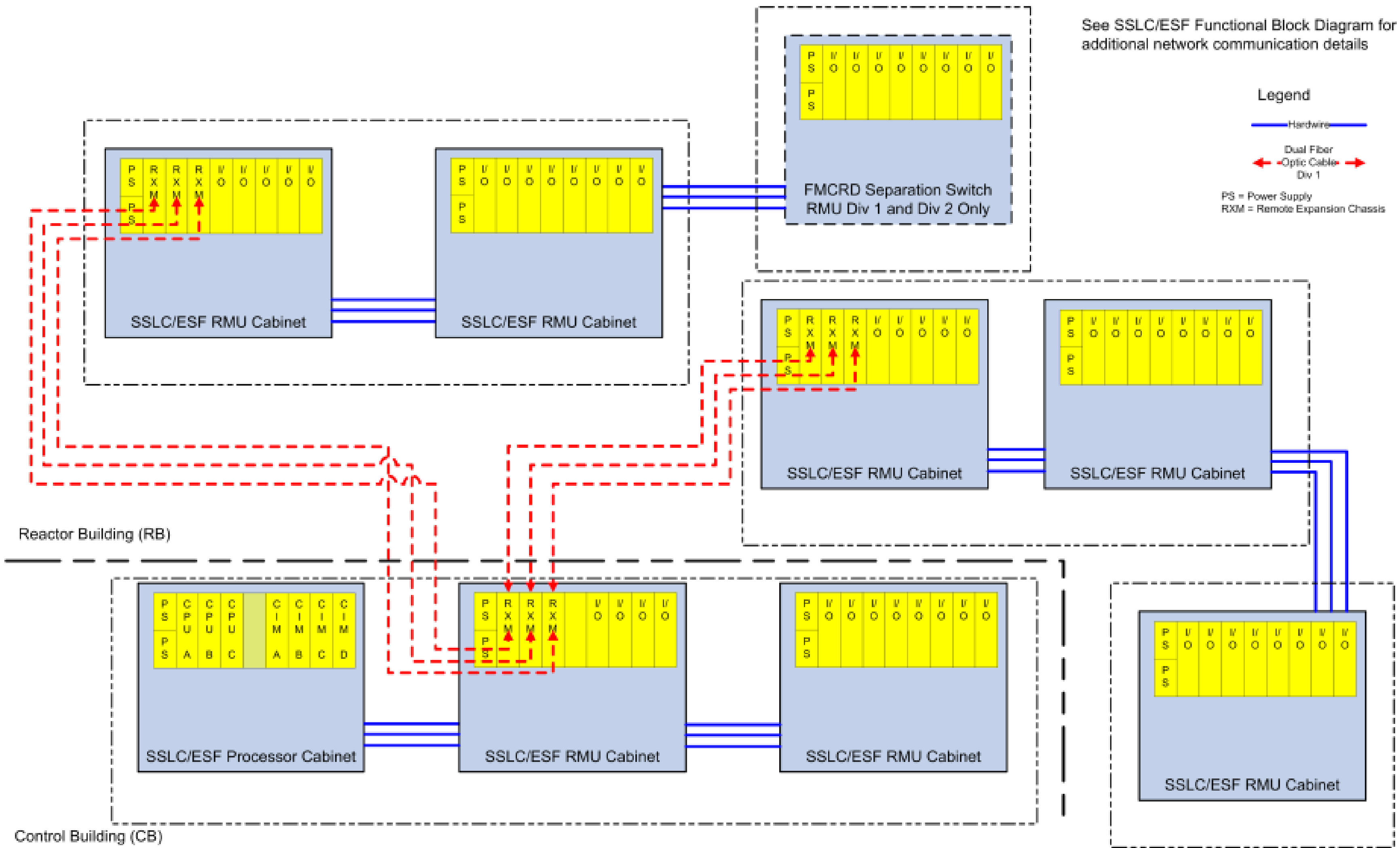


Figure 7.3-6
SSLC/ESF Division 1 Layout

GE HITACHI

Add'l Design Detail – New Fig. (5/8)… Figure 7.3-7 From: RAI 7.1-139 – Question 3

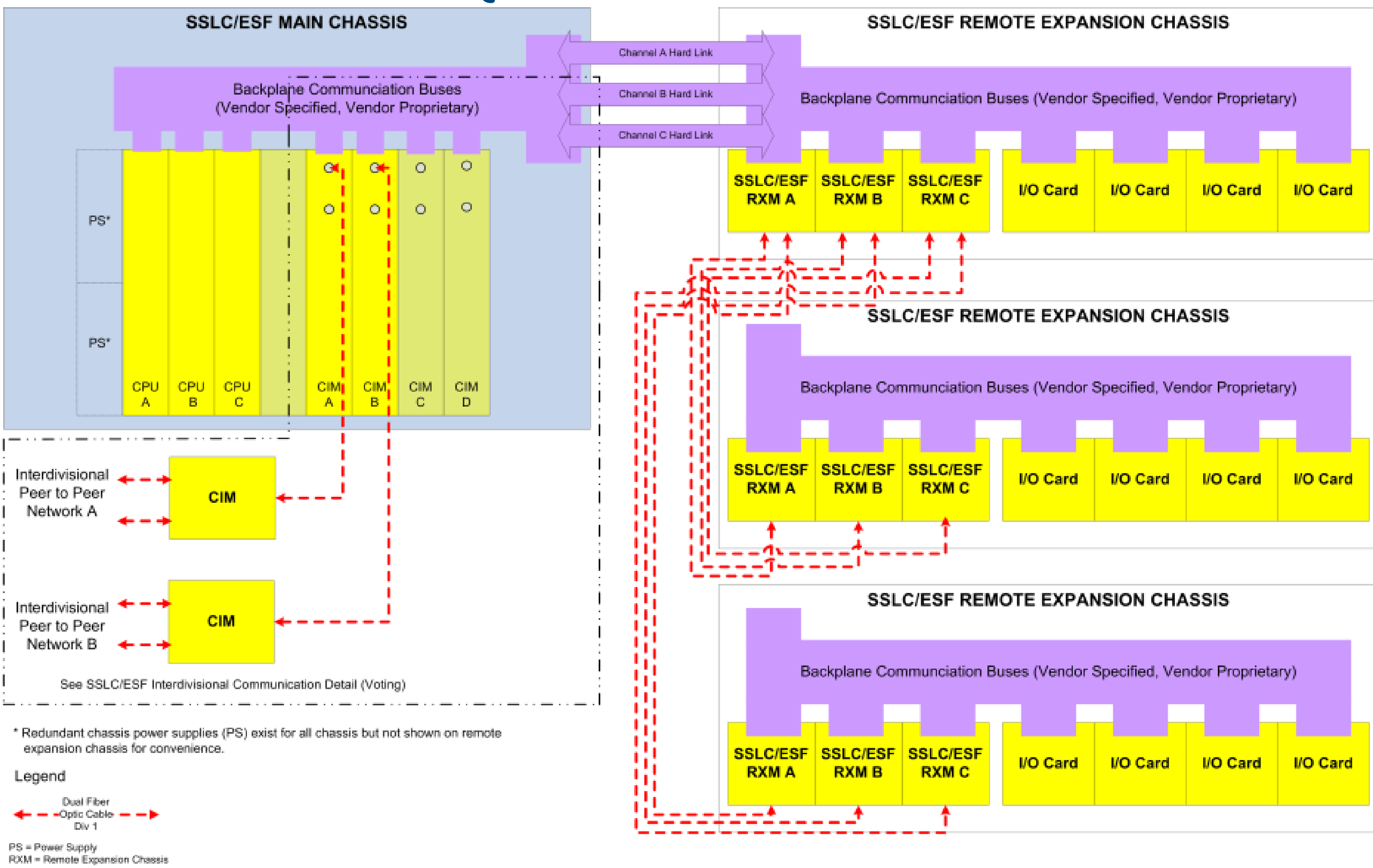


Figure 7.3-7
SSLC/ESF Simplified Functional Block Diagram

HITACHI

Add'l Design Detail – New Fig. (6/8)… Figure 7.3-8
From: RAI 7.1-139 – Question 3

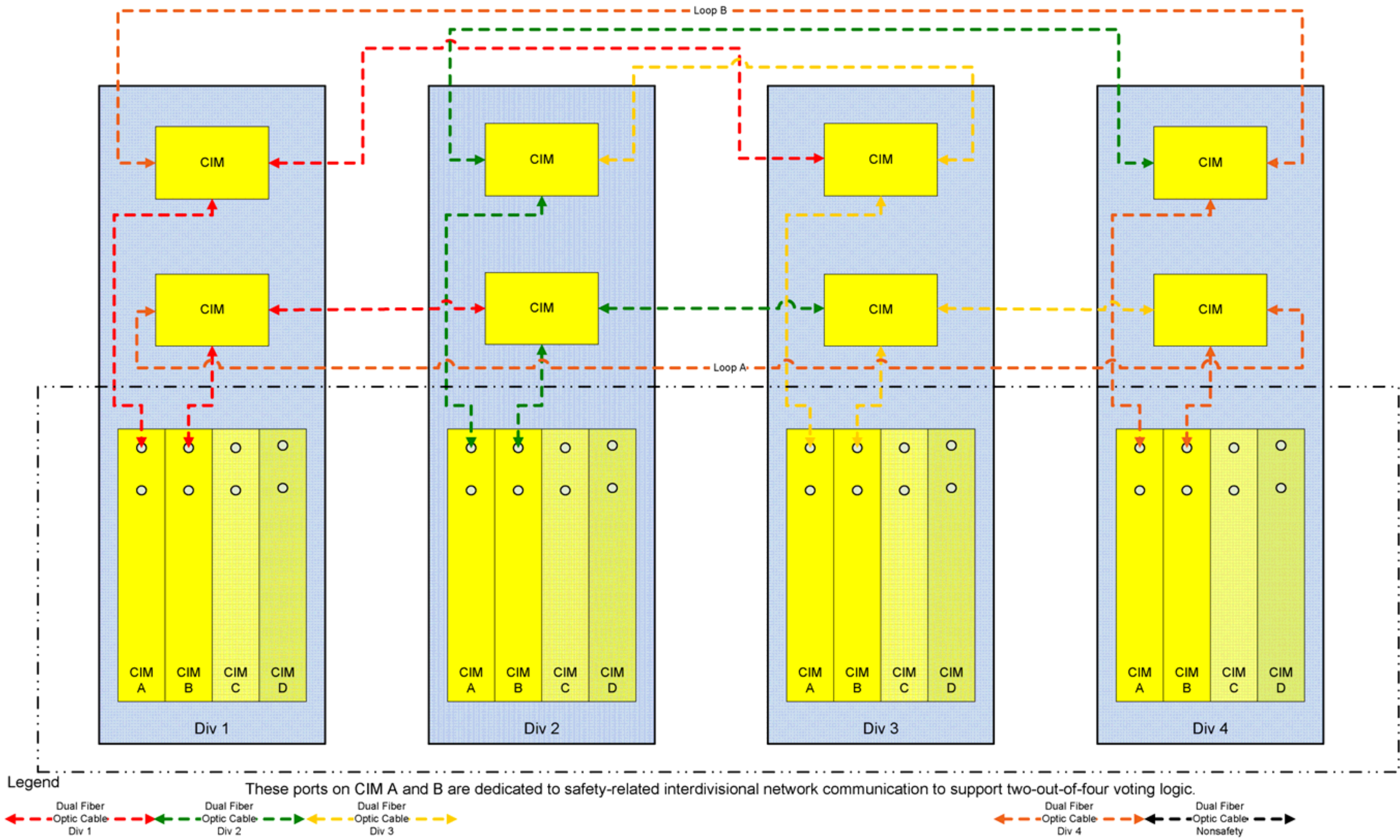


Figure 7.3-8
SSLC/ESF Inter-Divisional Communication Detail

HITACHI

Add'l Design Detail – New Fig. (7/8)... Figure 7.3-9
From: RAI 7.1-139 – Question 3

