Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
ABWR Subcommittee Meeting

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, May 20, 2010

Work Order No.: NRC-252 Pages 1-247

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)

+ + + + +

ABWR SUBCOMMITTEE

+ + + + +

THURSDAY, MAY 20, 2010

+ + + + +

ROCKVILLE, MARYLAND

The Subcommittee convened at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., Dr. Said Abdel-Khalik, Chairman, presiding.

SUBCOMMITTEE MEMBERS PRESENT:

SAID ABDEL-KHALIK, Chair

J. SAM ARMIJO

MARIO V. BONACA

CHARLES H. BROWN, JR.

MICHAEL CORRADINI

MICHAEL T. RYAN

WILLIAM J. SHACK

JOHN D. SIEBER

JOHN W. STETKAR

NRC STAFF PRESENT:

PETER WEN, Cognizant Staff Engineer and Designated Federal Official

MARK TONACCI

GEORGE WUNDER

STACY JOSEPH

FRANK TALBOT

DINESH TANEJA

GARY HOLAHAN

ADRIAN MUNIZ

JACK ZHAO

LAURA DUDES

ED HACKETT

ALSO PRESENT:

SCOTT HEAD
STEVE CASHELL
STEVE BLOSSOM
GREG SWANNER
ED BROWN
CHRIS CREFELD
TIM HURST
AKIRA FUKUMOTO
TOSHIFUMI SATO
JAY PHELPS
CAL TENG
ERIC FREDRICKSON
BOB QUINN
JERRY MAUCK
COLEY CHAPPELL

C-O-N-T-E-N-T-S

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

8:28 a.m.

OPENING REMARKS

CHAIR ABDEL-KHALIK: The meeting will now come to order.

This is a meeting of the ABWR Subcommittee of the Advisory Committee on Reactor Safeguards. I'm Said Abdel-Khalik, chairman of the subcommittee.

ACRS members in attendance today are Jack Sieber, Charlie Brown, John Stetkar, Sam Armijo, Mike Corradini, Bill Shack, Michael Ryan and Mario Bonaca.

Mr. Peter Wen is the designated federal official for this meeting.

The NCR staff review of the STP Combined License Application is generating safety evaluation reports with open items by chapters. In our last meetings on March 2nd and 18th we discussed the COLA FSAR and the corresponding SER with open items for chapters one, four, five, eight, 11, 12, 15, 16, 17 and 18.

In today's meeting we are scheduled to discuss chapters seven and 14.

We have scheduled additional ABWR subcommittee meetings through June, followed by a meeting of the full committee in the middle of the year. the agenda goes chapter by chapter, I expect today's discussion to be issue-centric although, related to the technical issues in the COLA and the SER.

The rules for participation in today's meeting were announced in the Federal Register on May 18, 2010, for an open/closed meeting. Parts of this meeting may need to be closed to the public to protect information proprietary to Toshiba or other parties. I'm asking the NRC staff and the applicant to identify the need for closing the meeting before we enter into such discussion to verify that only people with the required clearance and need to know are present.

We have a telephone bridge line for the public and stakeholders to hear the deliberations. The line will not transmit any signal from this end during the closed portions of this meeting. Also to minimize this service the line will be kept in listen-only mode until the last 10 minutes of the meeting. At that time we will provide an opportunity to members of the public joining us through this bridge line to make a statement or provide comments.

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

We will no proceed with the meeting, and I call on Mr. Mark Tonacci of NRO to begin the presentation.

NRO/STPNOC STAFF INTRODUCTIONS

MR. TONACCI: Good morning, and thank you for hearing our presentations this morning. I have no introductory remarks. However there are a few for George Wunder the lead project manager.

MR. WUNDER: Good morning. I'm George Wunder. I'm the lead project manager for the South Texas combined license review. Today we are going to be presenting two chapters, Chapters 14 and 7. We have elected to do them in that order because we anticipate the presentation on 14 will be briefer, and because of the interest that has been generated on Chapter 7 we thought that that might expand.

There is one thing that is not on your agenda; it's kind of a late-breaking issue. Gary Holahan, our deputy office director, will be making some brief remarks. We anticipate that he'll be done here about 10:30. And so if all goes according to schedule we would like him to make those remarks just before the presentation begins on Chapter 7.

For Chapter 14 today the staff will be represented by project manager Stacy Joseph and Frank Talbot of the quality and vendor branch, and the presentation for Chapter 7 will be done by project manager Adrian Muniz and Dinesh Taneja of the INC branch.

CHAIR ABDEL-KHALIK: Thank you.

At this time I guess we will begin with the applicant's presentation. And Mr. Scott Head will begin the presentation.

INTRODUCTIONS

MR. HEAD: Good morning. Thank you for this opportunity to brief the ACRS on Chapter 14. Look forward to the discussions today.

As to the agenda, this is our standard agenda, introduction of the speakers, summary, detail and the contents, departures, pretty much our standard agenda that we have used. And then at the very end we will have a discussion, short discussion, on the flow-induced vibration with respect to Unit 3.

Participating today is Steve Blossom, our Construction, Startup and ITAAC Manager for STP 3 and 4. And Mr. Miyamoto-san from Toshiba is joining us today also. He has extensive experience in startup operations, starting up seven BWRs and three ABWRs, a crucial member of our team.

Jay Phelps is also here with us today, who's presented in the past, previous chapters, our operations manager, and Steven Cashell, who presented tech specs recently, is also with us here today.

I'm going to go ahead and turn it over to Steve.

MR. CASHELL: Thank you, chairman and members.

The summary of Chapter involves an Initial Test Program in ITAAC. The Initial Test Program includes all the testing activities conducted following completion of construction, going all the way through to the startup of commercial operations.

ITAAC defined the activities that we take to verify that the as-built system conforms with the design features and characteristics that are in the design description for that system.

Contents, Chapter 14.1 was the old PSAR information. It's no longer applicable, so we added a 14.1S for the applicable regulations and Reg Guide. 14.2 are all the test descriptions for the Initial Test Program. We supplemented that 14.2S, and we'll discuss a little bit more about 14.2S involves on a later slide.

14.3 is a Tier 1 selection criteria and processes. And 14.3 the - is a selection criteria for site-specific systems, emergency planning and security ITAAC.

The departures that we took associated with the test descriptions, there were two pages of these, but Tier 12.4-3 is the RCIC pump pump/turbine design changes. We had to change the test descriptions to accommodate all that.

Tier 12.14-1 was your hydrogen recombiner elimination, so we changed some words there.

Tier 13.4-1 is the large departure on I&C architecture and nomenclature changes. That affects about 11 different test descriptions.

4.6-1, CRD performance testing equipment. The original design had a separate pump in there to test the control rod drive. We are just going to use the control rod drive pump. That has sufficient head, and we took a departure to do that.

Standard Departure 8.3-1 is the plant medium voltage design changes from 6.9kV to 4.16 and 13.8; we had to accommodate all that. 9.1-1 is fuel storage and handling equipment changes. We are not using the same equipment that was described in the

DCD, so we have to take care of that.

9.5-1 says simply a change in the Reg Guide status for a couple of the descriptions.

11.2-1 and 11.4-1 we changed quite a bit of the liquid and solid rad waste process equipment. So we had to change the TIS (phonetic) descriptions for those. 14.2-1 is a CRD friction test at rated pressure. We have about four different ways of doing this friction test now with the fine motion control rod drive that we have, so we can now do this test at cold pressure. If it passes at cold it will pass at heated, since things come into alignment as the vessel heats up.

Then finally standard department of vendor, throughout the test descriptions, GE Hitachi, the NSSS vendor, specifically all over the place. So we changed that to a more generic NSSS vendor.

And there are these six departures, Tier 1 departures, that affect ITAAC.

Tier 12.2-1 is rod control and information system power supply testing. There is two UPS, uninterruptible power supplies, and redundant controllers. Only we can lose one and still everything should work. So we are testing one and one to make sure that it all still works.

Tier 12.4-1 we increased spent fuel cooling by adding a third RHR look, RHR-A, to the spent fuel pool, so we are testing all the connections, and making sure that all works right.

Tier 12.4-3 RCIC turbine testing, we have new RCIC pumps, and turbines, so we are testing that - or have an ITAAC for this, sorry.

Tier 12.12-1, shop testing of - oh, the DCD specified minimum and maximum voltage testing for all electrical components. We are doing a lot of that in the shop now, the minimum and maximum, and correlating that with what we find in the field. So that is a departure. But the Tier 12.14-1, hydrogen recombiner elimination, again, and our old friend, Tier 13.4-1 that affects almost everything, the I&C nomenclature, and architecture.

In doing all this we had to supplement the Chapter 14 quite a bit. We wrote a startup administrative manual that describes how we are going to do testing, and then these chapters here, 14.2S.1 is organization and training in support of the initial test program. 14.2S-1 is a first of a kind systems. 14.2S-3, overlap of the Unit 3 test program with the Unit 4 test program. 14.2S-4, testing required to be completed prior to fuel load. 14.2S-12, site-specific test descriptions. So we have several site specific tests that we had to add. And 14.3S is the selection criteria for the site-specific systems, emergency planning, and security ITAAC.

COL License Information Items, we have nine, items one, two and three are accommodated by a commitment we made to provide the site-specific pre-op and test specs six months prior to the start of the initial test program.

Item four involves two additional commitments, one to supply the pre-op test procedures, and the other to supply the startup test procedures 60 days prior to the fuel load or prior to the start of the program.

And then items 5, 6, 7, 8 and 9 are all accommodated within the startup administrative manual. And that delineates that processes that we are going to use to administer the initial test program.

For ITAAC now, there is a separate section. Section 9 contains all the ITAAC, and ITACC were scattered all throughout the DCD. However, the selection criteria is in Chapter 14.3 and 14.3S.

The selection criteria methodology that we have chosen to use, is what was provided in 14.3, so we utilizing that for all the site-specific things, and also for emergency planning and physical security hardware. And the physical security and emergency planning ITAAC, they conform with the guidance in Reg Guide 1.206.

And now I'd like to turn it over to Steve Blossom -- he is our construction/startup and ITAAC manager - to go over the implementation of the test program.

MR. BLOSSOM: Thanks, Steve.

As Scott and Steve said, I am the construction/startup and ITAAC manager. And I'll tell you a little bit about why I'm in the position that I'm in. I'm approaching 40 years experience in nuclear. I used to count the years. Now I just round it up to 40.

I've been at South Texas for 22 years on 1 and 2 until three years ago I came to the new units as maintenance manager. Outage management, I was the steam generator replacement implementation manager back in 2000 and 2002. I've done work in work control, and prior to coming to South Texas in '88 I did multiple startups. I started up a fast breeder reactor, five PWRs, two boiling water reactors, and then I did a restart at a DOE reactor at Savannah River, a K Reactor. So I never thought I'd get an opportunity to start up another one and I'm very excited about it.

The initial test program, very similar to what we did in the `70s and `80s, just divided up into very distinct phases. Construction test phase, sometimes referred to as component testing, which include things such as flushing and hydro, initial calibrations on equipment, wiring checks, initial valve stroke, initial energization. Essentially what this phase does is get the system ready for pre-op testing.

Pre-operational testing will be pre-fuel load testing to verify that the systems operate in accordance with the design. Also during that phase we will collect baseline data for use as the plant moves forward. We will run in equipment to shake it out. We will evaluate system performance on an integrated basis with respect to other systems, and then we will have a strong effort in that phase to train personnel in both engineering and operations, so that as the plant moves forward, people are equipped to operate it like that.

And then the startup test phase, that is the fuel load, the commercial ops, refuel and shut down power level testing, nuclear heat up, the NOP/NOT testing, from the 5 percent to the 100 percent plateaus, divided up into three phases, low power, mid power and high power testing, and all culminating in a warranty run, and then declaration of commercial ops.

Next slide shows how we've laid out our test program using Reg Guide 1.68 as our bases, our procedures, and organization are tailored around the same requirements as you will see in 1.68, very typical standard to what you saw back in the `70s and `80s also. And that gives us the structure that we need.

I want to talk a little bit about the startup organization with respect to you've got your EPC, engineering procurement constructor contractors, who in our case are Toshiba, Fleur, Westinghouse and Sargent & Lundy make up the engineering procurement construction team, and they are responsible - the EPC startup manager who will be a Toshiba person, Mayamoto-san (phonetic) or one of his compadres, will be responsible for the day-to-day activities in the pre-op test group. Startup, EPC startup manager will be responsible for a smooth interface between the - our plant, the STP plant staff, and the testing organizations.

We will have the Joint Test Group in place that will approve all pre-operational test procedures, test results, test exceptions, and things that occur during the pre-op testing, and in my organization STP will provide oversight throughout this process, and will also supplement the EPC organizations to get that training we need to move the personnel forward.

Next slide, turnover. The process is broken down into - we will have two distinct turnovers. The first one will be internal to the engineering and procurement and construction teams. And that will be from construction to the pre-operational test groups. They will do pre-operational testing, and then there will be a final turnover from the EPC organization to STP, pre-fuel load. So that will allow us to move forward. And we will also use some configuration of a construction completion organization to work off exceptions throughout those turnovers, but I have made it very clear that the bar is very high for exceptions; don't want to take systems like we did back in the `70s and `80s and then your construction completion effort was very painful. So I've set the bar very high, and we are going to be very very picky as to what we will take as an exception, and almost nothing in the final turnover.

Next slide talks about ITAAC and the

relationship to the initial test program. ABWR, we have 939 ITAAC, approximately 38 percent will be completed during construction, and pre-operational test phases. The completion of the ITAAC, particularly given the back -end loading, will require very close coordination between the test organization and the ITAAC completion organization, and I'm sure you remember one of my titles is also the ITAAC, so I'm - I'll be overseeing this effort as well and providing oversight.

And the bottom bullet there is the 52.99 and the 52.103(g) process. And that is the process that is tailored around any NEI 08-01, and as a project and myself the person, I've had significant input into the development of NEI 08-01, with respect to ITAAC closure and ITAAC maintenance. So I think we will be well positioned to meet our obligations with respect to ITAAC closure maintenance.

Next slide, fuel load. I'll assume the responsibility as the startup manager for fuel load and commercial ops. I will be responsible for day-to-day operations in interface between all the various organizations. At that point in time we'll have a plant ops review committee in place that will also approve test procedures in that phase, exceptions, test results. I'll provide technical direction for plant startup activities via use of test directors. But again EPC will be very involved in it; they'll be more in an advisory capacity at that point in time.

As again in an operational environment the operational staff will be under the leadership of the operation shift supervisor, and with respect to the direction of tests and data collection and all that, that will be administered out of my organization, people out in the field collecting data.

The next slide reflects Toshiba's experience with ABWR construction and initial testing. As you can see they've got three ABWR here identified. Scott introduced Miyamoto-san, in addition to starting up these three ABWRs in Japan, he has also started up seven BWRs in Japan. So Toshiba has significant experience associated with ABWR startups, and to capitalize on all this experience we have created a very comprehensive lessons learned process where we have taken NUREG-1055 and INPO and Okiluto and right now we are translating the lessons learned from the ABWR startups in Japan and loading them into our database so that we capitalize on that experience as well.

And slide #21, you see kind of an outline of the preoperational and startup test phases. Right now we are tracking to our preoperational test window is going to be approximately nine months in duration followed up by fuel load and startup testing which is seven months in duration. So a very aggressive schedule but doable.

MEMBER SIEBER: I have a question. To what extent or what separation is there between Units 1 and 2 plant organization and Unit 3 startup?

MR. BLOSSOM: The Unit 1 and 2 operations were completely separate.

MEMBER SIEBER: And management also?

MR. BLOSSOM: Yes.

MEMBER SIEBER: So basically these are independent units on a single site?

MR. BLOSSOM: Correct. Now we have interface arrangements where if we are doing work on 3 and 4 we have a process to evaluate the impacts --

MEMBER SIEBER: Impacts, right.

MR. BLOSSOM: -- on the operating units, and mitigate those. But no, the organizations are distinctly different. The only time they become common is at our chief executive office.

MEMBER SIEBER: Okay. Again, will it stay that way after commercial operation?

MR. BLOSSOM: I think that is a little bit unknown with the ownership situation. I think the ABWR, the boiling water side and the pressurized water side will be separated to some extent.

MEMBER SIEBER: Yes, you will have dual licenses.

MR. BLOSSOM: But I can't predict what the ownership of 1 and 2 and 3 and 4 will be seven years. So.

MEMBER SIEBER: Well, that is not all that complex. At site BP where we had three units with three totally different ownerships; it works.

MR. BLOSSOM: It will complement each other.

MEMBER STETKAR: Steve, thanks for the good overview. I went back to the ITAAC, especially with regard to what we are going to be talking about later today. Could you give us a - it's on slide 17 - could you give us any general idea of what fraction of those 939 ITAAC or 356 during construction and pre-op involve design acceptance criteria in particular? And I'm not talking about pipe hangers or things like that. I'm more interested in digital INC, either the reactor trip or SFAS (phonetic) functions. Because I've reads that indeed you know the process is invoking the concept of DAC in terms of the digital INC, and I was just curious how much of that is getting carried through into the ITAAC process versus closeout at the COL issuance phase.

MR. BLOSSOM: I'm not sure I know the answer with respect to percentage of the 38 percent. Perhaps Craig, would you?

MR. CASHELL: I see an audience member that knows.

MR. SWANNER: Hi, my name is Craig Swanner. I'm working with Toshiba America through NPR. I've been associated with the INC team for the last two years or so for the - I've been working with ComFerdet on the DAC effort, pilot effort here with STP.

