Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards ABWR Subcommittee on STP COLA

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Tuesday, February 8, 2011

Work Order No.: NRC-696 Pages 1-14

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)

+ + + + +

MEETING OF THE ABWR SUBCOMMITTEE ON STP COLA

+ + + + +

TUESDAY

FEBRUARY 8, 2011

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B3, 11545 Rockville Pike, at 1:00 p.m., Said Abdel-Khalik, Chairman, presiding.

COMMITTEE MEMBERS:

SAID ABDEL-KHALIK, Chairman

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR., Member

JOHN D. SIEBER, Member

JOHN W. STETKAR, Member

ACRS STAFF PRESENT:

MAITRI BANERJEE, Designated Federal Official

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

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

12:59 p.m.

CHAIRMAN ABDEL-KHALIK: The meeting will now come to order. This is a meeting of the Advanced Cooling Water Reactor Subcommittee of the Advisory Committee on Reactor Safeguards.

I'm Said Abdel-Khalik, Chairman of the Subcommittee. ACRS members in attendance today are Charlie Brown, John Stetkar, Dennis Bley and Jack Sieber. Ms. Maitri Banerjee is the designated federal official for this meeting.

All through last year, we were briefed by the Applicant, STPNOC, now called NINA Nuclear Innovation North America, and the NRC staff regarding the South Texas project combined license application, and the corresponding safety evaluation report prepared by the staff. The full Committee was briefed in July and wrote an interim letter to the Chairman.

In today's meeting, we are scheduled to discuss Chapter 7, I&C. This chapter was presented to us before when the SER had open items. Today, the staff will discuss how they have resolved those open items. The staff and the applicant may also discuss follow-up action items from previous ABWR Subcommittee meetings.

The rules for participation in today's meeting were announced in the *Federal Register* on January 28th, 2011, for an open/closed meeting. Parts of this meeting may need to be closed to the public, to protect the information proprietary to the Applicant or other parties.

I'm asking the NRC staff and the Applicant to identify the need for closing the meeting before we enter in such discussion, and to verify that only people with the required clearance and need to know are present.

We have a telephone bridge line with the public and stakeholders to hear the deliberations. This line will not carry any signal from this end during the closed portion of the meeting.

Also, to minimize disturbance, the line will be kept in a listen-in only mode until the last 15 minutes of the meeting. At that time, we will provide the opportunity for any members of the public attending this meeting, in person or through the bridge line, to make a statement or provide comments.

As the meeting is being transcribed, I request that participants in this meeting use the microphones located throughout this room in addressing the Subcommittee. Participants should first identify themselves and speak with sufficient clarity and volume, so that they can be readily heard.

We will now proceed with the meeting, and I call on Mr. Mark Tonacci of NRO to begin the presentation.

MR. TONACCI: Thank you Dr. Abdel-Khalik and members of the Committee. I hope that today we have a good dialogue, and productive dialogue, and that in the end, we've addressed all the questions and concerns that you may have. That is really the full extent of my opening comments, and I am ready to begin.

CHAIRMAN ABDEL-KHALIK: We'll move on to the Applicant, Scott.

MR. HEAD: Okay, thank you very much. Yes, today we're going to brief you on Chapter 7. Here's the proposed agenda for today. As you noted, we did brief last year on May 20th on Chapter 7. Discussion points for today, we want to discuss setpoint methodology, current Reg Guides and codes and standards applied to Common Q, and then this new FSAR Tier 2, Appendix 7 DS that we created, and go over that in some detail for you today.

The attendees shown on this slide. I will go ahead and use this moment to clarify the NINA perspective. On January 24th, the project transitioned from STPNOC being the applicant to NINA being the lead applicant, with STPNOC basically, S-T-P-N-O-C being the secondary applicant.

What that means is that NINA will be responsible, obviously after NRC approves, NINA will be responsible for the licensing, design and construction of the project, and at the 103(g) point in time, it will transition the STPNOC, S-T-P-N-O-C, to operate the plan. So that's the application that we now have in front of NRC. It came in in Rev 5 of the COLA.

With respect to maybe of more interest to you, your review and the staff's review, and individuals like myself, Mike Murray, Coley, others, STPNOC employees and right now loaned employees to NINA, and we will be continuing to fulfill the licensing role that we have had and we'll just be basically seeing that through.

So in terms of interactions and interactions with the staff, you should not see any change from that perspective. So that's the important message out of this transition, and the transition really reflects NINA's desire to not only build 3 and 4, but to be involved in building future units also, assuming our success.

CHAIRMAN ABDEL-KHALIK: Thank you for that clarification. That's very helpful.

MR. HEAD: Okay, and with that, I'm going to turn it over to Mike Murray.

MR. MURRAY: I'm Mike Murray. I'm the IC manager for NINA in the STP 3 and 4 effort. When we say setpoint methodology, we have discussed it in previous meetings, but there was one open item, one item that needed to be addressed, and that was in the setpoint methodology, we had referenced a post-COL stability methodology report.

What we did was we moved the methodology into the -- that we would have expected to see in the stability report. We moved those type of calculations into the setpoint methodology. So that the setpoint methodology now incorporates the oscillation power range monitor, which was the follow-up item. So that's been completed.

Next slide. We continue to, and this next one is on the Common Q platform. Originally, our perspective was that we would use the original Reg Guides and industry codes that were when the Common Q platform was approved.

CHAIRMAN ABDEL-KHALIK: Can we go back to the previous slide?

MR. MURRAY: Certainly.

CHAIRMAN ABDEL-KHALIK: It doesn't specify which code will be used to generate the DIVOM curve, the methodology.

MR. MURRAY: I don't know the answer to that. The question is what code issues will the methodology?

CHAIRMAN ABDEL-KHALIK: Right. What code will be used to generate the DIVOM slope for this OPRM trip setpoint?

MR. MURRAY: We can get you that answer. Okay. I don't have that with me. Any other questions? The original Rev 4 guides that we had in our response was to use the original platform guide that were -- or the original guides that were in place when the platform was approved.

Since then, what we've done is we've gone through and we've eliminated those exceptions to the Common Q platform. So the Common Q platform, as we'll apply it to STP 3 and 4, we've committed to use the codes and standards in effect six months prior to submittal of the COLA. So it will be using the same codes and standards as the other digital platforms being developed.

MEMBER BROWN: What's the date of that?

MR. MURRAY: When did we make that change?

MEMBER BROWN: Yes. You say six months, and I've forgotten what the dates were.

MR. HEAD: That MOA was -- I believe it's mid-March '07.

MEMBER BROWN: March '07.

MR. MURRAY: Well, what we've got now is alignment of the technical standards through all the digital I&C systems.

PARTICIPANT: Yes.

MEMBER BROWN: Ed, which -- I've got three revisions of the WCAT-1, 01 and 2. Which ones are you --

(Simultaneous speaking.)

MR. ED BROWN: This is Ed Brown from Westinghouse. It is Revision 1. Revision 2 has been submitted to the NRC. It has not been reviewed and approved.

MEMBER BROWN: Okay. So Revision 1 is the one you're all operating under?

MR. ED BROWN: Yes.

MEMBER BROWN: Okay, thank you.

MR. TONACCI: And Mr. Brown, your question was when was the COLA submitted?

MEMBER BROWN: Well, when you said six months prior to submittal of the COLA, and so I just asked what was the date of the submittal of the COLA, and you said March '07.

MR. TONACCI: No. It was September '07.

VOICES: September 2007.

MS. BANERJEE: September 20th, '07.

MEMBER BROWN: Thank you.

MR. TONACCI: Six months prior to that is when you get into the March time frame.

MR. MURRAY: Okay. Any other questions sir? Next slide. Okay. We've also, throughout our processes, we received feedback where there was a simple task to find all the information on the digital I&C platforms.

MEMBER BROWN: Excuse me.

MR. MURRAY: Yes sir.

MEMBER BROWN: On the platform revision, I didn't want to read all three of them. Is there a big difference between 1 and 2? I looked at a few areas, and a couple of areas between Rev 2 and Rev 0, and I just wondered if it was a massive revision, or was it just cleaning up loose ends and consolidating some stuff?

MR. ED BROWN: In Revision 2, there are

some additional information. For example, it discusses changes in equipment that since the original revision. That's one of the differences. Another difference is it describes the process used to evaluate changes to the hardware and software, to screen it for prior approval by the NRC, and those, I believe, were the major changes.

MEMBER BROWN: It came another way at the communication scheme, the whatever the memory thing was between AC, you know, and all that. Potentially it stays in that concept?

MR. ED BROWN: Yes. Functionally, it still operates the same, exactly the same, Charlie.

MEMBER BROWN: Okay, thank you.

MR. MURRAY: Move on to the next slide. So let's discuss -- what we did is we developed the appendix for the FSAR. We call it seven delta S or seven DS is what I refer to it as. Our purpose there was to consolidate information from various parts of the COLA, applicable technical reports and topical reports regarding the design principles, redundancy, independence, determinism, diversity and discretion on simplicity.

What we included or described, there were no new design changes or departures, and it was just consolidation of information. The scope included is the reactor trip isolation system and the safety-related neutron monitoring system, as well as the engineered safety logic and control system, which is implemented by the Common Q platform.

MEMBER BROWN: Do you expect the FSAR, this appendix to be implemented or included in the FSAR prior to receiving approval of your --

(Simultaneous speaking.)

MR. MURRAY: Yes sir, yes sir. Additionally, where we've had sections in the write-up, where we've had areas that have covered either ITAACs or DACs, what we've done is we've mapped over the specific design criteria as we discussed them, and made a table that relates it to inspectable DAC in the area there.

So that's the purpose of our seven DS. What we're going to do now is we're going to transition into discussions on the two platforms, specifically our overview, an overview of it, redundancy, independence, determinism, diversity.

What you have is a set of slides that are brought up. What I've got is for your convenience, the diagrams. So if we pass one, you can have it to look at as we continue the discussions through for convenience. So there should be a set of acronyms, as well as a set of slides, the slides that are in the presentation.

Okay. So let's go ahead and go on to the picture there. Okay. So you have a slide there. I'll just go to the slide, and it's better to see the picture as we work through this. We have the digital trip function, which is up at the top, and the digital trip function, and in this case what it does, and this is for the RTIS and NMS platform, it takes the -- it does the digital conversion from the hard-wired sensors into a digital space.

It compares the signals, the setpoints and determines the sensor trip status, trip and status. Then the next block down is the trip and logic function. It receives the sensors. It receives the input from the digital trip functions, and takes them in and performs the two out of four voting determinant. There's an automatic divisional trip required.

It sends the divisional trip and output information to the, what's shown there as an OLU, which an operating, output logic unit. The output logic unit then receives the automatic trip and divisional data, and then it redistributes it to the load drivers for reactor trip, and it does it for main steam isolation.

So that's the simplified picture of how the RTIS works.

MEMBER BROWN: If everybody didn't notice, I don't -- you didn't specifically state it, but the entire RTIS and the NMS is field-programmable data array implemented, there's a little word here on the previous page.

MR. MURRAY: That's correct.

MEMBER BROWN: You're just amplifying it?

MR. MURRAY: That's correct. Okay. So if you all use this, as we continue this out, keep your bearings on where we are. Some of the information is going to be redundant, in the fact that when you get into independence and redundancy, some of it overlaps in that area.

MEMBER BROWN: Is the overlap?

MR. MURRAY: Pardon?

MEMBER BROWN: Is the overlap new in FPGA?

MR. MURRAY: No sir. It's required not to be. Is that correct?

MEMBER BROWN: Is that explicitly stated in the FSAR?

MR. MURRAY: Yes.

MR. DITTMAN: This is Kyle Dittman. I'm NINA's supervisor, I&C supervisor. The OLU is due to D-3 as a diverse type of logic. In this case, it's gated logic.

MEMBER BROWN: Just demand more data and all that kind of stuff? Okay.

MR. IKEDA: This is Jun Ikeda from Toshiba. What we have is based on the solid state I&C technology and the real logic.

MEMBER BROWN: Okay.

MR. MURRAY: So platform redundancy. In the NMS, there's four independent redundant divisions, it takes the -- brings the signals to, develops the trip signals and status to the divisions of RTIS. RTIS has four independent redundant divisions as well. Each includes DTF, TLF and OLU. We have some of the functions are divisions of sensors bypass, and also trip logic output bypass.

Get the divisions bypass, you go to a two out of three vote logic to accomplish the functions. Each division is an independent and redundant power sources. So the division 1 feeds division 1 channels, two power sources, two, three. So there are four complete redundant divisions there. Any question on redundancy?

Let's talk about platform independence, and we're still talking reactor trip isolation and neutron monitoring system. Four independent divisional power sources, independence from non-safety systems. Any communication to a non-safety system is isolated and independent.

Electrical isolation and physical separation, following the criteria that the design criteria is is isolated between the divisions as well as non-safety systems. Four independent RTIS and NMS sensor divisions, and that determines sensor divisional signals, trip signals. There's no communication between the sensor divisions.

If you look at the block diagram again, you'll see that the DTFs do send the signals to the TLFs, but they don't communicate amongst themselves. The only trip and status information is communicated across the division boundaries, and that's for the two out of four voting logic functions.

There are four independent RTIS, TLFs and OLUs. So trip logic function and the output drivers are full of those. Communication isolation and independence is maintained there, as well as electrical isolation and physical separation. Any questions?

(No response.)

MR. MURRAY: Now we'll discuss more about the independence of communication and the RTIS across the divisions. As we discussed, the DTS, when it sends their signals to the TLFs of the other divisions, communicates trip and status information in fixed link, fixed content and predefined format, and that's very important for finding errors in the messages.

It's qualified, isolated, point-to-point, unidirectional fiber communication, and each communication link has its own buffer for a memory buffer. Yes sir.

MEMBER BROWN: Okay. The -- make sure I get the question right. So this is like a field which us from the DTF to the other division, TLFs. So and I'm trying to think this through. It's not the equivalent of a dry contact open and closed. It actually has other intelligence, such as a header and footer and something in between that's supposed to contribute or communicate?

MR. MURRAY: It does have a header, but when you get into the message, it's almost like a contact, because in specific locations, it is either -- one is in that specific location. So once you get through identification of the message, then there's a predefined place for each command, and that command can either -- or not command; that's a bad term.

Piece of information. It's either a one or a zero, which gives you the trip status of that particular function, or the point status. It gives the vote.

MEMBER BROWN: Okay. Let me ask again. You've answered the question. Okay so, this is a single fiber optic wire cable that goes from channel, Division 1 to Division 2's TLF.

MR. MURRAY: Okay.

MEMBER BROWN: It goes into fixed locations, not like it has to be scanned or sampled.

MR. MURRAY: No.

MEMBER BROWN: It goes from Point A, like you say and has to go out of the other one.

MR. MURRAY: That's correct.

MEMBER BROWN: Yes, whatever the filtering, the buffering you do. What is the purpose of that header or is something giving it something. It sounds like an address as opposed to something that's not necessary to this.

MR. FUKUMOTO: I am Akira Fukumoto with Toshiba again. We do have a header or pipe header to identify the data piping, and then we do have some master coding here, and then we do check some goal to identify it. If we can't find the header, we will find something wrong in the communication.

So with this header we have a set of files containing the information. Those are the ones going to one to zero, showing trip status or other status. Did that answer your question? No?

MEMBER BROWN: Oh you probably did, but I didn't, I won't say I understood it, and you know it's coming out of Division 1 and it's going to the other divisions, three divisions, and it's a yes or no, respectively, and yet you're sending information in advance of the actual piece of critical information, which is a trip or non-trip.

I guess I'm trying, I was trying to figure out a reason, and as to why you did that, and I didn't know whether it was related to the synchronous operation within each divisions have PGA, they have PGA, they have PGA.

In other words, you have to coordinate and synchronize within that in order to get your data transfers and hand-offs, to stay deterministic, I think. I'm not an expert on this stuff. So I'm liable to say a lot of wrong things.

When you go division to division, you're not synchronized between divisions, and so one of my questions later was how do you achieve a satisfactory data transfer between non-synchronized divisions? I'm trying to relate a little bit of the header, why you do it this way? It just seems an over-complication. And I'm not questioning that it won't work. That's not the point. I was just trying to get a better understanding of how it operates.

MR. FUKUMOTO: Each divisions in FPGA modules and the areas, and then you are right. We are not doing a synchronization among the divisions. When we send the data from DTF in the division to other three divisions across one more division, that's solid division.

This is the data by all fiber optic cable. That's all sending by in 20 seconds, and then the FPGA runs. For example, typically for full function it takes let's say a few, maybe 20 seconds. So the data transmission rate is very slow the second time because of processing. It's very time consuming.

So the transmission is made a signal, and if you look at those other divisions, other transmission is done in signals. In a receiving mode, you will attach the header to getting the data to the bottom.

From that point, the synchronization among the modules stops.

MEMBER BROWN: Within the TLF?

MR. FUKUMOTO: Yes, yes.

MR. MURRAY: So the header was the question. What is the purpose of the header; correct?

MEMBER BROWN: Well, it's varying the other question of how do you transfer the data, to get it to work properly? Looks like you did talk about within the division, you have to synchronize and orchestrate so the next FPGA doesn't do these things. I was told that there's data available, okay, so but it's got to have proper plugging that it comes and looks for it at the right time, every cycle.

So I'm just -- so I was trying to figure out, because I presume you don't have headers all through the division. You only do it when you go from division to division? Is that, or just --

MR. FUKUMOTO: Let me explain.

MEMBER BROWN: It's starting to look more like a microprocessor, if I start throwing headers and footers and other stuff like that into it. That's all.

MR. FUKUMOTO: Here's a receiver, here's a sender. Sender don't know what is the status of the receiver. So this sender send the data periodically based on this synchronization. This one is really for the header, and knowing the header, it's diagnosed that is coming. So based on that information, this receiver take that data into the buffer. It's all deterministic by the hour.

And if this receiver complete getting the data from the transmission line to the buffer, then this guy send a pulse to the next FPGA. So that is how the divisions work.

MEMBER BROWN: So it's a non-synchronous synchronization at the time of data transfer. Is that -- I'm trying to simplify this down to something my simple brain can comprehend. Did I say that wrong? I mean it sounds like you're providing an ad hoc synchronization, but not requiring the other divisions be synchronized. You're starting it out when you want it to.

MR. FUKUMOTO: No synchronized.

MEMBER BROWN: All right. Why don't we go on?

MR. MURRAY: Yes. The next point we'll talk a little bit more about that as well, Mr. Brown, on the self-diagnostics, and I think that's where this package also plays in, that header plays into the self-diagnostic as well.

So the next point that we want to make is on the communication, includes that self-diagnostic function. It does the quality checks of the data when it comes in, and it continuously monitors for proper communications. So that's done in the receiving and the sending areas.

If it detects a failure, the division is marked inoperable. So if it doesn't get the right set of framing and communication as it's doing its parity and framing checks, then it will mark the division as -- that particular division as inoperable and then provide a fail-safe trip condition for the -- and the operator additionally is alerted.

MEMBER BROWN: Okay. I read that in the appendix.

MR. MURRAY: Right.

MEMBER BROWN: So that when -- is that within the divisions or the Division 1 or say Division 2, if Division 2 TLF detects that the data sent to it is wrong? I didn't read that as having a cross-division. That would just be one data, one of four pieces of data that would be focused, and you would still operate on two out of three. So, you know, in terms of that division of voting?

That's -- but the trip function was if you get something within the division that's incorrect, then the division itself would be declared out of service?

MEMBER STETKAR: Suppose Division 2 now, okay, receives an identified corrupt packet from Division 1. Does Division 2 then interpret that as a Division 1 trip input signal to Division 2, such that within Division 2, you then need a coincidence of trip from Division 2 or Division 3 or Division 4 to satisfy a Division 2 output signal? Is that the way it works?

MR. MURRAY: That's correct. The message comes in and it's gone through, it goes through and gets the quality checks on the message, and at that point the quality checks are successful. Then it will flag that data --

MEMBER STETKAR: Division 2 data.

(Simultaneous speaking.)

MR. MURRAY: That's correct.

MEMBER BROWN: Thank you. That's what I was --

MR. MURRAY: Is that what you were looking for?

(Simultaneous speaking.)

MR. MURRAY: On each input that is monitoring the quality of the data that's received, and if it's not, if it doesn't meet the quality checks, then it flags it as bad data, doesn't accept that data --

MEMBER STETKAR: So it's like in principle that Division 2 is looking at all four divisions. If it sees corrupt data from Division 1 and Division 3, that would satisfy the Division 2 output decision.

MR. MURRAY: If you had two divisions that gave the bad data, you would meet that --

MEMBER STETKAR: You wouldn't necessarily trip the reactor if the other three divisions are reading something as correct/incorrect. I don't know how that happens, but --

MEMBER BROWN: Going to one of the questions before, if Division 1 is sending its data to four different TLFs.

MR. MURRAY: Right.

MEMBER BROWN: And is it sent over four separate -- I presume it's sent over four separate fiber links.

(Simultaneous speaking.)

MEMBER BROWN: Yes, well yes.

MR. MURRAY: This is where the figure, if you look in the upper part, where the DTFs are sending to the TLFs, they say there that it's sending to its own divisional TLF, and then separate fiber optic links to each of the other TLFs.

MEMBER BROWN: Yes.

MR. MURRAY: Okay. So they are separate lines, separate receives, separate buffers. The diagnostics looked at each one of the --

(Simultaneous speaking.)

MEMBER BROWN: Okay. That gives --

MR. MURRAY: Did I get you there?

MEMBER BROWN: Yes. That's what I was expecting, based on my --

MEMBER STETKAR: And each division is physically separated --

MEMBER BROWN: I just didn't know whether they had a common, a common connection going through it. It just wasn't obvious.

MR. MURRAY: Okay. Starting into the discussions, so we finished the independence discussions. We're talking to determinism in the FPGA platforms. The FPGAs are -- they're a synchronous clock-sequential circuit. Each FPGA, it only starts processing if it's seen a completed, completion from the previous, so they work in a series.

So each only starts when the data is transferred into the FPGA, and sends the data to the next module when the process is complete. So it's a set up with timing. Changes in state occur only at selected control timing signal. This is within that functional unit.

All FPGAs perform a signal processing functions. Modules are monitored by a watchdog timer looking for timeouts and it's a hardware-based watchdog timer that will again sense that if there's a stoppage in that process, it will sense it. When it times out, it marks the module as inoperable again, if it's a trip signal in for that particular function, and the operator is alerted.

MEMBER BROWN: Okay. I think that answers one of my other questions, but let me make sure that -- you didn't explicitly state that the diverse hardware-based, because I don't remember reading that or not. So you answered the question here about it, but it's not --

One of my questions is is that going to be, is it built -- it's not part of the FPGA. You say it's diverse. To me, that means it's a separate piece of hardware that monitors the FPGA; is that correct or not?

MR. FUKUMOTO: Each module has a watchdog timer, and watchdog timer is included in the IC, not FPGA. That watchdog timer is in the module.

MR. MURRAY: It actuates -- is it a contact actuation within the module? The contact actuation within the module hardware?

MR. ED BROWN: Yes. It's a circuit. So it's a circuit in the ICs.

MEMBER BROWN: Okay. Well, page eight is where you talk about that in the first paragraph, and that's it. There is no other reference in there, and I couldn't find it anywhere else in chapter, in FSAR. So I mean the issue of being a separate hardware and watchdog timer that's not built into the FPGA function itself.

It's part of the module where they're housed, but it's not embedded in the FPGA itself. It's not addressed. Either that or am I reading it incorrect?

MR. MURRAY: I see what you're saying. We did discuss the watchdog -- we did discuss the watchdog timer in that paragraph, that's right.

MEMBER BROWN: And I didn't -- I went off in key word. Hopefully, I got the right key words.

MR. MURRAY: You looked at the hardware?

MEMBER BROWN: I did not find anything in the rest of the FSAR that discusses the diverse hardware-based functionality of that, which I think is important to the overall operation.

MR. MURRAY: Okay. Did we answer your question on that?

MEMBER BROWN: Yes. Yes, you did.

MR. MURRAY: Okay.

MEMBER BROWN: As long as it gets incorporated somewhere.

MR. MURRAY: I understand.

MS. BANERJEE: Are we taking -- this is Maitri Banerjee. Are we taking any action item on this?

MR. MURRAY: Yes. We'll respond to that.

MR. HEAD: Do we intend toward revising that?

MR. MURRAY: No.

MR. TONACCI: This is Mark Tonacci. I'm sorry. I didn't catch what the request and the action is going to be there. Can you repeat that please?

MEMBER BROWN: One of my questions, based on reviewing the appendix and the other parts of the FSAR Rev 4 that was sent out with Chapter 7, was to look at the watchdog timer and was it independent hardware and diverse from the FPGA itself, and the answer is yes. So I went and looked and say is that anyplace? I asked that question, so I looked in the other locations. Now whether I found them all, I don't know. If it's in the FSAR, that's fine. If it's not, the need for it to be independent and hardware-based and diverse ought to be in the FSAR. That's the question.

MR. TONACCI: So you're asking for us to put that information in the --

MEMBER BROWN: If it's not there, yes. If it's not there.