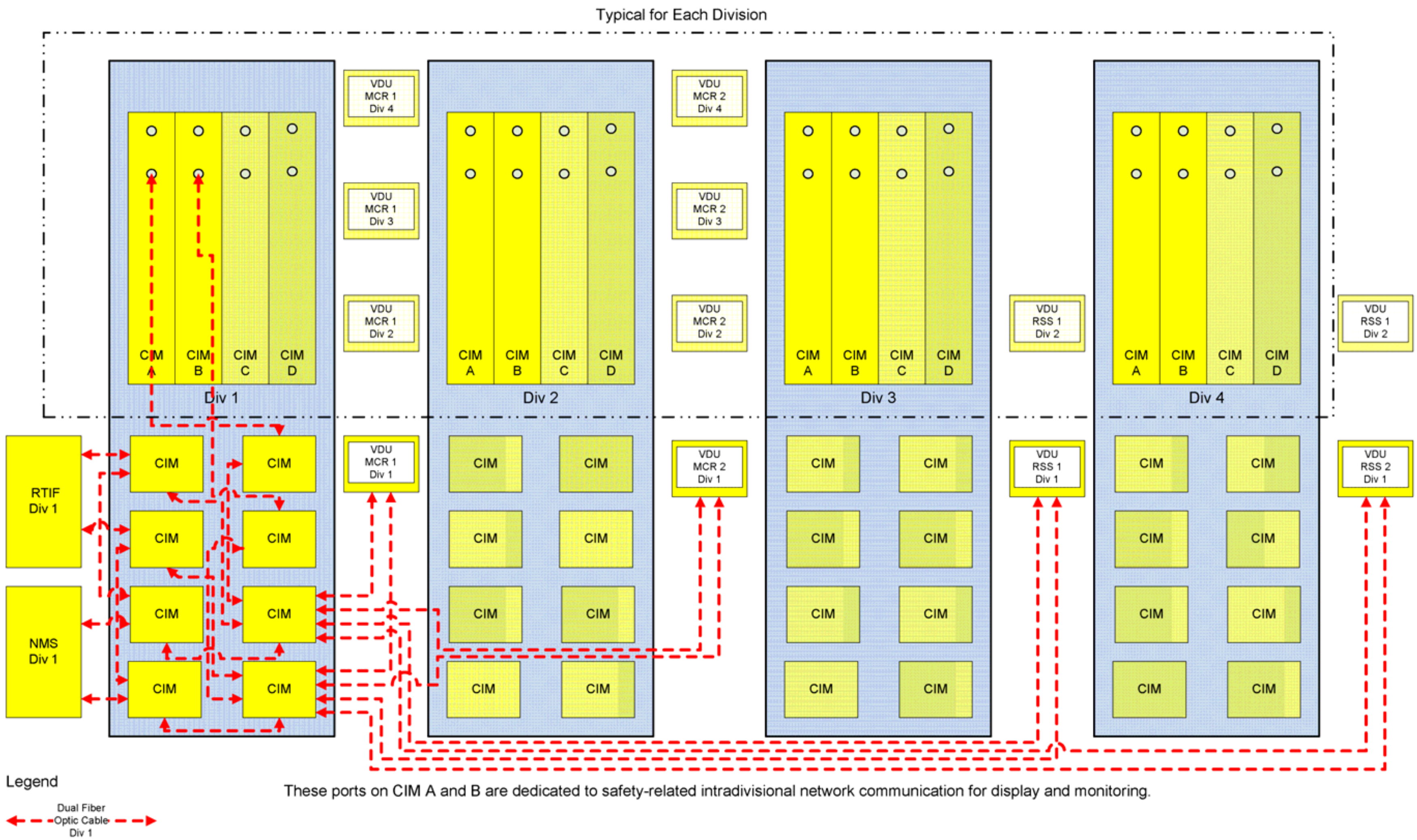


Figure 7.3-9
SSLC/ESF Safety-Related VDU Communication Detail

HITACHI

Add'l Design Detail – New Fig. (8/8)... Figure 7.3-10
From: RAI 7.1-139 – Question 3

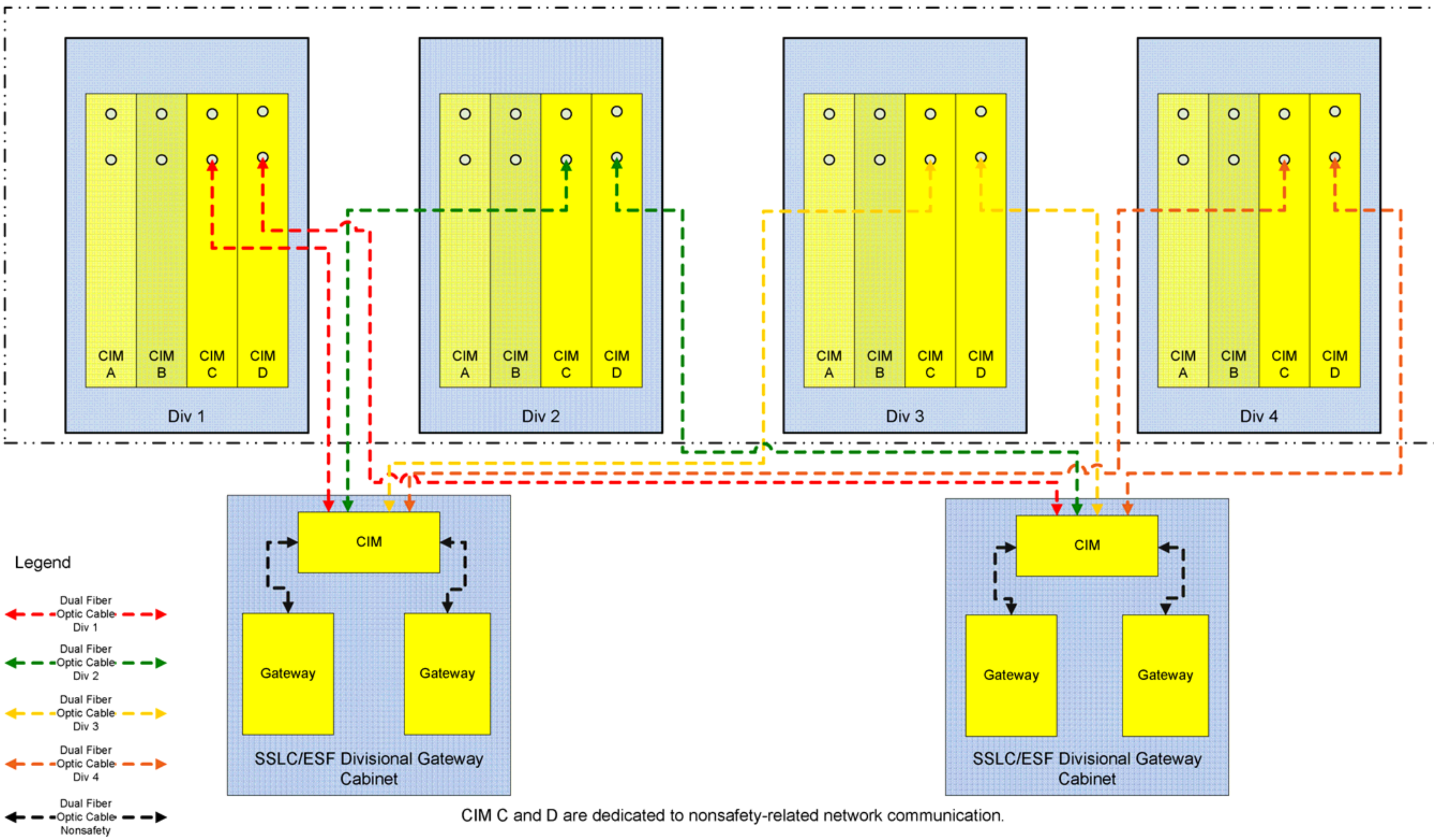


Figure 7.3-10
SSLC/ESF Nonsafety-Related VDU Communication Detail

HITACHI

End

GE Hitachi Nuclear Energy

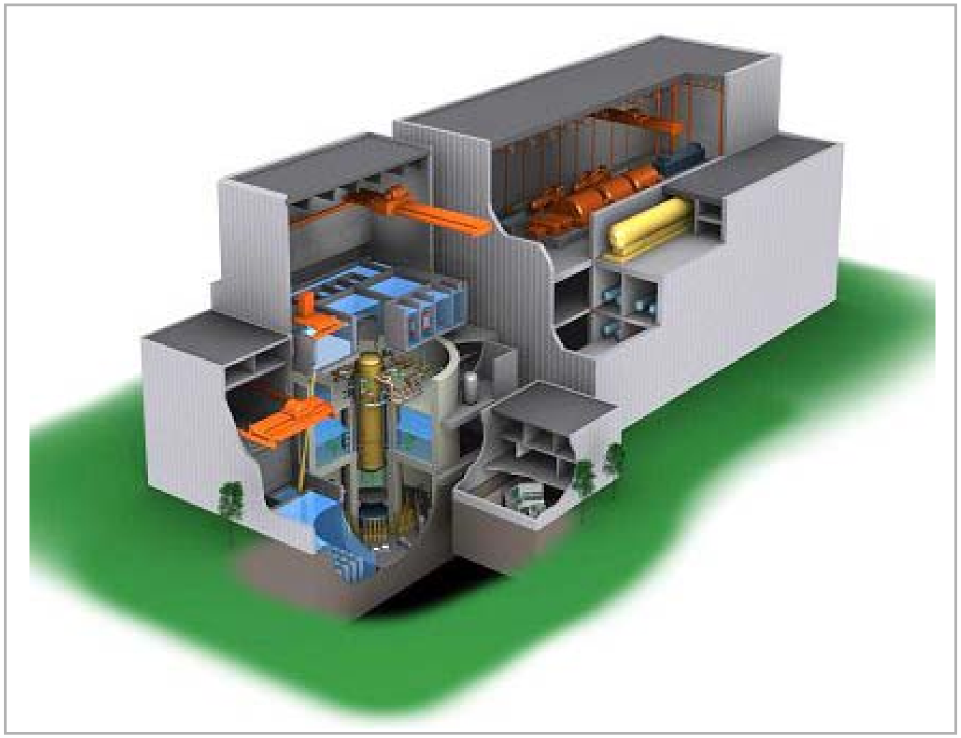
ESBWR DCD Section 6.4 Control Room Habitability System

Advisory Committee on Reactor Safeguards

Mike Arcaro

Wayne Marquino

September 24, 2010



HITACHI

Agenda

- Control Room Habitability Area (CRHA) Technical Specification (TS) for Heat Sink Temperatures (TS 3.7.2)
- ESBWR Control Building (CB) Passive Heat Sink Validation
- Bounding ESBWR Standard Plant Site Parameters
- Reactor Building Temperature Monitoring Requirements

ESBWR CRHA Passive Heat Sink Issues

- CRHA heat sink temperatures are maintained below the initial analysis values by maintaining the average of the air temperatures in the areas in TS Table B3.7.2-1 below the specified limit
  - Permanently installed temperature sensors will be provided in various locations and elevations inside CB with sensors feeding the plant computer for averaging and continuous monitoring of the CRHA heat sink areas
- When the average temperature of one or more rooms is greater than the limit specified in SR 3.7.2.1 (Applicable in Mode 1, 2, 3 & 4), Action A.1 requires that the average air temperature of each CRHA heat sink be restored within 8 hours
  - Prior to the CR reaching 85 F (above the 74 F LCO), Redundant CRHA / CB HVAC started and CRHA non-essential N-DCIS loads secured in CRHA
  - CRHA non-essential N-DCIS loads tripped at 85 F CR temperature

ESBWR CRHA Passive Heat Sink Issues

- Action A.2 requires that the average temperature of each CRHA heat sink be restored to within limits within 24 hours
  - If the average of the CRHA air sink temperatures exceed the specified limit, restoration of the CRHA heat sinks is verified by <u>administrative evaluation</u> <u>considering</u> the length of <u>time and extent</u> of the CRHA heat sink average air temperature excursion outside of limits, **or** <u>by direct measurement of the CRHA heat sink area structural materials temperatures</u>
  - An evaluation can be used to provide temperature profiles based on initial conditions (initial ambient temperatures, initial CRHA air temps, CRHA heat loads) to assess heat sink performance in lieu of actual heat sink (concrete) temperature measurement
  - CRHA heat sink temperature monitoring could be used to assess and ensure CRHA heat sink performance under TS 3.7.2 by measuring CRHA concrete surface temperature and predicting heat sink average temperature

ESBWR CRHA Passive Heat Sink Issues

- If A.1 or A.2 are not met, must be in MODE 3 in 12 hours and Mode 5 in 36 hours
- COL Item 6.4-1-A, CRHA Procedures and Training, will develop procedures and training for control room habitability including administrative evaluation of CRHA heat sink

ESBWR Passive Heat Sink Validation

Summary from ACRS question:

Discuss why an Analysis was chosen as the ITAAC method for the CB heat sink; Would it be beneficial to add an operational test of these passive heat sinks?