There are - for INC there are seven design acceptance criteria specified during Section 3.4(b), and they are in table 3.4, item seven through 14. There are specifically seven through 11 are from the hardware and software development process.

MEMBER STETKAR: Those are - I'm glad you mentioned that. Those - I've read those, those tend to be programmatic. I was more interested in terms of actual verification of the design itself and how it functions.

MR. SWANNER: There are ITAAC in 3.4 which are one through six which verify the functionality of the design as installed. But the program and process ones are seven through 11.

MEMBER BROWN: So seven through 11 - yes I went through those also. They are not listed, they are just listed as ITAAC, there is no cryptic word like DAC stuck in there. So you are saying seven through which, 14?

MR. SWANNER: Seven through 14 - in NUREG 1503, ABWR DCD SER it identifies DAC for 3.4 as the ITAAC-associated with Section 3.4(b). Those are seven through - and let me correct myself - it seven through 15, not seven through 14, I am sorry.

MEMBER STETKAR: Seven through 15.

MEMBER BROWN: Okay, again I'm just reiterating John's comment. Those are very very general, and they say almost nothing. I mean I hate to be blunt, but there is just so little detail it's tough to figure out what is being verified. So there are a few other ones that are pulled out of ITAAC in Tier 1, Section 2.7.5, excuse me, and I will probably bring it up later, but I'll bring it up now. For example, when you talk about evaluating the deterministic behavior of the system, it just says that the report will be issued showing it's deterministic. That is the acceptance criteria, which is not exactly soul satisfying when you look at the pre-COL licensing determination, particularly relative to the Common Q platform, the FPGA when it is a little bit - it's different, since you have got two different platforms you are dealing with.

I guess I would have looked for a little more detail on what somebody was going to do as far as the DAC relative to timing analysis, relative to stackup or microprocessors in series, the interrelation of the event-driven communications from microprocessor to microprocessor as opposed to a fixed period. I'm just iterating that from the standpoint of design acceptance criteria this - both the FSAR and the DCD original, if you go back to where you pull out - only four sections changed when we went from the DCD to the FSAR, I think it was 3, 4, 12 and 13 or something like that, so it had some changes to it. So the rest is back in the original setup, the original plan for DAC.

So anyway you've just confirmed what I think John and I both in looking at this.

MR. BLOSSOM: A preview of the discussion this afternoon, maybe?

MEMBER BROWN: Indeed, just wanted to ask.

MEMBER STETKAR: Another question, relating to the ITAAC or pre-op testing for the digital INC or safety systems called SSLC logic control. In the pre-op test description it says something to the effect that operability of the system from input sensor to driven equipment shall be demonstrated during a series of overlap testing, and then it pulls out some examples of verification that is going to be performed. That leads me to believe that there won't be any end-to-end functional testing where you actually go out to the sensor, trip it, or insert a signal depending on which it's supposed to do, verify that indeed the signal goes through all the analog to digital processing stuff, that the digital stuff does everything that it wants to do, that the output devices function, and indeed eventually the valve opens or closes and the pump starts.

Are you going to do any of that end-to-end functional testing?

MR. BLOSSOM: My intent would be to do that.

MEMBER STETKAR: It doesn't say that you are going to do that. That's why I was asking. I see descriptions saying, well, you are going to test the intermediate stuff to make sure that the microprocessors all work, that you are going to test the analog to digital converters, you are going to check to make sure that the calibrations are correct, you are going to make sure that the equipment works given an actuation signal. But I didn't really see anything that says, you are going to make sure the whole system works.

MR. BLOSSOM: Let me take an action and get back with you on that.

MEMBER STETKAR: I'd appreciate, because it's something that --

MEMBER SIEBER: Won't that sort of happen automatically during cold functionals and hot functionals?

MEMBER STETKAR: Not necessarily. There's been examples in the existing fleet where people test bits and pieces.

MEMBER SIEBER: You have protection systems, unless you intentionally test those every track you may not get those, but the regular flood control --

MEMBER STETKAR: Oh, regular, no, but I'm talking about the protection, SFAS, reactor protection and safeguards actuation from the process sensor.

MEMBER SIEBER: You're right on that, that has to be tested.

MR. CASHELL: All surveillance requirements in the technical specifications will have to have been met when we startup, so that will cover those systems.

MEMBER STETKAR: Well, except those surveillances can be done without doing an end-to-end function.

MR. CASHELL: Well, the way we've designed our functional test is an end-to-end, and we have also specified verification of setpoint during those, so I think you will see that those particular systems will be tested.

MEMBER BROWN: Yes, but doing a setpoint check you can do with a test device or some input device or a laptop feeding into a microprocessor checking it. I mean it's a software setpoint.

MR. CASHELL: Functional software, itself is a --

MEMBER BROWN: Yes, the only thing I found when looking at this was in the original DCD section, I guess the reactor protection pre-op test, and in that particular test there is what you call a channel response time check, which goes from the process variable to the de-energized state of the SCRAM pilot valve solenoids. So I think that might be an example, is that an example of what you are looking for? That was in Chapter 14 of the original Rev. 4 of the DCD.

MEMBER STETKAR: Yes, I'm reading Chapter 14 of the --

MEMBER BROWN: Of the FSAR.

MEMBER STETKAR: Of the COL FSAR.

MEMBER BROWN: Yes, which is - but this part wasn't changed. Regardless of the change in platforms. But other than that in terms of other response, of linear responses, did anything - did everything get installed as it's supposed to? I mean did you do multiple point checks? That is not the only thing you should put in a signal, check that it trips and ends up tripping something else. I don't disagree with that. That is a good thing to do. But typically you would expect in a preoperational test if you go back through and say here is a range of inputs from the bottom of the scale to the top of the scale. All my indicators, my plant displays, all respond in a satisfactory manner. Yet that is not in this - there are very general words, proper system operation will be demonstrated.

MEMBER STETKAR: I think in particular what bothered me if you want a reference, it's Section - here we go - 14.2.12.1.11, which talks about STD or standard departure T13.4-13(b) which is engineered safety features actual system tests, so there is a reference. It says, it specifies three tests. It says setpoint validation using input simulation and automatic self-test feature. Trip logic test of SLF using input simulation and automatic self test feature, and equipment operation using input simulation or manual. That to me sounds like separate tests of the sensors, the intermediate processing logic, and input signal to the final output device separately, not in an integrated end-to-end test. And that's what I'm asking about in particular.

MR. HEAD: May I suggest that we might be able to answer that in more detail this afternoon.

CHAIR ABDEL-KHALIK: Okay, let's proceed then.

MR. HEAD: Any other questions for Steve at this point?

CHAIR ABDEL-KHALIK: Let's continue with the presentation.

MR. HEAD: Okay, then we will go to - we

just want to have a quick briefing on flow-induced vibration. Our plan here is to provide a briefing on the technical aspects in our Chapter 3 discussion that we did want to inform the ACRS that STEP had originally was going to be a non-prototype, relying on K-6 as being the prototype. As we reviewed the expectations with respect to Rev. 3 and some other questions, we've decided to designate ourself as the prototype plant in accordance with the Reg Guide 120, Rev 3. And this will involve performing STP-specific predictive analysis. We will use K-6 to form our scope and expectations, and the STP will then be a Category 1 non-prototype plan.

So the approach we'll be using will be similar to what's done for extended power uprates on operating BWRs.

CHAIR ABDEL-KHALIK: Just for reference what is the steam line velocity for this plant vis-à-vis some of the plants that have gone extended power uprates?

MR. HEAD: Do we have anyone who could answer at this point?

We may not be able to answer that, but we will get that answer I think today.

CHAIR ABDEL-KHALIK: Okay.

MR. HEAD: And certainly in the Chapter 3 briefing I would have expected us to give the answer to that.

With respect to this change that we have made, the last bullet is the deliverables there were in support of the COL review, and the dates that those will be provided, including - well, there will be a testing program that will be a part of that that the NRC will be able to witness, and the dates that are there will support our COL review schedule.

And as I said we will have a more detailed technical discussion on invocations of this change we will be able to provide in our Chapter 3 discussions.

Any questions for me at this point?

MEMBER ARMIJO: What is the experience of the steam dryers in the K-6 and K-7 units? Did they have problems that lead you to expect you might have problems with STP Unit 3?

MR. HEAD: No, sir.

MEMBER ARMIJO: So this is kind of confirmatory work?

MR. HEAD: No, this is really quite frankly a regulatory strategy for the Rev 3, the changes that came with Rev 3, between K-6, and today there were other issues with dryers that may be some of the expectations are different than they were originally envisioned when the DCD was licensed. And then overarching all of that there is the potential that we are going to do an uprate for Unit 3, and that would - it would meet its own expectations with respect to the testing program. So all of that combined together just made the idea of becoming a prototype for the rest of what we hope is an ABWR fleet, domestic fleet, it just seemed like reasonably good idea for us.

MEMBER ARMIJO: Okay, thank you.

CHAIR ABDEL-KHALIK: Now the flow-induced vibration test associated with the fuel itself, and right now you are sort of going with the GE7 fuel, and eventually you will change to a more modern fuel. Is that part of the amendment when you sort of decide to change the fuel? Is that part of the acceptance of the new fuel design?

MR. HEAD: When we do the amendment, for the fuel --

CHAIR ABDEL-KHALIK: Right.

MR. HEAD: -- then aspects of the ABWR for the current ABWR, and if we do an extended power uprate, it will have to be considered as part of that amendment if there are any aspects that have to be addressed.

I don't know if I have answered your question.

CHAIR ABDEL-KHALIK: Not quite, but we will get to that issue I guess at the appropriate time.

MEMBER BROWN: I have one other - well, one more question, anyway, whatever it leads to. In going through the list of testing, you had a table, in the old DCD, which is then amplified or modified in the FSAR based on the changes, you do have a specific reactor protection system preoperational test, it runs through a whole series of things. There are - you refer in the rest of all the text, in Chapter 7 and 8, to the ELCS, which is the Engineered Safeguards Logic Control system I think. But when I went and looked at where is the test of that overall system, there is not even - ELCS is not even used anywhere in the chapter. It is absent. So I searched and searched, could not find an equivalent test for the overall engineered safeguards system, the logic control system testing at all. Now some of those - and it's been comprised of I don't know, two hands full with various systems under various accident type scenarios. For instance under a LOCA there are a number of systems that come into play that have to play in a certain either sequence or manner based on certain signals coming in through the progress of a transient. And there is no mention of any type of testing that tests that type of an integrated beginning to end equivalency for those - an integrated application of all those various systems. They are all tested individually but not on a - sort of piece wise, and whether this is piece wise or linear or not, I don't know, but I guess what I'd be familiar with is if you had an integrated system test of the overall safeguards systems under the various accident conditions under which it is supposed to operate. Now whether it is subsumed somewhere else in the safety logic system pre-op test is another - really deals with a set of either FPGA or microprocessor based logic blocks, whether they are digital trip functions or trip logic functions, or whatever. They didn't seem to apply to the overall test. That seemed to be absent. Just an amplification of the previous discussion of the overall integrated testing.

MR. HEAD: Someone in this room I think will be able I think to address that this afternoon.

MEMBER BROWN: Okay.

CHAIR ABDEL-KHALIK: Now the models and

the analyses that will be performed to support the steam dryer qualification will be completed I see by the middle of December, and I suspect the subcommittee would like to look at those reports. So we will work with the staff on scheduling when we would have an opportunity to evaluate these reports.

(Off the record comments.)

MR. HEAD: And I think that was our presentation on Chapter 14.

CHAIR ABDEL-KHALIK: Thank you. At this time the staff will make their presentation.

STP COLA FSAR CHAPTER 14

MS. JOSEPH: Good morning. My name is Stacy Joseph, and I am project manager for the staff's review of Chapter 14 in South Text project application. I am joined today by Frank Talbot, from the Quality and Vendor Branch, who is the lead reviewer for the initial plant testing portion of Chapter 14.

In addition to Frank's contribution to Chapter 14, reviewers listed on this slide were also contributors to the technical review of this chapter.

Today we are going to be discussing the staff's review of Chapter 14 verification programs. Frank Talbot will be discussing the staff's findings in Section 14.2 which covers initial plant testing. Section 14.2's review of Tier 1 and Tier 2 departures, several COL licensing information items, and startup administration manual.

Next, I'll be discussing Sections 14.3 and 14.3S of the staff's SER. I will be discussing our review strategy for Tier 1 departures presented in Section 14.3S, and we will be presenting a summary of the ITAAC review discussed in Section 14.3 of the SER.

With that I'll turn it over to Frank.

MR. TALBOT: Hello, my name is Frank Talbot, I'm in the Quality and Vendor Branch A of the Office of New Reactors.

For STP 14.2 I reviewed the FSAR in accordance with NUREG 0800, SRP 14.2, and Reg Guide 1.206, and also in accordance with Reg Guide 1.68 and the other 18 Reg Guides that are referenced in Reg Guide 1.68.

The section 14.2 of the DCD was incorporated by reference with several departures. The staff reviewed three Tier 1 departures and 9 Tier 2 departures affecting FSAR Section 14.2, and we also reviewed COL information items and the startup administration manual. The staff issued 13 requests for additional information on STP Units 3 and 4 FSAR

Section 14.2. Next slide, please.

We had the two open item issues, and the issues related initially to STP not taking credit for Japan K-6 as the prototype plant for STP Units 3 and 4 has a nonprototype category one plant related to the flow induced vibration assessment program. Recently on April 20th, 2010, STPNOC informed the staff that STP Unit 3 would now become the prototype plant, and STP Unit 4 would be the nonprototype Category I plant.

STPNOC plans to submit revised responses to the two open items we have related to RAI 14.2-06 and 14.2-08 regarding the flow induced vibration program test abstracts. The flow induced vibration program test specs for Unit 3 prototype plant is already provided in the ABWR DCD Section 14.2 The revised flow induced vibration assessment program for STP Unit 4 which is the nonprototype category I plant will be evaluated in the STPNOC update to FSAR Sections 3.9.2 and 14.2 to identify what flow induced vibration tests are needed for Unit 4.

MEMBER BROWN: Why would they be different? I understand the prototype match, but I presume the design is the same. I mean there is no variation. So all you are looking for is a subset.

MR. TALBOT: Well, if you look at Reg

Guide 1.20 --

MEMBER BROWN: I didn't, so I'll give you the benefit of doubt.

MR. TALBOT: Yes, Reg Guide 1.20 basically specifies what you test for prototype plants. And then for a non-Category I --

MEMBER SIEBER: It's a subset.

MR. TALBOT: -- it's a subset of what it is for the prototype plants. And you don't have to do as much testing before the --

MEMBER BROWN: I understand that. I don't disagree with it. But since I'm not familiar, I hate to tell you this, but I'm not familiar with 1.2. I'm an electrical geek, not a mechanical geek.

MR. TALBOT: Right.

MEMBER BROWN: But does it bound the conditions? I mean is there some type of requirement in there that you bound the conditions, that you test endpoints or something like that, so that you at least know what you got on the beginning and at then end?

MR. TALBOT: Oh, yes, you would take your bounding conditions for the prototype plant, and then what you can take credit for on the prototype plant, or the nonprototype plant Category I there may not be as many testing requirements for the nonprototype

Category I plant to meet the guidance in Reg Guide 1.20.

MEMBER BROWN: Okay, thank you.

MEMBER ARMIJO: I'm still a little confused. By designating Unit 3 as the prototype instead of K-6 does that require that STP perform more testing than they would have done otherwise?

MR. HEAD: Yes, extensive testing.

MEMBER ARMIJO: You have made a big commitment on much more testing?

MR. HEAD: Yes, sir, we have made a very big commitment, and we feel like it's an appropriate thing to do, and will set the stage for --

MEMBER ARMIJO: Other things.

MR. HEAD: Yes.

MR. TALBOT: Scott, you may want to talk about for the dryer that you have more testing related to this information.

MR. HEAD: Yes, the predictive analysis will be extensive, and we are using previous approaches that the NRC has already reviewed, and then the analysis will obviously be confirmed as part of the testing, the pre-op testing, and then the testing throughout the startup phase, and then operational phase also. So as you look at it it's a very big commitment, and that then will set the stage for a more limited process with respect to Unit 4.

MEMBER SHACK: Have you chosen the people who will be doing the analytical model for the acoustic expectation?

MR. HEAD: You mean the predictive analysis?

MEMBER SHACK: Right.

MR. HEAD: Which company is that?

MR. HEAD: It's being led by Westinghouse. And it's similar to the AP1000 approach that has already been reviewed. So it's --

MEMBER SIEBER: And how will you establish the acceptance criteria for the prototype testing results? Are you just going to say it didn't fall apart?

MR. HEAD: Oh, no, it's much more exotic than that. The expectations will be defined with respect to stresses and --

MEMBER SIEBER: So you don't have any of that at this point? What the criteria will be, how it will be based?

MR. HEAD: I think those are really a Chapter 3 type discussion, that we will be more than prepared to do in Chapter 3. I think today was more really from a testing standpoint, sort of our coming out, that we are making this change.

MEMBER SIEBER: You got this group and they are going to do these things.

MR. HEAD: Exactly, we have large number of people who are creating this product to support the schedule that you saw in here.

MEMBER SIEBER: Well, as you can probably tell this is an area of great interest to us.

MR. HEAD: Yes, sir, and it is to us, and that is part of the reason the decision, while important and far reaching, it was relatively easy for us to do, because we recognized how important this issue is, and how much has changed since the original certified design.