MR. TONACCI: And I think I heard STP saying they're willing to do that.

MR. MURRAY: We will.

MEMBER BROWN: I didn't hear them say that.

MR. MURRAY: Yes. We agree, that if that's a bullet factor which we also agree the hardware diversity there is, that we will take an action to incorporate it.

MEMBER BROWN: Now does the part, does the watchdog timer, all that uses is just solid state logic circuits. I take it the watchdog timer ceased their operations with the FPGA, or did they -- is there anything in the entire division that you can, you know, for completing -- I probably think it would, but I'm just asking the question. Does it stop at the watchdog timers, the modules that have the FPGA circuits.

MR. FUKUMOTO: Watchdog timer, we put the watchdog timer in the module. Which through the essential central processing for safety conscious, and in watchdog timer, it operates with the --

(Simultaneous speaking.)

MEMBER BROWN: Okay. So it feeds -- if it doesn't, if you have a watchdog timer operation, it feeds the OLU and says hey, go do something?

MR. FUKUMOTO: Yes.

MEMBER BROWN: But the TLF has a watchdog timer as part of it, since it's FPGA?

MR. FUKUMOTO: Yes.

MEMBER BROWN: Okay, and the operation of the watchdog timer doesn't bypass the OLU and go directly to the load drivers? It goes into the OLU and then to the load drivers in terms of triggering a trip?

MR. FUKUMOTO: Let me confirm with my Japanese authority, sorry.

(Off record discussion.)

MR. FUKUMOTO: Yes, sorry. The output of the, you know, watchdog timer goes to TLU, and TLU commands, you know.

MEMBER BROWN: Well, the TLU is really a TLF.

MR. FUKUMOTO: TLF, TLF.

MEMBER BROWN: But the TLF is also in FPGA. So I presume it has its own watchdog timer.

MR. FUKUMOTO: That's right, it does.

(Simultaneous speaking.)

MEMBER BROWN: So look at something after that. So it can't feed itself. It's got to do something else. I'm just trying to figure out where the watchdog timers execute the designation of the division as being a trip.

MR. MURRAY: And send that to the OLU, is what I understood from he just, Mr. Fukumotoson said.

MEMBER BROWN: All right. Just a standard solid state line and then you allow process after that. Okay, all right. You can go on. Thank you.

MR. MURRAY: And then the last bullet on this particular slide is that the timing is verified by analysis and simulation during the design process.

So in platform diversity, RTIS/NMS platforms are diverse from the engineered safety features.

MEMBER BROWN: Oh, I might as well cover this one as well, since we're talking about the timing analysis.

MR. MURRAY: Okay.

MEMBER BROWN: That's also covered on page eight, and you refer to Notes 8 and 10 in the table, which you refer to, where it performs the correlation over to the ITAAC and back, and those two particular notes reference DAC 8G and H, and number 11. In looking at those, there was no change in those from the old, original DCD approval document in 1993.

So they're very, very general and process-oriented. There's no reference to timing. You won't find the word in there anywhere, in terms of confirming the overall timing analysis, which is critical for a deterministic type performance.

All I'm saying is that the deterministic nature or that need to verify does not explicitly state it in those DAC items. Now I went back and read this. The only ones that change are something like three and four and 11 and 12 or 12 and 13, and this number 8 and number 10. It's number 8, number 11, and neither of those had any modifications at all relative to the whole change in FDDI multiplexing and to the platforms you have now.

MR. MURRAY: And the reference to Note 16, you just said it was on page eight also?

MEMBER BROWN: Yes. You'll see a little note, second paragraph, the little superscript.

MR. MURRAY: Yes.

MEMBER BROWN: And then on the next one, it says superscript 10. If you go into find it, it refers you to the DAC paragraphs and so I went and looked at those.

MR. MURRAY: And what we've done there is we've provided the criteria in the FSAR, that's about the timing and the existence of the timing report. We pointed it to that DAC, so that you can make that match back to say --

MEMBER BROWN: But you use in these paragraphs --

(Simultaneous speaking.)

MR. MURRAY: That is correct, that is correct.

MEMBER BROWN: --to those particular DAC requirements.

MR. MURRAY: Right. So the FSAR will say these are the important pieces for this particular design criteria, and it quotes to the DAC. Then you can cross back and say where can I find the answer to this question? You go back to the FSAR section, and it gets you to those, the timing test, description of the timing. Those are the areas that we cover for meeting that requirement.

MEMBER BROWN: Okay. So by incorporating this cross-reference table in here to that effect, but you do include the --

MR. MURRAY: That's correct.

(Simultaneous speaking.)

MEMBER BROWN: Okay.

MR. MURRAY: That's fine. So it points back to the critical reference -- okay. So now we're moving on to platform diversity. We talked, I think, first where ESF and reactor trip and makes the isolation in neutron monitoring, and the systems are diverse in the ESF function.

The RTIS and NMS is diverse for non-safety balance of plant functions. They're not the same type platforms. So they're diverse as well. RTIS is diverse also, as required, from the ATWS circuitry as well, which is done with relays and relay logic. Any question on diversity?

(No response.)

MR. MURRAY: Simplicity, these are our

thoughts on simplicity of the system. Separation of the safety and non-safety functions. There are no non-safety functions that are going on in the safety platforms.

Complex activities for calculation of, for reactor core physics type calculations, they're not done in this system. It's done in the non-safety system, so it doesn't complicate or make this system complex.

Uses the non-rewritable FPGA technologies. Its function uses fixed gate and deterministic timing, and that timing can't change short of the design process and redesigning --

MEMBER BROWN: But you changed -- I just wanted to confirm. You changed the design or one of your algorithms that you used to burn the FPGA. You want to do that, a modification. You then have to take the FPGA out and put a new one in.

MR. MURRAY: That's correct.

MEMBER BROWN: That's my understanding. I just wanted to make sure of that.

MR. MURRAY: You would design the module to take the place of that functional module that you were using previously, and it would be redesigned to implement those modified functions that were required.

And there's interdivisional communications. It's only, only where it's necessary to get two of four coincidents logic, from a simplistic perspective. Any questions?

(No response.)

MR. MURRAY: I'd like to transition now into the ELCS platform, and again, this is --I'll go through an overview of redundancy and talk about independence, determinism, diversity and simplicity also.

In here, I'll bring focus to the diagram's page 18 slide that you have on your supplemental slides there, and page 19, which are 7 delta S-3 and 7 delta S-4. So let's move to four, or to the next slide, Craig, band then we'll back up to here, because we don't need to talk too much about this slide.

We just wanted to make sure, because of the fact that when we get into the ESF area, it's a little different in the fact that we've got sensor divisions. We have four sensor divisions, but then it goes into three ESF divisions. So that's the purpose of this slide, and also it shows the interrelationship there. Any questions on that? Again, four sensor divisions. Signals go into the SLS for the three ESF divisions, to carry out the three divisions of ESF functions.

Okay. So now we back up to the other one, if that's okay. Okay. Now in here, looking through the flow of it, the simplified flow here, we have the digital trip function, remote digital logic controllers. These will be in remote locations, and they do data acquisition. This where the conversion from analog to digital will happen.

That's set to the digital trip function, which it compares, and this is the point where the predetermined setpoints are compared to the process values, and the safety function initiation status for that division is developed.

Then it sends all of the divisions, the four sensor divisions then send it into the sets of SLFs, which are division order as well. So the DTFs send their signals to the SLFs. The SLFs then do the two out of four vote function.

Then get back then, progressing down through it, if the safety logic function remote digital controller, it receives the system level, the system level automatic and manual system actuation signals to the -- from the SLFs.

Then it provides the logic to determine the component actuation, control functions, commands to the final vote function, which is shown at the very bottom, okay. In the final vote function, it receives the individual inputs from the -- for the component actuations and controls, and it also performs the two out of two where necessary, and we've had that discussion previously.

MEMBER STETKAR: And that's documented in Chapter 16, those drawings?

MR. MURRAY: Right. We had had that previous discussion about where --

(Simultaneous speaking.)

MEMBER STETKAR: Right. That's not all of them.

MR. MURRAY: Not all of them, that's correct. So we want to make sure we pointed that out in the presentation. Okay.

MEMBER BROWN: Just a minute. Not all the -- not all functions are two out of two.

MEMBER STETKAR: Not all safety functions.

MR. MURRAY: That's right.

MEMBER STETKAR: That's the point. ADS, for example, is definitely two out of two.

MR. MURRAY: That's correct. Those consequential --

MEMBER STETKAR: Some others are one out

of one.

MR. MURRAY: And some of the voting, two out of two voting is done with component and valve, for example, that it may not be with the voting in the final device, but by system voting. It has to have both, to this and that, in order to do the function.

MEMBER STETKAR: Well, each individual component might be just a single signal.

MR. MURRAY: That's correct.

MEMBER STETKAR: A single signal to start a function, but if the valve doesn't open to --

MR. MURRAY: That's correct, and some will be two of two voting to the components. That's right. You have a good understanding from our previous discussions.

(Simultaneous speaking.)

MR. MURRAY: Yes sir?

MEMBER BROWN: I want to make sure I understood how that worked. Within your picture up here, all of the SIMs operate based on a two out of two of the two RDLCs.

MR. MURRAY: This typical picture we show, that you would -- it looks for two of two out of the SLF RDLCs.

MEMBER BROWN: All of those have to go in order to tell the SIM to actuate a safety function from that, one of those three divisions?

MR. MURRAY: And that's correct. If one of the, for example, logics are bypassed, then the SIM is in a one out of one logic when it has that bypass.

MEMBER BROWN: Yes. I got that. Now each division feeds some number of safety functions, whether it be an ADS command to actuate or a HP something, whatever, that other thing --

MR. MURRAY: High pressure core flooder.

MEMBER BROWN: Yes, core flooders or whatever the number of them are, and you made the comment in the FSAR that -- in the appendix, that not all of them, not all of the safety functions are fed by all three divisions. I can --

MR. MURRAY: Right.

MR. SWANNER: Yes, that's correct.

MEMBER BROWN: What I meant by that is like the ADS thing. Apparently only two divisions --

MR. MURRAY: Two divisions.

MEMBER BROWN: --would give a parallel command to start, for the ADS function to operate.

MR. MURRAY: Right.

MEMBER BROWN: Others may require all three, may have three divisions to command. I don't know --

(Simultaneous speaking.)

MR. MURRAY: There are some --

MEMBER BROWN: I'll have to find a list of saying which functions have required two divisions, which ones require only one, which ones require three. I couldn't find it.

MEMBER STETKAR: They pointed us, I think -- let them answer.

MR. SWANNER: There's actually, I think, two questions here, but there's maybe more. But we'll start with these two. The first question is how many, you know, where are the functions of ECCS and how many divisions there are, and which divisions are on which division of ELCS.

ECCS is broken into three divisions, excuse me, lower pressure core flooder is in all three divisions. There are three divisions of that. There are three divisions of diesel, so they're in each of the divisions.

In ADS, there's only two divisions necessary, so they only operate on SLF-1 and 2, and then there is no ADS function on SLF-3, because there --

MEMBER BROWN: SLF-3?

MR. SWANNER: Well, the third division of ELCS.

MEMBER BROWN: You mean the third division of ELCS?

(Simultaneous speaking.)

MR. SWANNER: Yes, that's correct.

MR. MURRAY: Yes, division.

MEMBER STETKAR: It might help, if you don't have the figure, there's a Figure 7.1-2 --

(Simultaneous speaking.)

MEMBER STETKAR: That shows what you're talking about now.

MR. SWANNER: That's exactly what --

MEMBER STETKAR: That's the easiest to see the allocation of functions among divisions.

MR. SWANNER: FSAR and what Member Stetkar said was FSAR, Tier 2 Figure 7.1-2 provides a listing of which ESF functions are on which division of ELCS.

(Simultaneous speaking.)

MR. SWANNER: That say -- basically it shows, and let me get to here. It shows Division 4 without any ELCS. Okay.

MEMBER BROWN: I understood that. That part I understand. There's only three divisions that actuate.

MR. SWANNER: And your next question, moving a little bit forward, was which functions require a two out of two vote, and which functions require only one out of one vote, and that's a different question. Each function like low pressure core flooder, Alpha initiation of that pump, all these functions are listed in the technical specifications, in Section -- Tech Spec Section 3314.

In that section, in the bases for the tech spec, it identifies which function has redundant voters and which has only one voter.

MEMBER STETKAR: Yes. Now the reference is you don't have any more figures. It's Chapter 16, tech spec bases, Figures B.3.3.1.4-1 through -5.

MR. SWANNER: Yes. I apologize for that.

(Simultaneous speaking.)

MEMBER STETKAR: -- to try to figure it out.

MEMBER BROWN: Well, I think you found the low pressure core flooder even listed in the 7.1-2. So there's no LP.

MR. SWANNER: It's probably called in that figure RHR, for residual heat removal.

(Simultaneous speaking.)

MEMBER BROWN: Oh, okay. All right.

MR. SWANNER: Those pumps have multiple functions, one of them being residual heat removal, one of them being low pressure core flooder.

MR. MURRAY: So the assigned functions are distributed through the division, D division for the assigned function off of the -- from the SLFs that are required to complete those functions.

MEMBER BROWN: Okay.

MR. MURRAY: So then we start asking why --

(Simultaneous speaking.)

MEMBER STETKAR: Well, there's apparently a reason. I understand ADS, okay.

MR. MURRAY: So what we covered just then was basically Slide 17 that we passed by, which is this. We just went through the flow using the diagram for explanation, because it was just easier to follow the diagram.

So with that, let's move to Slide 20, thank you, and let's talk about ELCS redundancy. There's four, again four independent redundant sensor divisions, as we discussed, three independent ESF divisions, and it does safety function system level initiation as well as actuation and control for that particular division's components.

Four independent redundant divisional power supplies. They're the power supplies that feed -- power sources, excuse me, that feed the Division 1 are independent and from the Division 2 power sources 3 and 4. Any questions?

(No response.)

MR. MURRAY: 21. ELCS independence, and as we come down, we'll transition into the communication independence. There will be another slide that we'll transition into for that section.

MEMBER BROWN: Well, let's go back one.

MR. MURRAY: Okay, yes sir.

MEMBER BROWN: I think.

MR. MURRAY: Redundancy, Slide 20?

MEMBER BROWN: No. It's on bypass. Go to the figure on that one.

MR. MURRAY: Sure.

MEMBER BROWN: Okay. I'm going to have to wing it and write it down. You talk about bypass of sensors and how that takes out a division, in terms of visibility, to develop an actuation signal.

MR. MURRAY: Yes sir.

MEMBER BROWN: And then bypass of sensors to me means the first little circles of X's and the next box, the DTF.

(Simultaneous speaking.)

MEMBER BROWN: If you think of what you're taking out, they'll do the voting from all the other divisions.

MR. MURRAY: That's correct. You do bypassing of the sensor portion of it. So I could bypass Division 4 sensors and the Division 1, 2 and 3 would then be voting on 2 and 3, develop signals, completely completing the functions.

MEMBER BROWN: Okay. If a -- is there a bypass for the entire division?

MR. MURRAY: There's a separate bypass for the logic, the SLF down. There's a separate bypass for it, and there's -- in this case, you could bypass either SLF Alpha, shown in that drawing. I'll just go back to the other ones. It's probably easier to see.

If you go SLF down, you could bypass that logic for the ESF, and then you could also bypass the Bravo side. So you can bypass those separately. So if I bypass the Alpha side, I'd have functionality through the Bravo side that's shown there, to complete the function as well, and when this is bypassed, I think it goes to one out of one on the SIM.

So I have the ability to test and bypass the logics with the redundancy, and I also have the ability to go to one out of one if that bypassed logic. So I can take -- since there's two different defined bypasses, sensor function bypass, which is what we describe first when you asked your question, and then there's the logic bypass.

MEMBER BROWN: Okay. There's a -- is there a circumstance under which a division could be out of service, and still remain, the plant could remain operational? In other words, you don't have any other. Can you operate under that circumstance?

MR. SWANNER: Yes, yes.

MEMBER BROWN: Are those safety functions which only have two actuations, that's the EDFs, that would mean that I don't have redundancy.

MR. MURRAY: The technical specifications have those rules. That's where you go. You drive down to the technical specifications. It has rules for out of service logic bypass, and then it would have rules for basically your requirements for, I'm trying to remember the term, and I've lived in operating plants so much.

MR. SWANNER: Limited conditions for operations.

MR. MURRAY: Limited conditions for operations. So that's where it drives you, what those requirements are.

MEMBER BROWN: I'm going to go back to the original DCD, Chapter 14.

VOICES: Sixteen.

MEMBER BROWN: Sixteen, and I'll have to admit I thought of this late enough that I was not able to gain a good understanding. I finally found the one on Instrumentation, OOSs and stuff.

But I couldn't find the delineation of a whole division. I found the breakdown on the sensors. I never saw the whole division and that's -- if it's -- I'm going to have to take your word for it, I guess. But that's not a negative comment.

MR. MURRAY: I understand that was Craig.

(Simultaneous speaking.)

MEMBER BROWN: A whole division is out of service. Somewhere that's specified in that chapter.

MR. MURRAY: It may be function by function specified.

MEMBER BROWN: Well, I wouldn't look at the functions, you know. I picked one or two of them, the ADS and then I look at the HDCF, not knowing which ones was which, which ones just had two, or the HPCF, and those are under the functional safety aspects and really didn't address the instrumentation system being out of service.

Although I guess if you think about one, it now takes one -- it takes one of the redundant paths out. Maybe that's -- but the date, the time for those was long. It was like days, as opposed to some of the other stuff was in the category of hours to be out of service, on the instrumentation side.

And it seemed incongruous to have an ADS system out of service for seven days or something like that, or HDCF out of service. Anyway, we can go on. I can do it. I guess I can have somebody explain that to me out of this meeting.

MR. COLEY: We need to understand maybe a little bit more about the question. So when you ask --

MEMBER BROWN: A whole division of instrumentation is out of service. Say it's the ADS and it feeds the ADS. So that means you've only got one ADS division that can actuate the ADS. So you don't have redundancy for it. If you have, if you're operating with that out of service, you now can assume one of the other ones failed.

MR. COLEY: Well, there should be an instrumentation spec that covers ADS function, as well as an ECCS specification that covers ADS.

MEMBER BROWN: Yes, and they are. They are there. I just said I couldn't find one that covered the whole division being out of service. I didn't have --

MR. SWANNER: There are some.

MR. COLEY: They're broken down by function, and if you take ADS as an example, it's broken down by function. So you can look at the level function, you can look at the drywell pressure function that ties in, for example.

MEMBER BROWN: So if I look for ADS out of service, a whole system out of service, that would give me my answer?

MR. COLEY: If you look at the specification, for example, 3.3.1.1, 3.3.1.2, I forget where it is exactly, the functions are delineated and will show what that function's for. So if we lost a division or an entire division of sensors, then it would impact a number of functions, and those functions would be used to determine the operability of the systems.

MEMBER BROWN: Yes, I can look.

MR. SWANNER: Sensor channels are in 3.3.1.1. The actuation for ESF is in 3.3.1.4.

MEMBER BROWN: Yes.

MR. SWANNER: Okay. When you try to pull those, when you try to pull a full division out, it's in ECCS. That's a separate specification. That's in 3.6.1, and it permits various different pumps, you know, pumps, whole trains to be out. So if you take out a full division, that's a specification that would end up --

MEMBER BROWN: Yes, I saw that, and I looked at that, and I finally figured out I wasn't looking for that, and then I never got back to it. But I finally figured out what I was looking for.

MR. HEAD: And John, you should I think help us here. I mean interpreting the tech specs and what you -- what action statement you're in, you can be in different places, and you could take some out and have a number of different functions out, and the time would be limited to whatever the sort of time frame is.

So there's, somehow the tech specs are going to work exactly like the current operating specs, and the operators are going to have to go in and say okay, this is inoperable. I may be in this ECCS spec, I may be driven by something else. The time would be whatever is the shortest that they'll be dealing with.

MR. SWANNER: That's right.

MR. MURRAY: To restore that function that's specified. Go ahead and move on?

CHAIRMAN ABDEL-KHALIK: Yes, move on.

MEMBER STETKAR: I know what? I looked at this a long time ago and I've forgotten --, but as long as Charlie raised the question, the tech specs do allow me to have a sensor division out of service coincidentally with a logic channel in another division. For example, I would have Division 1 sensors bypassed and Division 2 logic bypassed simultaneously, right? Is that true? Are they explicitly prohibited --

MR. HEAD: I never offer an opinion normally on tech specs, unless I'm looking at them. That's just my training.

(Simultaneous speaking.)

MEMBER STETKAR: -- I believe you understand what I was talking about.

MR. HEAD: Well, right. But you still, you wouldn't trust what I said, I'm sure, unless we were both staring at them. So that's, you know.

I would imagine as time has moved forward since the 80's, that some of the risk insights would allow certain configurations to happen for certain periods of time, just because, you know, we've applied the risk insights as to the probabilities during those time frames and the remaining functionality of the rest of the equipment.

But actually I wouldn't offer on what's actually in there right now, unless I was staring at it.

MR. MURRAY: From a practical perspective, having the sensor division out, you still have three functional sensor divisions to carry about that function, and with the logic out, you still have the other two channels that have got --

MEMBER STETKAR: I'm just interested, you know, in terms of the tech spec, since we're talking about tech specs, what is sort of the minimal configuration that the tech specs will allow you to legally be in, you know.

You obviously can't have ten sensor divisions out at the same time, if I recall that. I think that's true. I'm not quite sure if that's true. Anyway, that's -- and I'm trying to look up things real time here.

(Simultaneous speaking.)

MEMBER STETKAR: The tech specs are 155 pages between the changes and --

MEMBER BROWN: Are we going to have -- I think there's a change to Chapter 16. Is there going to be another meeting on Chapter 16?

MS. BANERJEE: Yes. I think it's next month, if I remember correctly.

MEMBER STETKAR: It seems so. I've only got Rev 3 and 16 also is my problem. I don't have Rev 4.

(Simultaneous speaking.)

MEMBER STETKAR: So we'll get a chance to --

MEMBER BROWN: That's why I said we ought to go on, and I can try to --

CHAIRMAN ABDEL-KHALIK: We'll look at Chapter 16 on March 9th.

MEMBER BROWN: In March? Okay. Oh, March 9th. I'll be back.

CHAIRMAN ABDEL-KHALIK: Please continue. What page are we on?

MR. MURRAY: I'm on page 20.

(Laughter.)

MR. MURRAY: So we've discussed, I think we've discussed all of this slide, that we have the independent redundant divisional power sources, I think, is where we are going to. Actually on 21 is where we need to be now.

So we're getting into the ELCS independence discussion, and the independent power sources again fit into the picture, as well as the independence from the non-safety system, electrical isolation, physical separation from non-safety.

Four independent ESF sensor divisions, we've discussed that. Three independent safety functional actuation systems with electrical isolation, physical separation. So we've discussed that. In the communication independence, we'll transition into the next few slides that talk more about that. The safety-related communications are isolated in independent, and non-safety related communications are isolated in the independent as well. These are fiber optics.

So in this next slide, we'll talk a bit. In it, we're talking about the communications, and once you have a picture of it, it's a very simplified diagram that we consider non-proprietary, of how an ELCS controller functions.

MEMBER STETKAR: Mike?

MR. MURRAY: Yes.

MEMBER STETKAR: Before we get too deep here, I'm trying to look ahead. Are you going to talk about the maintenance and test platform communications at all?

MR. MURRAY: We didn't have a slide for that.

MEMBER STETKAR: Okay. Let me ask you about that then, while I'm interrupting.

MR. MURRAY: Okay.

MEMBER STETKAR: Each division has its own maintenance and test panel that's online, continuously connected operating; is that correct?

MR. MURRAY: That is correct.

MEMBER STETKAR: Reading in the appendix, that thing, that panel seems to provide several functions, and it also seems to communicate with both ELCS and the normal plant information control system. Is that --

MR. MURRAY: It is the conduit of information out of the ELCS system that goes through the isolation from the maintenance and test panel to the first status indications out to the plant computer system.

MEMBER STETKAR: From what I read about it, if you're going to change setpoints, trip setpoints, for example, in the ELCS, this is the place where a technician will enter those new trip setpoints. Is that also true?

MR. MURRAY: That is correct, with the system out of service. It has to be out of service, and that's the point where that entry will be made.

MEMBER STETKAR: Is there something that prevents the maintenance and test panel from surreptitiously inserting? I understand administratively how it doesn't do it, but I'm -- since it's online and continuously communicating.

MR. MURRAY: I think there's switch permissives that have to be made, in order for those functions to be enabled. The continuous online is the communication monitoring. Isn't that correct, Ed? Make sure that I'm correct with this.

When you get into the testing, you have to put it in test configurations, and when you get into changing setpoints, you have to go into those configurations, and it requires actual physical switch manipulations on the maintenance and test panel.

MEMBER STETKAR: You also use the maintenance and test panel to change setpoints or control algorithms for the normal plant information control system --

MR. MURRAY: No. Remember, maintenance and test panel is only for ESF functions, okay.

MEMBER STETKAR: Well, but since it communicates from A to X, it's just --

(Simultaneous speaking.)