Response:

ITAAC T 2.16.2-4 (CB), A Control Building and Reactor Building Environmental Temperature Analysis for ESBWR, will be performed using the as-built heat sink dimensions, the as-built heat sink thermal properties, the as built heat sink exposed surface area, the as-built thermal properties of materials covering parts of the heat sink, and the as-built heat loads. An operational test that would simulate limiting design conditions would be extremely difficult to perform. The analysis method is Tier 2*

HITACHI

ESBWR Control Building Passive Heat Sink Validation

- CB Passive Heat Sink performance is assured by analysis rather than testing because critical as-built parameters can be readily verified
- The heat capacity of the control room concrete mass and name plate heat loads will be validated in an ITAAC.
  - No tests of the structural components of the concrete are required. It's inconsistent with other passive functions (e.g. building structure response) to test the heat capacity of the concrete or physical cooling processes.
- Limiting design parameters associated with the passive heat sink can not be readily reproduced during performance testing (i.e. 117 F ambient temp, ground temp 86 F, Temp Range 27 F, high humidity conditions 92 F db / 88 F wb)
- A performance test would require verification of CRHA heatup with minimum safety-related loads <u>for a period of 72 hours</u>

ESBWR Control Building Passive Heat Sink Validation

- Test would require tripping the non-safety DCIS equipment, which terminates control of the equipment. There is no equivalent challenge to the non-safety DCIS planned
- The startup test would require 72 hour to perform after all MCR equipment and DCIS room equipment is installed and then deliberately turned off (Critical Path Startup Test)
- The test would impose a significant schedule challenge, to sequence when the loads are available to be powered, but where interruption of the NDCIS would not disrupt the plant pre-operational or startup tests

Conclusion:
Sufficient information is provided to ensure CB passive heat sink will function as designed

HITACHI

ESBWR Standard Plant Site Parameters

Summary from RAI question:
RAI 6.4-24S02 requested clarification for site characteristic values related to daily temperature range and high humidity diurnal swing associated with ESBWR Standard Plant Site Parameters 0% exceedance

Response:
Response to RAI 6.4-24 S02 has been provided to NRC Staff

Conclusion:
DCD S 3H3.2 has been revised under revision 8 to incorporate NRC comments

ESBWR Standard Plant Site Parameters

3H.3.2.1.1 Maximum Temperature Analysis Conditions

For the summer conditions the 0% exceedance maximum dry bulb and coincident wet bulb ambient outside air temperature [47.2°C (117°F) DBt and 26.7°C (80°F) WBt] was considered. The Daily Temperature Range applied for this analysis is Δ 15°C (27°F).

The Daily Temperature Range for summer conditions is defined as the dry bulb temperature difference between the 0% exceedance maximum dry bulb temperature and the dry bulb temperature that corresponds to the higher of the two lows occurring within 24 hours before and after that maximum.

The Maximum Average Dry Bulb Temperature for the 0% Exceedance Maximum Temperature Day is defined as the average of the 0% exceedance maximum dry bulb temperature of 47.2ºC (117°F) and the dry bulb temperature resulting from a daily temperature range of 15ºC (27°F), which is 39.7ºC (103.5°F).

3H.3.2.1.2 Minimum Temperature Analysis Conditions

For the winter conditions the Cont rol Room Habitability Area Minim um Temperature Analysis conside rs the 0% exceedance minimum dry bulb am bient outside air temperature (-40°C/°F). The Daily Temperature Range applied for this analysis is Δ 15°C (27°F).

The Daily Temperature Range for winter conditions is defined as the dry bulb temperature difference between the 0% exceedance minimum dry bulb temperature and the dry bulb temperature that corresponds to the lower of the two highs occurring within 24 hours before and after that minimum.

The Minimum Average Dry Bulb Temperature for 0% Exceedance Minimum Temperature Day is the average of the 0% exceedance minimum dry bulb temperature of –40ºC (-40°F) and the dry bulb temperature resulting from a daily temperature range of 15ºC (27°F), which is -32.5ºC (–26.5°F).

ESBWR Standard Plant Site Parameters

3H.3.2.1.3 High Humidity Analysis Conditions

For high humidity conditions the 0% exceedance non-coincident maximum wet bulb temperature [31.1ºC (88ºF) WBt] and High Humidity Diurnal Swing [Δ 4.4ºC (8ºF) DBt] are applied to the methodology for the analysis presented in Reference 3H.4-8.

The High Humidity Diurnal Swing is defined as the dry bulb temperature range determined by the maximum and the minimum wet bulb temperatures for the worst three-day period over which the 0% exceedance wet bulb temperature occurs. The maximum wet bulb temperature (31.1ºC/88ºF) has a coincident dry bulb temperature of (33.3ºC/92ºF). These temperatures define the maximum dry bulb and wet bulb temperatures for three days in the analysis. The minimum dry bulb temperature is defined as the coincident dry bulb temperature (28.9ºC/84ºF) for the highest of six low wet bulb temperatures (27.2ºC/81ºF) occurring in each of the three 24-hour periods before and after the 0% coincident maximum wet bulb temperature. The High Humidity Diurnal Swing is the difference between the coincident maximum dry bulb temperature (33.3ºC/92ºF) and the highest daily low dry bulb temperature (28.9ºC/84ºF).

The overnight low wet bulb temperature in the high humidity CONTAIN analysis is 28.9ºC (84ºF), which is conservative relative to the 27.2ºC (81ºF) wet bulb temperature in the High Humidity Diurnal Swing.

The WBGT index value is determined by the dry bulb temperature multiplied by 0.3 plus the wet bulb temperature multiplied by 0.7.

The Maximum High Humidity Average Wet Bulb Globe Temperature Index for 0% Exceedance Maximum Wet Bulb Temperature Day is defined as the average of the WBGT index values for the temperatures used to determine the High Humidity Diurnal Swing. The WBGT index value for the maximum dry bulb 33.3ºC (92ºF) and wet bulb 31.1ºC (88ºF) temperatures is 31.8ºC (89.2ºF). The WBGT index value for the minimum dry bulb 28.9ºC (84ºF) and wet bulb 28.9ºC (84ºF) temperatures is 28.9ºC (84ºF). The average of the WBGT index values is then 30.3ºC (86.6ºF).

Reactor Building Temperature Monitoring Requirements

Summary from ACRS question:
How are assumptions of the Reactor Building passive heatup calculation assured ?

Response:
DCD provides assurance that monitoring is performed to maintain RB temperatures below limits

Conclusion:
Sufficient information is provided to ensure RB temperatures will be maintained below EQ limits

HITACHI

Reactor Building Temperature Monitoring Requirements

- ESBWR GTS do not include an LCO for monitoring EQ related temperatures in RB rooms containing safety-related (SR) equipment because it does not meet the criteria of 10 CFR 50.36. This is consistent with the current STS (NUREGs 1433 & 1434), which evolved as follows:
  - The old STS (i.e., NUREG-0123) included an LCO titled “Area Temperature Monitoring,” which ensured that SR equipment in various areas was not subjected to temperatures beyond the defined EQ envelope.
  - During development of the current STS, the NRC Staff agreed that the Area Temperature Monitoring LCO did not meet the criteria for including in TS and, therefore, the requirements of the LCO could be controlled outside of TS.
  - Compensating provisions considered to support the change to the STS include the existence of monitoring instrumentation and control room annunciators for high area temp which will alert the operator to take corrective action. These compensating provisions also exist for the ESBWR design.

Reactor Building Temperature Monitoring Requirements

- Indicators including flow rates, control damper position, filter pressure drop, building pressure with respect to atmospheric, temperatures, battery room hydrogen concentration [ref. DCD S9.4.6.5]
- Alarms for high or low conditions including airflow rates, temperatures, filter pressure drop, building differential pressure, smoke detection, and high battery room hydrogen concentration and temperature [ref. DCD S9.4.6.5]
- DCD Table 9.4-8 Design Parameters for RBVS provides normal & design temperatures for RB safety related components
- Table 3H-3 Thermodynamic Environment Conditions Inside RB for Normal Operating Conditions
- Table 3H-9 Thermodynamic Environment Conditions Inside RB for Accident Conditions
- Table 18.1-1a Minimum Inventory of MCR Alarms, Displays, and Controls Description Alarm Display Control- RB Area Temperature High

Summary

- CRHA design meets GDC 19 habitability requirements
- CRHA Design Validation / Surveillance Procedures assure functions will be met
- Bounding ESBWR Standard Plant Site Parameters can be interpreted and implemented by COL Applicants
- Reactor Building Temperature Monitoring Requirements ensure EQ life of equipment

Follow up to ACRS Subcommittee comment on Ch 16

Passive Safety System – Inspection Frequencies

Summary of Concern from August 2010 ACRS Meeting

Staggering of the surveillances for inspection of the passive safety systems should be considered

Response

The following changes have been made, and will be included in Revision 8 of the DCD.

LCOs 3.5.2 and 3.5.3 – GDCS:

- Verify the flow path for each GDCS injection branch line is not obstructed – every 24 months on a staggered test basis for each pair of GDCS injection branch lines (was once/10 years)
- Verify the flow path for each GDCS equalizing line is not obstructed – every 24 months on a staggered test basis for each equalizing line (was once/10 years)

LCO 3.7.1 – IC/PCCS Pools:

- Verify each IC/PCCS pool subcompartment has an unobstructed path through moisture separator to the atmosphere – every 48 months on a staggered test basis for the flow path associated with each moisture separator (was once/10 years)

ACLCO 3.5.1 – GDCS Deluge Function:

- Verify the flow path for each GDCS deluge line is not obstructed – every 24 months on a staggered test basis for each deluge line (was once/10 years)

HITACHI

Backup Slides

HITACHI

ESBWR CRHA Passive Heat Sink Issues Table B3.7.2-1

Heat Sink Group	Established Design Temperature
CRHA Heat Sink Group 1	
Control Room Habitability Area: Main control room panel Rooms: No 3270, 3272, 3271, 3201, 3202, 3273, 3206, 3205, 3204, 3275, 3207, 3208	23.3ºC (74ºF)
Corridors: [1] Rooms 3100, 3101 and Rooms 3200,3203, 3277, 3274	25.6ºC (78ºF)
HVAC chases: [1] Rooms 3251, 3260	25.6ºC (78ºF)
CRHA Heat Sink Group 2	
Q-DCIS equipment rooms: Rooms No 3110, 3120, 3130 and 3140	25.6ºC (78ºF)
N-DCIS equipment rooms: Rooms 3301, 3302, 3303, 3300	25.6ºC (78ºF)
Electrical chases: [1] Rooms 3250, 3261	25.6ºC (78ºF)
CRHA Heat Sink Group 3	
HVAC equipment rooms: Rooms 3401, 3402, 3403, 3404	40ºC (104ºF)
Safety Portions of CRHAVS: Rooms 3406, 3407	40 ºC (104ºF)

1. Access corridors, electrical chases, and HVAC chases, although part of the CRHA heat sink, are not monitored because these areas do not contain heat sources and their temperatures are assumed to match the average of the associated group.