MEMBER SIEBER: Correct.

CHAIR ABDEL-KHALIK: As I said earlier, we will have the opportunity to review those models once the reports are completed. Thank you.

MEMBER BROWN: Can I ask one question?

CHAIR ABDEL-KHALIK: Yes, sir.

MEMBER BROWN: You commented that you are going to use the same method or the same approach used on AP 1000, and this is an education question, so excuse me gentlemen, that's a PWR, this is a boiling water reactor, and I would think that the flow regimes, the velocities, the mechanical configuration are different. Am I right or wrong? The extrapolation of a model from a PWR to this, it's not hard?

CHAIR ABDEL-KHALIK: It's not an extrapolation.

MEMBER BROWN: Sounds like it. I don't know, when I do that in the electrical world things blow up. (Laughter)

MR. HEAD: Obviously pressures and flows and stressed will be different, but the process that you go through to get the predictive analysis has been defined, and we are in essence using that as a model to go through. And so it's really our statement that some people have been through this before, and now we are going to be repeating that is really what that says. Clearly for the ABWR the results, flows and everything else, will be different.

MEMBER BROWN: Okay, like I said it was an educational question. I'm half educated now. (Laughter)

MR. HEAD: That's better than I normally do.

MEMBER SIEBER: Well, maybe just as an

extension, and maybe this is too detailed for this stage, but steam dryers, steam separators in BWRs have been noteworthy in drawing attention to their construction and operation and durability, but the rest of the BWR internals has had a host of historical problems, a lot of which are materials related, some of which are flow related and so forth. Are you going to do anything more than has been done with the current generation of BWRs to ensure that the whole core internals will satisfy lifetime objectives for durability and performance?

MR. HEAD: I believe we will be. I mean we obviously are factoring in all the experience that you alluded to and the current, which we think is of significant benefit is that before we are operational, for pre-op testing, the Japanese plants will have continued to operate. So that is one of the - that's one of the things that we -- even though we are not using K-6 as a prototype, we clearly are going to use K-6 as both the testing and any results that come out of that in this intervening period to our advantage, and so that's close to answering your questions. Probably there will be some more detailed discussions maybe on some of those failures you are alluding we will talk about in the Chapter 3 discussion.

MEMBER SIEBER: Thank you.

MR. TALBOT: Okay, the last issue that we have is related to license conditions, next slide. And STPNOC proposed three COL commitments - proposed COL commitments to address post-COL license information items. The staff has identified that the commitments should be license conditions to meet 52.79(a)(28) and Reg Guide 1.206 Regulatory Positions.

There are five post COL license conditions for STP, ITP, as you see listed. And an RAI that we have issued to STP the staff requested that the COL applicant inform the staff as to whether these license conditions are considered appropriate to support STP Units 3 and 4, for the combined license. And that was the summary basically of 14.2. We found that the departures in the startup admin manual that they submitted to the staff were acceptable, but because of the open item, 14.26 and 14.28, related to the flow induced vibration assessment program for STP the staff cannot finalize our conclusions until we see the additional reports that STPNOC is going to submit on the docket relating to flow induced vibration assessment program.

CHAIR ABDEL-KHALIK: Thank you.

MS. JOSEPH: All right, the next section

of the staff's SER evaluates - 14.3 of the FSAR identifies the Tier 1 selection criteria and processes. This section of the FSAR is completely incorporated by reference. Chapter 14.3 of the staff's SER is basically a summary of the Tier 1 and Tier 2 departures - sorry, Tier 1 and Tier 2* departures identified in revision three of the COLA.

This section of the SER does not contain any technical evaluations, but instead simply provides a roadmap to identify where in the SER each of these Tier 1 and Tier 2* departures are evaluated.

Section 14.3S of the staff's SER evaluates the inspections test analysis and acceptance criteria proposed by FTP in Part 9 of the application. Part 9 contains changes to the design certification ITAAC. Site specific ITAAC, emergency planning ITAAC, and physical security ITAAC. There are six Tier 1 departures in Revision 3 of the COLA that affect changes to the ITAAC identified in Tier 1 chapters two and three of the DCD.

The staff reviewed changes to the ITAAC in conjunction with changes to the design in the Tier 2 chapters, and determined that the changes made to the ITAAC are consistent with the changes made to the design and are acceptable at this time. There are no open items related to design certification ITAAC for those identified in Revision 3 of the FSAR.

The site also reviewed site specific ITAAC proposed in Part 9. In general the site specific ITAAC were developed to address the interface requirements identified in Tier 1, Chapter 4, of the DCD. Evaluations of the site specific ITAAC identified on this slide are located within the evaluation of that design and in another section of the SER.

Evaluation of offsite power ITAAC, breathing air ITAAC, and structural evaluations for the site specific ITAAC are located in Section 14.3S of the FSAR.

There are two open items identified in Section 14.3S related to the structural evaluation of the site-specific ITAAC. These two open items deal with general process for - general process question for performing structural analysis ITAAC, and also there is a request for an addition of ITAAC for the diesel generator fuel oil storage.

Since publication of the SER with open items, STP has responded to the staff's request, and the staff has determined that the response has adequately addressed those concerns.

Therefore for the evaluations provided in this section of the SER, there are no open items, and the staff determined that the ITAAC will ensure that the systems perform in accordance with the design.

Finally in Part 9 of the COLA contains ITAAC for emergency planning and physical security. The emergency planning ITAAC is evaluated in Section 13.3 of the staff SER, and the evaluation for physical security ITAAC is ongoing and will be provided in the SER with no open items at a later time.

And in summary, as Frank stated, because of the open items in Chapter 14, and in the related design chapters, staff cannot finalize their conclusions at this time.

CHAIR ABDEL-KHALIK: Are there any questions for the staff? Yes, sir.

MEMBER BROWN: Yes, the other thing - I guess I wanted to just backtrack a little here, not too much though. But in going through there was a mention and I can't remember where it was in the FSAR, on cybersecurity relative to all the plant data and network or whatever it's called, that this would all be addressed later. I mean it was very very sparse, and when I looked, I would be thinking that maybe it doesn't sound like it's site specific but it appeared to me to be a big whole relative to the expectations. I mean like there has been no thought process at all. Is that true?

MR. HEAD: No, we have responded to the NRC on that I think what is there is what present at the time. We just submitted an amount of information provided to the staff about cyber security. So we could again discuss that in more detail this afternoon if you like.

MEMBER BROWN: Okay, no, that's fine, it's not a critical comment. I just noticed the absence in the listing of the ITAAC of addressing how does cyber security work. Can you attack it? Can you get past firewalls, whatever.

MR. TONACCI: This is Mark Tonacci. The cyber security reviews were postponed until later in our SER development. They are going to be done as part of Chapter 13. They aren't quite ready yet. But Chapter 13 will be coming to you I think later on this month, but that portion for cyber was deferred because of rulemaking activities in the security office. So we will look into that, but it's not going to be this cycle of SER reviews.

MEMBER BROWN: But let me backtrack again slightly, even though it is addressed there, isn't there - wouldn't there have been some need to have ITAAC associated with cyber security reflected in Chapter 14, or at least --

MR. TONACCI: I really cannot answer that. I can take that as a lookup, but they have not proposed any at this time to us, but they are not finished with their reviews either.

CHAIR ABDEL-KHALIK: We may have to revisit this.

MEMBER BROWN: That's fine. It's just an absence of information, and I couldn't find it anywhere else.

MS. JOSEPH: All the reasons for planning ITAAC is in the evaluation of Chapter 13 anyway.

MEMBER BROWN: So is that considered emergency planning, cyber security?

MS. JOSEPH: I guess not. Sorry.

(Laughter)

MEMBER BROWN: That would be a real emergency.

(Off the record comments.)

CHAIR ABDEL-KHALIK: Before we end our discussions let me just try to capture the action items. STP has an action item with regard to end-to-end functional testing.

MEMBER BROWN: Including the ELCS system which seems to be absent.

CHAIR ABDEL-KHALIK: Okay, they also provide comparison of steam line velocities versus plants that have extended power uprates. And I guess we'll work with the staff on scheduling the time the committee will hear the analyses when they are completed by the end of December?

MR. TONACCI: Yes, that will go obviously out into next year, first quarter, probably.

CHAIR ABDEL-KHALIK: Are there any other action items or open items that we need to keep track of?

MR. TONACCI: None.

CHAIR ABDEL-KHALIK: Okay, at this time we are way ahead of schedule, and rather than taking a break, if the applicant is ready, we can move on with Chapter 7, and then we will take a break at an appropriate time.

(Off the record comments.)

STP COLA FSAR CHAPTER 7

CHAIR ABDEL-KHALIK: Is the applicant ready to proceed with the presentation?

MR. HEAD: Let us do a maneuver here and

we'll be there.

CHAIR ABDEL-KHALIK: Thank you.

(Off the record comments.)

MEMBER STETKAR: Our reporter will take care of you if you don't.

MR. HEAD: Okay, we will go ahead and get started on Chapter 7. We appreciate the opportunity because there is a lot to discussion this topic.

The attendees today, myself, we have Mike Murray who has presented before on Chapter 18. Joining us also today is Kyle Dittman. Mr. Ikeda-san, vice president with TANE, Craig Swanner, you've already heard from earlier this morning. And Dr. Fukumoto-san, a senior fellow from Toshiba is here today to help us with the presentation. And Mr. Mr. Fredrickson from Westinghouse.

Also joining us today in preparation for this discussion are other people who could be available to hopefully answer questions that we will either get or that we have already received. So this is an important topic, and in preparation for this we have attempted to obviously get ready for today's presentation.

With that I'm going to turn the discussion - oh, I missed the agenda?

MR. MURRAY: Michael Murray, I'm the manager of the I&C platforms at the STP #3 and #4, thank you. If you follow through the agenda, a lot of the first up front is bookkeeping discussions of what we have changed. I think a lot of the interesting discussions I would say will be when we get into the I&C protection system basic architecture. And there are time when I say, can we hold that discussion, because what we will have there are some pictures and diagrams that we will be able to talk through some of the questions better.

So that - you may hear me say that, and I will ask your help in that.

Chapter 7 summary, we've listed a few of the sections there, the controls and instrumentation section, the control panel section, we listed it because there are a lot of changes there. That is where the demultiplex changes came from that we will describe later. And the 3.4 which is the main instrumentation and controls system for the ABWR.

The COLA incorporates by reference the ABWR DCD information, functionality and logic, that is being incorporated by reference. Departures are taken - are for incorporation of the advances in technology as well as provide clarification. We found a number of places where clarification was required to better describe the functionality of the design. Next slide.

The chapters in it is the introduction, 7.1, 7.1Sierra, which is instrumentation control platforms. 7.2, which is the reactor protection trip system, and then the 7.3 which is the engineered safety feature system. 7.4, which is the systems required for safe shutdown. 7.5, information systems important to safety. 7.6, all other instrumentation required for safety, 7.6 Sierra, interlock systems important to safety. 7.7, control systems not required for safety, and examples of those would be rod control systems, the recirc flow control system, important systems but not for safety.

7.8, the COL licensing information, diverse instrumentation and control systems which will be in 7.8Sierra, and in 7.9Sierra, data communication systems, 7Alpha, 7Bravo and 7 Charley, defense in depth, Appendix R, and implementation of hardware and software development.

We'll start into discussions on departures. We will cover some of it, will actually be repetitive as we get more detail on it. Our departures are driven - and I'll keep my paper away from the microphone there - the advances in technology are what's driving the departures. We replace the obsolete fiber distributed data interface multiplexer system.

We're using more current technologies, point to point, serial data links primarily. We've simplified the safety systems, the safety system logic control, the SSLC system. We have - with that we have done separation of the reactor trip and isolation system, and the ESF system. Original DCD had it in one complex multiplexed system. Ours is simpler than that design.

MEMBER BROWN: Okay, in nomenclature terms, trying to get this moved, SSLC means both the ELCS and the RPS, it's that whole --

MR. MURRAY: Including safety related radiation monitoring.

MEMBER BROWN: That's fine.

MR. MURRAY: The safety systems --

MEMBER BROWN: That's when you talk about - I was trying to see what the hierarchy was and what was the pyramid underneath it.

MR. MURRAY: And typically we don't talk much more about the SSLC, but that is a good picture, that is the correct picture of it, that is correct.

MEMBER BROWN: Thank you.

MR. MURRAY: Some of the changes were nomenclature changes to improve our standardization. For example the original DCD had terms that were more fitted for the platform that was being applied, like trip logic unit, which was a component within the platform. We have used some generic terms for that to facilitate standardization of that. We will use the term, trip logic function, for example.

MEMBER BROWN: I take it those are algorithms. Data comes in, and there is a function that processes data and develops the trip or something?

MR. MURRAY: The trip logic function --

MEMBER BROWN: Software.

MR. MURRAY: The voter hardware -

MEMBER BROWN: There's processing and then there is software voting?

MR. MURRAY: That's correct. And it's the function and not necessarily --

MEMBER BROWN: But implemented by software.

MR. MURRAY: That is correct, or hardware in the case of the FBGA.

So next slide. Again, advances in technology. The final platforms we selected, we then had to implement into the design. Incorporation of - we have also incorporated the generic boiling water reactor I&C enhancements, the adoption of the boiling water generically approved oscillation power range monitors, so we have incorporated that into the design.

And we had discussed at a previous meeting that we had eliminated the main steam high radiation trip and main steam isolation. That was supported by safety evaluation reports, and generic owners' group work with the staff.

Departure clarification: we did a lot of clarification in Tier 2 specifically. A couple of examples here of some clarification on the automatic depressurization system logic. It wasn't clear how the timers were being used, how they were functioning within the logic, and also the logic between for example Reactor Vessel Level 1, and the high drywell pressure. What we did there was we made sure it was clear that we were - the functional requirements that we were implementing. So we did clarification there; that's on example.

Another example in the Residual Heat Removal system, suppression pool logic was not as clear as it needed to be for what the functionality that was being done, and also residual heat removal shut down cooling, so we did clarification there of those functions that were not the primary functions but secondary functions for residual heat removal to make sure it was clear how those functions were being implemented.

MEMBER STETKAR: Mike?

MR. MURRAY: Yes, sir.

MEMBER STETKAR: We've had enough discussions in the past to know that I'm a kind of detail oriented guy. So tell me when in your presentation you'd like to discuss specific details about some of these changes. Do you want to get more into kind of an overview first, and how the --

MR. MURRAY: Why don't we get through the overview, see if we --

MEMBER STETKAR: I don't want to interrupt kind of a stream of consciousness by putting specific questions.

MR. MURRAY: Well, let's see if we can answer some of the questions as we go, and then the specifics on the change you ask, and I'll have people that can help and we'll be able to answer the questions.

MR. MURRAY: I just want to know when is

the best time to sort of start that discussion?

MR. MURRAY: I'd like to get through the technical discussions on the platforms, and I think at that point we will see if we can answer some of the questions you've got and then continue, if that is okay.

MEMBER STETKAR: No, that's fine.

MR. MURRAY: Again a little more detail on the Tier 1 departures: control system changes, input test, hardware. We had a Tier 1 departure because it impacted the Tier 1 test requirements. And rod control and information system, we read the original requirements. It made it look like the power supplies were not independent, that either power supply would take down the entire system; actually they are redundant. So we had to clarify that so that when we tested it it would be tested properly for further design, which is much more robust than I was defining the test.

Again, the deletion of the mainstream isolation closure trip, we have discussed that previously.

And then in the Tier 1, 3.4-1, and this is where we'll have a lot of discussion later, we eliminated the data communications technology, the obsolete technology, unnecessarily inadvertent ESF actuations, we'll discuss that further also, and we got that covered.

Have you got questions on that, I guess.

MEMBER STETKAR: Now is the time on that one.

MR. MURRAY: Now is the time on that one, that's correct.

MEMBER BROWN: On which one?

MR. MURRAY: This would be the second bullet which is the unnecessary inadvertent ESF logic.

MEMBER STETKAR: Detail question: how many - you call them - I can't read it with my glasses on, I can't read with my glasses off - safety system logic functions is the terminology which is used in the FSAR, SLF like Frank. I don't know whether those are microprocessors or what they are. They are little boxes on the drawing. How many of those exist in each division? Two, 20, 30?

MR. MURRAY: Ed Brown, introduce yourself, please, he'll be able to answer those detailed questions. Now this is - what we'll be answering first with Ed would be in the ELCS, or ESF logic and control system. Is that where your question comes from?

MEMBER STETKAR: Exactly, I'm interested in ELCS, that's right.

MR. BROWN: My name is Ed Brown. I work for Westinghouse.

I have 41 years of experience in nuclear power plant I&C. I am a technical adviser to the director of safety monitoring systems, and I'm assigned full time to the ELCS system for South Texas Project #3 and #4.

The question if I understand it correctly was how many safety logic functions are there within the ELCS in each division.

MEMBER STETKAR: That's correct.