MR. MURRAY: All that goes out of there to the non-safety systems --

MEMBER STETKAR: The communications is just a conduit to --

MR. MURRAY: It is a one-way communication, and it doesn't look for acknowledgment from the plant information system.

MEMBER STETKAR: I was just curious whether from that panel you could somehow affect both trip setpoint signals into a safety division, and controls signals or algorithms out into the normal plant control system. It wasn't -- it's clear that it's a conduit from PLCS out to PICS -- it was used otherwise.

MR. MURRAY: There's no shared function between the ELCS and the ESF, and the non-safety functions.

MEMBER STETKAR: I'm thinking of things like steam generator level, trip actuation, EFW, emergency feed water actuation on steam generator level and, for example, algorithms to control feed water flow out in the non-safety part of the plant.

Does that somehow affect both of those things from the same place?

MR. MURRAY: I can only speak from my analog background in that, and those functions were diverse there as well. The controls were in a NSSS group that did the controls, that used the control signals that came in to control. But I couldn't change the algorithms from the protection sets. So it was diverse in that, and it's very similar here, is the -- only in the actual signals, make sure I'm right with this, the plant information control system's not using the data out of ELCS for decision-making or control algorithms anywhere.

MEMBER STETKAR: I understand that, but I'm not quite sure that -- I might not be communicating very well here. I'm concerned that if -- let me ask it this way. If I want to change the steam generator level program out in the secondary side of the plant, the thing that's -- I'm sorry.

(Simultaneous speaking.)

MEMBER STETKAR: The reactor vessel level control. That's, sorry --

PARTICIPANT: He can do that one too.

MEMBER STETKAR: I can be stupid. I'm allowed to be stupid.

(Laughter.)

MEMBER BROWN: It's a steam generator.

MEMBER STETKAR: It's a steam -- yes, that's -- a good steam generator.

(Laughter.)

MEMBER STETKAR: Anyway, reactor vessel level program or heat up/cool down or something like that, out, you know, which is a secondary -- well, I'm not sure it's reactor vessel level control. I'm trying to think of a secondary function that would add a program, let's say --

MR. MURRAY: Feed water control.

MEMBER STETKAR: Turbine, you know, feed water control is a good one. Yes, boiler level, reactor vessel level feed water. Is that information, how is that information entered into the -- you know, you have digital feed water controls, part of the PICS.

How do you enter a new algorithm for changing, you know, bias, for example, on a feed water flow control valve? Is that entered through this same maintenance and test panel?

MR. MURRAY: That vessel. Well, that would be in feed water control system, where you would actually go in and it's a non-safety system. There, you would take and make this algorithm, control algorithms changed if you needed to change the tuning parameters for that particular function.

MEMBER STETKAR: Okay, okay. That's basically what I was looking for. I'm looking for common points where I can affect control and potentially protection things. Thanks.

MR. MURRAY: Okay.

MEMBER STETKAR: Sorry about the --

MR. MURRAY: You have a question.

MEMBER BROWN: Yes. I could take it somewhat more simplistic. It's a very complicated thought process, and I thought that the MTP, it may be a misconception; that's why I'm asking the question. While it's there and online all the time, it's all -- by being online, it's in the receive mode from the ELCS, as opposed to an active transmit mode, unless into the actual safeguards processing of all these core divisions.

MR. MURRAY: I'm going to try to answer that, because --

MEMBER BROWN: Unless you turn those switches. That's, I thought it was isolated.

MR. MURRAY: For testing and taking it in bypass, you have to use the switches, and you need to remember that in the control room, you have flat panel displays, okay. The flat panel display commands come back through the maintenance and test panel. I mean that's why it's on the AF-100. That's wrong. Thank you. So it is in a receive mode until it's --

MR. ED BROWN: It's in a receive mode, I mean other than transmitting information for the control room for certain displays. I imagine you can monitor it up there.

MEMBER BROWN: It doesn't do that either?

MR. ED BROWN: It does it only for diagnostic alarms. It's sitting there passively in the system. It does do one active thing for the ABWR. There's a function called and automatic ESF logic channel bypass, that's as a result of a diagnostic failure, and the MTP will be utilized for that function.

MEMBER BROWN: So it sends a fail signal or initiates a trip or --

MR. ED BROWN: No. It analyzes failure, which is usually reported multiple times. It ensures that the redundant feature on the channel is not, and it's a logic channel only, so there's two redundant logic channels. But the redundant channel is operable, and then it will allow an automatic bypass.

MEMBER BROWN: You're talking about the A-B?

MR. ED BROWN: Yes.

MEMBER BROWN: Sequence, the SLFs and the RDLCs?

MR. ED BROWN: Right. It will allow one of those two to be automatically bypassed if there's a failure in one, if there's a fatal error.

MEMBER BROWN: But does it initiate that bypass itself?

MR. ED BROWN: Yes. The diagnostic is set to it, and it will allow that automatic bypass. The operator can disable the automatic bypass feature, and use only the manual bypass feature. That's been a design feature of the original DCD since day one.

MEMBER BROWN: So it senses, it senses some problem with the information it's receiving.

MR. ED BROWN: Right, receiving.

MEMBER BROWN: Relative to the SLFs and/or the RDLCs, for either A or B in all four --

MR. ED BROWN: No, only in one. One MTP for each division.

MEMBER BROWN: Oh. So it only looks at one division. Okay. So it can't communicate an allowance mode to all four divisions, based on erroneously obviously, but it couldn't -- okay. I guess I didn't understand that. That's a nuance. I'll probably forget that one.

MR. ED BROWN: That's unique to the ABWR.

MEMBER BROWN: I understand what you said. Thank you.

CHAIRMAN ABDEL-KHALIK: Okay.

MR. MURRAY: So focusing back on the diagram we have up there, this is an ELCS controller. Within the ELCS controller is two microprocessors. One is the communication processor; the other is the application processor. A communication comes in, a message comes in and it comes in on a unidirectional serially fiber-isolated signal.

It has a fixed periodicity transmissions, and it has fixed length, fixed format. The data mapping is fixed and data redundancy is also provided in those messages, and then also the cyclical redundancy checks, CRC check is done in that diagnostics.

So the message comes in and the communication processor looks at it and does the diagnostics, to see if the message is an acceptable message. Acceptable message, it takes the information, put it in the shared memory buffer.

The application processor that is running and is on cycle, not dependent on the communication processor, will go read these, the shared memory and use the data to perform its applications.

If faulty data comes in, use the word "corrupt" or bad data is the best word for it, if bad data's coming in, the diagnostics that were described, which is -- it will flag that data as bad. It will take in the right-hand side of the picture, as you're looking at it, it will take its last good data, read it to the shared memory buffer, and it will also carry the bit that says "this data is bad."

The application processor sees that, says the data that's in the register or the data coming in from this particular area is bad data. Then it goes from its local memory and extracts out a predetermined value that it uses for those calculations.

At the same time, the operator is notified of bad data through watchdog parameters and the data diagnostics. So a bad message comes in. First, the communication processor will detect it, analyze it, detect it as such. It would then flag the data as bad for that particular input. The application processor would not react to bad data. It would only take the data that comes in.

It would see bad data coming from that particular location, and for that location it would then use a predetermined value. So the data coming in bad doesn't make it to the application processor.

MEMBER BLEY: So when you say a "predetermined value," that's some value that's deemed to be safe under most conditions?

MR. MURRAY: It's according to what the function is, but that's correct.

MEMBER BLEY: I'm sorry?

MR. MURRAY: It's according to what the function is, whether it's a fail/safe or fail as is.

MEMBER STETKAR: Well, all of this is fail as is.

MR. MURRAY: I can't answer that. There's a part that is finessed. The DCD requires --

MR. SWANNER: LDS.

MR. MURRAY: That LDS, link detection is actuate, right.

MEMBER STETKAR: So in some cases, if I can just call it true and false, true being a trip actuate and false being do not actuate the trip. In some cases, function let's say. In some cases that bit would be set to true, and in other cases it would be set to false, based on whatever function is being evaluated.

MR. MURRAY: Correct, on the application side.

MEMBER STETKAR: On the application side.

MR. MURRAY: On the application side.

MEMBER STETKAR: Because I was confused. You know, the words in the appendix just says "a predefined value based on the desired failure state," which to me doesn't say anything.

MR. MURRAY: Right. You get into whether it's fail as is or --

MEMBER STETKAR: Does that predefined failure state then, in the application bring the renewed coincidence log to a one out of three, if I understand how it works?

MR. MURRAY: This is a single one of the SLFs, and it was four. So you still would go out, and you'd still have the two out of the four vote. So you'd still have to take -- excuse me, two out of three vote. So you'd have a two out of three vote with one set of bad data. Is that correct Ed?

MEMBER BROWN: That's going to have a two out of four vote.

MR. MURRAY: Let Ed answer this one.

MR. ED BROWN: It's essentially two out of three, except for LDS, which would be one out of three. You'd have one LDS that would be in because of the predefined state. So another --

MEMBER STETKAR: So Ed, let me see if I understand this. For LDS, you're saying that they remain -- if we talk about divisions, if Division 1 SLF, you know, receives bad data input from Division 1, let's say. For LDS, you would then get an actuate signal if you had a valid actuate signal from any one of the three remaining divisions. Is that correct?

MR. ED BROWN: Yes. This is Ed Brown, that's correct.

MEMBER STETKAR: Okay. But for example, for high pressure core flood, under the same conditions, Division 1 would require two of three valid signals from the remaining three divisions; is that correct?

MR. ED BROWN: That's correct sir.

MEMBER STETKAR: Okay.

MEMBER BLEY: Something that I hadn't thought about as you go through this. The old systems, if we have a logic failure and we get a trip or whatever, the operators respond to the trip and carry on. Now in the control room, we have a signal saying what's going on now is due to bad data.

If you guys thought through two things. One is do you have any idea how often bad data signals come in? Two, what are you telling the operators to do when they see this thing coming in?

MR. ED BROWN: You are telling them that there is a failure, and this is Ed Brown from WEC. You're telling them that there's a failure.

MEMBER BLEY: Are we writing any procedures about this?

MR. MURRAY: It would be Annunciator Response Procedures, which are typically you would expect to go --

MEMBER BLEY: So wherever we go we'll have those Annunciator Procedures.

MR. MURRAY: In fact, the human factors team is looking at the response to those particular -- that's part of their function, looking at response and making sure that it's properly -- one, what level is responding, making sure that the operator has the right information to provide the right decisions, just what you're talking about.

MR. SWANNER: But it's important to also understand the frequency, so that it doesn't become a distraction. You have intermittent pieces, so they have the capability to disable, you know, disable a sensor that was causing an alarm, or if the alarm has failed, then they can take it to a failed state.

But that it's not, it's managed. It's information that's managed, and Human Factors are looking at that and it can be the programs and procedures will be in place should those evolve.

MEMBER BROWN: But that won't be in place until much later in the process?

MR. MURRAY: That's correct.

MEMBER BROWN: After the COLs. Okay.

MR. MURRAY: Ed, did you have something that you needed to add on the operator experience.

MR. ED BROWN: Yes, just the operating experience of the system, which has been in service in a number of safety-related applications in the U.S. and Europe. It's a very infrequent occurrence, and typically occurs when a module failure occurs, and typically fails hard. So you very seldom get bad data, because the transmission medium is fiber optic.

MEMBER BLEY: But you'd see something. Any valid idea of how often you see it in a plant?

MR. ED BROWN: The key words are very infrequent. Very few.

MEMBER BLEY: Once a month?

(Laughter.)

MR. ED BROWN: I would say less than once a month.

MR. MURRAY: But that's an opinion from operating experience.

MR. ED BROWN: Where else would they come from?

MR. MURRAY: So in looking at it, this is what we try to get the points across, of how the data is managed through the processors. So going into the, and we'll repeat some of the same information again. I'm on Slide 23, and here, the DTF transmits the trip signals the SLFs, and it's unidirectional, serial-linked, fiber.

It's fixed periodicity of transmission. All the data's transmitted. Even if it's not changed, it doesn't do different reporting. It basically transmits it again, cyclic processes there. It's fixed link, fixed format. The data map is the same data point, the same position. The data redundancy is provided in the message and the CRC functions are being reported there.

This all supports the detection of corrupted data, and preventing it from being carried forth into the system. I just wondered if you had a question.

MEMBER BROWN: I already had my robust discussion with Warren in several other meetings, and I'm not going to repeat that discussion again.

MR. MURRAY: Okay, okay.

MEMBER BROWN: I won't get to the inability to lock up all the processes. It's still there. But it's all good stuff, and this system is the same configuration, a similar configuration. So you'd have to make the same argument. It is a fail, fundamentally fail as is, and you have to -- except for the LDS function.

My fundamental thoughts are, you know, you've got to have a backup to it. We haven't gotten to that point. There is -- maybe I'll just ask the question. If after going through everything, there is no diverse, automatic diverse actuation system in this design. It's all manual, from what I could gather. It's all manually actuated by somebody.

MR. MURRAY: It is hard-wired.

MEMBER BROWN: It's hard-wired, but it's going to be somebody to actually do something.

MR. MURRAY: Right.

MEMBER BROWN: And you -- and I couldn't find any real analysis that said, or a reference to an analysis that said there's enough time for a manual backup based on a realistic, not a worst case analysis, but based on a best estimate of realistic, or a PRA or something like that, that says hey, the operators have enough time before you do some damage.

It's just that's the way it is. That's the design as it's been explicitly defined. With no other backup for critical functions, and/or an analysis that says the manual is okay. That raised a little bit of question, that if they all locked up, nothing happens. You've got to, somebody's got to figure out to go do something, and hopefully the timing is okay.

So that's -- but we can go on, but that's just the way it is.

MR. ED BROWN: Mike?

MR. MURRAY: Yes, Ed.

MR. ED BROWN: We do not believe that all the processors can be locked up.

MEMBER BROWN: Oh, I know that. I just don't want to go through that again. I've had to argue -- I've had that discussion with Warren at least twice, and there's no reason to work ourselves back through that one again.

I mean I've had personal experience where everything locked up on me, and it actually created two things: an over-speed trip device to say I'm not going to trip, and a command to have the turbines to speed up simultaneously.

Everybody said it never happened and it did happen, and we just barely caught it before it exceeded 150 percent RPM and almost killed people. So when people tell me something's never going to happen, I don't really -- but I've accepted it. So if you want to move on, you can. I really won't work on this one anymore.

MR. MURRAY: So let's go on through the discussion and --

MEMBER BROWN: Yes, I can go on. I just want to make sure you knew I just hadn't changed my position. That's all. I'm consistent, even if you think I'm wrong.

MR. MURRAY: We've completed -- okay. So we're on Slide 24 now. The SLF, when it receives the data communication, the communication processor, application is communicating through shared memory, as we discussed previously. Communication receives. Its link failure diagnostics are checked, provides error status for bad messages.

Additionally, the CRC diagnostics provides error status for bad message. Data redundancy diagnostics provides error status, and stores the message in a unique location in the shared memory, if it's acceptable data.

The application processors reads the message. Bad message status causes the data to be replaced by a predetermined value. We've already discussed that, and then the alarm message is sent to the operator. That's where it's detected, if there's a problem with the data.

Next slide, 25. Okay. The ELCS application processor. The application processors has no external interrupts. It does have clocks and it has internal but not external interrupts. The internal clock uses a precision timer, cyclic execution of the application software, based on the timing, predetermined fixed execution cycles. Maximum processor load is maintained at less than 70, and it's actually reinforced by continuous monitor, a self-diagnostic that verifies that it's less than 70 percent loading on the processor.

The buffer from external communication, the read and write data buffered the memory on the fixed cycle, and it's independent communication on the interface data system. Communication interfaces flags -- the interface flags the corrupt data, as we discussed previously. Then the application uses then again the predetermined value for bad messages.

Diagnostics will provide an operator alarm. The watchdog hardware timer output would be monitored by an independent controller, and overrun of cyclic execution times is monitored by self-diagnostics and then communication also is monitored by the application.

Slide 26. Determinism of the communication processor, it uses a deterministic protocol, which will be described further down in the billets, and all data, again, is transmitted, even if none is changed. It's doesn't, it's not doing exception transmission. Fixed link, fixed format message is mapped. Redundancy checks and CRC checks on it.

Deterministic intervals, based on the fixed, the internals of the application processor requests that messages be sent. Deterministic reception intervals based on fixed message. Again, reception intervals and transmitting are in from transmitting controllers.

The communication process is buffered from the application processor by shared memory, and then basically the diagnostics again provides operator

Annunciation, watchdog, loss of communication and message diagnostics is communicated to the operators for status and conditions.

In the determinism, response time analysis is done. The criteria is based on the safety analysis requirement for the system. It includes all delay elements, and in the criteria, both the minimum and the maximum acceptance criteria, the response time out is established for the validation testing. This is all documented in a report.

Then validation testing itself validates the analysis and is documented in a report.

MEMBER STETKAR: I understand, you know, that this will be done on day one, zero minus or whenever, for the original system.

If you make changes to the application software or communications protocols or whatever, does that then -- this is not post-installation. Does that then trigger need for a new timing analysis, to verify that that timing is still, and where is that requirement documented anywhere?

MR. MURRAY: I would answer it would, but where it's documented I'm not certain.

MR. ED BROWN: It's documented in the project's software management plan, which states the requirements for software changes, configuration control throughout the entire process.

MR. MURRAY: And it would be through a design change modification process also. Any other questions on this slide?

(No response.)

MR. MURRAY: Diversity and ELCS. Are we on, am I on the right one? Next slide. I was. ELCS diversity. Diverse equipment accredited for mitigation of ELCS failure and it's the diverse equipment that's hard-wired. Then there's diversity between the RTIS and NMS in the microprocessor base and then also from the FPGA and microprocessor bases, system are diverse.

It is also diverse from safety-related control systems. Different microprocessors are used in different software, different communication technologies and equipment.

MEMBER BROWN: I did have a question on there. You made a comment about hard-wired switches, manual switches to do this, and in your Appendix 7C, there's a, I don't know if it's a contradiction or not, and it talks about -- let me get the right words.

It says "control switches for individual control pumps and valves are transmitted from the operator's control stations to the SSLC, and then through ECF, as stated above." Yet the statement's been made, is that those switches someplace, I couldn't find it, but the switches go directly to the actuating component.

I couldn't find an explicit statement in the FSAR or in the appendix, the new appendix that you submitted, that explicitly stated that those switches go directly to the components, like the pumps or the valves, etcetera. That's on page 7C-3 under "Common Mode Failure Analysis."

Now it's under a header that talks about June 1993, but yet you have changes to it, based on the last -- this is Rev 4 of the FSAR.

MR. MURRAY: Right.

MEMBER BROWN: So that there seemed to be a conflict or an inconsistency between the -- which implied to me that the switches go into the SLL, and then get transmitted down to the OLU.

Now if you look at your picture at 7, there's another figure you can look at also, and that figure shows manual switches going to the SLF, and it shows something else going down to what looks like an either/or gate for the components. That's why I'm asking the question.

MR. MURRAY: Okay. So let me try to explain that then. From ELCS, from a control room perspective, even if it's one of the diverse components, high pressure core flooder. Charlie, is that right? Let's use that for an example.

The operator has full capabilities of operating it in the ways that he would have for Bravo, for example, in the control room, to go --

MEMBER BROWN: What do you mean for Bravo?

MR. MURRAY: For which it doesn't have diverse, okay.

MEMBER BROWN: You mean just different components?

MR. MURRAY: Different components. He has the ability to interface with the ESF system, to start and stop the pump and those functions. In the event of the loss of the system, then you go to the remote shutdown control function of it, which basically isolates the digital system inputs and you use the manual hard-wired control of the device, which is as described.

MEMBER BROWN: So there's a nuance. If I look at Figure 7C-1, where that -- in other words, there's a set of manual controls that go into the SLFs, and then there's another set of manual controls that go directly to the components?

MR. MURRAY: I'd like to see the figure. Let me make sure I understand it. That is correct, in that the SLFs -- in other words, operator ability to control the component from the control room, he has the ability to start and stop it with logic that's carried out through the ESF -- ELCS system basically.

In the event of an ELCS failure, and he has to go to the remote operation of it, there is -- you basically have to transfer it to a set of independent switches that can perform start/stop functions off that same high pressure core flooder, and monitor it with diverse indications.

MEMBER BROWN: So that's in the remote shutdown procedures?

MR. MURRAY: Remote shutdown systems.

MEMBER BROWN: In another location?

MR. MURRAY: That is correct, outside control room location.

MEMBER BROWN: So that's the difference.

MEMBER STETKAR: But from the control room, that comes through the SLF, not to the output.

MEMBER BROWN: That's what's implied by the ELCS. Now that I've heard this --

MR. MURRAY: Ed, you want to clarify

something there?

(Simultaneous speaking.)

MR. ED BROWN: Yes. I believe the diverse controls are in the control room, and the control circuit is wired, is that the manual control will defeat the ELCS control.

MEMBER BROWN: Or bypass it or whatever?

MR. ED BROWN: Well, defeats it. For example, if the ELCS control sends "stuck pump," it disconnects that part from the --, so there's no conflict. It's all hard-wired.

MEMBER STETKAR: That's, for example, for high pressure core flood sealing. Let me take like RHR Train B, which doesn't have a diverse actuation, is that true?

MR. ED BROWN: As far as I know.

MR. MURRAY: Yes, that's true.

MR. SWANNER: That's correct. There is no diverse.

MEMBER STETKAR: If I'm an operator, I push a button that says "start RHR Pump B." That signal goes to the SLF four division, two I guess it would be.

MR. SWANNER: That's correct.

MR. ED BROWN: If you're going to manually an individual component, it goes, using the F-100, it goes directly to the SLF RDLC and starts that pump. It bypasses the --

MEMBER STETKAR: Does it go to the SLF, which now communicates through the ELCS?

(Simultaneous speaking.)

MR. ED BROWN: Yes. It does through the SLF RDLC.

MEMBER STETKAR: Only that's not what this drawing says.

MEMBER BROWN: Well, there's only three functions shown: the RCIC, the CUW and the HPSF. Those are the only ones shown that have a direct connection to the hardware.

MEMBER STETKAR: Because those are the diverse -- I'm trying to get to non-diverse. I'm trying to figure out what a divisional SLF failure prevents me from doing manually.

When I put, if I had a Division 2 SLF fail, and I'll just call it failed, not there, and I push a button to start RHR Pump B, will it start from the control room?

MR. ED BROWN: You have -- let me just clarify. This is Ed Brown from WEC. Let me just clarify the question for a second. I have RHR to an

Alpha and a Bravo SLF. If one of those SLFs has failed, the operator can manually bypass that SLF, or he can -- it will be automatically bypassed by a diagnostic.

The logic will change to the other logic channel, one out of one. So that the system level controls will still operate. The manual control, an individual component with a flat screen display, soft control, that does not go through the SLF. The SLF is for system level functions.

Individual component control goes from the flat screen through the AF-100, down to the area where component control was done, which is the SLF RDLC, and it controls that component. So a malfunction of the SLF --

MEMBER STETKAR: Will not prevent that way of--

MR. ED BROWN: Will not prevent.

MEMBER STETKAR: I may have to circle the, you know, I may have to open three valves separately and start a pump, but I can still do that, for example.

MR. ED BROWN: That's correct.

MEMBER STETKAR: Okay.

MEMBER BLEY: Because we almost had an

opposite comment, and I thought --

MR. HEAD: Could I suggest maybe at the break we look at this drawing and make sure that we're all in agreement, and then we'll report back after the break, to make sure if there's any clarifications?

CHAIRMAN ABDEL-KHALIK: We're getting close to the end of your presentation. But is this a good time to take a break, or should we wait --

(Simultaneous speaking.)

MR. HEAD: I'd like to suggest a few minutes before we take a break.

CHAIRMAN ABDEL-KHALIK: Great, thank you.

MR. MURRAY: So we were on Slide 28, where we talked about the differences between the non-safety and the -- the non-safety systems from the out system. So in page 29, like simplicity, separation of the non-safety. There are no shared votes again. ELCS controls are performed in ELCS, within ELCS.

No non-safety digital control communication links have -- we don't use any priority modules in our design. So that's a point of simplicity. Unidirectional serial links, automatic and manual isolation, ESF safety functions simplify the architecture. We minimize inter-divisional data communication as well.

The next slide was, and we've already talked through an example of this, by the way, of the discussions we've had. But this was an example of one of the attributes out of the 7 delta S. For example, if there's a -- this happens to be a Tier 1, Table 2.75. ITAAC-2 requires deterministic communication.

So in the FSAR section, we basically bracketed the area that was applicable to deterministic communication, and have mapped that over to the ITAAC in this case, so that they point back and forth as we discussed previously. We just wanted to show one example of this.

So coming to a summary in this, we had an Action Item 7 from the May 20th discussion, which was to further discuss the need on the application of Common Q independence and determinism. I feel that we've, the explanation in the Tier 2 appendix 7 delta S and the ELCS presentation information, we feel that we've explained the data corruption does not compromise communication and independence.

We feel we've explained the interdivisional communications and compliance with the independence and determinism requirements, and also explained the compliance to determinism requirements additionally, okay. So in our opinion, we feel that the platform has overall compliance with the design requirements.