HITACHI

ESBWR CRHA Passive Heat Sink Issues

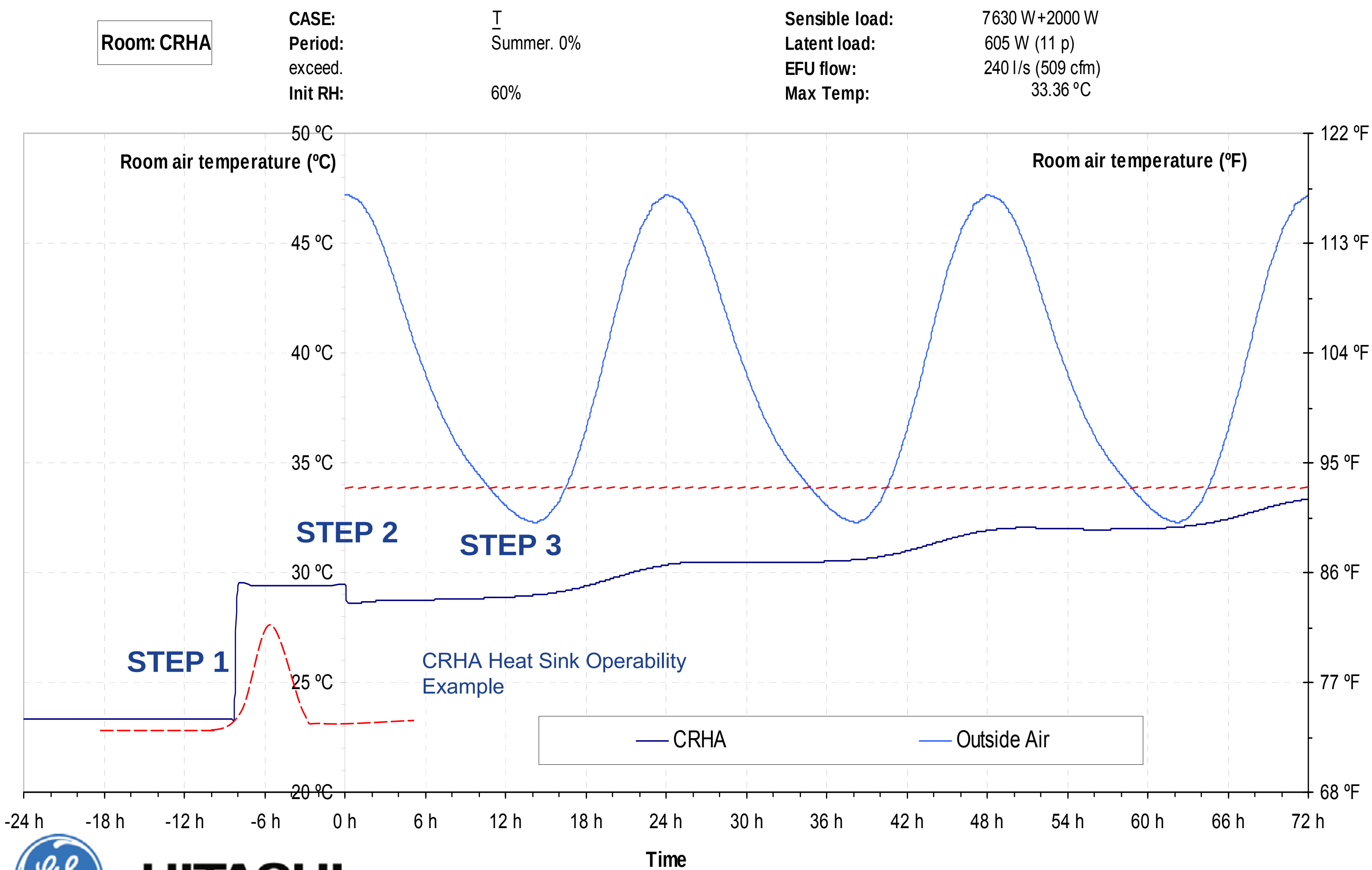
Parameter	Value (ºF)	Discussion
CRHA Normal Operating Limit (at 0% summer exceedance)	70* to 74*	Comfort level. URD specifies 73ºF to 78ºF. Value allows margin to N-DCIS trip setpoint and provides initial condition for CRHA heat sink structural material temperature while considering ventilation system operating costs and margin for long term structural degradation.
Alarm/ Tech Spec Action	74*	CRHA heat-up analysis assumes CRHA heat sink structural material (e.g., concrete) is 74ºF or less
Tech Spec Surveillance Limit – Heat Sink Temp.	74* (for CRHA)	If the heat sink air is above analyzed temperature (e.g., 74ºF for CRHA*), after air temperature has been brought back down (8 hour limit to accomplish this), the complete heat sink must be assured of having returned to (or never exceeded) the assumed limit(s). Restoring the CRHA heat sink average air temperatures to within limits within 8 hours limits the temperature excursion of the CRHA heat sink structure; i.e., restoring CRHA heat sink average air temperature begins the process of cooling the CRHA heat sink structure.
Select N-DCIS Trip Setpoint – CRHA Air Temp.	85	Setpoint will provide reasonable amount of time to restore CRHA ventilation or reduce CRHA heat loads prior to trip of certain loads, including some N-DCIS loads.

HITACHI

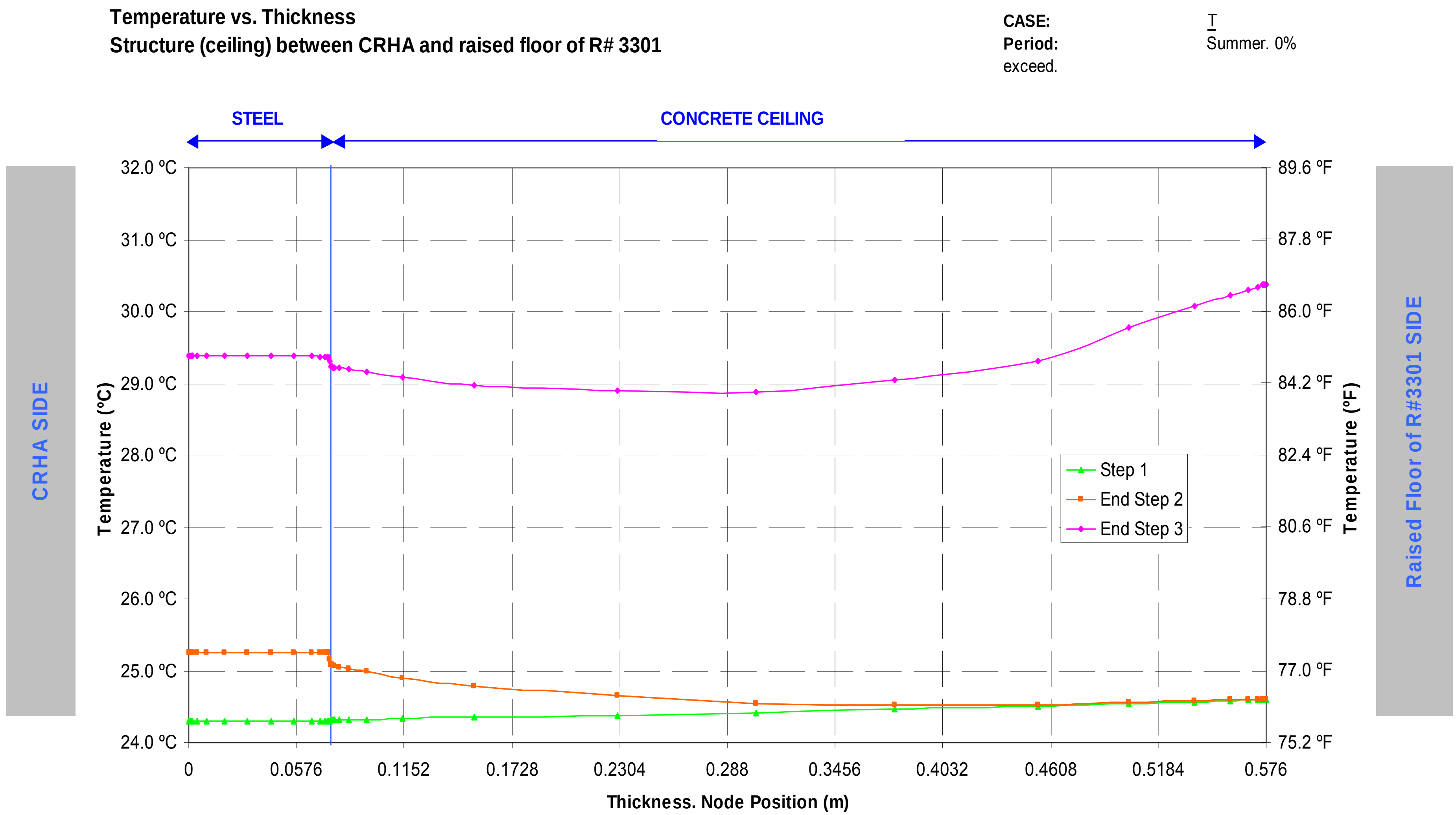
ESBWR CRHA Passive Heat Sink Issues-Conditions for Simulation

- Step 1- Room air temperatures under normal operation with these temperatures artificially maintained in CB rooms
  - All room air temperatures are kept steady until all temperatures across the structures reach a steady state simulating full operation of the CB HVAC system
- Step 2- The structure temperature profile in structures calculated previously is considered as initial temperatures, and the model is run for 8h
  - All room air temperatures are kept the same as in step 1 during 8h with the exception of the CRHA air temperature, which is maintained at 29.4°C (85°F)
  - The concrete temperatures on the surface and inside the CRHA structures increase slightly because they are in contact with air at a higher temperature
- Step 3- The event of an SBO is considered where this transient calculates the room air heatup curve inside the CRHA and rooms housing safety-related equipment in an SBO during 72h

ESBWR CRHA Passive Heat Sink Issues



ESBWR CRHA Passive Heat Sink Issues



HITACHI

ESBWR Standard Plant Site Parameters

Ambient Design Temperature: (6)	***0% Exceedance Values*** - Maximum: 47.2°C (117°F) dry bulb 26.7°C (80°F) wet bulb (mean coincident) 31.1°C (88°F) wet bulb (non-coincident) - Minimum: -40°C (-40°F) ***Maximum Average Dry Bulb Temperature for 0% Exceedance Maximum Temperature Day***(17) 39.7°C (103.5°F) ***Minimum Average Dry Bulb Temperature for 0% Exceedance Minimum Temperature Day***(18) -32.5°C (–26.5°F) ***Maximum High Humidity Average Wet Bulb Globe Temperature Index for 0% Exceedance Maximum Wet Bulb Temperature Day***(19) 30.3°C (86.6°F)

HITACHI

Presentation to the ACRS Subcommittee

ESBWR Design Certification Review

Chapter 7, “Instrumentation and Controls”

September 24, 2010

Chapter 7 Review Team

- Technical Review Staff
  - Ian Jung, Branch Chief, ICE2
  - Hulbert Li
  - Joseph Ashcraft
  - Dinesh Taneja
  - Deanna Zhang
  - Eugene Eagle
  - Sang Rhow
  - Kimberley Corp

- Project Manager
  - Dennis Galvin

Chapter 7 Overview

The staff is required to evaluate safety of the I&C system design in accordance with the Commission's regulations by following SRP guidance

The staff's safety evaluation is based on the design information provided in the design control document (DCD) and the referenced technical reports. The staff's evaluation is documented in the SER as follows:

7.1 Overview of I&C systems, including:

- Conformance to regulations – GDCs, IEEE-603, TMI Action Items
- Software development activities – LTRs NEDE-33226P and NEDE-33245P
- Diversity and defense-in-depth – LTR NEDO-33251
- Setpoint methodology – LTR NEDE-33304P
- Data communication
- Secure development and operational environment (SDOE) – LTR NEDE-33295P

Chapter 7 Overview (cont.)

7.2 Reactor Trip System

7.3 Engineered Safety Features Systems

7.4 Safe Shutdown Systems

7.5 Information System Important to Safety

7.6 Interlock Logic

7.7 Control Systems

7.8 Diverse Instrumentation and Control Systems

General Finding

- The staff has evaluated safety of the I&C system design and finds the design to be safe and in compliance with applicable regulations
- I&C design follows safe design principles:
  - **Independence**
  - **Determinism**
  - **Redundancy**
  - **Diversity and Defense-in-Depth**
- Safety-related I&C design employs **Simplicity** in many aspects
- I&C systems are designed to conform with the following applicable regulatory requirements:
  - 10 CFR Part 52
  - 10 CFR Part 50, including 50.55a(h) (IEEE Std. 603)
  - 10 CFR Part 50 Appendix A (GDC)
  - 10 CFR Part 50 Appendix B (QA)
  - 10 CFR Part 50.34 (TMI items)

Independence

- The staff found that the I&C system design provides sufficient independence in compliance with IEEE-603 (10 CFR 50.55a(h)) and GDC 21
  - Safety-related platforms are organized into four physically separated and electrically isolated divisions
  - Communication independence is achieved using following design features:
    - Inter-divisional data communication in safety-related systems is limited to:
      - Voting logic
      - Bypass
      - Data authentication
    - Inter-divisional data communication in RTIF/NMS platform is point-to-point unidirectional via optical fibers. Faulty or loss of data communication is interpreted as a trip signal (fail safe)
    - Inter-divisional data communication in SSLC/ESF platform uses redundant Ethernet networks for 2/4 voting logic. Networks are doubly buffered to prevent data corruption to adversely impact both networks

Independence (cont.)