MR. BROWN: Okay, the COLA describes that there is a minimum of two and they are segmented by function, low pressure injection functions, and high pressure injection functions. So there is a mode of functional diversity that is required by the COLA. We have further segmented the functions to provide for basically additional fault tolerance, so we have now six SLFs per division, and that is per each one of the three divisions of engineered safeguards. The SLFs that have very important functions like ECCS are duplicated --

MEMBER STETKAR: Let me, before we get to that, one statement you made was that the SLFs were segregated by high pressure and low pressure functions, and unfortunately the only information I have is Figures 7.1-2 in the FSAR. And it wasn't at all clear to me, looking at the actual allocation of functions on that figure that indeed they are allocated strictly between high pressure and low pressure. For example in one division I see a diesel generator start allocated to high pressure core flood, which seems to make sense because you need the diesel for that function, but in another division I don't see the diesel allocated to high pressure core flood. So I'm curious about how those allocations actually exist and whether there is a very explicit documentation of how they are actually made. Or whether there were active decisions about why some things that don't seem to be high pressure are with low pressure, and things like that. I got a little confused.

MR. MURRAY: Could we have Mr. Swanner provide more information.

MR. SWANNER: Hi, my name is Craig Swanner. I previously introduced myself.

The statement that Ed Brown is referring is in 7.1S.2, where we have a detailed description of the ELCS system, the ELCS platform. And that section has been revised, and Revision 1 to our response to RAI A7-6.

MEMBER STETKAR: I have that material here with me, and I still couldn't figure out how the high pressure and low pressure are allocated among the SLFs, because it doesn't tell me that. I have the text. I have read it.

MR. SWANNER: There is a statement in there that identifies that.

MEMBER STETKAR: It says the same words that we heard this morning. I'm looking at a drawing that doesn't seem at all clear that it supports those words. So I'm curious whether the drawing - whether I'm misinterpreting something on the drawing or whether the drawing isn't correct. I'm looking for an explicit list so that I can indeed confirm that statement that is in the text. This is sort of verifiability of something that is stated in a text with something that can indeed be checked when I'm looking at the actual functioning of the system.

MR. MURRAY: I would like to take that back after the break if we can.

MEMBER STETKAR: Take it back, because it could be some just rearranging - the drawing may not replicate what is actual, but on the other hand if the drawing does there must have been some active decisions made, and I'd like to really understand what those decisions were.

MR. MURRAY: We will discuss that at the break and we will follow that up. The question is the allocation --

MEMBER STETKAR: The question is the allocation of the high pressure versus low pressure in terms of the basic functional allocation between those redundant processors, if you want to call them that. Sorry to interrupt you. Now we can get to the redundancy of individual SLFs for a particular function, which is where you started when I interrupted.

MR. BROWN: You had I think a question. That is the topic, I wondered what the question you might have concerning that.

MEMBER STETKAR: Okay, the question I had is that looking at the - I tried to understand where the coincidence logic, if I can call it that, is applied to specific components and functions in the design, and I read through several of the RAIs and the responses, and in the technical specifications, background documentation, I was finally pointed to that, there are a set of five figures that show difference schemes of implementing coincidence logic, serial versus - two out of two coincidence logic, to prevent spurious operation of some equipment, single actuation for other things where you are apparently not so worried about spurious actuations.

I was curious about where I could find in the documentation which specific equipment is applied - to which specific equipment are each of those five different actuation schemes applied? Again, what I'm trying to do is verify something in the design that will point me to an actual logic that is applied to something that could later be verified.

And I couldn't find it. I can find it for ADS, so ADS, don't give me ADS as an example, because that is the one place where I could find it. I'm interested in other things like RCIC or specific containment isolation valves or things like that.

MR. SWANNER: This is Craig Swanner again. Did you - just a question for you - did you just look at the figures and the bases, or did you look at the text that introduces the figures as well?

MEMBER STETKAR: I did both. But the text --

MR. SWANNER: I understand.

MEMBER STETKAR: The text, again, gives

me kind of generalities, so it gives me a sort of philosophy, but it still doesn't take me down to a design. And I actually went back and looked at the functional logic diagrams as much as I could in Section 7, and for some functions I could find it, ADS is pretty clear, but obviously there has been a lot of attention paid to it. I'm worried about the rest of the safety functions.

MR. MURRAY: Well, I think the strategy was applied where we had the redundant and the voting requirements, I will admit that ADS is one, but there was also the RCIS, and high pressure core flooder. Also low pressure core flooding, those systems that could actually inject water and cause a significant plant transient. Those are the systems that got the - we did not affect the redundancy on and the voting, is that correct, Ed?

MR. BROWN: Yes, basically, just to clarify a little more, it's ECCS function. The containment isolation functions. And the functions that are not redundant do not have a - they are a failure, you almost have a degrading effect on plant operations for safety.

MEMBER STETKAR: I hear those words, I've read those words. I'm still interested in finding documentation in the FSAR. Essentially the equivalent of functional logic diagrams for the individual actuated equipment to show me where that two out of two voting versus that single point actuation is implemented. And the reason, for example, low pressure core flood is not something that I'd be particularly concerned about spuriously actuating during power operation, because it isn't going to do anything. On the other hand, if you implemented a serial two out of two coincidence logic requirement you've doubled the likelihood for failure of that function during the conditions when you need it to operate, at least as far as the availability of those SLF logic modules are concerned.

So I'm curious about what type of integrated thought process went through when you made the decisions to retain a two out of two voting logic, which as I understand the original design was strictly two out of two for everything. So you have made the decision to remove that for some functions and retain it for others, and I'm curious about what criteria were used, and I can't even infer the criteria by necessarily looking at the design because I can't see the details of the design.

MR. MURRAY: Ed, do you need time on

that, or can you handle that now?

MR. BROWN: No, I think I can elaborate now. And basically it was picking up that the very important functions, the ones that were highlighted in the DCD dealing with ECCS would remain with duplicate SLFs and two out of two redundancy. That was the design principle. The containment isolation system, because that would have an inadvertent effect on operation if that were not duplicated.

The systems that are selected for one out of one are typically ventilation type systems or of the supporting systems, some of which do not even receive an actuation signal. In HPN2 is an example. Some of the cooling water control functions, some of the - say are the less critical functions where an inadvertent actuation really wouldn't be indicating either cause plant damage or a transient that would cause or degrade safety function. That was the philosophy.

MEMBER STETKAR: Okay, I hear that philosophy, and at one level it sounds fine. I think I was asking was, where in the FSAR can I find documentation to show how it was implemented. You are talking generalities about, well, for some of the cooling water functions, and for containment isolation. I'm looking for something like a list of every safeguards actuated compound, with a reference to which of these particular logic coincidences, and there are five of them, applies. So that for example if I was looking at the design as it is finally implemented in the plant, you see where I'm going, implemented in the plant, I can actually verify that indeed that design philosophy, if I understand the design philosophy, at this stage of the licensing process and agree with the philosophy, I can actually verify that it was implemented when the plant was constructed. And at the moment I don't have that second part of the check. I can't even figure out the first part of the check at this time.

MR. MURRAY: I think we will have to take an action to get back on that, but I understand your question.

MEMBER STETKAR: Thanks, that's all I had.

MR. MURRAY: I'm glad we had a discussion on that topic. That's why I paused. Again, I'm back on slide 11, and we've covered the top two bullets. We will cover the first one in more detail later, under 3.4-1.

Clarification of the digital control

nomenclature and systems. We've done that as well as final selection of platforms. We've specified these final platforms, as well as testing and surveillance, some of the testing and surveillance changes would have been, originally there was a very complicated automatic surveillance test controller. We have simplified that. For example in the ESF logic and control system we'll do all blind testing and bypass, manually initiated automation. We are maintaining the automation, but we are not doing it continuous automated testing, it's very complex strategy with that.

And in the - yes, sir.

MEMBER BROWN: Did you - I guess I lost that, because in reading the - I thought in reading the FSAR that you had retained the end process testing, did you - I guess I lost that, because in reading the - I thought in reading the FSAR that you had retained the end process testing, certain types, and it looked like there was a restriction, in other words you weren't trying to trip things, but yet operation from input to output of a particular processor you were running a set of automated tests to see that all of its functions were performing. Now it didn't - I mean it might take a half an hour to do them, because you are going through whatever the cycles are. So I guess I don't understand your comment that you have eliminated the process testing.

MR. MURRAY: Let me clarify it then I'll have Ed give even more clarification on it. My comment was that the auto surveillance test controller function, we are not using that function.

MEMBER BROWN: In other words, a separate test?

MR. MURRAY: Yes, but we are using an automatic test function that you just understood and described.

MEMBER BROWN: There are self diagnostics within the process?

MR. MURRAY: That is correct. So Ed, why don't you make sure that Mr. Brown has the clearest picture on that.

MR. BROWN: Okay, this is Ed Brown again from Westinghouse. We have retained the online diagnostics, which gave a comprehensive fault monitoring during the operation of the system while it's online; that means it's not bypassed and it's operating at power. This extends through all of the processor modules, the communication links, and everything, including the final voting element, but it doesn't not actuate.

The self - the original self-test controller was doing signal injection, and was bypassing components during operation, and it was coordinating these tests between divisions, so to make sure that self test did occur. This type of test significantly increases the complexity of the software, significantly increases the difficulty of assuring you will not get a spurious function.

What we have done based on experience with other installations has relied on the self diagnostics for plant power operation. Then there are the technical specifications which require sets of tests to be performed at intervals.

MEMBER BROWN: Those are operator-initiated tests?

MR. BROWN: Those are technician or operator-initiated tests.

MEMBER BROWN: And the plant will be in some controlled mode of operation, shutdown or whatever.

MR. BROWN: No, the plant will be - it has to be performed online.

MEMBER BROWN: Okay, I got it. So for example where we have a fourfold redundancy of the digital trip functions, we will go to a sensor bypass and then operator will put the system in bypass, the operator must follow if there is a manual interlock to request the test mode, the bypass must be present.

Then he performs a series of automated tests for the test controller makes a test panel, and the processor associated with that, injects software signals as close to the sensor, and tests all of the logic for the DTF. That would like a Phase I. The second phase we take credit for the diagnostics between - this is what is called overlap testing. The diagnostics which run continuously on the communication link for sending data between a digital trip function and the two out of four voter.

MEMBER BROWN: That's the TLF, in other words, the trip logic function.

MR. BROWN: Well, they call it an SLF in the in the ECCS.

And then for the SLF, you would then go to an SLF bypass, you would bypass the SLF and the same signal injection into the two out of four logic in that one division would occur. The division would remain operable, and then you would test the down portion. The final test which tests the actuation of the device is performed on refueling interval basis.

There actual sensor signals are injected through multiple divisions, and components are allowed - components that can be actuated in a particular mode of operation will be actuated, but they are typically not actuated during normal plant operation.

MEMBER BROWN: Okay, I understand.

MR. MURRAY: Now the field-programmable gate array systems are similar in that we do offline testing and bypass. There is diagnostic continually running as well. And we test and check strategies for surveillance testing.

Next slide. Examples of departures for technical specifications, these departures required NRC approval. The first one there which is on the rod control and information system, it was - the reason it required the changes, there was some discussion on the bases, so that drove us to requiring NRC approval. Other than that in this departure what we did was, we clarified the functions of the rod control system as it is applied in the operating current ABWR in Japan, the rod control information system. We clarified such terms as in the design the DCD, it had single rod, rod gain, step, continuous, in and out. The current technology uses similar controls, but uses terms such as step, notch, continuous, insert, withdraw. So we aligned those terms, clarified how those functions were performed. So that was a lot of what we did with that particular departure.

And then the setpoint control program is another area where we did a standard departure as well. We implemented the approach in the ISG-08, and we elected option number three, for the setpoint control program.

There are two aspects of that, and that is the program itself as well as the setpoint methodology for it. We have listed there the documents. We've got those implementing documents prepared, and the setpoint methodology is based on a similar methodology that is used by Westinghouse in PWRs, so we looked carefully at those differences in those, and had a good understanding. We used the setpoints that are used in existing plants to do comparison of whether our results were as we expected when we went through that process, and gained confidence that the approach, the Westinghouse approach to setpoint methodology, would be suitable, and also the staff is familiar with that methodology.

Any questions on that?

CHAIR ABDEL-KHALIK: If you can tell me

when would be an appropriate point in your presentation to take a break?

MR. MURRAY: This would be a good place. I think this is a good place, because we will start getting into - not long we'll be in more detailed discussions.

CHAIR ABDEL-KHALIK: So why don't we take a break at this time. We will reconvene at 10:30.

(Whereupon at 10:10 a.m. the proceeding in the above-entitled matter went off the record and resumed at 10:28 a.m.)

CHAIR ABDEL-KHALIK: We are back in session.

Please continue.

MR. MURRAY: Okay, we had completed Slide 12 discussion of setpoint program. And Slide 13, I use the word, numerous, because instrumentation and controls as you've reviewed it, it covers a lot of areas, and that is the nature of the equipment. We had just a few of the departures listed. These are not requiring prior NRC approval. They were all addressed and reviewed in the Part 52 process, typically again for clarification of content, and advances in design. For example, one of the examples is, on the average power range monitor, and the oscillation power range monitor, the trip signals are separated. That just gave us some - it reduced the potential for inadvertent trips out of that. And just made a much simpler design. And we did that in Tier 2 changes.

MEMBER STETKAR: Is it the appropriate time to insert a long interruption on a few examples on these?

MR. MURRAY: Yes, sir , if you have questions specifically.

MEMBER STETKAR: First question I had, one of these examples for reference it's Department 7.2-2, has to do with the SCRAM - it's called SCRAM-actuating relays, but indeed the change I think is the backup SCRAM relays. And the departure as it's listed seems to describe a fundamental change in the way that those backup SCRAM relays are actuated from the drawing in the FSAR which is Figure 7.2-8, which has not changed from the design certification FSAR to the COL FSAR. Those backup SCRAM relays are shown as if I can call it a deenergized actuate, in other words the output signal from the reactor protection line deenergizes the relay, when the relay is deenergized a normally closed coil - a normally closed contact closes which in sub - which subsequently through a two out of four logic energizes the backup SCRAM solenoids. If anybody is following that.

It seems like the logic has been changed such that those relays now, the interfacing relays, are normally deenergized and the output of the reactor protection logic now energizes those relays and a normally open contact closes through a two out of four logic to energize the backup SCRAM solenoids.

Is that - first of all I want to make sure that I understand that the change actually is as I just described it.

MR. DITTMAN: I am Kyle Dittman, I supervise I&C at South Texas. This departure was as you described it. The backup ultimate rod insertion SCRAM solenoids are changed from a normally energized to normally deenergized, to spend their life and prevent --

MEMBER STETKAR: These are the relays themselves?

MR. DITTMAN: Yes, these are the coils, the actual solenoid valves will be the --

MEMBER STETKAR: Well, the solenoids, I thought the solenoids were always deenergized.

MR. DITTMAN: Okay, on the backup, in the DCD in this design they were energized.

MEMBER STETKAR: The solenoids themselves were continuously energized.

MR. DITTMAN: The ARIs were normally energized. We are changing it to normally deenergized, which is consistent with existing BWRs I used to work at here in the United States with backup ARI solenoids. Now the primary solenoids are only energized, the SCRAM solenoid valves. They will continue to be.

MEMBER STETKAR: I am not talking about the primary SCRAM, the change as I understand it is only the backup, the ARI.

MR. DITTMAN: The ARI.

MEMBER STETKAR: It's the air dump off the accumulator.

MR. DITTMAN: Dump air header blocked in blowdown.

MEMBER STETKAR: I really don't - okay. You are going to have to explain it to me again, because what you explained didn't come through in my understanding of the description of the change in the FSAR or in the departures report, and I couldn't rationalize the description of the change with the unchanged functional schematic drawing. The description in the FSAR says, if I can find the right one --

MEMBER BROWN: Are you looking at the standard departure or the FSAR?

MEMBER STETKAR: I'm trying to find me - I have too many notes, so bear with me for a second. STP 3 and 4 FSAR subsection has revised the wording of the relay logic contact status from normally closed to normally open, and clarified that the trip state is when the coil is energized. That is relay coil, it doesn't say anything about the actual SCRAM valve solenoids. I was under the impression that they had always been deenergized. This is talking about the interfacing relays that make up the two out of four coincidence logic to either energize or deenergize the solenoids, which I'm not sure what it does anymore. You were talking about a change to the solenoids themselves. This seems to be related to a change in the relays. But the drawing still shows normally closed contacts. I couldn't figure out exactly what the change was, and whether it's consistent with the drawing, and if indeed it's a change from normally a deenergized to actuate to an energize to actuate, I'm curious why that is a very simple thing that doesn't change how the system operates. Because it sounds like it changes the way the system operates. I'm kind of a PRA guy, and I'm worried about failure to open, I'm worried about what happens when I lose power for example, in the old design if I lost power I would get a signal from that one division for which I lost power. If it's now an energize to actuate, I don't get that signal. So I'm struggling to understand what that change actually is now, and even more so.

MR. DITTMAN: Maybe we can get some clarification.

MEMBER STETKAR: Do we have anybody was involved in that.

MR. MURRAY: We will get somebody --

MEMBER STETKAR: Okay, take it away for this afternoon. Maybe I can bring up another one here.

MR. DITTMAN: Let me make sure I can say it correctly.

MEMBER STETKAR: Yes, because the description seems to talk about the interfacing relays if you look at the drawing.

MR. DITTMAN: I may have been incorrect in clarifying that.

MEMBER STETKAR: The reason I was assuming that the solenoids themselves were deenergized even in the original DCD is every BWR I've seen is alternate rod insertion, is an energized to actuate.

MR. DITTMAN: It's an energize to actuate.

MEMBER STETKAR: To energize the solenoids themselves.

MR. DITTMAN: To dump their header on.

MEMBER STETKAR: That's right.