CHAIRMAN ABDEL-KHALIK: Thank you. Before we take a break, I think we ought to capture the briefings that you need to clarify. Number one, you're going to go back and look at Figure 7C-1, 7C-1 to try to answer John's question; is that correct?

MR. HEAD: Yes sir. We'll do that on break.

CHAIRMAN ABDEL-KHALIK: The other thing, I guess Charlie had a question about incorporating the statement regarding the watchdog timer.

MR. HEAD: Yes sir.

MEMBER BROWN: Yes, the explicit.

CHAIRMAN ABDEL-KHALIK: Right, an explicit statement.

MR. HEAD: Specifically that it's a hard-wired device.

MEMBER BROWN: That it's hard-wired diverse. Just replicate what they said in the slide.

MR. HEAD: Right.

CHAIRMAN ABDEL-KHALIK: And the third thing, you were going to find out which code is going to be used to generate the DIVOM slope, to set the OPR intercept point.

MR. HEAD: Yes, sir, and my proposal is that after the NRC presentation, that we would, you know, review on that.

CHAIRMAN ABDEL-KHALIK: On these three items?

MR. HEAD: Right, and then -- yes. Well, yes. We will certainly cover that, and the other item is that's a commitment to adjust our appendix, and we'll do that. The fourth one I've got is a future action item, I guess, is in our tech spec discussion on Chapter 16, we need to have some discussion --

MEMBER STETKAR: Be aware of that. We won't let you off the hook.

MR. HEAD: Well, yes. No, no. We will have some stuff in front of us just to show what can be out of service and the time frames and configurations that could be -- we could continue to operate and then maybe some configurations obviously would require an immediate shutdown.

MEMBER BROWN: One more item that I didn't bring up, because it wasn't germane. On the determinism side, the Common Q platform deterministic behavior was based on a less than seven percent load, and similar to what we discussed before, there ought to be some explicit test for that.

Once they have their application defined and all that other type stuff, put it in there, load it up, and then make sure it meets their actual, whatever their time response is when we're looking at similar, previous comments we've made.

There's no ITAAC or DAC for that right now. It's not explicitly called out. We did that before.

CHAIRMAN ABDEL-KHALIK: We can bring this point up when the staff makes the presentation --

(Simultaneous speaking.)

MEMBER BROWN: Yes, we'll bring it up. It's a matter for us to determine as a committee what we want to do with that, when we get to the point of writing the letter or what have you.

CHAIRMAN ABDEL-KHALIK: About the 70 percent load.

MEMBER BROWN: The 70 percent, that's right.

CHAIRMAN ABDEL-KHALIK: Okay. All right. Let's take a 15 minute break. We'll be back at ten after three.

(Whereupon, the above-entitled matter went off the record at 2:58 p.m. and resumed at 3:16 p.m.)

CHAIRMAN ABDEL-KHALIK: We're back in

session. At this time we'll hear from the staff.

MR. MUNIZ: Good afternoon. The staff is here today to present the Chapter 7 Advance SER of the STP COLA. My name is Adrian Muniz, the Chapter 78 Project Manager. Here with me today is Dinesh Taneja, the lead technical reviewer for Chapter 7. Our presentation will be focused on an open item related to the instrument setpoint methodology, and a discussion of a revised response to RAI 7.01-14.

The staff will also address an ACRS action item related to the Common Q platform, as well as evaluation of the Appendix 7 Delta Sierra, 7DS. With that, I would like to turn it over to Ian Jung, who has some remarks to make before we go into the technical presentation.

MR. JUNG: I am Ian Jung, and branch chief for the Instrumentation Control Branch in the Division of Engineering. I just have a couple of comments before Dinesh Taneja starts his briefing. We thank the Committee for this opportunity today, and we came before you in May in 2010, and this a follow-up to that meeting.

We'd like to be covering some of the open issues at the time and the progress that we've made. Two comments. We thank the Committee for your continuous and valuable advice on instrumentation control over the last couple of years.

You really helped us, working with the Applicant, and also for the staff ourselves, we have become the beneficiary of your comments. So we really value that and appreciate that.

Another note that we note that South Texas Project has been very, very responsive to both the ACRS, as well as the staff. As you know, South Texas has voluntarily participated in design acceptance criteria pre-fuel inspections, which is very valuable to both South Texas as well as the staff.

So I just want to recognize that, and we hope to receive your recommendation on Chapter 7 through this meeting, as well as the full Committee meeting coming up. So thank you. With that, Dinesh.

MR. TANEJA: So Slide 4. I'm Dinesh Taneja. You know, I've been involved with the review of this Chapter 7 from the start. So I've been familiar with the history, where we were and where we are going with the design here.

There was an open item we had in our May 2010 presentation, and in that open item was related to the setpoint methodology document, which was submitted as part of the setpoint control program under Chapter 16.

In that document, there was a reference made to a Westinghouse stability methodology topical report, which is a report that is being prepared for the fuel amendment, which is a post-COL activity, okay.

So we saw that in the methodology and we questioned it, saying that how can that be referred to if it is -- most of the design is based on the existing fuel design.

So that was retracted as a result of that RAI, and they put in the typical setpoint values in the methodology for coming up with the OPRM setpoints, and that methodology is based on what we already have in our certified design. So they didn't depart from that essentially.

CHAIRMAN ABDEL-KHALIK: But the point is the setpoints for the OPRM require the cycle-specific calculation of the DIVOM slope, and if they do not make any changes or do not have any departures from the current statement, the question is do they have access to GE codes that would allow them to calculate those DIVOM slopes?

MR. TANEJA: Yes. What the existing design is based on a BWR owners group stability analysis methodology, which is a owners group document, and you know, being part of the BWR owners group, you know, that was one of the documents that they do have access to. I think we looked into that.

CHAIRMAN ABDEL-KHALIK: But that was shown to be inadequate through a Part 21.

MR. TANEJA: Apparently, I think the OPRM methodology part of it, I went and I had discussion with our Systems Group people, and you know, about specifically on that methodology portion of it. I forget it was Method 2 or Method 3 in the OPRM.

CHAIRMAN ABDEL-KHALIK: It's Option 3.

MR. TANEJA: Was it Option 3? And they felt that, you know, that was okay, the Option 3 method. I don't know whether -- I'm not familiar with the Part 21 on that one. I did have a discussion with our Systems people on that one.

CHAIRMAN ABDEL-KHALIK: Are you going to have a discussion of this later on? Okay.

MR. TANEJA: So yes. So you know, I had, you know, up to that level. I went and I discussed with them, and they said well, this is what we already have in the certified design, and it's not a departure, and if they are staying with that.

I think the underlying reasoning is that, you know, as soon as this thing is done, there's going to be fuel amendment, and then we are reviewing this other methodology, WCAP, yes. But right now, you know, looking at, you know, it's exactly --

Assuming that we are staying with the certified fuel design, the BWR owners group methodology Option 3 is what is being used to demonstrate that they are going to use that for the OPRM calculation.

CHAIRMAN ABDEL-KHALIK: But that requires a cycle-specific calculation.

MR. TANEJA: Right.

CHAIRMAN ABDEL-KHALIK: For the DIVOM correlation, and that requires a specific code. The question is do they have access to the code that was specified for determining that DIVOM slope?

MR. TANEJA: Okay.

CHAIRMAN ABDEL-KHALIK: And that's -- we just have to focus on the task at hand.

MR. TANEJA: All right, understand. I think I understand.

CHAIRMAN ABDEL-KHALIK: Rather than saying we'll look at it when the fuel amendment comes in.

MR. TANEJA: Yes. I understand that.

CHAIRMAN ABDEL-KHALIK: At any rate, we

will address this later on today. Thank you. Let's move on.

MR. TANEJA: You know, but from the design of the logic, you know, that design, you know, we looked at the design as for the logic. The settings come from that analysis, and the design was looked at.

Next slide. This one also, you know, the Common Q platform that's being used for the ELCS application, it's already been reviewed and approved by the NRC, and our review was done based on a topical report dated 2000.

The basis for our review was the SRPs and the IEEE standards that were, you know, in effect at the time of our review. So in the initial part of the COL application, the Applicant was, you know, staying with the standards and SRPs and Reg Guides at the time.

Since then, you know, this one basically commits to meeting the current regulations and current Reg Guides and standards, which we were okay with, and we found that to be acceptable, and it's being tracked as a confirmatory item.

You know, from that May 2010 meeting, we came away with this one ACRS action item, which was very specific to the application of Common Q platform for the ELCS, and specifically I think there were two items of interest at that time, is the independence and determinism implementation of the Common Q platform.

You know, the Applicant has submitted that 7DS and we've looked at it. It consolidates the information and you know, what we had presented back then, I'm going to just go a little bit more, you know, into the same information, and hopefully we can address these two issues of independence and determinism.

So speaking of the independence, what there are in the Common Q system, there are -- it's a communication independence is a key issue here, what we felt, and that's really what I want to focus on, is that there are three or four different ways that the Common Q platform communicates.

One method for the inter-division communication is done by a unidirectional point- to-point fiber optic communication, okay. That is done, you know, they went over that slide this morning, which shows that a processor module has two sections. It has a processing section, and then it has the communications section. The communication processor is a separate processor which validates the signal adequacy and it does all kinds of checks, right?

Then the dual-coded RAM that is used as a buffer between the processing and the communication processors is a means of providing independence between the processing section and the communications section, okay. Now on the upstream of that processing module is the IO bus, okay. So all the IO data from the field and going out of the component is communicated on that bus.

That bus is totally independent of the point-to-point communication that's occurring inter-division, okay. So we have that communication. That has no relationship with the inter-channel communication, right.

Now each processor is limited to one output, okay, and it only can receive two outputs. So when I'm doing three out of four ruling, right, I have multiple processors.

Now, you know, I thought about the question that you brought up Charlie, about corrupt data, and I really, I looked at the topical report and, you know, I have taken the training, Common Q training. So I have the training manual, and for the last couple of weeks I've been really studying that. How can a corrupt data come in and take all four divisions out, right?

Data input comes into the communication part of the processor, right, which does all the checking, and after doing all the checking it places the data in a specific location of that dual-coded RAM.

The processor multiple is a cyclical operation. It looks at the IO bus for the new information; it looks at the dual-coded RAM, reads that information and does the processing of that information.

Now if that data, like explained this morning, if that data is going to be corrupt, that data is alarmed. Corruption is alarmed, and then it works to a known fail safe value, which is used by the processor at that time.

If it's a fail as is, then we are down to doing a two out of three essential voting on that, right. Now if a corrupt data did come in from a Division 1, right, it's going to go to a multiple different processors, okay. Plus it has to go through the communication processor, and it has to do that.

Now for me to have failures in all of them, all four of the communication processors have to go screw up, okay. Now if a data formatting is restricted, if it is of a certain structure, you know, I think I'm looking at multiple failures, not a single failure then, you know, if that is to happen.

You see, each division has not only -- even for voting purposes, you know, it is going to be more than one processor. Each processor is capable of only taking one input, so you have to use multiple processors.

So you know, for me to make that scenario work, I cannot. I can sit down with you outside of that; I can walk you through that, you know. I mean, I've got notes and I've got red lines and white lines, and I essentially could not get to that conclusion, that there is a corrupt data that's going to lock up all three processors.

MEMBER BROWN: Okay.

MR. TANEJA: All right. We can do that, you know. I mean but that was my thinking that, you know, I have these barriers, and you know, this is what we've seen over ISG-4 also. This is an acceptable means of providing, you know, independence between two different communications, okay. So that is on the inter-division communication part of it.

Then on the next slide, you know, we're talking about the inter-division communication. Now that inter-division communication occurs on the admin field bus, which is a different communication controller that's plugged into the rack, the 19-inch rack.

Now the inter-division was happening on the processor controller itself, on the high speed links. There are two ports of high speed links right on the microprocessor bolt, you know, plugs in, right.

For the AF-100 bus, the admin field bus 100, whatever. It's a proprietary field bus. There are two separate communication modules that got plugged into that rack, okay, to come up with a redundant communication network.

Now on that redundant communication network is your nodes for the -- I believe there are two nodes in the control room for each division, for the human machine interface, the operator control console. So each of them is on that same node.

Now each division is independent, right. So we have -- each division has a separate, you know, human interface on two separate controllers. Then also on that controller resides the MTPs, the maintenance test panel, okay. That's a separate node that's not -- it doesn't have the same functionality as the operator control console, okay.

So that bus really works very independently of the inter-channel communications, okay. It's totally independent. It works off of it, and that communication I believe occurs, and I wasn't able to clarify that information, but that communication occurs from the back plane of those, you know, of the rack.

You know, there is really -- that's the only way it communicates with the processors through the back plane in a global memory location, because there is no wires that jump over from the controller, right. So a means of independence is there for even that bus from that bus. So I corrupt that bus or that controller, my processor continues to function. It doesn't have any --

MEMBER BROWN: I never disagreed with that.

MR. TANEJA: Okay. So that part of it is what I came up with, the conclusion. Now we have another communication occurring, which is a communication through text, okay. Now that happens through the MTP. So MTP that the field bus has actually a dedicated bandwidth for the data communication, which is deterministic.

Then it has other communication feature

that's happening on the field bus. That's one part of it, and then there is a separate communication coming out of the MTP through a fiber optic cable, one-way isolated communication going out the back. That's strictly one where there's nothing coming back.

Now that is a transmit-only function, so it doesn't read anything back into that network. So we felt that that was, you know, adequate for maintaining, you know, independence for non-safety systems.

MEMBER BROWN: I didn't have a real problem with that part of it. My concern on the safety to non-safety aspects are when it leaves the PICS area, that function area and gets sent out like the technical support center in the EOL, which then has a set of what's called secure, I've forgotten the full name, secure communication -- I don't know.

Secure something. I have to go back and look at the figure and see what the word is. Secure something box, and then there's some words in the FSAR and the appendix, whichever one it was, that says "For example, a firewall."

Well, I don't think I've ever seen a firewall that couldn't get hacked, and that's what takes it into the corporate network.

MR. TANEJA: Yes.

MEMBER BROWN: So they even started talking about that. I think that's a cyber security issue.

MR. TANEJA: Right, it is.

MEMBER BROWN: I don't know how we do that, so I hadn't brought that up in the context of this particular discussion, relative to the operation of the retention system and the ELCS. I'm not looking at it from a corruption of getting down into the plant. It's only in terms of the communication between, you know, the situation between the main control room and the advice that may be gotten from technical support center folks, and are they looking at the same information.

In other words, if someone's able to done so, be it hack in via the corporate bus, -- that data, severed what this very sophisticated worm did and the destruction-type thing, okay. And we've had that discussion in another context. So I hadn't addressed that issue. But within the plant, I don't have any big particular problem with the -- unless John and Dennis have found something. I didn't see --

MR. TANEJA: From the safety system perspective, right, you know, we're looking at the independence of safety system from non-safety.

MEMBER BROWN: Yes. I didn't --

(Simultaneous speaking.)

MR. TANEJA: That one, you know.

MEMBER BROWN: I saw that seemed to be fairly healthy. I thought about it in terms of a 571. I thought that was kind of a Level 4 type differentiation. I didn't see where that was getting communicated back in. Now it may be because I don't understand all that much, and as I think about that some more, but I just haven't got to that point yet.

MR. TANEJA: You know, so you know, that I think is another area that probably, you know, the cyber area. It's outside, but I think right now we are trying to figure out what belongs within the Chapter 7 purview, and what belongs in Chapter 13, you know.

(Simultaneous speaking.)

MEMBER BROWN: I mean that's why --.

MR. TANEJA: So here, you know, my focus was, you know, hey. Is there anything in non-safety side that could propagate into safety and make it, you know, do an adverse impact to it, and I didn't find anything in their design, in that respect of it.

I am not a cyber expert. I wouldn't be

able to answer that question right now. I mean I have to become one, but not right now. I wouldn't be able to.

You know, we do have, you know, that document, 7DS, does a pretty decent job of mapping to the ITAACs, you know, and the different features of the, critical features of the design. But we do have an ITAAC Item 3 in Table 2.75 that requires testing to verify that only one-way data transfer occurs from safety to non-safety related systems.

Then we have another ITAAC, you know, Item 5 in that same table, that requires testing to verify that any loss of data or any bad thing happening in one division doesn't result in a transient or an erroneous signal, you know, going in and corrupting the other things.

MEMBER BROWN: Well, that's always -- but that depends on our data set. You can't test all possible data sets.

MR. TANEJA: True.

MEMBER BROWN: So you'll test multiple data sets within some, whatever you determine reasonable.

MR. TANEJA: And you know, what we are hoping is given that these data sets are prestructured data sets, you know, that it's not unlimited, you know, we could do a pretty decent amount of testing on that one. But that's up to, you know, that ITAAC activity is really, you know, something that they have show us, you know, how they've done it and we have to buy into that.

Next slide, number nine. On the deterministic performance, you know, one thing that we saw in their design is that they don't have any external interrupts coming into the processor, okay. There is a number of allocation of these ECCS functions occurring. I think there is within a division, there may be an allocation of ECCS functions between the low pressure and the high pressure. So they're allocated to a different processor. They're not running on the same processor, right.

Then within a processor, you know, the task manager, which has the highest priority, and then the control modules, which are running on that thing, that design, which requires that priority functioning to be allocated with the timing of the priority of running those controls, with no external interrupts.

The only interrupt that I saw in their design is the internal interrupt, which essentially interrupts these overhead tasks to start the necessary tasks that need to be performed in a given cycle.

MEMBER BROWN: I've forgotten what the time is, we had that discussion, I think Warren and I did, when he explained the timing in another aspect. But every two or five milliseconds, whatever it is, that task is interrupted and it's going and stopping whatever's going on and it's looking, do I need to do something else, yes or no, it's a higher priority, and then it restarts again, and you just keep on going.

MR. TANEJA: Right.

MEMBER BROWN: But there is an interrupt every two to five milliseconds.

MR. TANEJA: There is. There is.

MEMBER BROWN: So that is an interrupt that stops everything, and every time an interrupt occurs, you have -- that's an opportunity to have something not work right. You've got to go back, you've got to return.

MR. TANEJA: Right, right.

MEMBER BROWN: That's one point, and he went through the whole drill and that's why I -- my focus on the other thing was when they find that's the way it is.

MR. TANEJA: That is a design of this processor, right.

MEMBER BROWN: That's the way it is, and the key feature there is to take the application program, make sure you meet the metrics that are called out, and that they test to meet and show that they meet it with the 70 percent loading, in terms of all the stuff, and he figured out some way to do that. So I walk away happy; their specific thing stated to resolve the issue and that was the discussion. So that is -- do you want to amplify that?

MR. ODESS-GILLETT: Yes. This is Warren Odess-Gillett. My name is being used here.

(Simultaneous speaking.)

MEMBER BROWN: And you weren't satisfied?

MR. ODESS-GILLETT: Well, no. It's just that I just wanted to clarify in the other project that we, to the best of our ability, let's say we're moving unessential IO modules, that we'll try to maximize the CP load to the best we can. But to get to 70 percent, there's no guarantee we can get to 70 percent without actually manipulating validated software.

MEMBER BROWN: I accepted your resolution with some fuzzballs in there because you said there might be another platform in some time, and you couldn't define whether there would be a different number, and therefore you didn't want to use that number.

So I walked away that you were going to do it on this one to get to the 70 percent, even though I understood the methodology. So maybe I should have been more persistent.

MEMBER BLEY: I think you had the same caveat the last time.

MEMBER BROWN: Yes. I don't remember that. I told you I'm too old to remember that stuff, whether it's a day or an hour away with something like that. Thank you, Warren.

MS. BANERJEE: So we don't have an action item?

MEMBER BROWN: Yes, you do.

MS. BANERJEE: Okay.

MEMBER BROWN: You've got the same thing. They've got a whole set of different applications over here than what you're going to be running in the other --

CHAIRMAN ABDEL-KHALIK: Let's let the staff continue, please.

MR. TANEJA: Right. You know, processor loading is, you know, one of the functions of assuring deterministic behavior. Now limiting the load to an acceptable limit, I mean that is, you know, that is a given, okay, that we have to do that, and part of the -- you know, part of the exercise here is that for each of the applications, there is going to be an application-specific timing analysis, you know.

That is it's a formal analysis, a documented analysis, you know, and that analysis is validated by a formal testing, okay, and that's a given. Then you know, we do have ITAACs already in place which requires the communication protocols to be deterministic, okay, and this is -- in the certified design already we have those ITAACs.

(Simultaneous speaking.)

MEMBER BROWN: -- getting up to the 70 percent as close as possible.

MR. TANEJA: Now you see, if they have --

MEMBER BROWN: I love the analysis, but that's where the rubber hits the road.

MR. TANEJA: And I'm sure you've seen the topical report on the Common Q that, you know, the NRC staff has already looked at and approved, and there is a specific discussion in there about the loading to 70 percent in that topical report as well. Let's see.

So you know, we felt that we already had what we needed, you know, as far as the acceptance criteria, to assure deterministic performance of its controller.

MEMBER BROWN: If all you need is 22 percent and you need it, then that's what you -- you'd meet the performance and that's not good enough if you're at 50 percent or 60.

MR. TANEJA: Right.

MEMBER BROWN: So you don't know if future changes will run it up, what that will be --

(Simultaneous speaking.)

MR. TANEJA: Well, you know, there is a process in place for future changes, okay. The future changes have to be done formally. They cannot just be done ad hoc. There's a 5059 process that requires a thorough analysis of all these impacts, and then there is anything that is software, we have a software in a management plan, which has a formal, you know, modification to the software as a formal reverification process that has to be gone through, you know.

So it's not like an ad hoc that somebody's going to go and make a change. I mean we have a program that is already developed, verified, tested and locked in. Now you have that, you're running the plant. The change that you're going to make, whether you bring in new inputs or whether you put in new functionality, is going to require a formal change process.

So it's not something that is just done, you know, by an operator or a technician out in the field or anything like that, you know.

So you know, so we had looked at this topical, and here I went through all of the discussion on the deterministic performance, and looked at how the tasks are handled and how they are located, and this is part of the inspection that we'll do, you know, as part of the ITAAC inspection and DAC inspection, when they are actually developing and building these systems for STP-3 and 4.

MEMBER BLEY: Charlie's point there is that, and I'm going to rephrase it a little differently.

MR. TANEJA: Okay.

MEMBER BLEY: Even if you have a formal analysis process, if the requirement in the regulation and this will be essentially a regulation, is 70 percent loading, then when you do your calculations and they do their calculations, as long as they aren't approaching that 70 percent, they're meeting all the requirements.

The point that was raised if you've never tested the device up to that point, you don't know for sure if it's going to happen when you get there. So I think all of the safeguards aren't safeguarding against the point Charlie raised in the beginning.

MR. TANEJA: So what, I mean you know, I guess the worst case loading, you know, we could not figure that out, I mean what the worst case loading would be on the processor. There's a maximum/minimum times that we know that would be needed to complete that cyclical function that it needs to perform, right.

So we are setting up a cycle time for each of the applications that needs to run on a given processor, right. We have this logic diagram, okay. Typically, you know, if I look at a lot of logic, you know, the way it reads, it goes from left to right, you know. It will start here and I'll start looking at this input, this input, this input and on this function block, then it runs this function block, this function block.

From start to finish, from grabbing the input to generating an output, you know, it's going to take a certain time, right. So that timing, okay, I can test that timing. When I design it, I can run that on a simulation and I can look at that timing, right.

MEMBER BLEY: Yes.

MR. TANEJA: So I can look at that time and make multiple runs and say, you know, I can come up with a minimum/max under various conditions. So you know, the 70 percent, there was a white paper that I read. This task allocation, it said, you know, if we keep it below 70 percent, it will show the deterministic performance of a given processor.

It's just, you know, that margin is not really the margin for future changes, I don't think. That margin is just to assure that I can get a deterministic performance. Now if I want to build in --

MEMBER BLEY: And what Charlie has said is --

MR. TANEJA: If I build in capacity --

(Simultaneous speaking.)

MEMBER BLEY: --for that point, all you have is an analysis. You don't know for sure.

MR. TANEJA: No, no, no, no. The testing is part of the ITAAC that we have. It requires, ITAAC requires a test. It's not only an analysis. So there is a formal analysis, and that analysis is validated by a test.

MEMBER BLEY: Let me try something with what might sound like a stupid analogy, but it's the only way I can do this. We traditionally, in the old days, required strict time testing for motor operated injection valves. People did that under zero EP conditions. They met all of the things and the motors didn't over-torque.

Yet we had events when the valve had to stroke with actual real world EPs, and the valves didn't work, because we'd never designed the test to verify that indeed the equipment would perform its designed function under its design basis conditions. We just didn't do that.

This to me sounds like an analogous situation. We're not testing the system under its design basis conditions as specified in the regulation or the rule. So we don't know how it's going to work, the same way that we didn't really know, we convinced ourselves we know how those valves were going to work, but we were wrong.

MR. TANEJA: Well, I guess that's where some of the operating experience comes in. I would probably ask Westinghouse what's their experience has been with these type of issues, you know, because they've had application in Korea of the Common Q platform.