  - ICP platforms do not use multiplexing for data communication, I/O is hard wired
  - Data communication from safety to non-safety related I&C systems is unidirectional
- Any failure in a division does not prevent other redundant safety divisions from performing their intended safety function
- Diverse and independent diverse protection system (DPS) is provided as a defense-in-depth feature to cope with an unlikely scenario of a primary system malfunction (CCF or multiple independent failures)

Determinism

- Determinism means that a required safety function is always accomplished within the required time period specified by Chapter 15 DBA analyses
- Based on the following, the staff found that the real time performance of the safety-related I&C systems is deterministic and conforms to IEEE-603 (10 CFR 50.55a(h)) and BTP HICB-21:
  - Q-DCIS data communication protocols are deterministic
  - RTIF/NMS platform performs a cyclic real-time execution. The operating system is clock-driven and not event-driven, and it does not incorporate “interrupts”
  - SSLC/ESF platform runs cyclic programs that include both the application and diagnostics and do not incorporate “interrupts”
  - ICP platforms do not have an operating system
  - All platforms always react in the same way according to the order of events occurring at the point in time of plant conditions

Redundancy

- The staff found that the I&C system design provides sufficient redundancy in compliance with IEEE-603 (10 CFR 50.55a(h)) and GDC 21
  - All safety-related platforms are organized into four redundant divisions
    - 4 redundant divisions of RTIF/NMS platforms
    - 4 redundant divisions of SSLC/ESF platforms
    - 4 redundant divisions of ICP platforms
  - Each division has its own set of sensors, and no sharing of sensors between safety divisions is allowed
  - DPS utilizes 2/4 voting logic

Redundancy (cont.)

- RTIF/NMS platform uses dual redundant communication rings for intra-divisional data communication
- SSLC/ESF platform uses doubly buffered redundant networks for 2/4 voting logic
- Within each SSLC/ESF division, triply modular redundant (TMR) controllers are used for high reliability
- N-DCIS platforms use double or triple redundant controllers for high reliability and availability

Diversity and Defense-in-Depth

- The staff found that the I&C system design provides sufficient diversity in compliance with 10 CFR 50.62 for ATWS mitigation
- The I&C system design also provides diverse backup for RTIF/NMS and SSLC/ESF to address software CCF concern in accordance with the SRM to SECY-93-87, item II.Q
- LTR NEDO-33251, "ESBWR I&C Diversity and Defense-in-Depth," provides I&C system architecture and the analysis in conformance with BTP HICB-19 guidance
- DPS design is based on different technology, equipment, design personnel, signals, and functionality
- Diversity is provided both within Q-DCIS (three platforms RTIF/NMS , SSLC/ESF, and ICP are diverse from each other) and externally by a non-safety DPS
- DPS is classified as RTNSS and is developed via a rigorous, highly structured process similar to ones used for safety systems

Simplicity

- The staff found that the I&C system design employs simplicity in many aspects, which contribute to the staff's safety finding:
  - Each Q-DCIS division is independently monitored and controlled from its dedicated redundant set of safety related VDUs
  - Safety related components cannot be controlled from the non-safety related VDUs
  - Data communication from safety to non-safety related I&C systems is unidirectional
  - I&C system design meets "Independence – Isolation – Separation" requirements
  - Inter and intra-divisional communication is limited
  - ESBWR is a passive plant and the safety-related ESF functions are limited
  - Maintenance tool is not continuously connected

Logic Diagrams

- DCD contains adequate control logic design information for the staff to make a reasonable safety assurance finding
- Information described in the DCD will be used to develop logic diagrams
- Logic diagrams are produced and used during the I&C development life-cycle process
- Logic diagrams are finalized during the hardware/software design specification phase of the I&C system development lifecycle

Conclusion

- The staff has evaluated safety of the I&C system design and finds the design to be safe
- I&C systems are in conformance with the applicable regulatory requirements:
  - 10 CFR Part 52
  - 10 CFR Part 50, including 50.55a(h) (IEEE Std. 603 requirements)
  - 10 CFR Part 50 Appendix A (GDC)
  - 10 CFR Part 50 Appendix B (QA)
  - 10 CFR Part 50.34 (TMI items)
- I&C implementation DAC/ITTAC provided in Tier 1 are acceptable
- DCD Revision 8:
  - Provides clarity of I&C design information
  - No impact on I&C design
  - No impact on safety finding

Chapter 7 ACRONYMS

- ATWS Anticipated Transient Without Scram
- CCF Common Cause Failure
- DBA Design Basis Accident
- DCD Design Control Document
- DPS Diverse Protection System
- ESF Engineered Safety Feature
- GDC General Design Criteria
- ICP Independent Control Platform
- I&C Instrumentation and Control
- I/O Input and Output
- IEEE Institute of Electrical and Electronics Engineers
- LTR Licensing Technical Report
- N-DCIS Non Safety-related Distributed Control and Information System
- NMS Neutron Monitoring System
- QA Quality Assurance
- Q-DCIS Safety-related Distributed Control and Information System

Chapter 7 ACRONYMS (cont.)

- RG Regulatory Guide
- RTIF Reactor Trip and Isolation Function
- RTNSS Regulatory Treatment of Non-Safety System
- SER Safety Evaluation Report
- SSLC Safety System Logic and Control
- TMR Triply Modular Redundant
- VDU Video Display Unit

Presentation to the ACRS Subcommittee

ESBWR Design Certification Review

Section 9.4,“Heating, Ventilation, and Air Conditioning,” and Section 6.4, “Control Room Habitability System”

September 24, 2010

Purpose

- **Brief the Subcommittee on the staff's review of the ESBWR design certification application, Chapter 9.4, "Heating, Ventilation, and Air Conditioning," and Section 6.4, "Control Room Habitability System"; ventilation issues**
  - Address follow up items from the previous briefing on this issue held on May 19, 2010.
  - Address related follow up items from briefings held on August 17, 2010

- **Answer the Subcommittee's questions**

Project and Technical Review Team

- **Project Managers**
  - Dennis Galvin, Project Manager (9.4)
  - Bruce Bavol, Project Manager (6.4)
- **Technical Reviewers**
  - Jim O'Driscoll (6.4, 9.4.1 - 9.4.8) – Lead
  - Ed Forrest
  - Syed Haider
  - Shie-Jeng Peng
  - Brad Harvey (2.3)
  - Craig Harbuck (16)

Staff Follow-Up Items

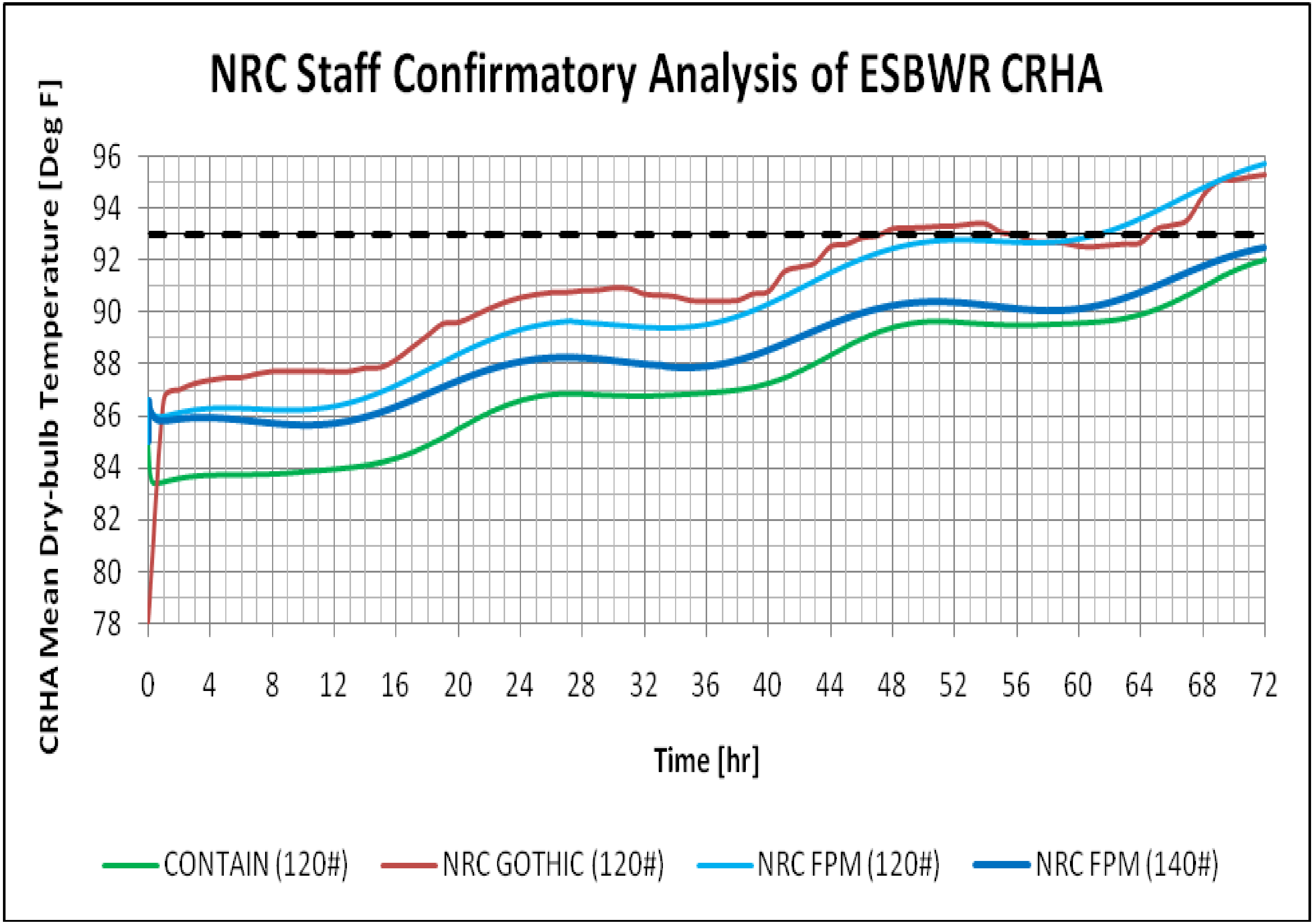
- **Provide and discuss heat up profiles for three models; CONTAIN 2.0, GOTHIC, and NRC First Principles Model (FPM)**
- **Discuss details of the Tech Spec Surveillance on Control Room Habitability Area (CRHA)heat sink temperatures**
- **Discuss details of verification of related site characteristics**
- **Discuss how assumptions used in the Reactor Building heat up calculation are assured**

Confirmatory Analyses

- **Staff review focus:**
  - **Suitability of applicant's approach using CONTAIN**
  - **Understanding of sensitivities**
    - **Heat sink properties**
    - **Heat sink initial temperature**
    - **Outside environmental conditions**
- **Summary of work performed:**
  - **Review of Applicants CONTAIN analysis**
  - **1 Run using updated GOTHIC model.**
  - **Review of GEH FPM / Development of Staff FPM**
  - **Over 24 sensitivity runs performed using CONTAIN and NRC FPM of GEH ESBWR CRHA.**

Confirmatory Analyses

- **Summary of findings:**
  - **Heat up rates of all models agree.**
  - **CONTAIN and FPM behave similarly in sensitivity studies.**
  - **FPM sensitivity result are 2 to 4 ºF higher than CONTAIN due to:**
    - **More heat is assumed to enter CRHA from adjacent rooms in FPM**
    - **Steel structures not modeled in FPM**
    - **Higher initial temperature of FPM heat sinks**
    - **½ Mass of concrete touching soil modeled in FPM**
  - **Staff conclusion is that there is no benefit to reconcile models further. Studies support use of CONTAIN. Applicants initial conditions are appropriately conservative. Difference in models results are small.**



NRC Staff Confirmatory Analysis of ESBWR CRHA
CRHA Mean Dry-bulb Temperature [Deg F]
96
94
92
90
88
86
84
82
80
78
0
4
8
12
16
20
24
28
32
36
40
44
48
52
56
60
64
68
72
Time [hr]
CONTAIN (120#)
NRC GOTHIC (120#)
NRC FPM (120#)
NRC FPM (140#)

Details of CRHA Heat sink TS Surveillance

- **LCO 3.7.2 requires maintaining heat sink temperature “within established design limit” (SR 3.7.2.1) (CRHA thermal analysis)**
  - **≤ 74 °F for CRHA**
  - **≤ 78 °F for Q-DCIS & N-DCIS equipment rooms**
  - **≤ 104 °F for HVAC equipment rooms and safety portions of Control Room Habitability Area Ventilation System (CRAVS)**
- **CRHA boundary passive heat sinks limit the CRHA temperature to the acceptance criterion of 33.9°C (93°F) for 72 hours post-DBA with no internal forced air recirculation or cooling.**

Technical Specification 3.7.2 "CRHAVS"

- **LCO 3.7.2 ensures that CRHA**
  - Average air temperatures will be maintained within acceptable limits for 72 hours following an event that includes loss of CRHAVS cooling, and
  - Heat sink bulk average temperatures are within design-basis analysis assumptions.
- **LCO 3.7.2 bases state that the CRHA heat sinks are operable when the air and heat sinks in the CRHA and adjacent spaces are maintained within the average temperature limits of SR 3.7.2.1.**
- **LCO 3.7.2 Required Action A.2 requires restoring the bulk average temperature of each CRHA heat sink to within limits within 24 hours.**
  - The 24-hour Completion Time is based on engineering judgment. Staff considers that 24 hours is reasonable and consistent with staff analysis.
  - Restoration of CRHA heat sink bulk average temperatures to within limits may be verified by
    - administrative evaluation considering the duration and extent of the CRHA average air temperature excursion outside limits, and/or
    - direct temperature measurement of CRHA heat sink structural materials.
  - Determination of CRHA heat sink bulk average temperatures is the subject of licensee procedures.