On - here is a simple one, I hope, and this one is STD departure 7.2-6. And it's simply a change in the instrumentation range for dry wall high pressure instrumentation, and the original DCD had a range of zero to 0.036 mega-pascals gauge, and for those of us who think in psig, that is zero to 5.22 psig. The change revises that range from 15.0 to 30.0 kilo-pascals gauge, which for those of us who think in psig is 2.18 to 4.35 psig.

The ABWR drywell is normally inerted, so it's normally at some pressure. Is there safety related instrumentation now that extends the pressure range available for display to the operators down to zero kilo-pascals or zero psig? In other words there used to be instrumentation that at least displayed pressure down to zero. That is important to me as an operator if I've got inerted containment that is normally pressurized to know whether I have leaks or things like that. I'd like to really know if I have positive pressure in that containment during normal operations, a lot of other issues.

MR. MURRAY: Cal, can you help us with that? You don't know the answer. Okay.

MEMBER STETKAR: So better take that. The question is, do I have safety? Since I have changed the range on the safety-related drywell pressure instrumentation that feeds into my protection logic, do I still have some type of safety-related instrumentation that provides indication to the operator down to zero pressure?

MR. MURRAY: I understand the question.

MEMBER STETKAR: The third one I had, and this one is STD Departure 7.3-9, and it has to do with shutdown cooling operation. This one I may not have fully understood the change. So you will have to help me on this.

As I understand it the original design had - let me set the stage first for context. Talking about signals to close the shutdown cooling suction valves, shutdown cooling suction valves being the suction from the reactor coolant system to the RHR, some normal RHR cooling suction valves. As I understand it the original design had a signal to close those valves on level three, and it's been retained, and it, I think, had a confirmatory signal to close those valves on Level 1, Level 1 being the safety related signal that starts low pressure injection of low pressure coolant.

The change seems to have removed the Level 1 confirmatory signal. Is that correct?

MR. DITTMAN: I don't know if I would say it was confirmatory. The change was essentially a signal from Level 3 that shut down cooling isolation valves, and the Level 1 signal was just redundant to that. It tried to shut valves already shut, so they removed that.

MEMBER STETKAR: Called a confirmatory or redundant. But there was a Level 1 signal?

MR. DITTMAN: Yes, it was, but they removed it because --

MEMBER STETKAR: In the current design if that Level 3 signal fails will I ever get low pressure injection? When level gets to Level 1? I would have in the old design. If the valve for some reason hadn't closed under the Level 3 signal.

MR. DITTMAN: If you weren't isolating all three, it would be important if more than one train failed.

MEMBER STETKAR: That is correct. My point is a designer at one time installed that Level 1 signal as a confirmatory backup because the designer apparently thought that it was really important to have low pressure injection available even if the Level 3 signal failed as a backup. A decision was made for whatever reason to remove that, and I'm curious about what is the rationale for that decision. It's a change. It was a multi-division Level 3 safety related signal in the old design. A decision has been made to remove that.

MR. MURRAY: That should be documented in our departure report. We just don't have it --

MEMBER STETKAR: Yes, I couldn't find - it's not documented. The departure report only says what you said, that the valve should already be closed from Level 3, but it should have been closed from Level 3 in the original design.

And one more just as an example. And this one I literally ran out of gas last night, so - this one is 7.3-13 is the departure and it's on the containment spray logic. Is - I got confused and I didn't have enough time to try to trace everything back - is drywall spray automatically initiated under any conditions in the current design?

MR. MURRAY: The answer is no.

MEMBER STETKAR: No? Was it in the previous design?

MR. MURRAY: No. Cal, can you help us with that? The answer is no, the previous design and current design.

MEMBER STETKAR: Fine. As I said, I ran out of gas, and there were words about manual and automatic. Thanks.

MR. MURRAY: The original certification.

MEMBER STETKAR: It was just clarifying that there is a manual override that has been changed a little bit.

MR. MURRAY: Yes, there was clarification of that. The override.

MEMBER STETKAR: This was more just a point of information, because I literally didn't have enough time to trace it. Those are enough examples. Thanks for bearing with me.

MR. MURRAY: We've got some follow up with you. We've got do we have a safety related instrument that resends zero pressure in the drywell, and also some more discussion on the normal energized, normally deenergized on the contacts for the ARI circuit as well as the discussion more on the Level 1 shutdown cooling.

MEMBER STETKAR: If we have more time later this afternoon I have more examples, but I don't want to bog down the - those are the top three or four that I came across.

CHAIR ABDEL_KHALIK: Please continue.

MR. MURRAY: Slide 14, please.

These are the COL licensing information items, cooling temperature profiles for the 1E digital equipment. We've got that addressed in ITAAC table 3.4 item 14Braveo. APRM oscillation monitor, we've included it in Section 7.2 The effects of station blackout on the heating, ventilation and air conditioning, we've got commitment tracking there, we will do an analysis on temperature rises. Electrostatic discharge, exposure of equipment and components, that's addressed by ITAAC 3.4, item 12, and that's also included in our EMC plan.

Localized heat spots in semiconductor materials for computing, that is addressed by commitment 7.8. We will do that with purchase order information as well some where appropriate will have continuous monitoring of equipment for that, and we'll be doing testing during all the factory tests.

MEMBER BROWN: I didn't understand that

too much. Are you literally talking about a chip heat, or are you talking about the physical location, and it's located in a high heat area?

MR. MURRAY: Ed is our subject matter expert somewhat on that. I think it is more localized heating in areas, chips in areas of the panel.

MEMBER SIEBER: Like for a CPU.

MEMBER BROWN: I understand CPUs, but all the stuff is fan cooled anyway, isn't it?

MR. MURRAY: Not all is fan cooled, no, sir. Some equipment is fan cooled, some is natural convection.

MEMBER BROWN: That was one of my questions that I hadn't gotten to yet.

MR. MURRAY: ELCS equipment is fan cooled, is that correct, E d? And the FPGA is convection cooled.

Are we answering your question there, or are there still questions?

MEMBER BROWN: Let me rephrase it. With all microprocessors as well as FPGAs, the more dense they get the hotter they operate. Is that the issue you are trying to address or evaluate in this application.

MR. MURRAY: Ed, can you help us?

MR. BROWN: Ed Brown from Westinghouse. Let me make one other clarification: typically the desire is, the harder you drive them functionally, they will also, there is a range of frequencies at which your clocks can operate. The higher, you get more data throughput, more bandwidth, all that good stuff, but the harder you push them the hotter they operate. So there is normally a design to push it down as low as you can and still meet the overall requirements.

MEMBER BROWN: Now I'll let you try to answer my kind of obvious question.

MR. BROWN: Okay, Ed Brown, Westinghouse. The original DCD had commitments to calculate temperature rises because the equipment had not been designed or built yet. This section now has descriptions of the type of cooling used for the systems because, for example, for ELCS, it's a well proven platform, heat dissipation is known, the clock speeds are known. The area of interest is the heat profile in the capsule added to find the ambient temperature. So what we've done for the ELCS for example is to find the external ambient consistent with the Chapter 3 analysis of the ambient condition of the drums. Then we allow for a designed temperature rise, which we then confirm during qualification testing, and they are in factory acceptance testing.

Because we are using forced air convection, we have added a temperature --

MEMBER BROWN: You just used a magic word. He said one is convection, the other one is fan cooled. I mean obviously forced cooling is convection.

MR. BROWN: Right.

MEMBER BROWN: I think one is non-fan cooled convection.

CHAIR ABDEL_KHALIK: Natural convection.

MEMBER BROWN: Natural convection.

MR. MURRAY: That is the term.

MEMBER BROWN: Okay, so the FPGAs, the LPS is going to be just natural convection. And the other ones are the forced convection.

MR. MURRAY: Forced convection.

MR. BROWN: Forced convection. And because they are forced convection, we thought it prudent to add a temperature monitoring device in each cabinet that would monitor local temperature and provide an alarm in case there was a rise that was unexpected, which could be indicative of a forced cooling problem. And that is a commitment - that commitment we are tracking there is to do those things provide those tests.

MEMBER SIEBER: And that is permanently installed?

MR. BROWN: Permanently installed, yes.

MEMBER SIEBER: Well alarmed.

MR. BROWN: Well alarmed.

MEMBER SIEBER: What is the operator supposed to do?

MR. BROWN: Well, he would send - dispatch a technician to find out -- he would go down and probably fix the failed alarm.

MR. MURRAY: That would be an alarm response procedure, and it would have the verification and notifications and responses required for that alarm. And being an engineer I would get the call.

MEMBER BROWN: Is this going to be in both the natural and the forced convection design?

MR. BROWN: No, it's in the forced convection.

MEMBER BROWN: It's only the forced?

MR. BROWN: The original DCD did not have that in because it was originally all convection cooled. So when we changed the ELCS to forced cooling, we added the temperature diagnostic.

MEMBER BROWN: As opposed to putting just two fans in?

MR. BROWN: There is more than one fan.

MEMBER BROWN: There is more than one fan? They all blow in the same direction?

MR. BROWN: Yes.

MEMBER BROWN: So they are there to assist each other?

MR. BROWN: Yes.

MEMBER BROWN: That leads to the next question: do you detect loss of a fan? In other words, are they supposed to work okay with just one fan in place, but you have two?

MR. BROWN: If there is the loss of a fan, we are not monitoring the fan itself.

MEMBER BROWN: Just the temperature?

MR. BROWN: Just the temperature in the cabinet, which is really the critical issue. Because it could also change due to unexpected ambient temperature rises due to failed cooling devices externally.

MEMBER BROWN: Okay.

MR. BROWN: So we set that limit below, well below, our qualification temperature limit so that there is a warning.

MEMBER BROWN: Okay. Glad I asked the question though. Thank you.

MR. MURRAY: Any other questions in that area?

MEMBER SIEBER: It makes you feel better.

MEMBER BROWN: It makes me feel better.

MR. MURRAY: Okay, any other questions on slide 14.

Go to slide 15. Supplement sections continued in 7.1Sierra instrument controls. What we found in this area, and the staff also addressed this in REI 07-06 was that the Tier 2 should define well what is supplied in Tier 1, and the detail that - there wasn't as much detail as was necessary to support the Tier 1 function. So we added this section, 7.1Sierra to provide that detail of the implementing platforms to support Tier 1. And we did that for the reactor trip isolation system as well as the safety-related neutron monitoring system. And we also explained that we would be implementing the - using non-rewritable Field Programmable Gate Arrays for the neutron monitoring system and reactor trip isolation system.

MEMBER BROWN: Now the RAI that you

answered provided the additional, another two or three pages over and above the two pages of very high level information in the original.

MR. MURRAY: That is correct, put more detail into the supporting information.

MEMBER BROWN: It would have been helpful if you had more drawings with more definition, because a thousand words don't integrate well. It's still hard to understand what is going on.

MEMBER STETKAR: Can I ask a question?

MR. MURRAY: On Slide 15?

MEMBER STETKAR: Finish 7.1 Sierra and then I'll ask a question.

MR. MURRAY: On 7.1Sierra, slide 16, we also clarified the - more additional information yet on the engineered safety features logic system, ELCS, provided - we provided the automatic actuation manual control operator interface descriptions, and that also explained that it provided the displays on safety related information on the other platforms. For example the reactor trip and instrumentation system and the neutron monitoring system, the operator - operations information was needed to support safety related indications goes up through the ELCS system and uses the display drivers there, division to division, not across divisions, and provides that information to the operators in the control room. And that system we explained was implemented in a microprocessor-based control system.

Any questions on slide 16?

MEMBER STETKAR: Yes, let me stop here. It's not particularly on slide 16, but part of the additional information in that section, it's under ELCS, discusses a maintenance and test panel, MTP. Could you - it's described simply as the maintenance and test panel will be used for technician surveillance, maintenance and test functions for each division. The MTP provides the means for operator or technician to change setpoints and certain remove bypasses for periodic testing and display detailed system diagnostic messages. It also notes that the MTP communication interface to the nonsafety systems provides for communication isolation to assure that data flows in a unidirectional manner from the ELCS to the nonsafety systems. Could you explain a little bit more what these MTPs are? It sounds - I first thought that they were some type of standby panel where people could perform testing and diagnostics and make changes to software and things like that, but it sounds like they are an actual online functioning system if they are porting the communications from the safety related to unsafety related parts of the instrumentation.

MR. MURRAY: That is one of the functions. That is located - Ed, again, can answer in great detail. The way you've got it pictured is correct. There are multiple functions for that particular panel, but the isolation also in that panel performs that isolation and communication safety, one way, to nonsafety, to be able to utilize the information out of the system. Ed, give us more.

MEMBER BROWN: Before he answers that, can I expand just a bit? Because when I read the stuff between the plant data network I thought - and I guess I didn't understand this well either until he asked the question - I had presumed that this was literally allowing the operator to see what somebody was doing at the maintenance test panel as opposed to the normal operational data that was sent, unidirectional, out to the consoles or other operational stations. So if you can answer that question in that context.

MR. BROWN: Yes, let me describe the general - my name is Ed Brown from Westinghouse. Let me describe the general functions of the maintenance and test panel. The system is centered on basically it is not involved in the safety actuation functions of the ELCS system. It is provided to support the safety functions. It is a safety-related system, the software safety rated, but it is not in the actuation path, and it's failure would not prevention actuation. It is continuously connected, a piece of equipment that is fully qualified. Now the maintenance and test panel, they are associated as two associated pieces of computing equipment. One is called a node box, and that node box has a display functionality for the maintenance technician. That node box also contains the interface card that allows us to speak to the external nonsafety system. We have two communications functions within ELCS, one is high speed serial link system we will talk about later that is directly supporting system actuation functions. We also have an interdivision network which is totally contained within the division that supports other safety functions that are not directly associated with the reactor trip functions.

MEMBER BROWN: You mean intradivision?

MR. BROWN: Within the division. Only within the division.

MEMBER BROWN: Okay, intra not inter? I

just wanted to make sure I understood.

MR. BROWN: Now, the status information and the diagnostic information is communicated on this intra-division network to allow it to be collected and displayed at the operator display stations in the main control board and at the maintenance and technician panel.

MEMBER BROWN: So it goes both places?

MR. BROWN: Both places. That allows the technicians to see all the alarms, to basically look and interrogate the system in a passive way. It also collects the information that is desired to be passed to the nonsafety related systems for further processing.

MEMBER BROWN: Such as?

MR. BROWN: Such as process values and the nonsafety system will do like a multiple division comparison. The nonsafety system will do things like bypass an inoperable status calculations, so the more complex calculations, especially things that you want to see done between divisions, are done in the process computer system. And that way the design is simplified. It minimizes the amount of interdivision data that is sent within a safety system. So each division has this MTP system, and it performs this function of collecting the plant data from this intradivision network, then buffers it, and then transmits it out through a separate card, unidirectionally, to the plant information control system, so that it's available for nonsafety processing. It's a design subject to buffering that it cannot receive data cross this fiber optic link, and it cannot be used as anything other than data; it cannot receive instructions and things of this nature. So it performs that buffering.

It also performs the functions that allow the operator - the operation staff to change setpoints. This requires that we have switch interlocks that are required and the support of administrative controls to access where these other functions which are alarmed in the operator's control room. And there you can enter a setpoint. It will be sent to the appropriate processor, and then it would be reported back to the technician interface on the MTP for confirmation.

MEMBER BROWN: When that's being done, the control room operator knows it's being done.

MR. BROWN: Yes.

MEMBER BROWN: I think you said that.

MR. BROWN: Yes, the program operator

knows it's being done, and that division for - it has to be a division of censored bypasses because we cannot change setpoints with the system online. So it must be bypassed for that operation.

MEMBER STETKAR: Are the bypasses enabled also in the same panel?

MR. BROWN: No, for the ABWR, the bypasses are controlled by hard switches in the control room.

MEMBER STETKAR: Okay.

MR. BROWN: The standard bypasses. If it were necessary to go through and do something extraordinary similar to what would be a wire jumper, you may be able to do that through the console depending on the function. But that is not currently a planned function for the ABWR.

MEMBER STETKAR: So if I'm hearing you correctly, although this panel provides the facility for people to input changes to setpoints, that facility must be enabled through separate switches that only exist in the control room? I'm worried about whether faults in this panel can lead to spurious input, changes to setpoints that nobody would know about this.

MEMBER BROWN: Let me, can I amplify that a little? My question to amplify, my understanding at this point is, in order to do any of these you have to manually engage a switch contact which allows access to the operation of the protection system, or the ELCS in this case, which we are talking about. Or is it online and energizes a safety switch that says, okay, start communicating in some way as opposed to a hard open contact break. If it's not called out one way or the other in either the DCD or the SER. Or at least I didn't find it.

MR. BROWN: To change any configuration which would be setpoints, the hard switch in the main control room does division of sensors bypass. You must bypass that division.

MEMBER BROWN: I understand the sensor bypass part of that, but now you have got to connect into the processor with whatever you are going to do to change the setpoint in the software.

MR. BROWN: Right.

MEMBER BROWN: Is that continuously connected and all you are doing is bypassing the sensors, or is there another contact that now connects the maintenance and test panel to that specific division's process?

MR. BROWN: The maintenance and test

panel is always connected, but the functions to change things are not enabled.

MEMBER BROWN: By what, a software block?

MR. BROWN: No, a hard switch that goes into software.

MEMBER BROWN: So there is not - it does not close that contact between the maintenance and test panel and the division cabinets.

MR. BROWN: Right, but if you don't have the division sensors bypass enabled you will not be able to update that setpoint because it can tell that that division is not bypassed.