MEMBER BLEY: And I think, from what we've heard, they've never loaded them anywhere above 25-30 percent.

MR. TANEJA: That's fine then, right.

MEMBER BLEY: No.

MR. TANEJA: I mean, I'm just saying --

MEMBER BLEY: I don't think we're communicating.

(Simultaneous speaking.)

MEMBER BLEY: It's right now. It's fine right now, but when --

MR. TANEJA: So what you're saying is, you know, we don't know what the maximum load it can take and still perform, right?

MEMBER BLEY: That's what we're saying. If you test it at 70 percent load, then you'll know that, and if later people loaded up to 50 percent, you won't have any qualms.

MR. TANEJA: Yes. That's a very valid point, you know. I mean I guess --

MEMBER BLEY: And what will all those analyses --

(Simultaneous speaking.)

MEMBER BLEY: --loaded over 70 percent. That's all.

MR. ED BROWN: This is Ed Brown from Westinghouse.

MEMBER BLEY: Yes.

MR. ED BROWN: We have run tests at loads of 70 percent during the original qualification of the platform, and the equipment worked satisfactorily at 70 percent. We do have some applications that run 65 percent, the time. The more correct analogy is like a setpoint versus the safety analysis limit.

Seventy percent is a maximum, and anything you run below 70 percent is margin. So typically you don't test your system by eating into your margin. The system will run satisfactorily at 70 percent load. That's been demonstrated through the original qualification testing.

MEMBER BLEY: Well, see now I don't recall ever hearing --

(Simultaneous speaking.)

MEMBER BROWN: There's no report of any of that testing --

MEMBER BLEY: Well, at least that's come through, through anything we've seen.

MEMBER BROWN: That's right.

MEMBER BLEY: This is the first time we've heard that --

(Simultaneous speaking.)

MEMBER BROWN: You know, we've only seen the topical report.

MEMBER BLEY: Or that you've got some running somewhere at 65 percent. Never heard that before. That's brand new information.

MEMBER BROWN: We haven't seen the actual test results.

MEMBER BLEY: It would be nice to see the test results. That would probably go a long way.

MEMBER BROWN: If the platform and its configuration have been tested at 70 percent, and the data is available to demonstrate, then I wouldn't have asked the question. But it's not there, or hasn't been presented to us.

MR. ED BROWN: Well, the data was presented during the original review in the 2002 time frame. I'm sure we can resurrect the data, and resurrect --

MEMBER BROWN: I'm open to any technical presentation that demonstrates that the thing performs.

MR. TANEJA: Now you know, to go back to

your --

MEMBER BROWN: Let me make one point, in that that was in the configuration of the specific controllers that were being used, the AC-160s, etcetera, etcetera, with whatever configuration, those components or those assemblies had at that time.

MR. ED BROWN: That's correct.

MEMBER BROWN: If in the ensuing eight year, nine year period, the constituency of those assemblies has changed somewhat, based on components that are either available or not available, even though the module and assembly stays the same, have each of those substitutions been tested to ensure that you still maintain the same performance?

That's another open question that comes along. But the concept of how the controller works is kind of universal, but is also somewhat dependent on the constituency and the types of devices, whether it's the memory devices or the processors or the blah blah blah. So you can get changes, just due to the nuances within the processors themselves.

MR. ED BROWN: Well, you have to test

the larger configuration with more applications to get to the 70 percent load. I guess that's the quandary. For the validated and verified software, unless it's changed, you can't change it above what its loading is at that time.

However, you can take a test configuration that's larger, has more software in it, and make it 70 percent and verify that it operates at 70 percent.

MEMBER BROWN: That's what we've asked for.

MR. TANEJA: See, the position would be -- Charlie, for the way the DCD right now is written, okay, the configuration for the safety system as it's configured is required to be tested, okay. It's required to be tested and verified to be deterministic. Now the question is if they do make a change and increase the loading on that, it has to go through the same validation and verification process just like the original design.

You're not just going to arbitrarily add load to it. It's going to have to go through the same testing process all over again if you were to change that loading. That's the way I understand the software program manual to be, you know.

CHAIRMAN ABDEL-KHALIK: I think several points have been made. Let's continue. This is an open issue that will be revisited. It's one of the four or five open items that we have.

MR. JUNG: Mr. Chairman, just to add, to wrap up, it's not clear and the staff's not against adding 70 percent capacity to that. I think it's, the burden should be on the South Texas.

I wonder if South Texas is willing to modify 7DS to include more specifics on 70 percent loading, to verify that either the loading is below 70 percent or, when it's in 70 percent or above, demonstrate through the testing there's a report that exists that demonstrates these functions.

It should be on South Texas to propose a solution for this.

CHAIRMAN ABDEL-KHALIK: It may be that the old data, the old tests that were run at 70 percent may satisfy the issue here. But we need to look at it. I'm sorry.

(Simultaneous speaking.)

CHAIRMAN ABDEL-KHALIK: If you were to resurrect that data and present it, that may satisfy that, I'm sure. But for the time being, this remains open. We're not going to resolve it here and now. Please continue.

MR. TANEJA: You know, the specific ITAAC that I was talking about is the Table 2.75, Item 3, which requires the testing of all the communication functions for deterministic performance, you know. There is a, it's a broad ITAAC, but all these specifics fall within that category.

You know, the point that I think is a slight dilemma, you know, this is really going back to the Common Q topical report, that we have a proprietary copy of that we had reviewed and approved as part of the overall Common Q qualification.

And you know, in that SER that we had also concluded in that SER that the operation of the AC-160 was determined to be a deterministic operation, and it met the guidance of BTP 7-21. In that SER, we have a plant-specific action item, 6.6, which also requires the licensee to review the timing analysis and validation tests, in order to verify that it specifies the plant-specific requirements for a system response and display response time presented in Chapter 13 action analysis.

So we have these specific requirements even in the SER for a very specific test that needs to be performed. I just wanted to, you know.

Slide 12. We had the opportunity to go through the Appendix 7DS, and you know, what we found in that is that it took and it consolidated the information that's already there in various different sections of the application. You know, it's a good, you know, piece of document. It's very helpful, you know. It actually helped me and you know, to --

But you know, we didn't find anything that would change our SER, you know. So it's a good addition to the COLA, with no impact to the SER.

Now if you guys would like, you know, the backup slides I have, our discussions from the May 2010 meeting, and at that time we talked about that the worse backup design that is part of the original certified design. I know, John, you had some questions about the hard-wired controls, and I can shed some light on that from my perspective, you know, what I know about that design. If you'd like.

MEMBER STETKAR: That's up to you and the rest of the Subcommittee.

MR. TANEJA: I'm just offering that information.

MEMBER STETKAR: Waste time to --

CHAIRMAN ABDEL-KHALIK: I think at this time, I'd like to move to next item on the agenda, which is a discussion of ACRS action items, unless there are some questions from the Subcommittee to the staff on the Chapter 7 material that has been presented. Any questions to the staff on Chapter 7 material that has been presented?

(No response.)

CHAIRMAN ABDEL-KHALIK: Okay, thank you. We'll move on to the next item on the agenda, which is discussion of ACRS action items.

MEMBER BROWN: While they're setting up, could I ask one question? This is for Ed or Warren.

MR. ED BROWN: Yes.

MEMBER BROWN: This is about the Common Q platform. Do you expect it from a -- the advertising is that the 70 percent allowed you to meet the deterministic behavior, okay, and was predictable in the field. As the bus loading -- this is an information question. As the bus loading increases, does the response time of the platform increase?

MR. ED BROWN: No, it does not.

MEMBER BROWN: It stays the same. So when you say it maintains its original performance characteristic over that 70 percent range, based on your own testing. So if the response time for that platform is advertised at 250 milliseconds, just to pick a number, that you can load it to at least 70 percent, and it will demonstrate that response each time, or within that range?

MR. ED BROWN: Yes, sir.

MEMBER BROWN: It may move around a little bit, which it most certainly will, because of the interrupt-driven nature of the processors, but it will still --

MR. ED BROWN: No. Actually, it will stay the same. The only reason that the response time would change is if the timing of the event relative to the cyclic nature. In other words, if an event occurs and the system has just read the process data before the event, it will have a longer response.

MEMBER BROWN: Right. I got that, and that's sometimes hard to achieve when you're inputting data. You've got to run a series of tests. I don't know. That's what I used to have to do. I used to go on multiple tests, because I knew I wasn't sure where the timing cycle I was getting.

MR. ED BROWN: That's how we get the maximum --

MEMBER BROWN: Yes.

MR. ED BROWN: It occurs just before or just after.

MEMBER BROWN: Okay, thank you.

CHAIRMAN ABDEL-KHALIK: Okay.

MR. HEAD: Before we went into the action items, we were going to address some of the issues or action items from the previous discussion.

CHAIRMAN ABDEL-KHALIK: Yes, sir.

MR. HEAD: Mike, did you want to say anything about the 70 percent discussion?

MR. MURRAY: Yes, I do. I want to present our position on the 70 percent discussion, but understanding that the qualification of the platform was qualified at 70 percent, and in expected configurations of the platform.

We'll design it to be less than 70 percent. We'll test and verify that we are less than 70 percent. We'll test, and those are normal configurations expected of the platform, and as we go through our development processes, we continually test for that loading.

If we were to do a test to 70 percent for our design, we would not test our design, is the point to be made, okay. We would have to configure a design that is not our design, that is not expected performance of our system, in order to make a test like that.

So on our position, we feel that understanding the continuously monitored 70 percent diagnostics, along with the design of the system to maintain less than 70 percent than is normally expected configurations, we feel is adequate for that particular --

CHAIRMAN ABDEL-KHALIK: What is missing in this argument is the first point you made, which is --

MR. MURRAY: The qualification.

CHAIRMAN ABDEL-KHALIK: That the

platform was qualified at 70 percent. We haven't seen that data.

MR. MURRAY: You haven't seen that then. Okay.

MR. ED BROWN: The committee might have seen that ten years ago, but this committee --

CHAIRMAN ABDEL-KHALIK: Has not.

MR. ED BROWN: Hasn't seen it, hasn't been able to resurrect it.

MR. HEAD: Okay. So that now, I would say, is a discrete action item that we have, to present that in a future discussion.

CHAIRMAN ABDEL-KHALIK: To show that the platform was qualified at 70 percent.

MR. HEAD: At 70 percent. That's what we're going to do.

CHAIRMAN ABDEL-KHALIK: Okay.

MR. HEAD: Is that all right?

MEMBER BROWN: Yes. The 70 percent. Yes. I thought I'd brought the SER with me for the Common Q platform, a copy of it, which had a very explicit statement at the end that said if anything changes, the NRC has the right to revoke.

CHAIRMAN ABDEL-KHALIK: Yes, but I understand the logic of your argument.

(Simultaneous speaking.)

CHAIRMAN ABDEL-KHALIK: We're just trying to make sure that all the pieces are there.

MR. HEAD: We understand, okay. Thank you. So the first one I propose is to go back to Figure 7C-1, which we have on the board, excuse me, on the board, sorry.

MR. SWANNER: On the large screen TV everywhere. Okay, and I think I could repeat Member Stetkar's question, which was how does the diverse actuation equipment work with, and what are the requirements of it? Basically, one of -- there are several diverse components that are in place in the design, in the original certified design, to mitigate common cause failure.

One of those is HP Charlie, or excuse me, HPCF Charlie. There's a manual start. That push button is in the control room, and it can start hard-wired, as shown here, the HPCF. It can start the pump, open the injection valve, close the test return valve, close the test bypass valve and it can auto start.

MEMBER STETKAR: And that's in your jargon a system level manual action?

MR. SWANNER: That's correct.

MEMBER STETKAR: One button, all of those things happen, the switch --

MR. SWANNER: That's correct. The same thing we were asked about where do the manual controls from the control room come into it. If there were a system level actuation, it would come into the SLF right here as shown. On a component level, if they just wanted to actuate a valve or a pump, it would actually come into the RDLC.

So that's where -- that was the confusion in the response. So and the other manual controls, as shown here, are similar. There's a, you know, RCIC steam supply inward isolation valve. You can control that manually, hard-wire directly from the control room to the component, as well as the cleanup system, inboard containment isolation valve as well.

And the components needed to safely shut the reactor down in the event of a common cause failure, all of that equipment and the diversity is listed in two places in the application. One is in Tier 1, 3.4 Charlie, and the other is in Tier 2, Appendix 7 Charlie.

One thing to point out is essentially these were incorporated by reference from the original ABWR DCD design. So if you just look at the COLA application, which only has the change paragraphs, you won't get much of the text there. So the actual requirements for the diversity are listed, you know, if you combine the documents.

MEMBER STETKAR: The question I had today didn't relate to the diverse equipment.

MR. SWANNER: Sure.

MEMBER STETKAR: It was making sure that the normal equipment could indeed be operated, albeit individually, perhaps starting several pumps and opening several valves individually. But still the operators had that capability to do that from the main control panel somehow, under a condition where ESLF itself, where you didn't have the system level --

MR. SWANNER: I understand.

MEMBER STETKAR: And, thanks. That helped.

MR. SWANNER: No problem.

MR. HEAD: Okay. The next one I think we'd like to discuss is the DIVOM question.

CHAIRMAN ABDEL-KHALIK: DIVOM.

MR. HEAD: Excuse me. That's what I wrote down, sorry. And I sense from the discussion that it's, at least initially, the GE7 aspect of it.

CHAIRMAN ABDEL-KHALIK: Well, there's a GE method.

MR. HEAD: Yes.

CHAIRMAN ABDEL-KHALIK: A GE set of codes that have been approved by the staff to do this, and the question is do you have access to those codes.

MR. HEAD: Well, we're a member of the owners group, and those, the analysis that's done is, you know, core-specific, and that's something that we would be expecting to do post-COL. If we decided to stay with the GE7 fuel, then that's what we would have to go do, and we would expect GE to have fixed their Part 21 issues.

Sorry. I was headed to where I think you were going, that they would have addressed their Part 21 issues. Now for what -- we obviously plan to make that irrelevant by what our plans with respect to Optima-2, and that we expect to being calculated with POLCA-T, and that's one of the codes that we presented to you back in October as part of the fuel --

CHAIRMAN ABDEL-KHALIK: The fuel

amendment aside, let's just look at your application right now, with GE7 fuel, what you're telling me that if you need to contract with GE to generate the DIVOM correlation, if that's what is needed, that's what you'll do.

MR. HEAD: Yes, sir.

CHAIRMAN ABDEL-KHALIK: Is that the --

MR. HEAD: Yes, sir.

CHAIRMAN ABDEL-KHALIK: Okay, I accept that.

MR. HEAD: Okay. Then I believe, as a result of the Chapter 7 discussions, I now have five action items. Oh, excuse me, there were five. One is the watchdog, which is -- we've agreed to correct. One is the tech spec discussion that we'll have on Chapter 16. The DIVOM I believe we've just answered.

The seven, Figure 7C-1, I believe we've just answered, and the 70 percent loading is a new one that we will carry and address in a future discussion. Okay. Maitri, is that --

MS. BANERJEE: So we have three?

MR. MURRAY: Correct.

MR. HEAD: Yes. Okay, so with that, I will turn it over to Coley to go through the two that we would like to talk about today.

CHAIRMAN ABDEL-KHALIK: All right, thank you. Thank you very much.

MR. COLEY: So this is our presentation that covers a couple of action items, basically a recap of an action item, and also a look ahead as to how we might address a future action item that is related to some of the discussions that this group has been involved in.

We have our same personnel up here, and we'll cover these two action items. Next slide please. So this is a recap of the inter-channel communication and determinacy for the FPGA and Common Q platform. This was Action Item 7 that was on the list, that we covered and summarized in the Chapter 7 presentation.

I know we have some additional action items that came out of the overall discussion, but this is intended to see if we've covered all the pieces, and then also the redundancy and diversity of the overspeed on the turbine generator.

So we had a, I'll give a brief discussion on that as well. So slide, please. All right. So this is the question that we were carrying forward as an action item, dealing with independence and determinacy, specifically for Common Q. I know we got into some pieces. So we captured all of the follow-on discussion from this, and can we consider this particular item close to those follow-on action items at this point.

CHAIRMAN ABDEL-KHALIK: From my perspective they have, but other Committee members may feel differently. The question has been posed.

MEMBER BROWN: Yes. The only items are confirming the 70 percent issue and the FPGA watchdog timer implementation, and other than --

MEMBER STETKAR: There's essentially no more information that they can -- we understand how that works.

MEMBER BROWN: Yes.

MR. HEAD: So our proposal would be since we have the two new ones, can we say that we've addressed this one?

MEMBER BROWN: I don't care how we do it administratively.

(Simultaneous speaking.)

MR. HEAD: Okay. I mean we'll just open two new ones, you know. We'll trade you two for three.

(Simultaneous speaking.)

MR. HEAD: Well, this was a big one. We had two very -- okay, all right. Now I feel better. All right.

MR. COLEY: The next one, quite the opposite. We're not attempting to close this one at all, but we want to give an update. Based on the meeting that we had with the staff last Wednesday to discuss some turbine overspeed RAIs, we discussed the acceptance criteria at this meeting for the SRP. We also discussed ITAAC and we've come out of that meeting with more understanding about how we're going to revise those RAIs.

So we'll put additional information in the FSAR, additional information that will explain how the SRP acceptance criteria is met, and provide more detail that supports the ITAAC. We expect those RAIs, we said in that meeting that we have RAIs to the staff for them to look at by next Wednesday.

So that's the time frame associated with that. I understand Chapter 10's coming up, so we wanted to give you an update as to this information. It will be available soon.

CHAIRMAN ABDEL-KHALIK: Chapter 10

will be discussed on April 6th. So that should be plenty of time for you to provide that information.

MR. COLEY: I believe that's the current schedule, yes, sir.

MR. HEAD: Did you summarize the middle -- do you want to summarize the middle paragraph?

MR. COLEY: I just -- yes, I didn't read. I mean we have, this is all stemming from a departure, in which we replaced the primary overspeed mechanically with the second electrical overspeed.

CHAIRMAN ABDEL-KHALIK: You sort of had some hesitation about the April 6th date.

MR. COLEY: I have heard that it may not be certain, but that's all I know.

MEMBER BROWN: It may not be what?

MR. COLEY: Certain.

MR. HEAD: We're striving to make it certain.

MR. COLEY: Okay.

(Laughter.)

MR. HEAD: If you get your stuff to us, it will be certain.

MR. COLEY: Exactly.

(Simultaneous speaking.)

MEMBER BROWN: I'm presuming, I mean I'm looking at our action item list, and there was -- I mean I had the question, and I think John also asked the question at the time. I'm frankly working the details --

(Simultaneous speaking.)

MEMBER BROWN: And we were kind of said hey look. In September, we were told this would be resolved later, and so we said okay, we'll wait. I presume we'll get this information prior to the meeting.

MR. HEAD: Yes.

MEMBER BROWN: Okay, all right.

MR. HEAD: Well, I mean --

MEMBER BROWN: That's not your action. That's their action.

MR. HEAD: Yes, part of the chapter. But when the RAI response comes in, that will be the detail of our position. So --

MR. COLEY: So I'm feeling very confident about April 6th.

CHAIRMAN ABDEL-KHALIK: That's really great to hear.

MR. COLEY: Okay. I think that's it.

Are there any additional questions? That's just an update on action items.

CHAIRMAN ABDEL-KHALIK: Are there any question to the Applicant regarding these two items? Charlie.

MEMBER BROWN: Not to the Applicant. Just a comment to the staff on one of them.

MR. TONACCI: Go ahead.

MEMBER BROWN: And that just you all commented that -- the comment was that we would see it with the final SEI with no open items. That was 45, the turbine overspeed trip, and all I would like to see is to make sure that we just don't see the safety evaluation that says we accepted the RAI and we agree with its conclusions.

I'd like to actually see the RAI performance. That's all. That was just an execution item, but that's all.

MR. TONACCI: Maitri, if we can amend that, so that we won't forget to see the RAI.

CHAIRMAN ABDEL-KHALIK: Anything else regarding these two items? Okay, so thank you very much. Is the staff prepared to present any discussion of any ACRS action items? No. Thank you. Okay. At this time, I would like to open the phone bridge line, in case there are any members of the public.

MS. BANERJEE: Yes. I was told last time that we have six people attending through the bridge line.

CHAIRMAN ABDEL-KHALIK: Well, let's open the bridge line and see if any members of the public would like to make a statement.

MEMBER STETKAR: This is always an uncertain process.

CHAIRMAN ABDEL-KHALIK: What was that?

MEMBER STETKAR: This is always an uncertain process. You typically have to ask somebody to make some sound.

CHAIRMAN ABDEL-KHALIK: Is the line open? Okay. Are there any members of the public on the phone line?

(No response.)

CHAIRMAN ABDEL-KHALIK: Okay, let me ask it again. Do we have anyone on the phone line?

MR. PINTO: Yes, you do.

CHAIRMAN ABDEL-KHALIK: Yes, sir. Could you please identify yourself?

MR. PINTO: Yes. This is Johnny Pinto, Sarasota, Florida.

CHAIRMAN ABDEL-KHALIK: Okay. Let me ask the question in a little more specific way. Are there any members of the public who wish to make a comment or a statement?

(No response.)

CHAIRMAN ABDEL-KHALIK: Okay. Hearing none, then I guess that item is closed. So we will close the phone line again, please. Before we conclude the meeting, are there any additional comments or questions that members of the Subcommittee would like to make?

MEMBER SIEBER: Nothing from me.

CHAIRMAN ABDEL-KHALIK: John?

MEMBER STETKAR: No. I think I'd like to congratulate STP. Good presentations.

CHAIRMAN ABDEL-KHALIK: Charlie?

MEMBER STETKAR: Oh NINA, I'm sorry.

(Simultaneous speaking.)

MEMBER BROWN: Yes. I'd just like to amplify that, that the Appendix 7DS I thought was extremely valuable, in terms of providing a raft of clarifications that weren't available in any other piece of paper or documents that you have, and they're pretty well presented. So I wanted to congratulate you. I thought that was a good job and I appreciate the effort that went into that.

MR. HEAD: Thank you.

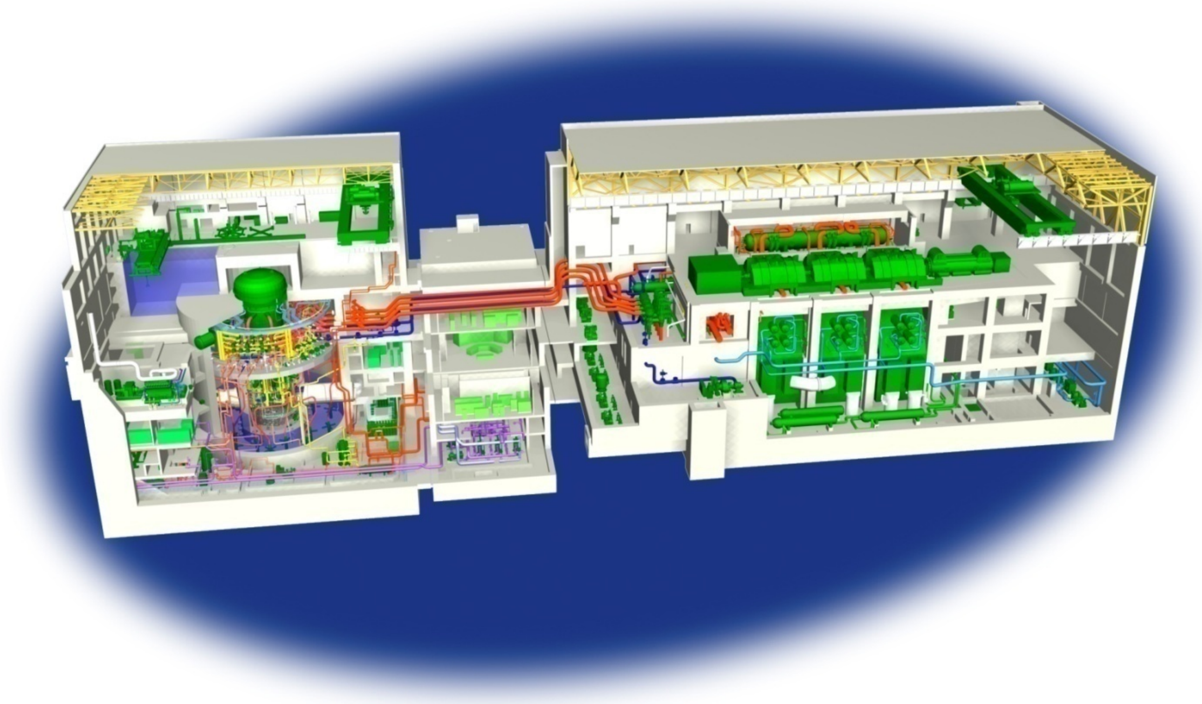
CHAIRMAN ABDEL-KHALIK: Well, thank you very much. The meeting's adjourned.

(Whereupon, at 4:20 p.m., the meeting was adjourned.)

South Texas Project Units 3 & 4 Presentation to ACRS Subcommittee

Chapter 7

Instrumentation and Control Systems



Agenda

Chapter 7 was discussed at ACRS ABWR Subcommittee on May 20, 2010.