Ambient Design Temperature Site Parameters

2% Annual Exceedance	Max	DB	96 °F
		MCWB	79 °F
		WB	81 °F
	Min	DB	-10 °F
1% Annual Exceedance	Max	DB	100 °F
		MCWB	79 °F
		WB	82 °F
	Min	DB	-10 °F
0% Exceedance	**Max**	**DB**	**117 °F**
		MCWB	80 °F
		WB	**88 °F**
	Min	**DB**	**-40 °F**
Max Avg DB for 0% Exceedance Max Temp Day			**103.5 °F**
Min Avg DB for 0% Exceedance Min Temp Day			**-26.5 °F**
Max HH Avg WBGT Index for 0% Exceedance Max WB Day			**86.6 °F**

Maximum Average Dry Bulb Temperature for 0% Exceedance Maximum Temperature Day

Site Parameter Value: 103.5 °F

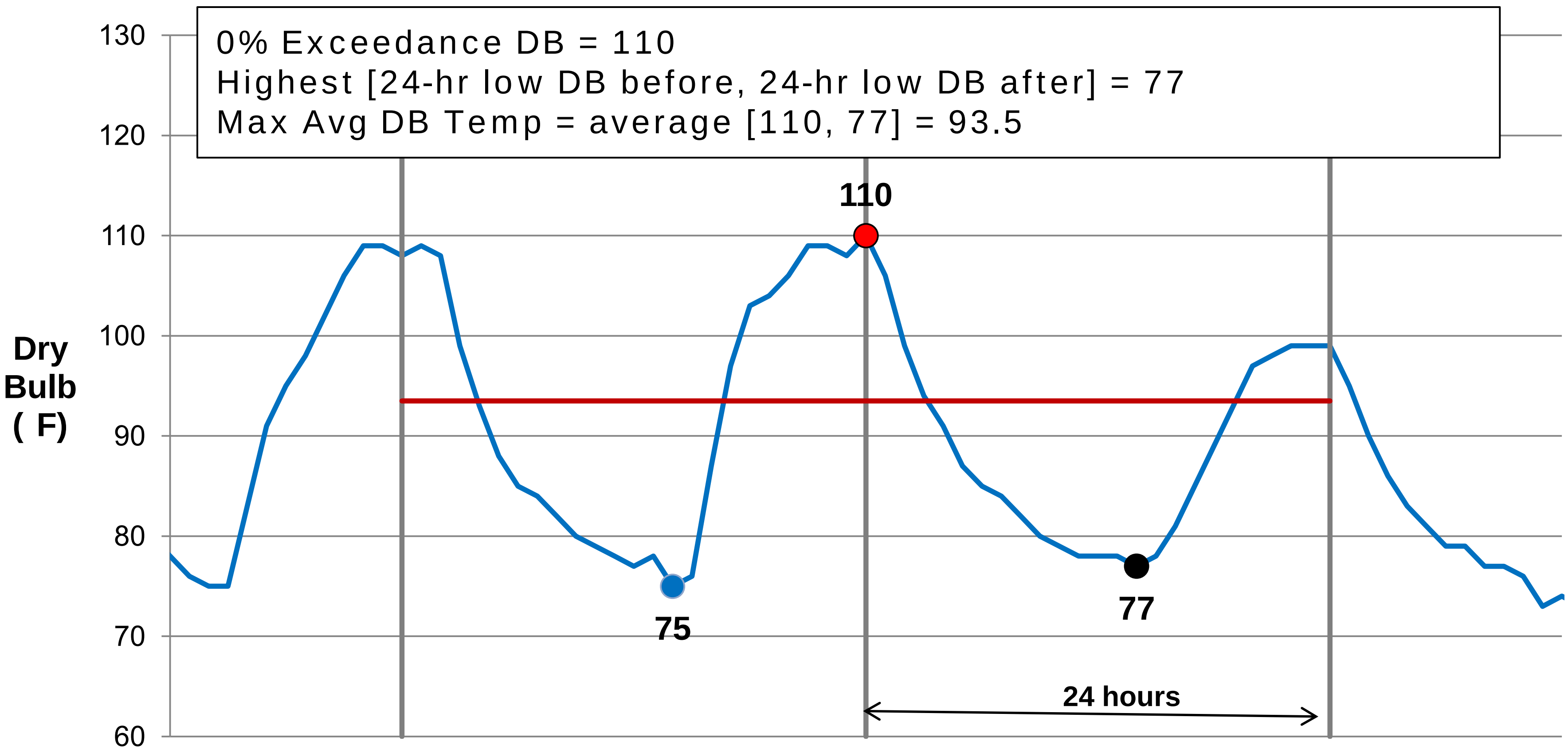
- **Defined as the average of:**
  - **0% exceedance maximum dry bulb site parameter value of 117 °F**
  - **Dry bulb temperature resulting from a daily temperature range of 27 °F**

Determining the Corresponding Site Characteristic Value:

- **Defined as the average of:**
  - **Site-specific 0% exceedance maximum dry bulb**
  - **Dry bulb temperature that corresponds to the higher of the two lows occurring within 24 hours before and after the 0% exceedance maximum dry bulb**

Verification of Related Site Characteristics
Example Calculation #1

- **Maximum Average Dry Bulb Temperature for 0% Exceedance Maximum Temperature Day: 93.5 °F**



Minimum Average Dry Bulb Temperature for 0% Exceedance Minimum Temperature Day

Site Parameter Value: <u>-26.5 °F</u>

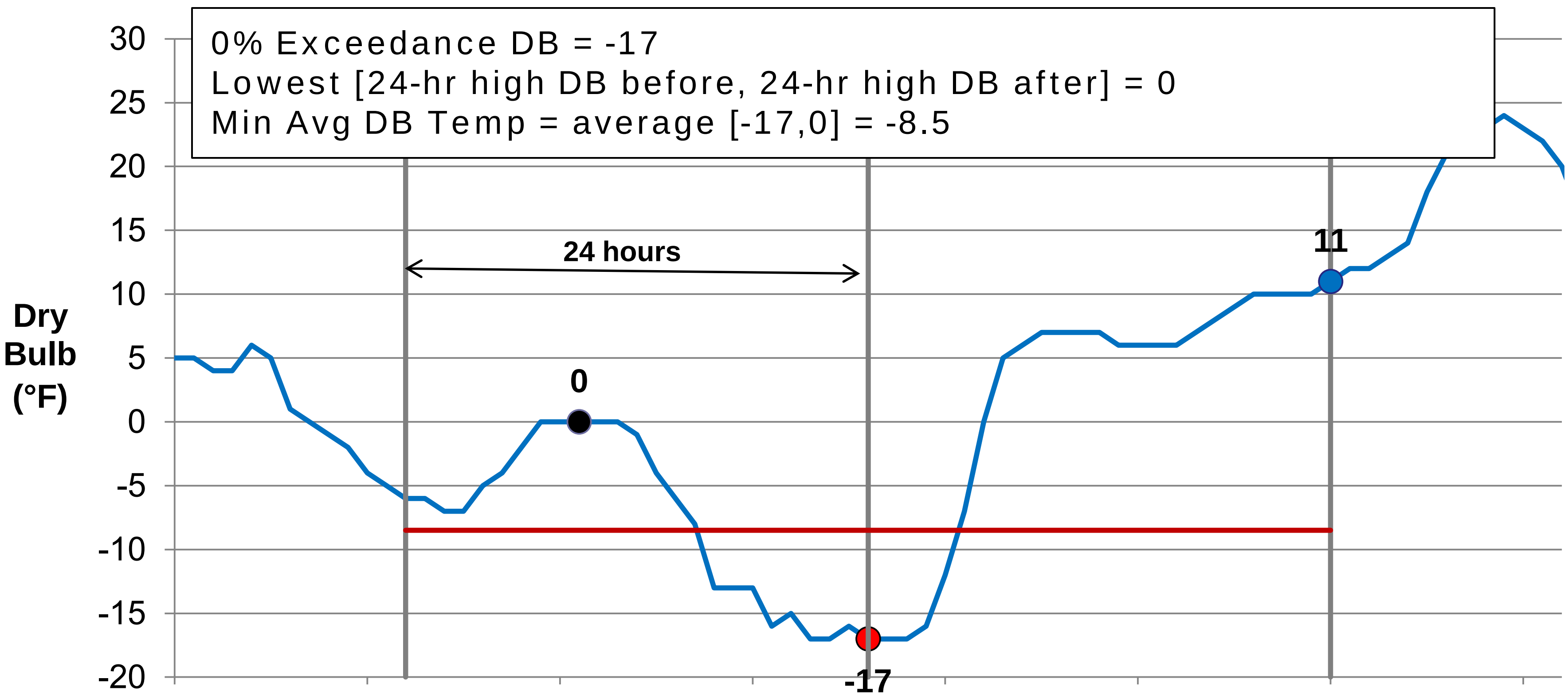
- **Defined as the average of:**
  - **0% exceedance minimum dry bulb site parameter value of -40 °F**
  - **Dry bulb temperature resulting from a daily temperature range of 27 °F**

Determining the Corresponding Site Characteristic Value:

- **Defined as the average of:**
  - **Site-specific 0% exceedance minimum dry bulb**
  - **Dry bulb temperature that corresponds to the lower of the <u>two</u> highs <u>occurring within 24 hours</u> before and after the 0% exceedance minimum dry bulb**

Verification of Related Site Characteristics
Example Calculation #2

- **Minimum Average Dry Bulb Temperature for 0% Exceedance Minimum Temperature Day: <u>-8.5 °F</u>**



Maximum High Humidity Average Wet Bulb Globe Temperature Index for 0% Exceedance Maximum Wet Bulb Temperature Day