MEMBER BROWN: I understand but the processor is connected all the time. If you had a software failure and started sending data, even if the bypass switch is not enabling it, you've got a hard connection, that's the way you phrased it.

MR. BROWN: Right.

MEMBER BROWN: So there is a data path. And yes, I agree, if you got your pressure going up and down or whatever it is you are trying to modify, you are going to have a hard time doing it. Now I've got a sensor feeding it and I've got the test panel putting in data. Which one does it believe? What kind of conflict do you get on the inputs? On the A to D converters or whatever.

MR. BROWN: Let me go through a few more steps. It takes multiple steps to change a setpoint. So it would be very unlikely that software - software doesn't really fail; it's either right or wrong. But a hardware failure or software problem to initiate setpoint change, because it takes multiple steps in the computing device. But in any case if you nonmechanistically proposed that single failure, and yes, you could fail a portion of that division, whatever setpoint we're changing. That's your one failure. You then have the four other sensor divisions, which are voted two out of three then.

MEMBER BROWN: No, I understand that, but it's not clear that you would know that that had an internal failure that started pumping data, so you can't count that - you still have to consider another failure.

MR. BROWN: That's not correct, sir.

MEMBER BROWN: I'm just gathering that, it's not clear.

MR. BROWN: When we talk about the communications later for this bus, we will discuss how the communications work.

MEMBER BROWN: Okay, that's fine.

MR. MURRAY: And the sensor bypass switch, by title, it actually bypasses the division, does it not?

MR. BROWN: It bypasses the division.

MR. MURRAY: So it's not just the sensors. I just - you were using a term, and I just wanted to make sure we are clear on that, that said, like the sensor was only being bypassed, and it actually bypasses the division.

MEMBER BROWN: No, no, that's fine, I understand that.

MR. MURRAY: Correct.

MEMBER BROWN: But if the switch doesn't get turned, and you had this other internal failure still permanently connected, you've got an output bus connection indirectly, and you can't consider that the single failure if you had an internal failure that is not protected, because you are trying to force this one channel. Now you have to - that channel may not respond, and now you've got another - now I've got two failures, after the single failure, there was an incipient failure that is not detected.

MR. MURRAY: I understood that portion of your question.

MEMBER CORRADINI: And it's not that -

you've operated that way for awhile.

MR. BROWN: We will speak to detectibility in the communications section.

CHAIR ABDEL-KHALIK: Okay, let's continue please.

MR. MURRAY: Okay, the interlock systems important to safety, that is 7.6Sierra, these sections, we added those sections to comply with Reg Guide 1.206. And it refers to information already provided, basically the information was already there, we just made the pointers to it.

7.8 Sierra, diverse instrumentation and control systems. A section was added to, again, meet the requirements of 2.206, and the Section 7C.5 had that subject material addressed, so it was again, it was required that there was a pointer.

Then data communication systems, we will also talk about these - we have a slide on the diversity that we will talk about a little bit more when we get into the technical discussions, more detailed technical discussions. But on the data communication systems, basically it describes both essential and nonessential is what was there, and we have corrected that for the data communications function which was in our departures. And includes data communication between systems and between divisions within the systems. And we will have slides that discuss that in more detail.

Any discussions?

(Pause)

MR. MURRAY: Mr. Chairman, we are getting into a transition area where we are going into the detailed discussions on what we discussed before, we will get into communications. And with that I'll turn this over to Kyle Dittman to lead that discussion.

MR. DITTMAN: My name is Kyle Dittman. I'll give you some of my background. BSEE, been in the nuclear industry for almost 22 years now. I started at Clinton Power Station in 1988, was there 10 years, I was what they called a managing employee, so I got sent to a lot of different - maintenance, quality, licensing. I became an STA, went on shift for five years as a part of the operating crew, as a shift technical adviser. And I came off shift five years and went to system engineering, and then I switched, or I actually changed and went up to Point Beach Nuclear Power Plant, and I was at Point Beach for 10 years, and I started out there as an I&C and electrical designer there. It was supposed to be just I&C. I did that for many years, and I slowly evolved into - became the I&C and electrical design supervisor before I left. And just prior to leaving Point Beach I was actually the project supervisor for different projects, project designs. That is my background.

What you are seeing here is a Japanese typical - or I shouldn't say that - it's a Japanese ABWR main control room. This is what our control room is going to be based on. We are upgrading it or changing it based on the human factors engineering that is being done. Also we are going to be incorporating operating experience from the Japanese ABWRs. We actually got feedback from the operators and stuff, so we are using that.

Also numerous or several STP people had gone over and had partaken in the simulator training that is offered over in Japan, and had provided feedback, so that type of feedback will be incorporated in this design step.

MR. MURRAY: Kyle and I both have been through the simulator training in Japan at the boiling water training center; quite beneficial.

MEMBER ARMIJO: Is that a K-6, K-7, or Hamaoka.

MR. DITTMAN: This is actually a Hamaoka 5 simulator is what you're seeing here.

MEMBER ARMIJO: That's the simulator?

MR. DITTMAN: Yes, this is actually their simulator. There have been some upgrades on this. If you would see like the K-6 simulator, the screen layouts are a little different on the front panel, the operating panel. It has split screens, and they did upgrades to the Hamaoka design. The other thing that we are incorporating in this is, also we are going to incorporate technical advances like flat panel displays and stuff like that, so there will be some differences. But the basic layout is going to be similar.

The original certified design used an essential multiplexing system for RPS and ESF systems. And ESF are essential safety functions which covers ELCS, RTIS, stuff like that, is the original term for the safety systems.

In three and four we are departing from that type of communication to more of a clear division of the safety functions. Specifically, RTS and ELCS are going to be partially independent with their own communication system. They are not going to have that one common communication per division. This simplification will help reduce the likelihood of the common cause failures. So there are advantages to that.

Also the RTIS and NMS is being implemented by FPGA platform, and ELCS is being implemented by a microprocessor-based platform, so this also reduces the probability of common - common mode type failure.

We also tried - and the whole idea is the simplification of these safety systems. So we also kept the nonsafety functions off the safety system, which Ed alluded to earlier, is like the bypass inop status determination, alarm processing, logging display, historian functions are going to be maintained on the PICS which is plant information peer system.

MEMBER BROWN: A data logging system, is that what you mean that?

MR. DITTMAN: Yes, data logging system. It's for long term history. We will be on PICS. And PICS itself is a separate and diverse microprocessor based platform from the safety systems, and PICS is our primary operator interface for operating plant normal operations.

Next slide, please.

MEMBER BROWN: Are you going to talk about that a little bit more in terms of the PICS? Are you going to talk about the PICS? You made the magic word: is your primary plant operation function --

MR. DITTMAN: I don't have any slides to talk about it more later, but if you want to talk about it now.

MEMBER BROWN: It's a nonsafety system. Therefore it is not necessarily redundant, so I'm interested in the --

MR. DITTMAN: It's not redundant but it's another diverse operating system --

MEMBER BROWN: I understand diverse just means different stuff that is used in the boxes. Do you have multiple stations which are independent within the PICS, that if any particular station fails the other ones - or is there a neck-down point when all the communications, when the operator wants to do something, has to go through one machine?

MR. MURRAY: Let me handle that. The design of PICS is a redundantly based type computer system. Each box, the boxes have redundancy. You have one box, that the function is redundant. The operator interface in the main panel, and you can see in this picture here it shows the displays in the main panel and there are some displays in the back, those displays are set up such that if one fails you can go for one right next to it and call up the same functionality and perform the same functionality from it. So we don't have where it's a direct control from that one display.

MEMBER BROWN: Well, is PICS - something has to feed the data out to all those displays. Do they all have their own feed? Do they all have their own little data processing computer that feeds each of the different display stations?

MR. MURRAY: Chris, if you will, help us with that. It's a distributed control system so it's going to do the standard --

MEMBER BROWN: Is my question clear?

MR. CREFELD: Yes. My name is Chris Crefeld, and I work for Westinghouse on the PICS system. The PICS platform is the Ovation platform which is Emerson technology, Emerson process management. The controllers on PICS, it's a distributed control system, the controllers are all redundant. The network of PICS is also redundant. And the work stations for certain critical applications are also redundant. For operator functions they are duplicated or multiple, as Kyle was explaining. There's multiple operator work stations in the main control room, and if one becomes disabled, the same functions are duplicated on another work station that the operator can access from they main control.

MEMBER BROWN: I am trying to look at the little picture down here with a couple of boxes. I see things that are called DPU-1 and DPU-2 and DPU-N. That means nonsafety based on the other little stuff in there. Now DPU-1, is that identical to DPU-2 functionally and in all operations? Does it feed certain stations?

MR. CREFELD: It's a security control system, so any operator work station can access the data from any of the controllers. So if you want to be a redundant pair of controllers that have certain plant functions assigned to them.

MEMBER BROWN: Okay, stop right there. Do they send their data out on separate buses?

MR. CREFELD: No, they --

MEMBER BROWN: So they all dump into the same bus?

MR. CREFELD: Correct.

MEMBER BROWN: So when a work station accesses DPU-1, or 2, or N, he selects that, but all the data is going through one what I would call a local area network bus?

MR. CREFELD: One redundant bus, network.

MEMBER BROWN: Okay, by redundant you mean there's two --

MR. CREFELD: Fully redundant in switches and --

MEMBER BROWN: Okay, but do you access it via - so you select the bus you go on?

I'm just trying to gain some understanding based on the lack of definitive detail in the drawings as to how you achieve the ability to not lose all of the process and control data with one thing. You say it's on the dual redundant bus, I guess that's what you're calling it, I added a word, you said it was a dual bus - what did you say?

MR. CREFELD: Fully redundant.

MEMBER BROWN: Fully redundant, and I'm trying to make it clear that those buses are separate, they run separate. Does somebody have to select the bus.

MR. CREFELD: No, it's all automatic.

MEMBER BROWN: So the bus decides whether it's working or not and shifts to another bus? You can't have data coming in - the same data coming in two places and ask the station, the work station, to figure out what you are getting. It's a decision process somewhere.

MR. MURRAY: Tim, can you help explain that, please?

MR. HURST: My name is Tim Hurst. I'm with STP. The system is designed to be fully redundant. From any point where you bring multiple signals together. It generally starts at the control processor, all the way through the network communication, and then to the work stations. Each device whether it be a control processor or a work station or a server can see both networks at all times. They can each look at and determine is there proper communication on that network. Am I communicating to the piece of equipment or finding the piece of data that I need. If not it will immediately go over and look at the other network for the data. So having the system fully redundant gives us a very high availability, and keeps all of the system - the system once it comes up will never be shut down, both in normal operation, refueling, it's designed to be modified online; because it's an important system throughout the plant life.

MEMBER BROWN: The word never is an interesting word to use. All right, I guess I'll let us go on here. It's not absolutely clear to me how this is connected. I understand the word, redundancy. It's a matter of a wiring diagram that shows that redundancy in a manner that is understandable. Right now it's just one line for everything.

MR. HURST: The diagram does not show the redundancy. Every one of the lines you see on there is redundant.

MEMBER BROWN: The DPU-1 has two redundant lines going to every work station.

MR. HURST: Essentially it does. It's not physical lines. You go into a network.

MEMBER BROWN: Okay, let's go on.

MEMBER ARMIJO: Well, Charlie, is that level of detail available now in drawings?

MEMBER BROWN: No, it's not in here, at least I didn't see it. This is even more than it's in the SR or in the DCD. So it just raised the question I looked at it. I couldn't get this out of reading the PICS discussion.

MEMBER ARMIJO: I understand the thought process. It sounds like Toshiba has got a lot more information available here from the description, from the design. I'm not quite sure, why don't we have it?

MEMBER BROWN: The interesting point is

between RTIS, NMS and the ELCS. All these feed into this common redundant bus also. So this bus has to be a pretty robust bus, and all LAN buses when you start dumping tons of information into them, you may or may not - you've got to make sure you've got the bandwidth for it. And if you run a bandwidth that gives you, I don't know, call it deterministic, but it's not because it's not on a LAN. You just don't know when the information is going to get there, and in my experience, we used to run stuff around one or two or maybe maximum of about 5 percent of the bandwidth, and for the most part, data packages don't run into each other. There is no discussion of the bandwidth or how far they loaded up in any of this discussion. It's just, a dual redundant bus, and that's about it. So it's just a concern about the nature of the bus, how it's utilized, and there is nothing that addresses it from an ITAAC or DAC standpoint, at least that I could find. So to me that is kind of an open item to make sure we got a clear picture of how all this data gets to the operators in a manner that it doesn't get conflicted.

That's all I can say.

CHAIR ABDEL-KHALIK: It's an open --

MEMBER BROWN: I would consider it open

right now to get some more information in terms of how we make sure this redundant bus actually operates, and to ensure the data gets there under some failure modes, whatever runs the buses.

MR. TONACCI: This is Mark Tonacci. I understand your questions well. What I don't quite get is, where is the nexus to safety? Where is that coming in?

MEMBER BROWN: Well, the operator has got to control something, so I guess it's a good idea for them to be able to get information.

MR. TONACCI: For economic benefit I understand completely, but for safety is where I'm coming from.

MEMBER BROWN: I guess I'm not supposed to be concerned about the operators having information available to them about what the plant looks like or the control functions? That's a safety issue to me if you don't know where the plant is.

MR. TONACCI: I wanted to make sure I understood the nexus to safety or operation of the plant.

MEMBER BROWN: Yes, operation of the plant requires knowledge of what the parameters are. If I'm off base - I thought displaying information was important.

MR. TANEJA: One piece of information that we are not paying attention to, each safety division has two operator interface consoles which are safety related and which are independent of PICS.

MEMBER BROWN: Nobody said that until you just said it. It just goes into a big bus; that's all it says.

MR. MURRAY: We are going to get there. Okay let's do some clarification here.

MEMBER BROWN: That's fine, we can go on. It just goes into a big bus, and they said they had a dual redundant thing that goes into it.

MR. MURRAY: I'd like to do some clarification then.

CHAIR ABDEL-KHALIK: Please continue.

MR. MURRAY: Let's do the clarification on this particular - when we say it does go into the plant data network into the bus, that is the signals that are used for - these same signals, the same equipment - or excuse me, statuses that are going into that bus are available in the safety related indications to the controller. In those displays that Craig is pointing out there.

MEMBER BROWN: And they are on a separate bus?

MR. MURRAY: They are on buses that are safety related.

MEMBER BROWN: So it's independent on the PICS bus?

MR. MURRAY: Absolutely.

MEMBER BROWN: Okay, why didn't you just do that?

MR. MURRAY: We didn't understood the question.

MEMBER BROWN: I thought I was asking the question, but I didn't get there. I'm sorry. I'm happy.

CHAIR ABDEL-KHALIK: Let's continue.

MR. MURRAY: And I think if we had gone through the communication processes you would have seen that. What I could have done is say this part is nonsafety. And what we are going to discuss next is RTIS and Internet safety section of the red bus in the red box, and discuss communication. This stuff right here is the PICS that we were just talking about on the nonsafety bus, which supplies for the normal operation of the plant, normal operator interface in the plant. That's where I should have added on, the safety interface to the plant comes up through these dedicated one -- you know, there's dedicated for division.

MEMBER BROWN: That's just the ELCS. The RTIS goes into this --

MR. DITTMAN: We'll get into communication in the next slide, and it does communicate and I'll show you how that works.

For RTIS it uses - this is the high level communication that RTIS uses - is RTS, NMS, they use the dedicated data links, which are deterministic. They are isolated electrically, and you use fiber optic base way to do that. They are point to point, and they use no handshaking.

MEMBER BROWN: Okay, but isolated electrically does not equal deterministic.

MR. DITTMAN: That's right.

MEMBER BROWN: Okay, just wanted to make sure.

MR. DITTMAN: They are deterministic, yes, I understand that.

MEMBER BROWN: It also doesn't make them independent.

MR. DITTMAN: I just wonder what your question --

MEMBER BROWN: We'll get into that. I'm

just saying, if you are trying to send a message, that makes them independent, it doesn't.

MR. DITTMAN: There are four types of communication paths in RTIS, and we are going to go RTIS, NMS and ELCS. The first is interdivisional, which is between divisions. It's an optical serial link to and from the other divisions. This is the two on port voters. It's one way and no handshaking, okay. This is - so this is the communication between divisions, and we are pointing out where those go. So it leaves the DTF, the digital trip functions, goes to the other divisions. You can see the 2R4 voltage that comes back into the implementing divisions for reboarding.

MR. MURRAY: It should be noted only one division is shown here.

MR. DITTMAN: Yes, this is only one division. For intra-divisional internal to the division RTIS communicates to ELCS so it can display on those screens we were just talking about the status from RTIS, so the operator will be able to see status on safety-related screens for this division. So if this is Div 1, the Div 1 ELCS screen will display the status of RTIS. And that is - that data communication is a serial link. It's optically isolated, it's one-way no handshake.

MEMBER BROWN: This shows - that's interesting - this shows an interface node box. Is there an interface node box for every division?

MR. DITTMAN: That's correct. Every division has an interface node box.

MEMBER BROWN: It depends on the ELCS node box for the RTIS communication to the operator; is that correct?

MR. DITTMAN: That is correct.

MEMBER BROWN: Okay, so RTIS - I want to say this a different way - -RTIS and ELCS do not have independent communications for their own systems to the operators? They all - each division, each RTIS division depends on a node box for each ELCS division. Even Division 4, which does not - I think it's Division 4 which is not performing --

MR. DITTMAN: There's no equipment, actually, since we only did four equipment --

MEMBER BROWN: -- the SFAS function. It doesn't do an SFAS function.