Discussion points for status update since last meeting:

- Setpoint Methodology
- Current RGs and Codes and Standards applied to ELCS (Common Q)
- FSAR Tier 2 Appendix 7DS
  - Four Design Principles
  - Simplicity

Attendees

Mike Murray (NINA)
Scott Head (NINA)
Coley Chappell (NINA)
Kyle Dittman (NINA)
James Cook (NINA)
Akira Fukumoto (Toshiba)
Hiroshi Sakamoto (Toshiba)
Kiyotaka Wakita (Toshiba)
Jun Ikeda (TANE)
Ed Brown (WEC)
Warren Odess-Gillett (WEC)
Bob Quinn (WEC)
David Herrell (TANE)
Craig Swanner (TANE)

Instrument Setpoint Methodology

- Response to RAI 07.01-16
- WCAP-17119-P Revision 2, “Methodology for South Texas Project Units 3 & 4 ABWR Technical Specification Setpoints” submitted on July 29, 2010
- Included a summary of methodology application and typical setpoints for the OPRM trip function

Current RGs and Codes and Standards applied to Common Q Platform

- Revision 2 to Response to RAI 07.01-14
- Westinghouse Common Q Platform (WCAP-16097) approved applying RGs and industry codes and standards in effect at the time
- NINA has committed to apply the RGs and codes and standards in effect 6 months prior to submittal of the COLA for all safety related DI&C platforms including ELCS (Common Q)

FSAR Appendix 7DS

- Consolidates information from various parts of COLA and applicable technical or topical reports regarding
  - Four Design Principles (redundancy, independence, determinism & diversity)
  - Simplicity
- Includes or describes no new design changes or departures
- Scope includes safety-related DI&C
  - Reactor Trip and Isolation System (RTIS) & safety-related Neutron Monitoring System (NMS) using Field Programmable Gate Array (FPGA) based platform
  - Engineered Safety Features Logic & Control System (ELCS) using Common Q based platform
- Maps Design Principles to applicable ITAAC and DAC

RTIS/Safety Related NMS

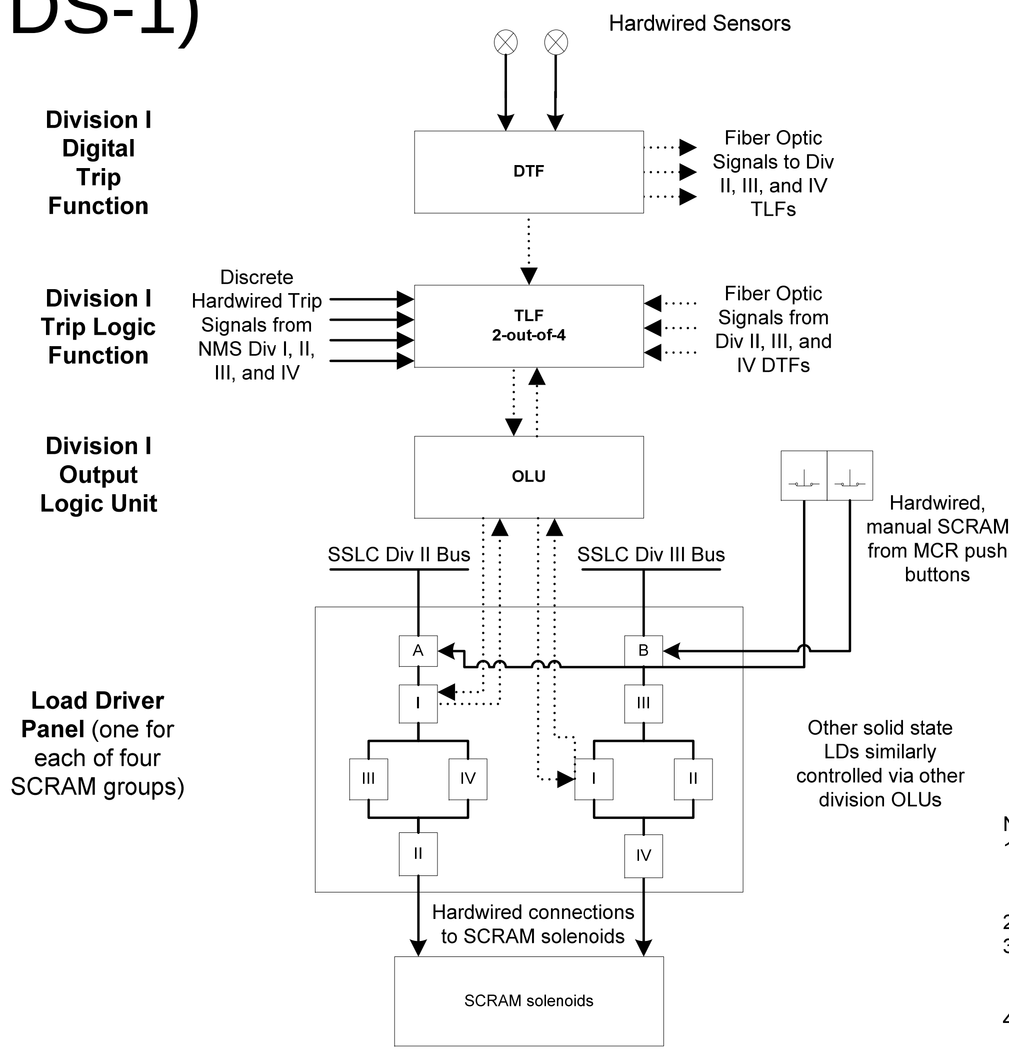
- Overview
- Redundancy
- Independence
- Determinism
- Diversity
- Simplicity

RTIS/NMS Platform Overview

- Digital Trip Function (DTF)
  - Analog to digital conversion of hardwired sensor input
  - Compares signal values to setpoints to determine sensor division trip and status
- Trip Logic Function (TLF)
  - Receives sensor division trip and status information from four redundant DTFs
  - Performs 2-out-of-4 voting to determine automatic divisional trip
  - Sends divisional trip to Output Logic Unit
- Output Logic Unit (OLU)
  - Receives automatic divisional trip from its divisional TLF
  - OLU distributes trip outputs to Load Drivers (LDs) for reactor trip and Main Steam Isolation Valve (MSIV) closure

RTIS/NMS Platform Overview

(Figure 7DS-1)



Notes:
1) RTIS-RPS Division I shown; other divisions typical. RTIS-MSIV equipment similar.
2) Not all communication links shown.
3) Figure 7DS-1 derived from Tier 1 Figures 2.2.7b and 3.4b and Tier 2 Figures 7.2-8 through 10.
4) Fiber Optic communication is denoted by dotted lines and hardwired communication is denoted by solid lines.

RTIS/NMS Platform Redundancy

- NMS has four independent & redundant divisions that provide trip and status to each division of RTIS
- RTIS has four independent & redundant divisions
  - Each division includes a DTF, a TLF, and an OLU
  - Division-of-Sensors bypass
  - Trip-Logic-Output bypass
- Each division has independent & redundant power sources

RTIS/NMS Platform Independence

- Four independent, divisional power sources
- Independence from non-safety systems
  - Communications isolation and independence
  - Electrical isolation and physical separation
- Four independent RTIS/NMS sensor divisions to determine divisional sensor trips
  - No communication between sensor divisions
  - Only trip and status information is communicated across division boundary to support 2-out-of-4 voting function
- Four independent RTIS TLF and OLU divisions
  - Communication isolation and independence
  - Electrical isolation and physical separation

RTIS/NMS Platform Independence – Communication

- RTIS Communication Across Divisions
  - Communicates trip and status information of fixed length, fixed content, and predefined format
  - Qualified, isolated, point-to-point, unidirectional fiber optic communication links
  - Each communication link has its own independent buffer
- Communication to Other Systems
  - Qualified, isolated, point-to-point, unidirectional fiber optic communication links
  - Each communication link has its own independent buffer
- All communications include Self-Diagnostics functions
  - Continuously monitor proper communication performance
  - Upon detection of failure, division marked as inoperable (i.e., tripped) and operator is alerted

RTIS/NMS Platform Determinism

- Each FPGA is a synchronous, clocked sequential circuit
  - Each FPGA only starts processing data when data is transferred into that FPGA, and sends data to the next FPGA or module when processing is complete
  - Changes of state occur only at selected times, controlled by a timing signal
  - All FPGAs performing signal processing functions on a module are monitored by a diverse, hardware based watchdog timer
  - Watchdog timer time out marks module as inoperable (i.e., tripped) and operator is alerted
- Timing is verified by analysis and simulation during design

RTIS/NMS Platform Diversity

- RTIS and NMS platforms diverse from the Engineered Safety Features (ESF) Control and Logic System (ELCS) which actuates ESF functions
- RTIS and NMS diverse from non-safety and balance of plant I&C systems
- RTIS diverse from Anticipated Transient Without Scram (ATWS) mitigation equipment

RTIS/NMS Platform Simplicity

- Separation of Safety and Non-Safety Functions
  - Non-safety functions are not performed in safety related equipment
  - Complex activities (e.g. cross channel checks and historian functions) are performed in non-safety equipment
- Non Re-Writable (NRW) FPGA
  - Functionality implemented in fixed gates with deterministic timing that cannot be changed
- Minimization of Interdivision Communication
  - Communication across division boundaries limited to trip and status information for 2-out-of-4 coincidence logic

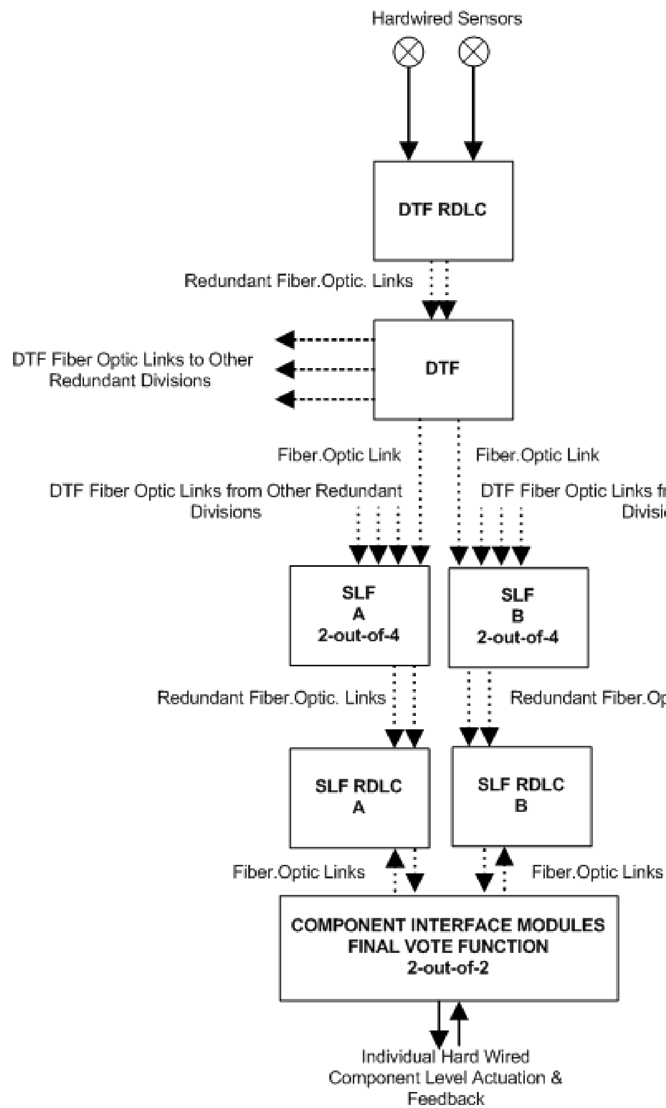
ELCS

- Overview
- Redundancy
- Independence
- Determinism
- Diversity
- Simplicity

ELCS Overview

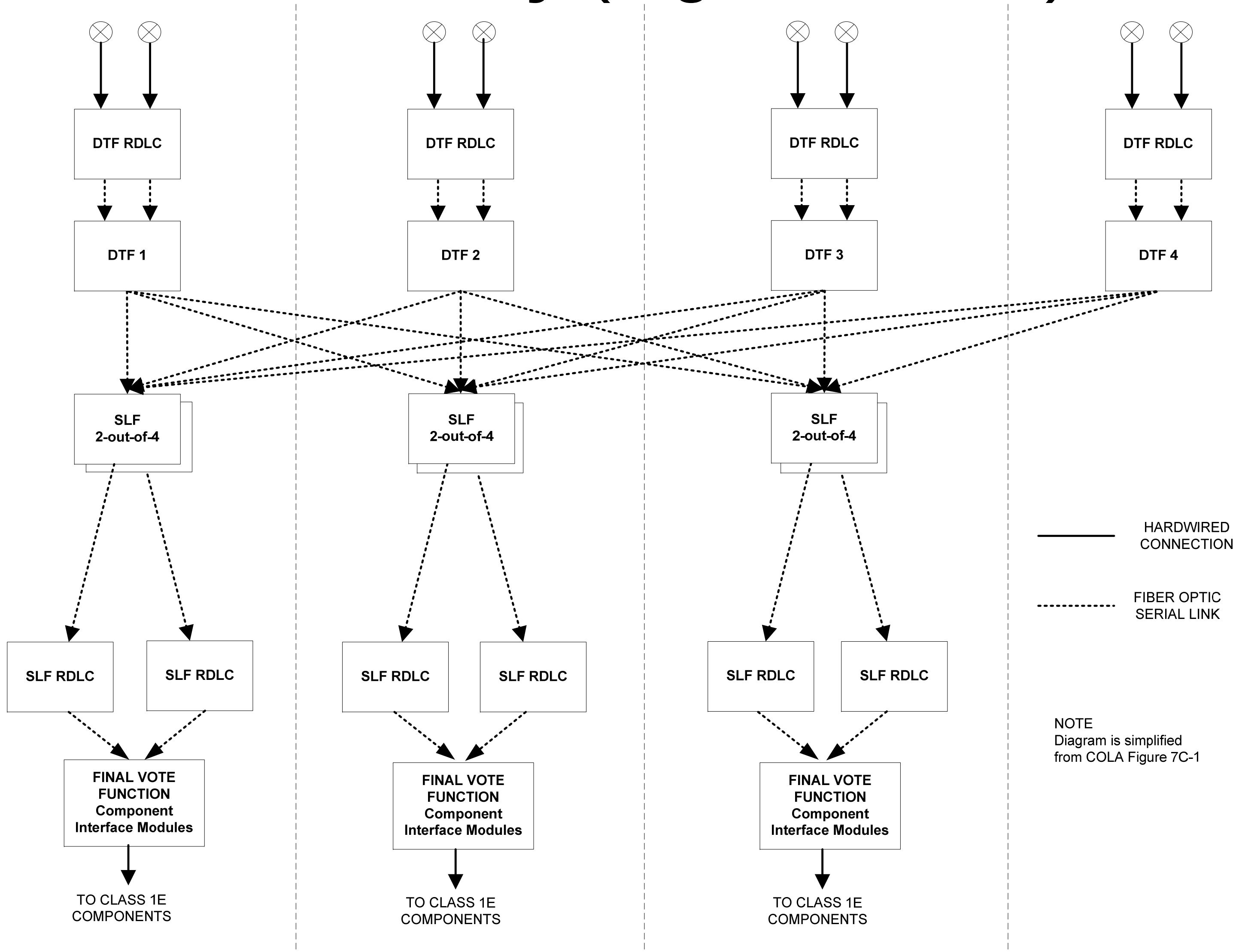
- Digital Trip Function Remote Digital Logic Controller (DTF RDLC)
  - Remote data acquisition of Engineered Safety Feature (ESF) sensor signals
- Digital Trip Function (DTF)
  - Compares signal values to setpoints to determine division ESF safety function initiation status for one division
- Safety Logic Function (SLF)
  - Performs 2-out-of-4 coincidence logic to determine system level automatic initiation status
- Safety Logic Function Remote Digital Logic Controller (SLF RDLC)
  - Receives system level automatic and manual system level actuation signals from SLFs
  - Provides logic to determine component actuation and control commands to Final Vote Function
- Final Vote Function
  - Receives individual component actuation and control commands
  - Performs 2-out-of-2 coincidence logic (where necessary) for component actuation and control

ELCS Platform Overview (Figure 7DS-3)



Note
Information on diagram is derived from COLA Figure 3.4b

ELCS Redundancy (Figure 7DS-4)



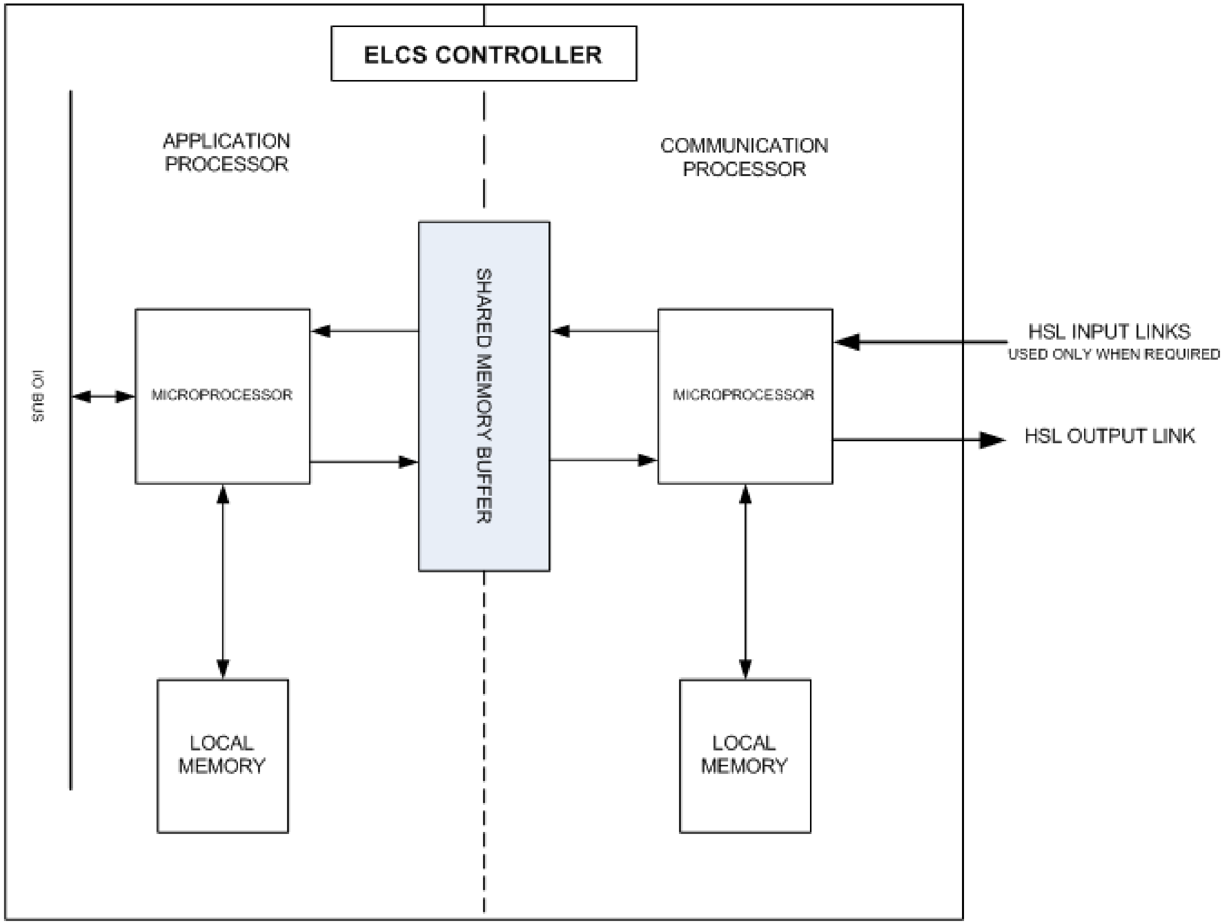
ELCS Redundancy

- Four independent & redundant sensor divisions
- Three independent & redundant ESF Safety Function Actuation divisions
  - ESF safety function system level initiation
  - ESF component actuation and control
- Four independent & redundant divisional power sources

ELCS Independence

- Four independent power sources
- Independence from non-safety systems
  - Electrical isolation and physical separation
- Four independent ESF sensor divisions
- Three independent ESF Safety Function Actuation divisions
  - Electrical isolation and physical separation
- Communications Independence
  - Safety related communications are isolated and independent
  - Non-safety related communications are isolated and independent

ELCS Controller Simplified Diagram



NON-PROPRIETARY VERSION OF FUNCTIONAL ARCHITECTURE FIGURE, SECTION 6.2.1.2.1.2 OF COMMON Q TOPICAL REPORT WCAP-16097-P-A

ELCS Independence
Inter-division Communication

- DTF to SLF Communication
  - DTF transmits trip status to SLFs
    - Unidirectional Serial Link with fiber optic isolation
    - Fixed periodicity of transmission
    - All data transmitted, even if none has changed
    - Fixed length, fixed format message
      - Fixed data mapping – same data point in same position
      - Data redundancy provided in message
      - Cyclic redundancy check (CRC) data provided in message
    - Supports detection of corrupt data

ELCS Independence

Inter-division Communication (cont'd)

- DTF to SLF Communication (cont'd)
  - SLF receives DTF communication
    - SLF has a communication processor and an application processor that communicate through shared memory
    - Communication processor receives message
      - Link failure diagnostic detects failed link
        - Provides error status for bad message
      - CRC diagnostic provides error status for bad message
      - Data redundancy diagnostic provides error status for bad message
      - Stores message in a unique location in shared memory
    - Application processor reads message
      - Bad message status causes the message data to be replaced with predetermined value
      - Alarm message sent to operator

ELCS Determinism

- ELCS Application Processor
  - No external interrupts
  - Internal clock uses precision interval timer
    - Cyclic execution of application software modules based on precision interval timer
    - Predetermined fixed execution cycle
    - Maximum processor load of 70% – enforced by self-diagnostic
    - Buffered from external communication – read and write data from buffered memory on a fixed cycle, independent of communication interface status
    - Communication interfaces – flag corrupt data as bad message
    - Application uses predetermined values in place of bad message
  - Diagnostics provide annunciation to operator
    - Watchdog timer hardware output monitored by independent controller
    - Over-run of cyclic execution time monitored by self-diagnostic
    - Communication self-diagnostics monitored by application

ELCS Determinism

- ELCS Communication Processor
  - Deterministic Protocol
  - All data transmitted, even if none has changed
  - Fixed length, fixed format message
    - Fixed data mapping – same data point in same position
    - Data redundancy provided in message
    - Cyclic redundancy check (CRC) data provided in message
  - Deterministic Transmission Intervals
    - Based on fixed intervals of application processor requests to send messages
  - Deterministic Reception Intervals
    - Based on fixed message reception intervals from transmitting controllers
  - Communication process is buffered from application processor by shared memory
  - Diagnostics provide annunciation to operator
    - Watchdog timer hardware output monitored by independent controller
    - Loss of communication monitored by controller receiving the communication
    - Message Diagnostics – CRC and data redundancy monitored by the controller receiving the transmission

ELCS Determinism

- Response Time Analysis
  - Criteria based on Safety Analysis requirements
  - Includes all delay elements
  - Determines minimum and maximum acceptance criteria for response time validation testing
  - Documented in a report
- Validation Testing
  - Validates analysis
  - Documented in a report

ELCS Diversity

- Diverse from equipment credited to mitigate ELCS failure
  - Diverse equipment is hard wired
- Diverse from RTIS and NMS
  - ELCS is microprocessor based
  - RTIS and NMS are FPGA based
- Diverse from non-safety control systems
  - Different microprocessor and software
  - Different communications technology and equipment

ELCS Simplicity

- Separation of Safety and Non-Safety
  - ELCS control is performed within ELCS
  - No non-safety digital control communication links with priority modules
- Simplicity of Communication
  - Unidirectional serial links for automatic and manual initiation of ESF safety functions simplify architecture
- Minimization of Interdivision Digital Communication
  - Only system level coincidence logic function uses interdivisional digital communication links

Mapping of Design Principles to Applicable ITAAC

- Example Supporting Information provided in Appendix 7DS
  - Tier 1 Table 2.7.5 ITAAC 2 requires deterministic communications protocols

Table 2.7.5 Data Communication

Inspections, Tests, Analysis and Acceptance Criteria		
Design Commitment	Inspections, Tests, Analysis	Acceptance Criteria
2. The ECFs use deterministic communication protocols	Tests of the ECFs communications protocols will be conducted in a test facility	The ECFs use deterministic communications protocols

  - Section 7DS.2.3.2.2 describes all steps in ESF communication timing
  - Section 7DS.2.3.2.2 statement "{Each step in the process is predictable and repeatable. This is the time response that is designed to meet the Safety Analysis requirements.}[16]" points to Note 16 in Table 7DS-1
  - Table 7DS-1 Note 16 links the bracketed description back to Tier 1 Table 2.7.5 ITAAC 2.