WBGT Index = 0.7×WB + 0.3×DB

Site Parameter Value: 86.6 °F

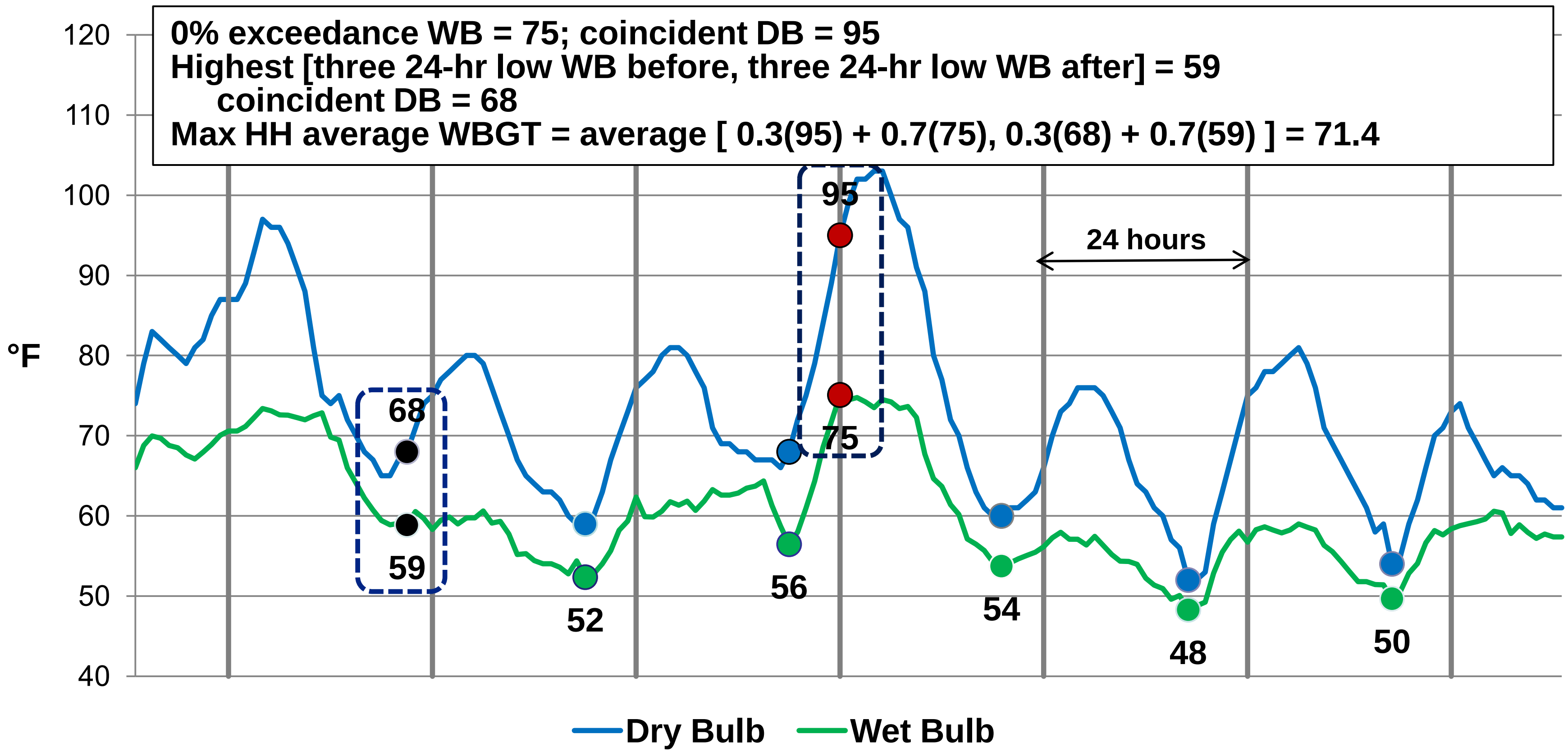
- **Defined as the average of:**
  - **WBGT index for the 0% exceedance wet bulb site parameter value of 88 °F (and a concurrent dry bulb value of 92 °F)**
  - **WBGT index resulting from a high humidity diurnal dry bulb temperature swing of 8 °F (dry bulb temperature of 84 °F and concurrent wet bulb temperature of 84 °F)**

Determining the Corresponding Site Characteristic Value:

- **Defined as the average of:**
  - **WBGT index for the site-specific 0% exceedance wet bulb**
  - **WBGT index resulting from wet bulb temperature that corresponds to the highest of the six low wet bulb temperatures occurring in each of the three 24-hour periods before and after the 0% exceedance wet bulb**

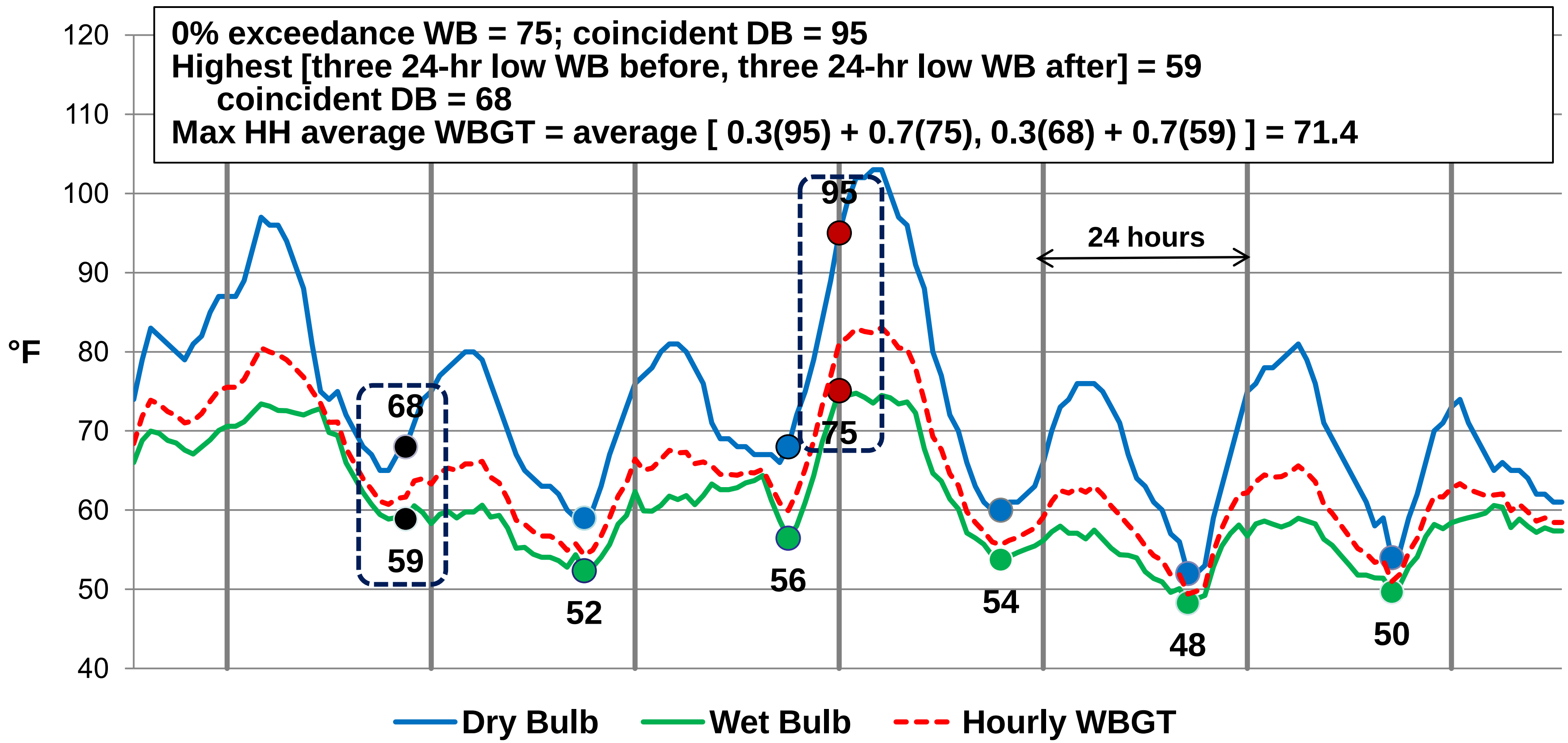
Verification of Related Site Characteristics
Example Calculation #3 (sheet 1 of 3)

- **Maximum High Humidity Average WBGT Index for 0% Exceedance Maximum Wet Bulb Temperature Day: 71.4 °F**



Verification of Related Site Characteristics
Example Calculation #3 (sheet 2 of 3)

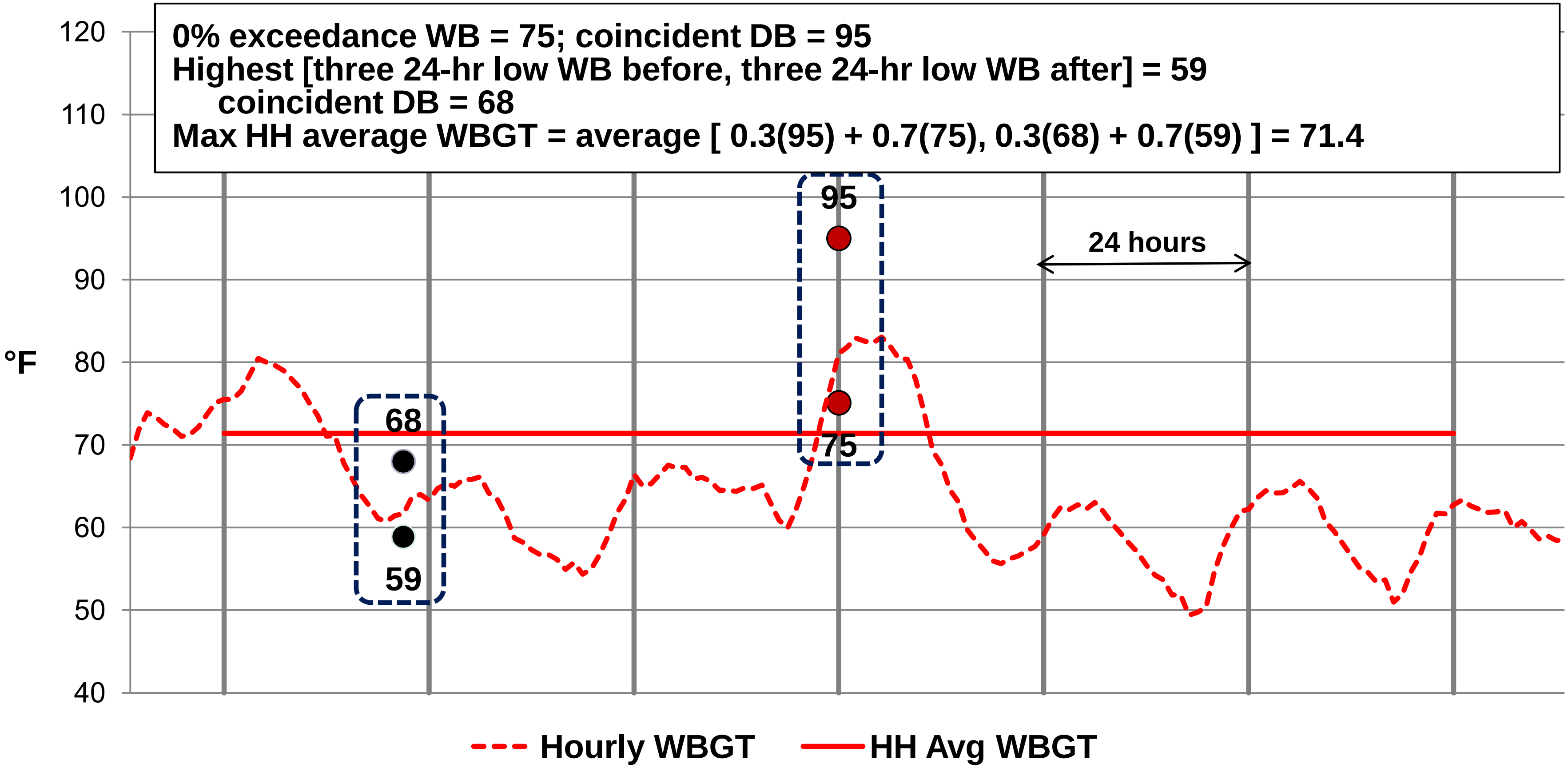
- **Maximum High Humidity Average WBGT Index for 0% Exceedance Maximum Wet Bulb Temperature Day: 71.4 °F**



Verification of Related Site Characteristics
Example Calculation #3 (sheet 3 of 3)