MR. DITTMAN: But it does, the RTIS 4 - Div 4 communication through the node box to ELCS for display on the panels.

MR. MURRAY: Within a division.

MR. DITTMAN: Within that division. So each division has their own panels.

MEMBER BROWN: I am listening.

MR. DITTMAN: And there are actually two safety-related panels, one in the front panel - this was in the previous slide, but the front panel then the back by the large panel display. So for each division there are two separate safety-related displays in the control room.

The next type of communication path is we have safety to nonsafety, and this is where feeds to our PICS or Plant Information Computer System, and other places. But it's optical in a serial data link to PICS is one-way no handshake. It's has the 1E and non-1E isolation.

Then the last type of communication you could have is nonsafety to safety. In this case there is no nonsafety communication to the safety division for RTIS. We don't have it.

Any other questions on this?

MEMBER BROWN: I'm not sure yet.

MR. DITTMAN: Okay, we'll go on to the next slide.

MEMBER BROWN: I don't know what message we had - I don't know whether we are there yet.

MR. MURRAY: By the time we are through with these slides you will see the big picture.

MEMBER BROWN: I am giving you some latitude here to finish these, and then I will ask my questions.

MR. MURRAY: That I think that will be perfect.

MR. DITTMAN: Okay, the next slide I wanted to talk about is the same type of communication but with NMS. In NMS there are again four types of communication that we have: interdivisional which is between divisions. In this case NMS does not communicate between divisions. It feeds its trip signals down to RTIS which does the interdivisional communication for two out of four voting.

MEMBER BROWN: Let me backtrack to this previous slide. Okay this is a picture still basically high level.

MR. DITTMAN: Yes, it's a simplified diagram for one division.

MEMBER BROWN: Very simplified.

MR. DITTMAN: Yes.

MEMBER BROWN: Okay, very simplified, there are other issues that aren't identified in it. I guess one of my questions is how does this configuration get translated into design, since it's not - the schematic, a pictorial of it, a block diagram, is not displayed in either the original DCD, it's not in the FSAR, the COL. Where does this definition get kind of locked in in terms of what the design is supposed to look like?

MEMBER SIEBER: That probably comes first.

MEMBER BROWN: No, this is how they are supposed to do the design. But it's not in --

MR. DITTMAN: This Figure 7.9S-1 is in the COLA, and what that is, you can basically take --

MEMBER BROWN: That was in Chapter 7?

MR. DITTMAN: It's in 7.9S, this figure is.

MEMBER BROWN: Not that one, I'm talking about this one.

MR. DITTMAN: That is basically taking the RTIS portion of this figure, and we added a little more detail for discussion purposes in this meeting.

MEMBER BROWN: You said it's in 7.9S?

MR. DITTMAN: This, the one that's presented right now is in 7.9S.

MR. SWANNER: This figure is slightly different than the one in the COLA because it was updated via a response to RAI 07.09-1.

MR. MURRAY: It is a docketed figure.

MR. DITTMAN: Yes, docketed in an RAI.

MEMBER BROWN: Yes, again, that one is a relatively even higher level. I'm just saying this is a breakdown of what that stuff looks like as opposed to -

MR. SWANNER: Most of the detail in this figure is on - it's almost the same level of detail. The only difference between this figure and the one shown right here is we've essentially broken out RPS and the RPS portion of RTIS and the MSID portion of RTIS.

MR. DITTMAN: The isolation logic.

MR. SWANNER: That's the major difference between those two. They are very - I'm not aware of any new communication paths shown on this that are not on 7.9S-1.

MEMBER BROWN: It's functionally more illuminating.

MR. SWANNER: I agree.

MEMBER BROWN: Because everything is not bunched in one block.

MR. SWANNER: That is right, and --

MEMBER BROWN: And it allows you to get a better picture of what four divisions look like.

MR. DITTMAN: That was the purpose of this was to try to break this up for discussion.

MEMBER BROWN: I'm just trying to say how does that get reflected - how do you end up with this in the end, that is part of the design, the DAC process, which is not very clear.

You can move on. I'm just haranguing you right now.

MR. SWANNER: One other note just on these figures, it does indicate like for safety to non-safety on this one figure, it is in green, so these green arrows, unfortunately it appears the way this got converted to a PDF that shows almost a solid line which would lead you to believe that it is hardwired, but the description over here is actually correct. It is an optical serial data link, so just to make sure that that is not confusing anyone.

MEMBER BROWN: Well, the printout shows it's dotted.

MR. SWANNER: That's good.

MR. DITTMAN: That's just the way of projecting here.

MR. SWANNER: The projection is maybe not fine enough, I don't know, but I just wanted to make sure there was no confusion.

MEMBER STETKAR: The colors are a lot more vivid in your display.

(Simultaneous speaking.)

MR. SWANNER: I understand.

MR. DITTMAN: Okay, NMS. That's back here where I left off. I did intradivisional internal, again NMS has a serial data link to ELCS which is, again, one-way no handshaking, and it supplies information to the panels in that division.

The next type of path is the safety to nonsafety. Again this leads mainly to PICS, and it's again optical serial, it's one-way, no handshaking, make sure we have the 1E to non-1E isolation.

And the last type is a nonsafety to safety. We do have one very specific nonsafety to safety communication path which is purely used for calibration functions of the ELCS LPRMS with the gain adjustment factors. And if you would go to the next slide.

MEMBER BROWN: What is MVS? In slide 22. Oh, got it.

MR. DITTMAN: It's the instrumentation.

Okay, this specific path, communication path, is a method to provide the off-the-line calibration activities that allow to transmit calibration PICS. Basically this is the same path or same calibration as the existing BWRs did, where they will run the TIPS system, get the information, it would be verified, and they would manually input it into the ELCS LPRMS to do the gain adjustment factors.

This system is going to have the capability through use of a key lock switch, because normally now when this division is operational the key lock switch blocks this through contact.

MEMBER BROWN: The calibration function?

MR. DITTMAN: This calibration function.

MEMBER BROWN: It's in a separate cabinet?

MR. DITTMAN: Well, it's --

MEMBER BROWN: Separate set of hardware? Say that again, I'm sorry I interrupted you.

MR. DITTMAN: The key lock switch is with the EPRM cabinet, EPRM equipment. So it's in that cabinet, so it blocks that signal coming into the APRs.

And the process that - there is a basic process that would be followed for this is, the division that you would be doing the calibration on you would put it in bypass, and then the next step you would take the key lock switch to enable, which would connect this communication path, and then the dataset that comes down is limited, and it's predefined, I mean it's very specific, this dataset, and it's accepted by NMS. And prior to returning that division to service, there is manual verification and acceptance at each LPRM of this data that - this calibration data, this gain adjustment, for each LPRMS its own gain adjustment factor, and it will be verified before we return. Each one will be verified for the whole division before we return it to service.

Any questions on this?

(No response)

MR. DITTMAN: Okay, then the next system I want to discuss is the communication path through the ELCS system, which is our ESF system. ELCS - and Ed Brown commented on this. There are two types of --

MEMBER BROWN: Are you every going to talk about the communication systems for the RTIs, or is it just because it's FPGA it's assumed to be okay?

MR. DITTMAN: It's FPGA, and it's all these dedicated serial data lines between all the modules. Could we back up a slide? Here. Every one of the communications between each module is a serial link between each module.

MEMBER BROWN: I'm not worried about the - what's in the intradivisional, it's the interdivisional communications.

MR. DITTMAN: Okay, between the divisions.

MEMBER BROWN: Yes.

MR. DITTMAN: Okay, it's the same type of single link to digital trip function, we send that information over to the other division for it to do two-out-of-four. So like here the other division will bring the two-out-of-four in from the other division and do a two-out-of-four.

MEMBER BROWN: Is it a continuous signal?

MR. DITTMAN: It would be data packets. Serial data link has data packets. Actually let's get Akira to help discuss this with you.

MR. FUKUMOTO: I am Akira Fukumoto. I am (Unintelligible) Eastern Nuclear (Unintelligible). And I have 20 years experience for developing of I&C systems in Japan. And let me ask you to repeat your question. You are asking is --

MEMBER BROWN: I'm trying to - let me state it again or try to. This is for the RTIS. I realize it's FPGA but you are going from the data trip function, and I understand it's burned in, hard logic, it's like combinational logic, take little circuits and you make - it's like take a hardwired computer as opposed to software controlled, but you still have to send data of some sort from division to division to accomplish the trip function. So when is that a - I already got one answer, it's a serial data link so that means there is a continuous set of data packets going over, and it's going into a preprogrammed logic, the TLS, in each of the divisions, and then that data is taken and it's voted on, and it's a hardwired voting logic. But - and I'm not an FPGA expert - but the point being, and I'll bring this up again with the ELCS system because it's different - when you send that serial data in you've got four channels. You've got you own channel feeding in, you've got three other channels feeding in, and that logic has to be processed. So you've got the data packets coming in, and if you get a corrupt data packet, okay, then it goes into the voting logic, this is my understanding of how you would do this, and little AND and OR case, okay, which may be wrong. And in that configuration when it's one single unit of little voting units or voting logic, one set of data can come in and you can possibly corrupt all three; the other three coming in.

So what I'm trying to figure out is can a corrupt data packet, okay, and now I'm not trying to deal with parity checks, checksums, or cyclic redundancy checks or anything of that nature. All that those do is say, the data that leaves the DTF is the same as the data that arrives at the TLF. It doesn't say it's good data. It doesn't say it's not data that can't compromise the entire voting logic. And on a microprocessor based system with an algorithm it very clearly can do that, in an FPGA system, I'm trying to wrap my head around, because it is a hardwired logic function, how you prevent one set of corrupt data packets from compromising every division, two out of four data configuration.

MR. FUKUMOTO: I do have some questions because I have some communication problems.

MEMBER BROWN: I speak too fast.

MR. FUKUMOTO: How do we avoid the data corruption?

MEMBER BROWN: Yes.

MR. FUKUMOTO: Between the --

MEMBER BROWN: Well, no, not prevent it. I'm assuming corrupt data arrives - in other words, the DTF for some reason, don't ask me why, it just happens, it says, here is a data packet, I'm going to send it, it's corrupt. It generates a checksum, a cyclic redundancy check, parity, whatever you use for that, it gets transmitted, it arrives at the other place, still the same, didn't get changed; it's still the same old crummy corrupt data packet. So it gets passed on through to the voting logic section. And my point being is, in the FPGA system can that corrupt data packet compromise the voting logic - because it goes to all four divisions, it goes to all three of the other divisions, so it can disable its own and it can disable all three of the others, and what I'm looking for is, can it, number one, because of the logic configuration of the chips, so I was hoping somebody could show me that, and if the answer is yes, have you taken some action to prevent that. I'm not sure what it would be, but that is my concern with the serial data issue. It's a different issue - it's the same issue in the ELCS system where it's obvious you can corrupt and block up every one of them. But in this one, in the FPGA system, it's not. So I didn't understand that. I couldn't get it out of here when it talks about compromise of independence. Because it only said, number one, I'm isolated, and I can do parity checks or keep alive checks, that just says the line is open, or cyclic redundancy as it checks, et cetera. So that was my question.

MEMBER SIEBER: It sounds like you want to know how do you detect?

MEMBER BROWN: No, I want to know if the data packet arrives and it goes into the voting logic, can it corrupt and stop the voting logic in the division from operating?

CHAIR ABDEL-KHALIK: Let's give them a chance to answer, please.

MR. FUKUMOTO: So first of all I have to say we have some detection guidance, as you said. We can (Unintelligible) in (Unintelligible) is located in (Unintelligible), it's in the logic card. So that detects some data coming, or realize --

MEMBER BROWN: That's a different issue.

MR. FUKUMOTO: So first are you talking about here if the transmitter send across data to the receiver and it goes through all three divisions --

MEMBER BROWN: It will, yes.

MR. FUKUMOTO: -- and in that case, how can we handle, how do you detect --

MEMBER BROWN: Will it corrupt the voting logic in each other division?

MR. FUKUMOTO: That will not corrupt --

MEMBER BROWN: Now why?

MR. FUKUMOTO: You know, what do you request? The logic?

MEMBER BROWN: To stop the voting logic from operating.

MR. FUKUMOTO: Okay.

MR. MURRAY: Akira, what we need to explain is what we discussed yesterday is that if a failed signal or a corrupted or bad signal, came in to the reactor equipment isolation signal, we know that it comes in, can that affect its ability to see the other three divisions and perform its function? And that's what - that and some data swap, and we discussed that yesterday. Just go through how that communication works and how it's sensed --

MR. DITTMAN: How do we ensure that the data that comes across can't be interpreted as a command that can cause the two-out-of-four vote to do something bad?

MEMBER BROWN: To lock up, not transmit a trip.

MR. DITTMAN: How do we prevent that?

MR. FUKUMOTO: The logic FPGA in the transmission and receiving LPGA works synchronously with, independent of the clock. So it's synchronous.

MEMBER BROWN: I understand it's a

synchronous.

MR. FUKUMOTO: And so if you have a corrupt data in Division 2, and the Division 2 looks at that data, that data comes from Division 1, Division 2 - 3 treat that transmission as Division 1.

MEMBER BROWN: How does it know it's fatal?

MR. FUKUMOTO: You do a survey.

MR. SATO: Toshifumi Sato, 26 years experience, and I have been (Unintelligible). So we intentionally used the short length fixed format for the transmission.

MEMBER BROWN: Fixed what?

MR. SATO: Fixed format, format.

MEMBER BROWN: Format? Okay, thank you.

MR. SATO: So we can detect the parity error, (Unintelligible) error easily by - even by their FPGAs.

MEMBER BROWN: All that does is say, the parity checks, checksums, and all that, all that says is that the data that got sent from the DTF and the data received at the other end are identical. It doesn't mean it's good; it doesn't mean it's bad; it just says it's a packet of data. That's all it does. The question is, does it - it sends the - the DTF generates corrupt data. No good. It generates a parity bit or a checksum, or a cyclic redundancy check algorithm number. It sends it. The other side duplicates that, says, oh it's fine, passes it on through. It's going to have to because that is the nature of parity checks, checksums, so all that does - that doesn't tell anybody. Now that corrupt data that doesn't represent reality, can that bad data compromise the two-out-of-four voting logic once it gets passed on in. That is the question?

MR. FUKUMOTO: As Sato-san says, we have fixed deterministic data format in the serial bus pipe. Any of it shows which division tripped, this kind of thing. That serial data go into a hardwired LPGA buffer in the (Unintelligible), so looking at each function of (Unintelligible) and those kinds of thing those are just ones and zeroes, binary data. So just one-zero there is no --

MEMBER BROWN: Serial data is a one or a zero. A series of ones and zeroes.

MR. FUKUMOTO: So one zero means a trip or no trip or those kind of things, just a digital communication. So you can see if one turns to the other that should be corrupt data for one trip. But in that case that data fed into the trip, that is true. But in that case we saw to it, logic, trip that data as a (Unintelligible).

MEMBER BROWN: Well, if it's a one or a zero, that is just fine.

MR. FUKUMOTO: There is no volume data --

MEMBER BROWN: So there is no other combination of data that gets transmitted. Therefore when it goes in - each division feeds into its other buffer? Or is it a common buffer for all divisions? Which way? I gave you two points: one buffer for every set of data coming in from each division or --

MR. FUKUMOTO: Each signal in a data buffer.

MEMBER BROWN: Independent buffer within each TLF? So each division's TLF has an independent buffer for each set of data coming in?

MR. FUKUMOTO: That is correct.

MEMBER BROWN: And there are only two states in which the data can be exhibited in this - in the way you all are transmitting the data, as a one or a zero?

MR. FUKUMOTO: Yes.

MEMBER BROWN: And then once it gets out of the buffer it obviously goes into a series of logic.

MR. FUKUMOTO: That is correct.

MEMBER BROWN: So the only methodology under which it can fail is if you had failed logic chip or what have you which could connect across or whatever, which is a different failure mode. Okay.

CHAIR ABDEL-KHALIK: Okay, let's proceed.

MEMBER ARMIJO: I had an easier question.

MEMBER BROWN: If it would have been - I'm not going to emphasize again, the only statements made in here relative to this ability to achieve independence are, it's isolated and it's a fiber optic line; that's all. If you had provided some information or discussion as to why is it independent. That's a good point. It's not in here. I sit around for three days trying to figure out in fourteen different chapters trying to find out information, and some pictures and some discussion of that nature, makes it clear as to why - it's not the fiber optics, it's not the isolation, it's not the electrical; it has nothing to do with it. It's data independence that counts in the form of the data. I had to make a statement. I'm sorry.

MEMBER ARMIJO: My question was on your safety calibration. When you input the new calibration data and then you turn that division to service, or at least for some period of time you get two divisions operating, one with the old calibration data, one with the new calibration, how do you handle that?

MR. MURRAY: That is a technical specification. Jay.

MR. PHELPS: Calibration frequencies.

MEMBER ARMIJO: You have to come up.

Do you immediately input the new data to the other divisions?

MR. DITTMAN: Yes, typically in an IT in the operating plant - I'll let Jay in a second - is you build one division and then the next. You do one and you build the next one. I'll let Jay.