ACRS Action Item Summary

Action Item 7 from May 20, 2010 ACRS Meeting

- Further discussion was needed on the application of Common-Q platform, independence and determinism

Response to Action Item 7

- Explanation in FSAR Tier 2 Appendix 7DS and ELCS Presentation Information
  - Explains that data corruption does not compromise communication independence
  - Explains inter-division communication compliance to independence and determinism requirements
  - Explains the compliance to determinism requirements

Chapter 7

Questions and Comments

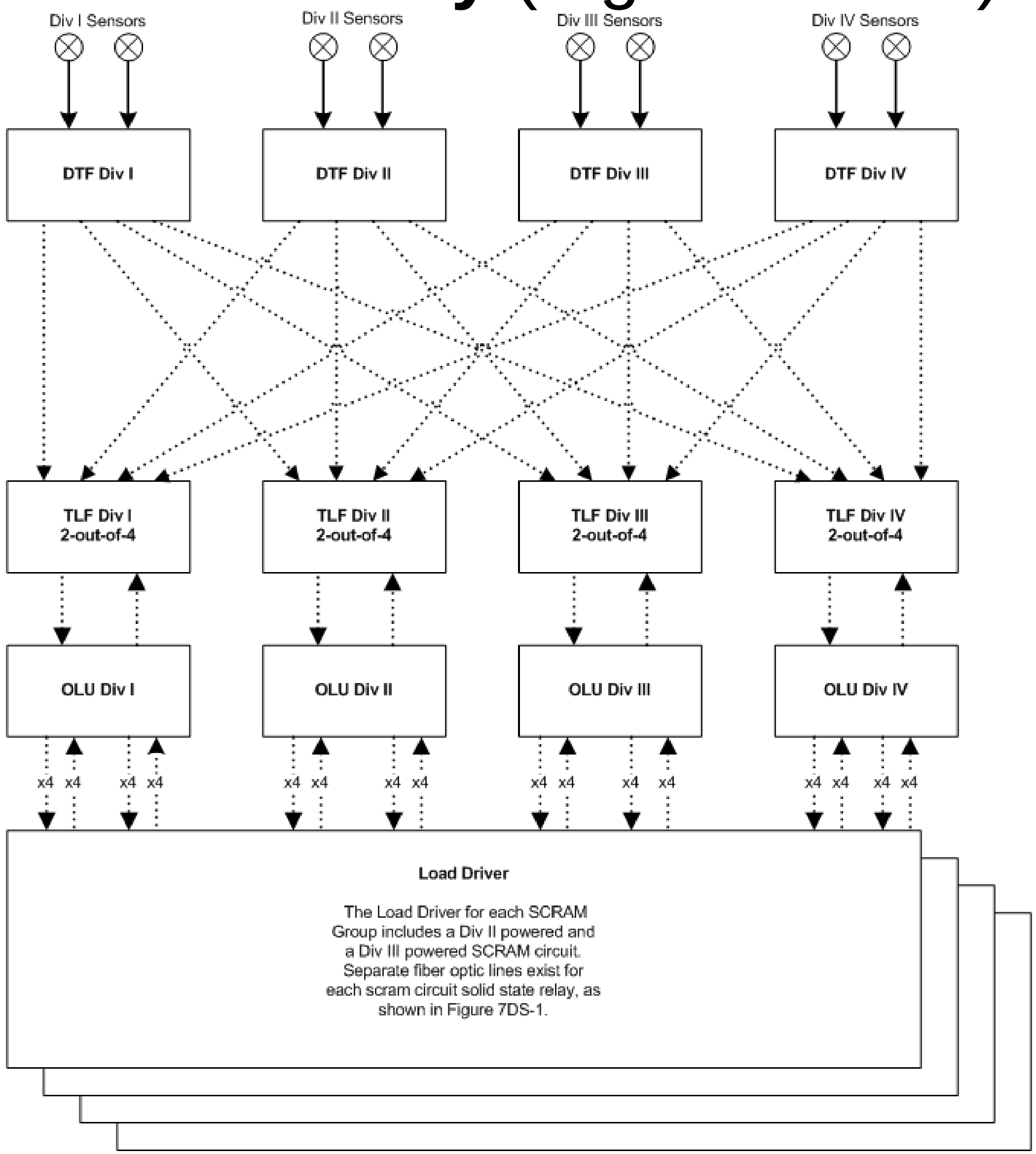
Acronyms

ABWR	Advanced Boiling Water Reactor
APRM	Average Power Range Monitor
COLA	Combined License Application
CRC	Cyclic Redundancy Check
DAC	Design Acceptance Criteria
DI&C	Digital Instrumentation and Controls
DIV	Division
DTF	Digital Trip Function
ECCS	Emergency Core Cooling System
ELCS	Engineered Safety Features Logic and Control System
ESF	Engineered Safety Features
FPGA	Field Programmable Gate Array
FSAR	Final Safety Analysis Report
HSL	High Speed Link
I&C	Instrumentation and Controls
I/O	Input / Output
ICRC	ITAAC Closure Requirements Checklist
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
LD	Load Driver
LDS	Leak Detection and Isolation System

Acronyms (cont'd)

LPRM	Local Power Range Monitor
MCR	Main Control Room
MSIV	Main Steam Isolation Valve
NINA	Nuclear Innovation North America
NRW	Non-rewritable
NMS	Neutron Monitoring System
OLU	Output Logic Unit
OPRM	Oscillation Power Range Monitor
RAI	Request for Additional Information
RDLC	Remote Digital Logic Controller
RG	Regulatory Guide
RPS	Reactor Protection System
RTIS	Reactor Trip and Isolation System
SLF	Safety System Logic Function
SRNM	Startup Range Neutron Monitor
SSLC	Safety System Logic and Control
TANE	Toshiba America Nuclear Energy
TLF	Trip Logic Function
WEC	Westinghouse Electric Corporation

RTIS/NMS Redundancy (Figure 7DS-2)



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Presentation to the ACRS Subcommittee

South Texas Project Units 3 and 4 COL Application Review

Chapter 7 Advance SER (with no Open Items)
“Instrumentation and Controls”

February 8, 2010

STP 3 & 4 COL Chapter 7 Staff Review Team

- **Project Managers**
  - George Wunder, Lead PM, DNRL/NGE2
  - Adrian Muñiz, Chapter PM, DNRL/NGE2
- **Technical Staff**
  - Dinesh Taneja, Reviewer, DE/ICE2
  - Jack Zhao, Reviewer, DE/ICE1
  - Eugene Eagle, Reviewer, DE/ICE2
  - Sang Rhow, Reviewer, DE/ICE2

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary of Technical Discussion Points for STP 3 & 4 COL Chapter 7 Review

SER Open Item 07.01-16	Open item 07.01-16 in the SER with OI (Phase 2)
RAI 07.01-14	2nd revised response related to applicability of NRC Regulatory Guides and Industry Standards to Common Q platform used for ELCS
ACRS ABWR Subcommittee Action	Application of Common Q platform, independence and deterministic implementation
Appendix 7DS	Staff evaluation of Appendix 7DS, "Digital Instrumentation and Control Design Verification for Safety-Related Systems"

SER Open Item 07.01-16

- Reference to post-COL document in COLA
  - In the setpoint methodology report (WCAP-17119-P, Rev. 1), a reference was made to WCAP-17137-P, “Westinghouse Stability Methodology for the ABWR,” for OPRM setpoints. This topical report is a part of the planned post COL fuel amendment activity, and can’t be referenced in the COL application.
  - In response to RAI 07.01-16, the applicant has agreed to remove the reference to WCAP-17137-P from the setpoint methodology report, and include typical setpoint values and associated uncertainties for the OPRM.
  - The staff finds this RAI response acceptable.
  - Proposed changes to the FSAR and WCAP-17119-P are being tracked as **Confirmatory Item 07.01-16.**

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RAI 07.01-14 2nd Revised Response

- Applicability of regulatory guides and industry standards to Common-Q platform used for ELCS
  - On September 23, 2010, the applicant provided 2nd revised response to RAI 07.01-14, which commits to meeting current NRC Regulatory Guides and industry standards for the Common-Q platform used for ELCS
  - This RAI response includes proposed changes to the FSAR Table 1.8-20, “NRC Regulatory Guides Applicable to ABWR,” and Table 1.8-21, “Industry Code and Standards Applicable to ABWR”
  - The staff finds this 2nd revised RAI response acceptable
  - Proposed changes to the FSAR are being tracked as **Confirmatory Item 07.01-14**

ACRS ABWR Subcommittee Action Item

- Application of Common Q platform, independence and deterministic implementation
  - Microprocessor-based Common Q platform is used for Engineered Safety Features (ESF) Logic and Control System (ELCS)
  - The following ELCS data communication design features described in the FSAR demonstrate **independence**:
    - Unidirectional serial point-to-point fiber optic isolated data links utilizing deterministic protocol are used to communicate ESF safety function information
    - Communication is buffered by the communication processor, which is independent from the application processor (sending and receiving end)
    - Separate communication equipment is used for interdivisional communication
    - Predefined formatting and data redundancy within the message minimize the possibility of malformed message from being used by the receiving controller

ACRS ABWR Subcommittee Action Item (continued)

- Each ELCS division includes an intra-division network that performs the following functions:
  - This network is separate from the ESF safety function communication
  - Loss of intra-division network does not affect the division's ability to perform ESF safety function
  - Communication with dedicated safety flat panel displays in the control room for ESF components control and status information
  - Communicate self-diagnostic information for display and alarm in the main control room
  - Provides detailed diagnostic information and the capability to conduct surveillance testing at the Maintenance and Test Panel (MTP)
- Each ELCS division has a unidirectional communications interface to non-safety Plant Information and Control System (PICS)

ACRS ABWR Subcommittee Action Item (continued)

- A division of ELCS will accomplish its safety functions regardless of the operation or failures of other safety divisions, or non-safety systems
- Tier 1 Table 2.7.5 Item 3 **ITAAC** requires **testing** to verify, in part, that only one way data transfer from SR to NSR system or devices is permitted
- Tier 1 Table 2.7.5 Item 5 **ITAAC** requires **testing** to verify that loss of data communication in one division does not result in generation of transient or erroneous signals
- In response to RAI 07.01-2, the applicant confirmed that the DI&C-ISG-04 is applicable, and the SSLC design conforms to the ISG-04 guidance

ACRS ABWR Subcommittee Action Item *(continued)*

The following ELCS data communication design features described in the FSAR demonstrate **deterministic performance**:

- ELCS response time for all ESF safety functions is predictable and repeatable, therefore it is deterministic

- Formal timing analysis documents the response times, which is validated by formal test

- Communications processor supports deterministic performance of the unidirectional serial data link communications

- Input communications are sent by a cyclic deterministic process from the transmitting processors

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

ACRS ABWR Subcommittee Action Item *(continued)*

- Scheduling of the execution of the application software is based on internal clock and is fixed by design
- There are no application processor interrupts that are driven by external process signals
- Output communications are initiated by the cyclic and deterministic application processor
- Each step in the process (input – application processing – output) is predicable and repeatable
- Tier 1 Table 2.7.5 Item 3 **ITAAC** requires **testing** to verify that the essential communication functions are implemented with a deterministic communications protocol

ACRS ABWR Subcommittee Action Item *(continued)*

– Westinghouse Common Q platform design has already been evaluated by the NRC and found suitable for use in safety-related applications (ADAMS Accession No. ML003740165). In the Common Q SER:

- The staff concluded that design features, operation of the AC160 PLC system, and Westinghouse's commitments to perform timing analyses and tests provide sufficient confidence that the AC160 will <u>operate deterministically</u> to meet guidance in BTP 7-21
- The plant-specific action item 6.6 requires the licensee to review Westinghouse's timing analyses and validation tests in order to verify that it satisfies its plant-specific requirements for system response and display response time presented in the Chapter 15 accident analysis

STP 3 & 4 FSAR Appendix 7DS

- STP 3 & 4 FSAR Appendix 7DS, "Digital Instrumentation and Control Design Verification for Safety-Related Systems"
  - On January 19, 2011, the applicant provided a site-specific FSAR appendix 7DS, which:
    - Consolidates information regarding key design features of safety-related digital I&C platforms
    - Facilitates mapping of applicable DAC and ITAAC that would verify implementation of these key design features
    - Does not change the SSLC design as already described in the STP 3 & 4 COLA
  - Information provided in appendix 7DS does not have any impact on Staff's safety findings documented in the Chapter 7 Advance SER

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Overview of STP RCOL Chapter 7

Discussion/Committee Questions

Backup Slides

Independence of Data Communication Functions

- Brief description
  - Data communication functions are inherent to each of the SSLC digital I&C platforms and therefore separate and independent from each digital I&C system and division within the systems. These data communication functions are designated as ECF (essential communication Function).
- Specific items of interest
  - The following data communication design features that demonstrate independence are described in the STP 3 & 4 FSAR that will be inspected and/or tested by ITAAC in Tier 1 Table 2.7.5:
    - ECFs are implemented through dedicated equipment in each of the divisions, with no direct electrical interconnections among divisions.

Independence of Data Communication Functions *(continued)*

- Specific items of interest *(continued)*
  - Data communication design features *(continued)*:
    - Data communication is provided between redundant safety-related divisions to support coincident logic functions.
    - Data communication is implemented through fiber optic based data links to ensure interdivisional isolation.
    - All communication is checked to prevent a division from impacting the performance of other divisions.
    - Each division has independent control of data acquisition & transmission.
    - System timing is asynchronous among divisions.
    - Loss of data communication in a division of equipment implementing the ECFs does not cause transient or erroneous data to occur at system outputs.

Independence of Data Communication Functions *(continued)*

- Specific items of interest *(continued)*
  - Data communication design features (continued):
    - Communication between safety-related (SR) and non safety-related (NSR) systems use isolating transmission medium and buffering devices. When the equipment is in service, data cannot be transmitted from NSR side to SR side.
    - Each division of ECF equipment is powered from its respective division's Class 1E UPS.
    - All equipment within Reactor Protection System (RPS) and Leak Detection and Isolation System (LDS) is designed to fail-safe, i.e., fail into a trip initiating state on loss of power or input signal.
    - All equipment within Engineered Safety Feature (ESF) Systems is designed to fail as-is, i.e., system controllers continue to operate based on the last command.

Independence of Data Communication Functions *(continued)*

- Specific items of interest *(continued)*
  - Tier 1 Table 2.7.5 Item 3 requires **testing of equipment** implementing ECFs to verify that only one way data transfer from SR to NSR system or devices is permitted, and no control and timing signal are exchanged between SR and NSR systems or components.
  - Tier 1 Table 2.7.5 Item 5 requires testing to verify that loss of data communication in one division of equipment implementing ECFs does not result in generation of transient or erroneous signals.
  - In response to RAI 07.01-2, the applicant confirmed that the DI&C-ISG-04 is directly applicable, and the STP 3 & 4 SSLC design is in accordance with the guidance provided in this ISG.

United States Nuclear Regulatory Commission
Protecting People and the Environment

Independence of Data Communication Functions (continued)

- Conclusion
  - The staff found reasonable assurance that the STP 3 & 4 data communication functions conform to all applicable regulations and guidelines, specifically, IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Deterministic Features of Data Communication Functions

- Brief description
  - A deterministic algorithm is an algorithm which behaves predictably. Given a particular input, it will always produce the same output, and the underlying machine will always pass through the same sequence of states.
  - In STP 3 & 4 I&C design, RTIS and NMS platforms are based on the FPGA technology with hardwired I/O. Interdivision communication uses isolated optical data links with deterministic communication protocol.
  - In STP 3 & 4, ELCS is designed with Westinghouse Common Q Platform based on deterministic communication protocol.

United States Nuclear Regulatory Commission
Protecting People and the Environment

Deterministic Features of Data Communication Functions *(continued)*

- Specific items of interest
  - In response to RAI 14.03.05-4, the applicant confirmed the following I&C design elements:
    - Safety-related I&C systems are deterministic.
    - Response times for the system elements, including architecture, communications (including timing and loading) and processing elements will be analyzed in accordance with BTP 7-21 to verify that the systems' performance characteristics are consistent with the safety requirements established in the design basis for these systems.
  - Tier 1 Table 2.7.5 ITAAC Item 3 requires testing to verify that the essential communication functions are implemented with a deterministic communications protocol.

Deterministic Features of Data Communication Functions *(continued)*

- Specific items of interest (continued)
  - In the Common Q SER, the staff concluded that the design features, the operation of the AC160 programmable logic controller (PLC) system, and Westinghouse's commitments to perform timing analyses and tests provide sufficient confidence that the AC160 will <u>operate deterministically</u> to meet guidance in BTP 7-21 and is, therefore, acceptable.
  - In the Common Q SER, the plant-specific action item 6.6 requires the licensee to review Westinghouse's timing analyses and validation tests in order to verify that it satisfies its plant-specific requirements for system response and display response time presented in the Chapter 15 accident analysis.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

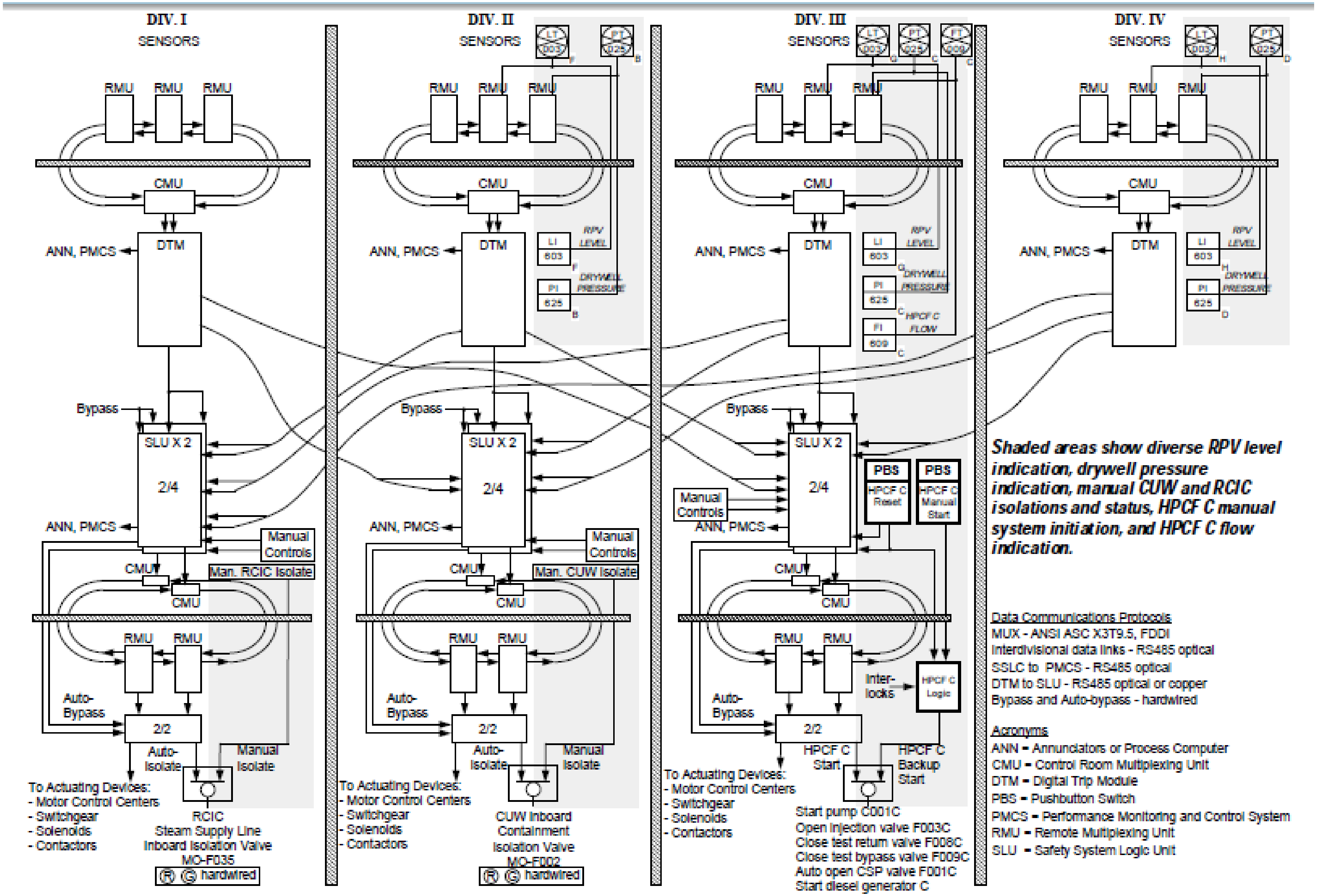
Deterministic Features of Data Communication Functions *(continued)*

- Conclusion
  - The essential communication functions of the STP 3 & 4 SSLC are implemented with a deterministic communications protocol.
  - Response times for the system elements, including architecture, communications (including timing and loading) and processing elements will be analyzed by STPNOC in accordance with BTP 7-21 to verify that the systems’ performance characteristics are consistent with the safety requirements established in the design basis for these systems.
  - An ITAAC in the COLA requires testing to verify that the essential communication functions are implemented with a deterministic communications protocol.

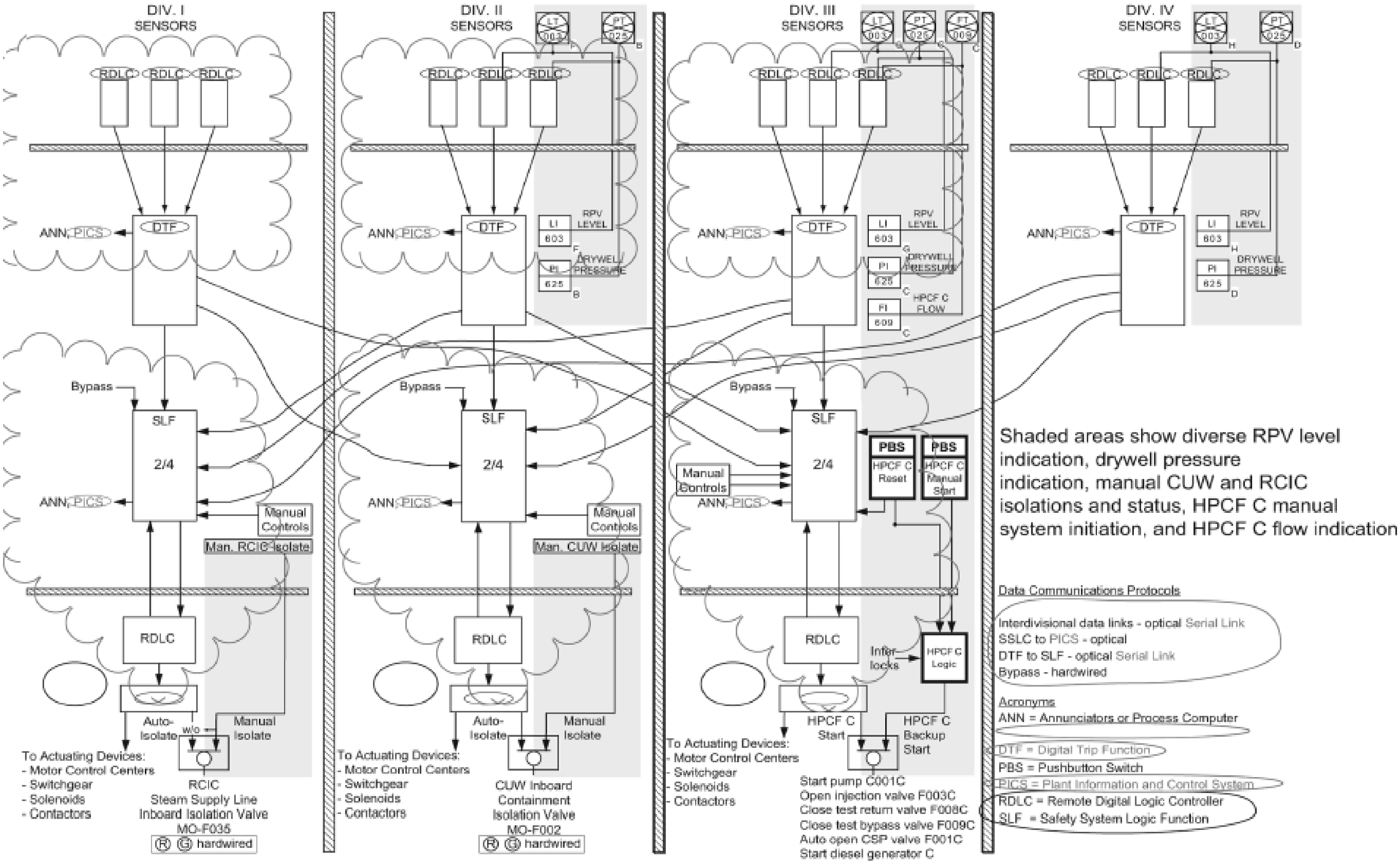
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Diversity and Defense-in-Depth

- Brief description
  - The certified U.S. ABWR design provides for diverse backup hardwired capabilities for reactivity control (reactor trip), core cooling (ESF actuation), containment isolation, and supporting diverse displays to cope with a postulated worst-case event, i.e., undetected 4-division common mode failure of all communications or logic processing functions in conjunction with a large break LOCA.
  - STP 3 & 4 COLA incorporates by reference (**IBR**) the diversity and defense-in-depth consideration and resulting diverse backup design features of the certified ABWR design **with no departures**.