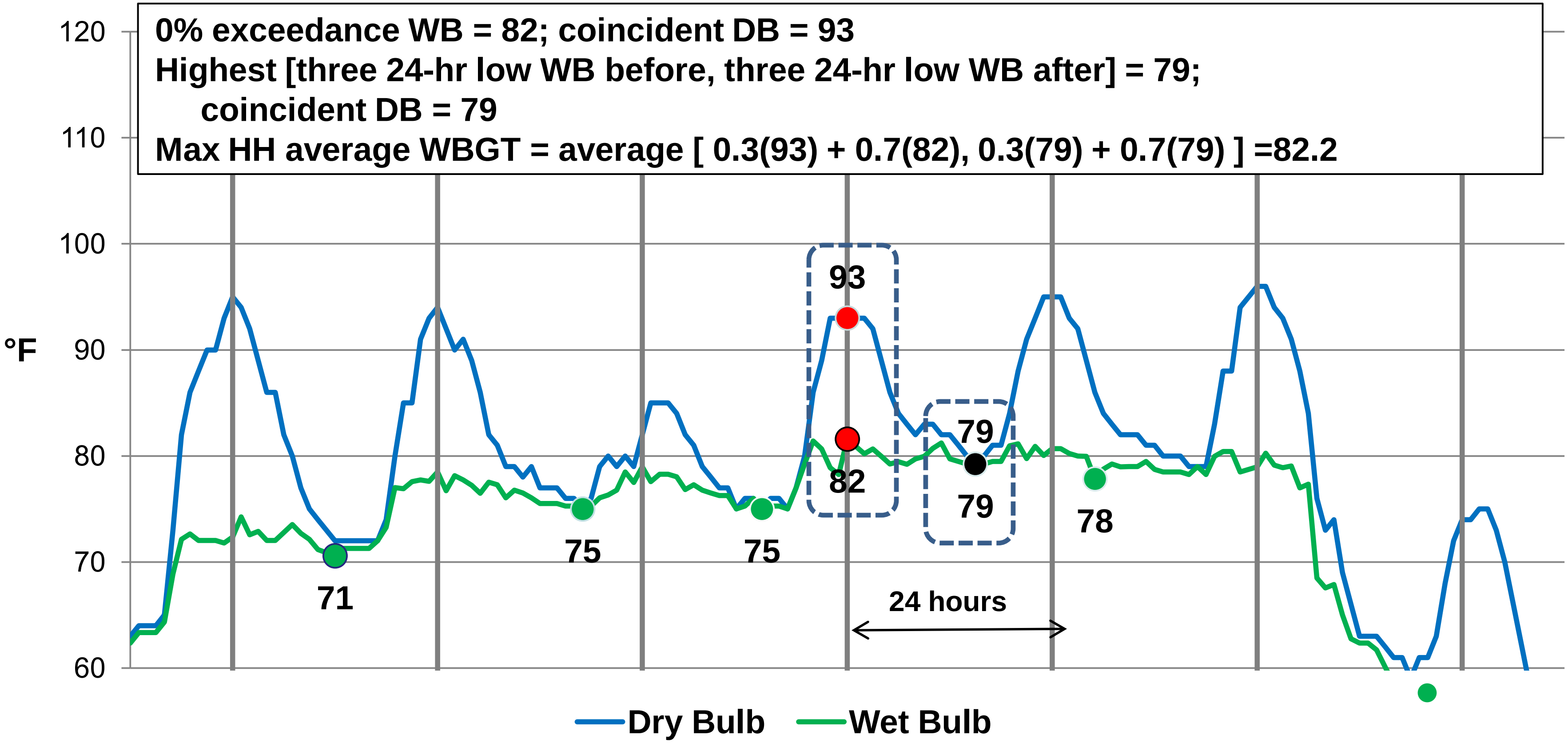
- **Maximum High Humidity Average WBGT Index for 0% Exceedance Maximum Wet Bulb Temperature Day: <u>71.4 °F</u>**

0% exceedance WB = 75; coincident DB = 95
Highest [three 24-hr low WB before, three 24-hr low WB after] = 59
coincident DB = 68
Max HH average WBGT = average [0.3(95) + 0.7(75), 0.3(68) + 0.7(59)] = 71.4



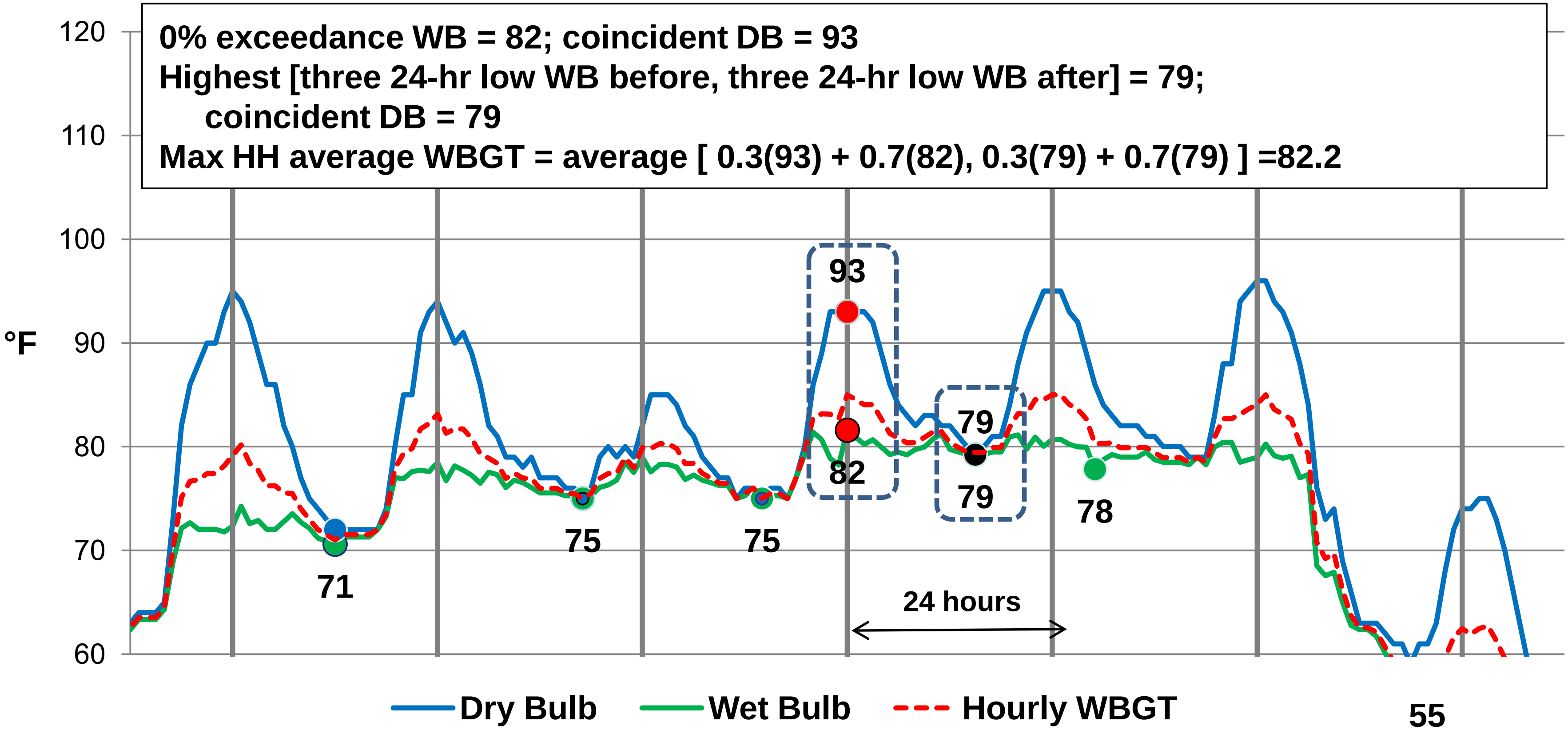
Verification of Related Site Characteristics
Example Calculation #4 (Sheet 1 of 3)

- **Maximum High Humidity Average WBGT Index for 0% Exceedance Maximum Wet Bulb Temperature Day: 82.2 °F**



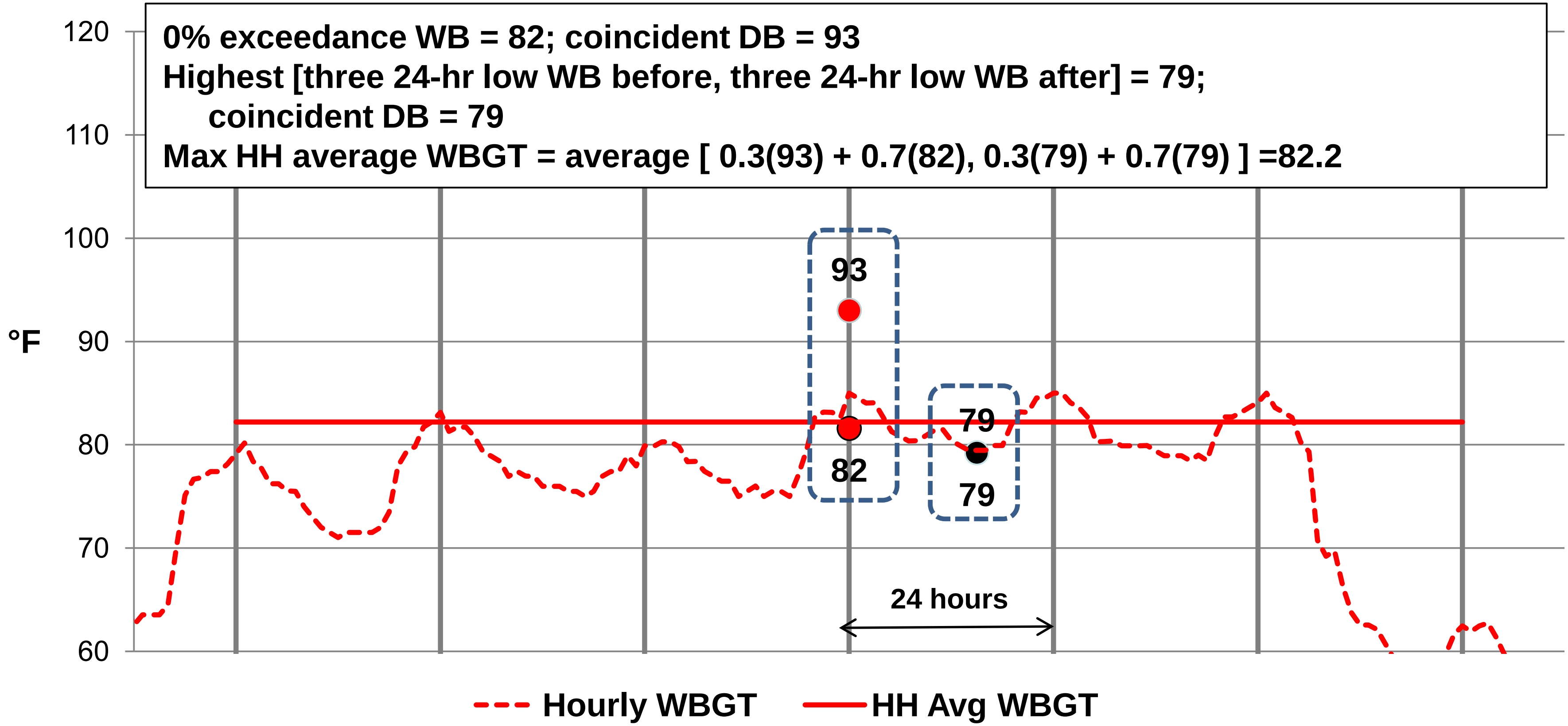
Verification of Related Site Characteristics
Example Calculation #4 (sheet 2 of 3)

- **Maximum High Humidity Average WBGT Index for 0% Exceedance Maximum Wet Bulb Temperature Day: 82.2 °F**



Verification of Related Site Characteristics
Example Calculation #4 (sheet 3 of 3)

- **Maximum High Humidity Average WBGT Index for 0% Exceedance Maximum Wet Bulb Temperature Day: 82.2 °F**



Assurance of RB Heat Up Analysis Assumptions

- **Staff reviewed the need for a reactor building heat sink temperature LCO similar to control building heat sink temperature LCO 3.7.2, "CRHAVS"**
  - ➢ CRHAVS meets LCO criterion 3; its passive cooling function depends on heat sink initial temperatures and is part of primary success path for DBA mitigation by supporting CR habitability required by GDC 19
- **1988 letter from NRR to Owners Groups (OGs) ("Split Report") - Staff's review of the BWROG's LTR regarding the application of the LCO criteria of the 1987 Commission Interim Policy Statement on TS improvements to the**
  - ➢ BWR4 custom TS (Hatch 1) and standard TS (Hatch 2), and
  - ➢ BWR6 standard TS (Grand Gulf 1)
- **Staff agreed with relocation of LCOs for**
  - ➢ ECCS and RCIC pump room air coolers from pilot plant custom TS (Hatch 1)
  - ➢ Area temperature monitors from pilot plant standard TS (Grand Gulf 1).
- **Purpose of these LCOs was to maintain equipment qualification (§50.49)**
  - ➢ LCOs should not duplicate regulations;
  - ➢ Improved STS do not include LCOs on **monitoring instrumentation** except for post-accident monitoring; **area temperature monitors are not in primary success path for accident mitigation and are not used to detect degradation of reactor coolant pressure boundary; equipment room temperatures are not initial conditions for any DBA**
- **OPERABILITY definition ➔ necessary support system functions**
  - ➢ RIS 2005-20, Rev. 1; operability assessment of degraded or nonconforming equipment
  - ➢ EQ is one factor in determining equipment operability
- **Conclusion: §50.36 requires no LCO for reactor building heat sink temperatures**