ABWR DCD Figure 7C-1 Implementation of Additional Diversity in SSLC to Mitigate Effects of CMF



COLA Figure 7C-1 Implementation of Additional Diversity in SSLC to Mitigate Effects of CMF

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Diversity and Defense-in-Depth (continued)

- Specific items of interest
  - For the purpose of ABWR I&C design diversity analysis, design basis events (DBE) described in Chapter 15 were analyzed with the following modeling assumptions:
    - A worst-case postulated common mode failures (CMF) of the digital safety systems was considered concurrently with each of the design basis events.
    - The analyses were done using “realistic” modeling as opposed to standard “licensing basis” modeling.
    - The analyses took credit for operator actions at the Remote Shutdown System (RSS) after one hour, but prior to that one hour period, all operator actions were limited to those which could be performed in the main control room, using equipment that was independent of the postulated CMF.

Diversity and Defense-in-Depth (continued)

- Specific items of interest (continued)
  - –In the certified ABWR design, EMS is common to all digital I&C systems within a division.
  - –Loss of EMS (A worst-case postulated CMF of the digital safety systems) adversely impacts the entire division of safety-related I&C systems (SSLC), thereby potentially rendering both RPS and ESFAS inoperable. Note that RPS is a fail-safe design, therefore any failure in the RPS (including EMS) would result in a division trip signal.
  - –STP 3 & 4 I&C design provides for independent and diverse RTIS and ELCS with inherent communications capabilities. Therefore, this I&C design is not subject to total loss of a safety division (i.e., both RTIS and ELCS) due to any postulated CCF of digital I&C systems.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Diversity and Defense-in-Depth (continued)

- Specific items of interest (continued)
  - –In STP 3 & 4 I&C design, the hard wired diverse features are independent of all digital I&C systems as illustrated in STP 3 & 4 FSAR Figure 7C-1.
- Conclusion
  - –Although STP 3 & 4 I&C design has reduced concerns with CMF in digital I&C systems, it incorporates diverse backup design features of the certified ABWR design with no departures.

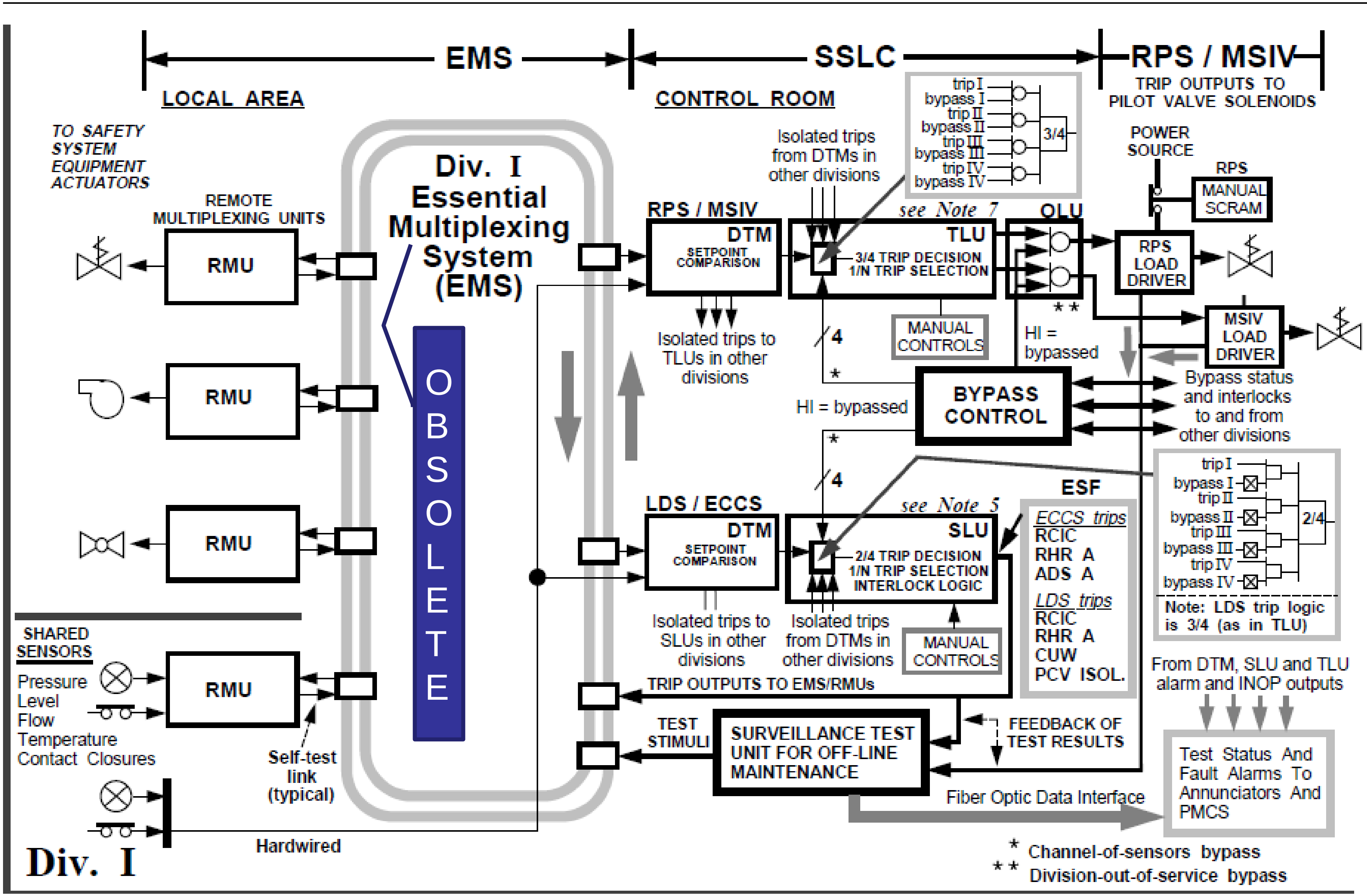
Simplicity of I&C Design

- Brief description
  - Safety system logic in the certified ABWR:
    - Uses only simple gating and interlock functions and does not require processing of complex algorithms.
    - Uses state-of-the-art program design methods to achieve highly reliable software.
    - These program design methods use simple data structures and modular, top-down programming to produce easily verifiable and testable programs that provide predictable performance.
  - STP 3 & 4 COLA incorporates by reference (IBR) this simplicity of I&C design concepts.

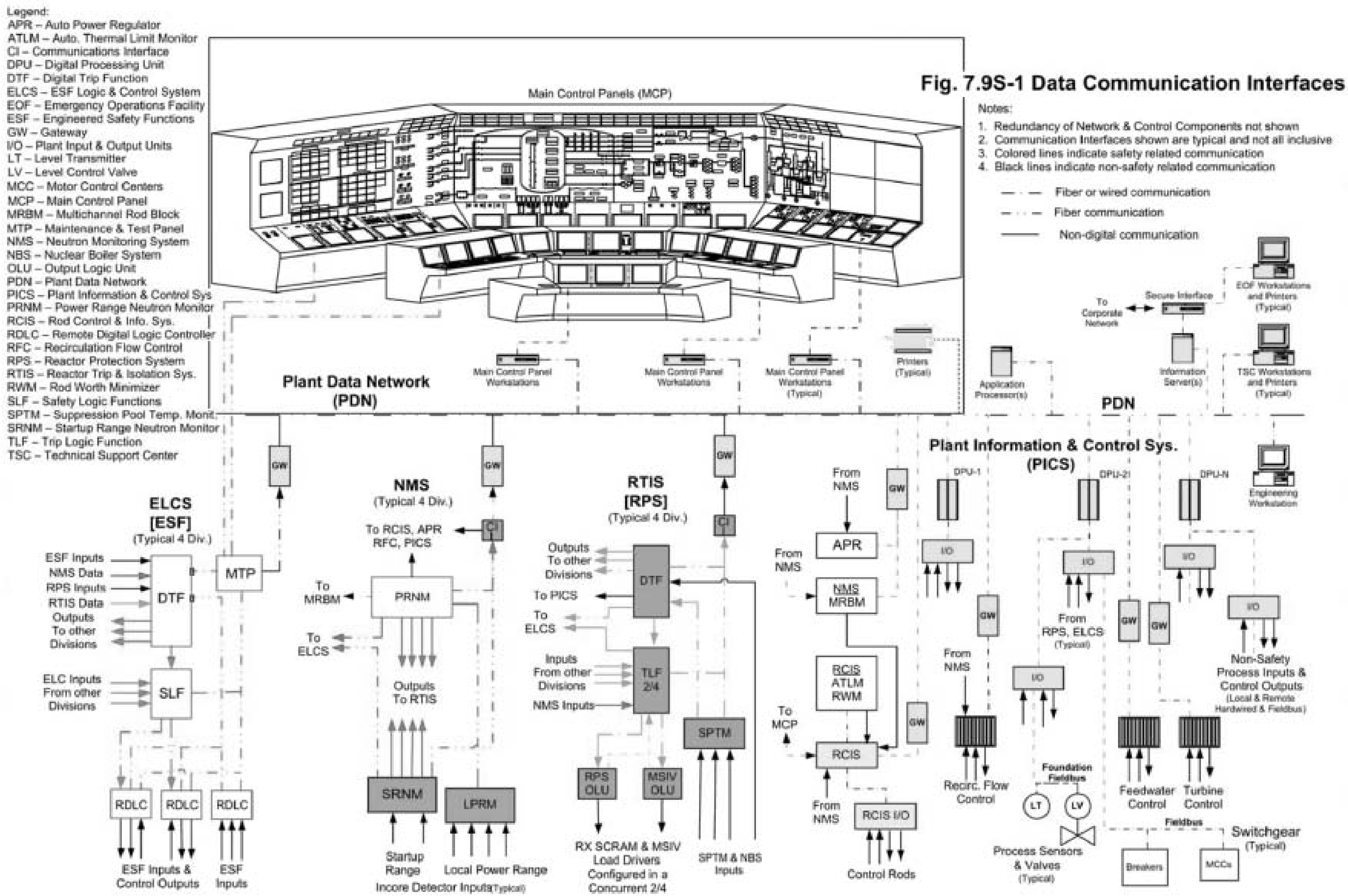
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Simplicity of I&C Design (continued)

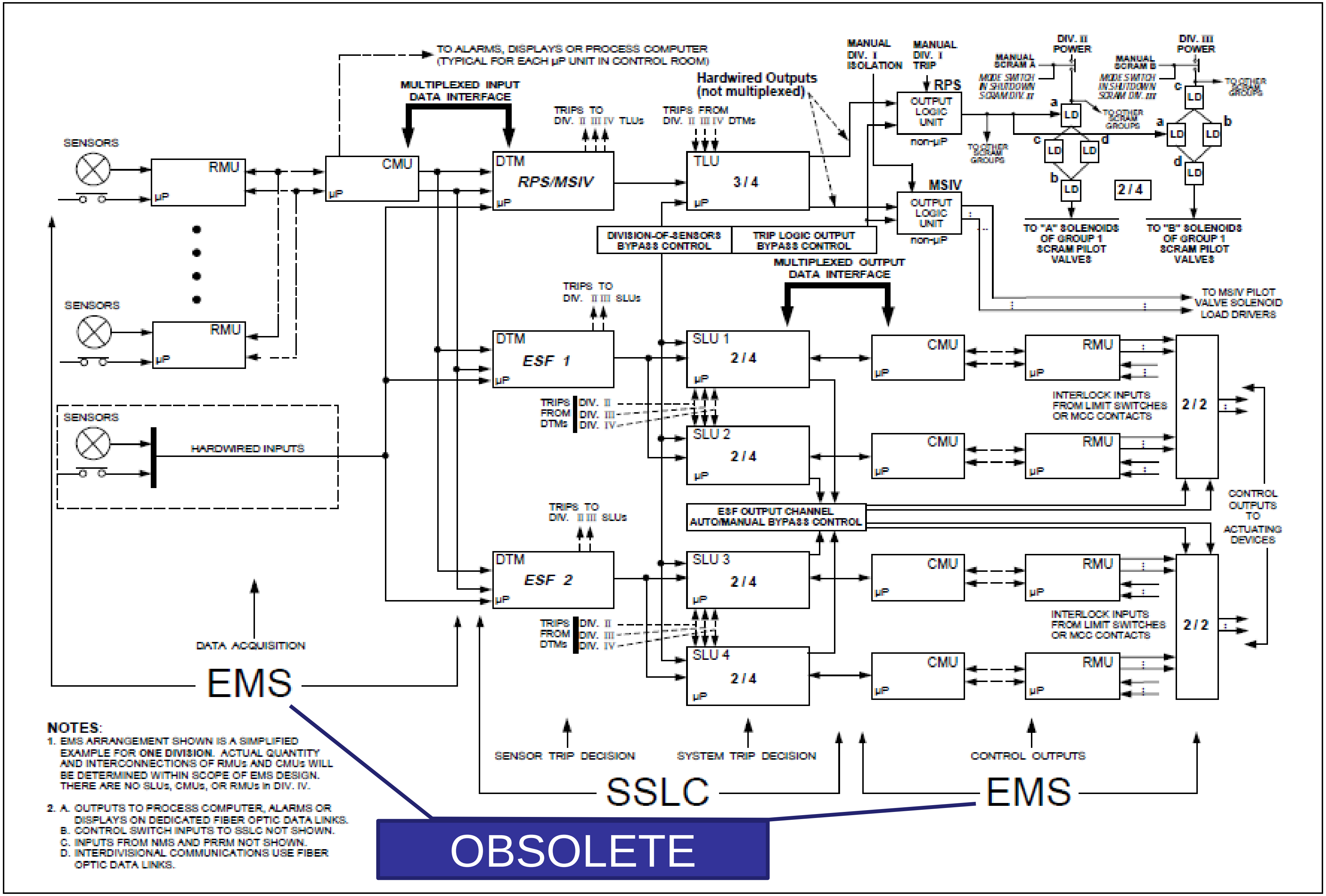
- Specific items of interest
  - Examples of simple safety system I&C design features:
    - Each SSLC division is independently controlled from a set of dedicated safety FPD (flat panel displays) in the main control room.
    - Only one-way communication is allowed from SR to NSR components.
    - Microprocessors are used for making “simple” logic decisions.
    - Software is developed as a structured set of simple modules.
    - Each module performs a prescribed task that can be independently verified and tested.
- Conclusion
  - STP 3 & 4 digital I&C design follows the philosophy of simple design employed in the certified ABWR design.



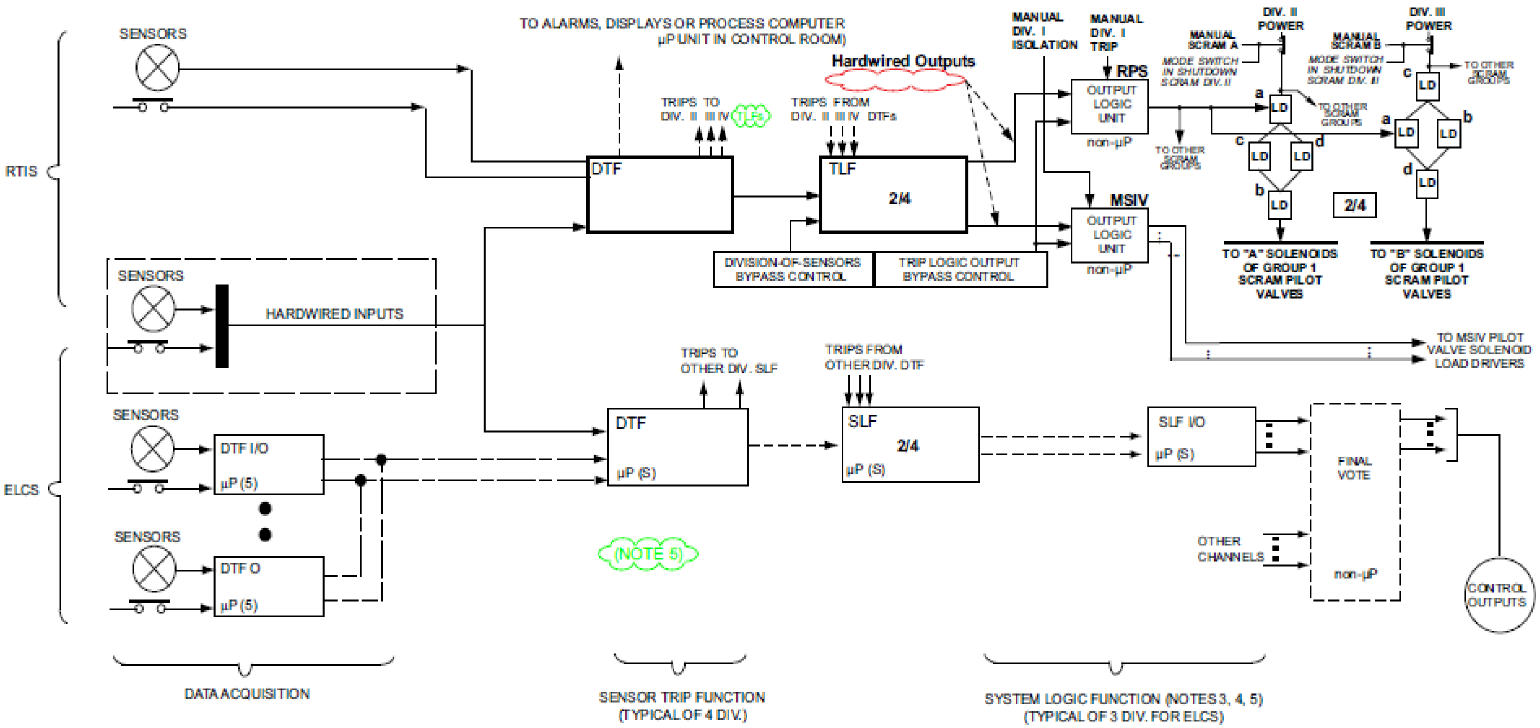
ABWR DCD Figure 7A-1 SSLC



COLA Figure 7.9S-1 Data Communication Interfaces



ABWR DCD Figure 3.4b SSLC Block Diagram



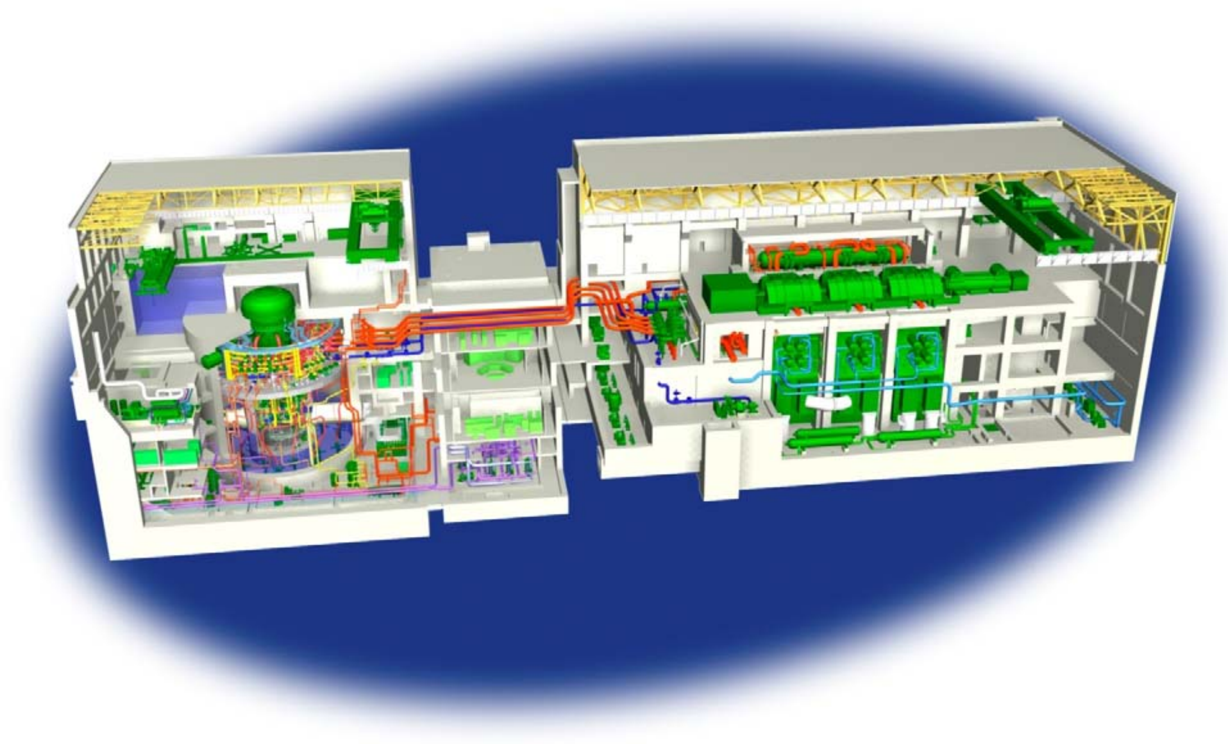
NOTES

1. ARRANGMENT SHOWN IS A SIMPLIFIED EXAMPLE FOR ONE DIVISION
2. A. NOT ALL CONTROL SWITCH INPUTS SHOWN.
   B. INPUTS FROM NMS AND PRM NOT SHOWN.
   C. INTERDIVISIONAL COMMUNICATIONS USE FIBER OPTIC DATA LINKS.
3. SAFETY SYSTEM LOGIC FUNCTION (SLF) FOR ECCS FUNCTIONS IS IMPLEMENTED WITH REDUNDANT CHANNELS WITH A MINIMUM 2/2 VOTE OF THE OUTPUT SIGNALS TO PREVENT INADVERTENT COOLANT INJECTION OR DEPRESSURIZATION DUE TO SINGLE SLF ELECTRONICS FAILURE. THE OUTPUT VOTE MAY BE ACCOMPLISHED EITHER BY DIRECT VOTE OF SLF OUTPUT SIGNALS OR BY A SYSTEM VOTE WHERE BOTH VALVE AND PUMP ACTUATION IS REQUIRED TO INITIATE SYSTEM ACTION. BYPASS OF A FAILED SLF CHANNEL MAY BE PROVIDED AS LONG AS THE REMAINING OPERATIONAL CHANNELS PROVIDE A MINIMUM OF TWO SLF CHANNELS FOR ECCS FUNCTIONS.
4. SAFETY SYSTEM LOGIC FUNCTION (SLF) FOR SOME ISOLATION AND SUPPORTING ESF FUNCTIONS MAY BE IMPLEMENTED WITH REDUNDANT CHANNELS WITH A NORMAL MINIMUM 2/2 VOTE OF THE OUTPUT SIGNALS WHERE INADVERTENT ACTUATION OF THE FUNCTION MIGHT REQUIRE UNREASONABLY SHORT REPAIR TIMES TO ELIMINATE OPERATIONAL IMPACT. FOR THESE FUNCTIONS, OPERATIONAL CONTROLLED BYPASS TO ALLOW OPERATION WITH A FINAL 1/1 VOTE IS PERMITTED.
5. EACH FUNCTION MAY BE ACCOMPLISHED BY MULTIPLE PROCESSORS TO MINIMIZE THE HARDWARE AND SOFTWARE COMPLEXITY OR OPERATIONAL IMPACT OF HARDWARE FAILURES, PROVIDED THE MINIMUM REDUNDANCY OF NOTES 3 AND 4 IS MAINTAINED.

STP COLA Figure 3.4b SSLC Block Diagram

South Texas Project Units 3 & 4
ACRS ABWR Subcommittee Presentation

ACRS Action Items



Attendees

Scott Head	Regulatory Affairs Manager, NINA
Mike Murray	I&C Manager, NINA
Coley Chappell	Regulatory Affairs, NINA

Agenda: Action Items for Discussion

- (#7) Inter-channel communication and determinism for FPGA and Common-Q platform (Recap)
- (#45) Provide RAI responses regarding redundancy and diversity of turbine overspeed sensors including power supply – ITAAC very general in scope (Update)

Action Item #7 (Recap)

Address FPGA (field-programmable gate array) in more detail, e.g., inter-channel communication and determinancy. Consider application of Common Q platform, e.g., independence and determinancy.

Response: Based on 5/20/10 meeting, action item as related to FPGA is closed.

Application of Common-Q platform including independence and determinancy, and protection from corruption via data communication between divisions, were discussed with the preceding Chapter 7 presentation.

Action Item #45 (Update)

Provide RAI responses regarding redundancy and diversity of turbine overspeed sensors including power supply – ITAAC very general in scope. (Also addressed in ACRS letter 8/9/10.)

Response: On 2/2/11 NINA met with NRO staff to discuss issues related to redundancy and diversity of the turbine overspeed system. As a result, RAI responses related to SRP 10.2 will be revised, and will supersede those provided in STPNOC letter 10/15/10 (U7-C-STP-NRC-100231).

NINA will submit additional details for the STP 3 & 4 departure to use two electrical overspeed systems, to be included in the FSAR as needed to further explain how the redundancy and diversity of the overspeed systems meet the SRP acceptance criteria, and how the design will meet the ITAAC inspections and acceptance criteria.

Based on EDO letter 9/10/10, resolution will be presented with final SE with no OI.

ACRS Action Items

Questions and Comments