MR. PHELPS: This is Jay Phelps, I'm the operation manager on STP #3 and #4. The calibrations that they are discussing are the frequency based identified in the technical specifications. So as they specify we will, go through and do a channel calibration on the frequency identified, whatever the parameter identified in the technical specifications, and if a calibration is required in the case of the maintenance test panel, that would be usually setpoint, not being able to reach out to the actual instrument that provided that input. But if a setpoint required changes, that's how you do it, one channel at a time, return it to service, just like we do in the existing plants, if you go out and calibrate an instrument in a division you will do one of those, return it to service, do the next one, return it to service, on whatever frequency is required.

MEMBER ARMIJO: My question is --

MR. DITTMAN: Can I restate your question?

MEMBER ARMIJO: Do you understand my question?

MR. DITTMAN: Can I restate it? You are asking, I calibrated one, now I did two and did three and did four, and calibrate, how do I account for that they are now in a calibrated position that may have a little different information on it --

MEMBER ARMIJO: The system has got two sets of data for some period of time. I just wanted to make sure you understood my question.

MR. DITTMAN: And you do gain adjustment factors, and I'll go off my experience from operating an ABWR, you go on the duties, gain adjustment factors, for like Div 1. You are not going to be doing huge changes to these gain adjustment factors.

This is minor. Changes to the gain due to the burn on the detectors, the LPRM detectors. And it's done in a frequency enough that the changes aren't huge. So they did one, and once that is done and they are okay with the calibration, and they bring it back into service, there is not that much different than the other divisions. Then you move on, you would do again - all four divisions are driven by tech specs.

MEMBER ARMIJO: So you do them one right after another?

MR. DITTMAN: One right - then you move on to 2, and then you move on to 3, then 4.

MEMBER SIEBER: But things like temperature and pressure you don't do it when you are online because you have no way to vary the parameters.

MEMBER ARMIJO: No, I didn't say that.

MEMBER SIEBER: Like channel alpha q block, you bypass with a key, it's a manual operator action. Then you can get into the plant information system to change setpoints or whatever it is you want to do to check that and then return it to service by Q block.

MR. MURRAY: We are talking hours, not months. I think that is your question.

MEMBER ARMIJO: Yes, it just seems

confusing to have two sets of calibration data on independent divisions. At some point -

(Simultaneous speaking.)

MEMBER STETKAR: The fact of the matter is, we have that now. This is not different. We have that now.

CHAIR ABDEL-KHALIK: Let's continue, please.

MR. DITTMAN: Next slide, 26 I believe.

This talks about, Ed alluded to it earlier, ELCS has two types of internal communication which is the actuation communication.

MEMBER BROWN: Actually do you want me to ask the other question on the FPGA system for the RTIS before we get on to --

MR. DITTMAN: Yes.

MEMBER BROWN: Is that okay?

I guess my next question is, and again I probably need help from you gentlemen, probably, you got - the way I see this being hooked up, you have a multiple set of FPGAs, you've got a set for the DTF function, hard wired, you've got another set or another FPGA for - I'm presuming this now, it's not all in one - for the trip logic function. And then I'm trying to remember the drawing or the block diagram, I think out of the trip logic function that is an analog style signal that goes to your load drivers or something; is that correct? That's what I got out of the major block diagram.

MR. FUKUMOTO: This is Akira. I need help from Sakamoto-san. He is responsible for our RTIS engineering. But from our view --

MEMBER BROWN: After the TLF.

MR. FUKUMOTO: That one discrete signal --

MEMBER BROWN: A discrete signal.

MR. FUKUMOTO: -- transmitted by fiber.

MEMBER BROWN: That's fine, and it goes to OLU, which is an analog, but what is that, is that another FPGA?

MR. FUKUMOTO: OLU, it's a hardwire, so it's safe.

MEMBER BROWN: Okay, it's semiconductors wired -- and tell me what the OLU.

MR. FUKUMOTO: Output Logic Unit.

MEMBER BROWN: Logic Unit, right. But that -- you are now generating, that's -- you have already generated a trip, haven't you? There is an OLU in each division.

MR. FUKUMOTO: Yes.

MEMBER BROWN: But from the picture it only showed the TLF from one division feeding the OLU in one division.

MR. FUKUMOTO: Right.

MEMBER BROWN: And then the OLU, it looks like all that does is convert your one or your zero into a signal that drives the driver of some kind.

MR. FUKUMOTO: -- what is the contents of your signal transmitted from OLU to the rod driver, rod driver is not shown here, I think that is --

MEMBER BROWN: The OLU output is a state -- I'm just trying to understand -- some type of a state signal that triggers a driver. It can be optically coupled. It's given enough power to drive the actuator.

MR. FUKUMOTO: Yes.

MEMBER BROWN: Is that the output of an OLU?

MR. FUKUMOTO: Can I translate? Sorry.

MEMBER BROWN: Go ahead, keep talking.

MR. FUKUMOTO: (Speaking in Japanese.) Sorry. What you are saying is like, this is transmitted, the state signal, the trip signal, from OLU to rod driver. But the state is driven by frequency, the light frequency.

MEMBER BROWN: Fiber optic.

MR. FUKUMOTO: Frequency is very short, it's a zero --

MEMBER BROWN: It's a one or a zero.

MR. FUKUMOTO: One or zero.

MEMBER BROWN: From the OLU to the driver.

MR. FUKUMOTO: To the rod driver.

MEMBER BROWN: Okay, there is a reason for not using the TLF to do that?

MR. FUKUMOTO: We need some -- like a on-off type of state. This is a frequency high or low. So that's why we need to put it to --

MEMBER BROWN: Now that I understand that I'll ask my question, okay. My question is relative to the timing on the deterministic behavior. You make the statement that this is deterministic. You've got two FPGAs in series, each driven by a clock obviously because that's how the data gets stepped through the various logic gates. How --

MR. FUKUMOTO: You are talking about the response-time issue?

MEMBER BROWN: Well, my issue is deterministic performance of -- I mean I built from LPGS systems back in my previous existence; it's been

15 years.

(Simultaneous speaking.)

MEMBER BROWN: It's been a long time since I did some of these, and I've just forgotten the details. My previous understanding is, it was deterministic performance, but now I don't remember what, with the FPGAs, and I thought because I had -- it was both predictable and repeatable. That is my definition of deterministic behavior. And I'm trying to understand now with the multiple sets of FPGAs how do I get my timing such that I get both a predictable and a repeatable performance. I did a little reading, and my conclusion from the reading, which was not very good, is that if you don't get the timing right between FPGAs, when using them in series, that you may not get the right results; in other words you get real variability. Now am I correct with that?

MR. FUKUMOTO: Yes.

MEMBER BROWN: So my question is, how do you make that happen in the right manner and such that I can analyze and say the time response ought to be X, and when I test it I will get an X plus or minus some very small amount. How do you do that and keep it fixed? They are both operating asynchronously.

MR. FUKUMOTO: Yes.

MEMBER BROWN: Okay.

MR. FUKUMOTO: If it's your circuit or board or trip we will verify that the redundant property of it was used step by step. We built like a subroutine or software, we built a small set of our logic in LPGA, then we verify it. We call it --

MR. DITTMAN: Functional element.

MR. FUKUMOTO: -- functional element, and we test it, then afterwards, based on, we select or we collect that verified functional step into the logic. And then we verify it. That is the way we verify the result by logic in the timing of the LPGA. So in the end, after that verification we have a pretty confident data of the timing of that card. Based on that knowledge we are analyze the response of the -- each asynchronous response of each card, so in that card, when we observing response to damages it is very --each card runs asynchronously and we can know how fast it runs.

MEMBER BROWN: Okay, I got that.

MR. FUKUMOTO: So based on that knowledge, we assume the response time from the very bottom to the top, assuming the maximum time response to that. For example you can assume that two cycles for a single response time. And each cycle is very short, milliseconds' order.

MEMBER BROWN: Okay.

MR. FUKUMOTO: So --

MEMBER BROWN: Okay, so you got a clock in each FPGA and they are asynchronous, and they will vary. Do you account for the uncertainty, for the variability of the clock, as it's operating? No matter how good your clock the frequency is going to vary somewhat.

MR. FUKUMOTO: Yes, yes, we assume that but, again we verify that in the testing arena, our testing and the variation test.

MEMBER BROWN: All right, thank you, I appreciate that. That's fine, sorry.

CHAIR ABDEL-KHALIK: Okay, thank you, let's continue, please.

MR. DITTMAN: Yes, thank you.

As we talked about a little bit earlier, there are two types of communication in ELCS, specifically internal. One is the first type of communication is the actuation communication. It's unidirectional point-to-point, serial link, deterministic, isolated, and it's a dedicated single function communication links between the logic and final actuated component.

What I mean by that is, it works its way through the logic. You got the transducer, goes to the DTF, you get the digital trip function, which trips all that, which then goes directly to the two-out-of-four voter, and out of the two-out-of-four voter it goes to the system level actuation. So it's a very specific pathway for this communication.

This actuation communication is where the actual, the manual initiation like a high pressure core flood, and the auto initiation of a high pressure core flood, is actually -- this is the pathway that does that, okay.

Then there is the intra-division network, which is the division communication. It's a bus mastered network, and it is internal to each division. It is deterministic, because you use a bus master type setup. The thing is, a failure of this network will not affect the actuation communication. The actuation communication will continue to run if this network goes down. The main purpose for this network is to display the information to the operators on the flat panel displays. It also is for if the operators want to manipulate from the displays, they want to manipulate like a valve or a starter pump, shutdown pump, as communicated through this network. It also communicates the diagnostic information for ELCS, and it's connected to the maintenance panel for maintenance test support. Next slide please.

Again, I'll go through the four types of different communications for ELCS. For interdivisional, and this is between divisions again, it's again point to point, serial, deterministic, one-way, no handshake.

Intra-divisional, we just covered that. It's basically the two networks, so you got safety actuation, and then the intra-divisional network before getting to the displays, giving the displays data, stuff like that.

Then the safety and nonsafety type of communication is isolated, one way, no handshake, and basically goes through PICS, okay.

And the last type of communication is nonsafety to safety, and again in this case, in ELCS, there is no case of that. We do not communicate from nonsafety to safety in ELCS.

Any more questions?

MEMBER BROWN: It depends on how long you want to spend.

MEMBER STETKAR: Let me ask a quick one before Charley rolls out.

MEMBER BROWN: We'll be here until 2:00 o'clock.

MEMBER STETKAR: We'll hopefully get this one done before lunch. This is just kind of a mundane question. In the figure that you have there, you show a DTF RDLC, that is characterized at least on this display as an interface device with what is called ESF inputs that feed into the DTF. Can you give me an example of what those might be? I thought I understood how the system worked in terms of processing -- is -- oh, I'm sorry, I guess I'm reading that wrong, is that my actual sensor inputs coming in through that?

MR. DITTMAN: Correct.

MEMBER STETKAR: Okay, never mind. I told you it was quick.

CHAIR ABDEL-KHALIK: My intent is to break for lunch as close to 12:30 as possible. So if there is a good point to stop at this time. Or if you can finish. We can revisit those after lunch.

MEMBER BROWN: We can come back. I am happy to go on.

MR. DITTMAN: Okay, we will go on to the next slide, and come back to this.

The next area I'd like to discuss is

diversity and defense in depth, otherwise known as D3. In our case we incorporate our D3 design by reference, we did not depart from it. All the AWBR DCD diverse features have been retained including, for example, the manual reactor SCRAM, the manual switches, or the switches, the high pressure core flood Charlie, the diverse manual control, the diverse display and specific process parameters that were in DCD were retained, and the diverse hardwired controls, they go directly to the components and bypass the digital platforms.

Any questions?

MEMBER STETKAR: You say they go directly to the components, that is directly to the circuit breaker?

MR. DITTMAN: That is correct.

MEMBER STETKAR: Having not lived through them, I'm just stalling for time here to wait for Charlie, having not lived through the ABWR design certification process, is there some reason why only high pressure core flood Charlie, and I don't care about the division of high pressure cores, what I'm interested in is why only one high pressure core flood division was selected for D3, and not for example one division of low pressure core flood. And/or one division of ADS. In other words, why only the high pressure core flood function was selected

MR. DITTMAN: I understand, you are asking why that function?

MEMBER STETKAR: Why not also the ability to depressurize and get low pressure.

MR. DITTMAN: I'm going to let Cal Teng, knows D3 pretty well, so I'll let him respond to that.

MR. TENG: Yes, my name is Cal Teng. I'm with Westinghouse I&C engineering, and I did look through the ABWR certification, so I have a background I can share with you. At the time you were discussing D3 with NRC, the analysis, I think, we can read from Appendix 7 Charley, it was -- discusses the fact that NRC did not let the applicant at that time take credit for the feedwater control system, and the question is asked, what else can you offer up to have the high pressure system that can inject water into the HPCF Charley was chosen for that.

MEMBER STETKAR: But I mean basically in terms of my question, the history is that it was strictly related to diverse method of reactor SCRAM, and a diverse method for high pressure cooling without a consideration of any low pressure cooling functions. That is essentially I think whatever --

MR. TENG: In addition to the HPCF Charlie, the condensate pump was taking credit for being able to inject water in the reactor condensate pump is a relatively low pressure system. And that is taken credit for in the PRA analysis. So we basically have a low pressure condensate pump, and a high pressure safety related PCF Charlie that can --

MEMBER STETKAR: Okay, thanks.

CHAIR ABDEL-KHALIK: Next slide is conclusions, and Charlie would like to get back to slide #27, is that correct?

MEMBER BROWN: Yes.

CHAIR ABDEL-KHALIK: So and your discussion will likely take more than five minutes. So what I would like to do is break for lunch at this time, reconvene at 1:15. And we will take Charlie's discussions at that point.

(Whereupon, at 12:22 p.m., the proceeding in the above-entitled matter went off the record and resumed at 1:15 p.m.)

CHAIR ABDEL-KHALIK: We are back in session.

I guess we will get back to where we stopped on slide #27, and Charlie has some questions.

MEMBER BROWN: Okay, let me start with

the first one I guess, and this is on -- and the DTF and the SLF both consist of maybe the other SLF RDLC also, but I think I'm -- is that third one down there also a common Q platform?

MR. BROWN: Each one of those devices are built around -- each one of those boxes is built around a Common Q platform. There may be other ancillary equipment in there.

MEMBER BROWN: That's fine, the Common Q platform is the fundamental platform for the CPU process or whatever?

MR. BROWN: That is correct. Yes.

MEMBER BROWN: Okay, thank you.

I guess my question here is that if you look in the FSAR and the DCD and the others -- well, not the DCD, but the FSAR and the other supplements you sent, the evaluation of these as being independent is solely based again on the fact that the data is sent over a fiber optic link and therefore it is electrically isolated from -- this is interdivision, not within a division, this is interdivision communication. So in other words this transmission of the DTF trip signals to the LFF for the two-out-of-four voting, and then whatever process sends that voting signal to the SLF RDLC which then also generates some outputs. So that's three of them in a row. And that's reflected in one of the figures, I forget, 3.4b or something like that, Tier 1, 3.4.b, or b. Now and so the statement is they are independent, yet in each of these circumstances -- this is literally a high speed serial data link, in other words, it's generating a packet of data that gets sent from the DTF to the SLF for the voting. The voting unit is a software voting unit, not like the FPGAs, where it is a set of combinational logic, digital hardware gates. And it goes from one to every one of the other ones.

So when you are unplugging a set of serial data from division one, pick one, to two, three and four, into that ESLFs, and therefore that one packet, same question, one packet of corrupt data can go over and it can literally in this case lock up the computer.

MR. MURRAY: Eric or Ed, would you try to address that? What we are trying to get to is your confidence that a single corrupt data packet cannot halt basically the other --

MEMBER BROWN: The other three microprocessors.

MR. MURRAY: Right.

MR. FREDRICKSON: I am Eric Fredrickson, Westinghouse, eight years, nuclear Navy, and 2-1/2 at Westinghouse as the project manager for ELCS. Very similar to the FPGA case, the data packet that is sent over to the voter function consists of bi-state status, it's a bi-state of status zero/one type of bit, and does not include instructional information. So on the other end, on the SLF side, when it receives that it puts it into a memory location and the SLF logic will then look to that memory location to get the zero and one bit. It can't go there to get independent instructions. So there is nothing that could corrupt the functionality of the SLM vote function that would have come across the HSL or the high speed link.

MEMBER BROWN: Does that include the lead -- I'm trying to understand the function of the buffer. I presume that input is a buffer, effectively, to hold in place. So there has got -- normally it's more than just a one or a zero that is sent. You normally have a lead header and a -- I call it a header, but some packet identifier that is at the beginning, and another part at the end. And you are saying those two pieces in no way can -- those are read by the processing section. I understand your one/zero point on this, but there is a part of those data packets that are read in the TLF processing unit, and so I understand your point, it's similar to the FPGA, but it is not exactly the same. So -- and because this is an interrupt-driven system all the way along, particularly on the data transmit and the data receive functions, and that comes from the Common Q -- I went and looked at those in the Common Q category, it's unpredictable from that standpoint relative to the -- I mean as long as you are reading all that stuff, you are now putting extraneous data -- FPGA, you are putting a one or a zero, that is very clear, that one is easy. But here you have got to read that. It's got to say, this is what it is, and that data in itself could end up corrupting the voting function process for that, or at least it's probably difficult to prove a negative in this circumstance. But it is still a circumstance, where you are putting in place a potential to have those processes, if it's bad enough to corrupt one it'll do the same thing to the other ones. And that is one of my major concerns.

CHAIR ABDEL-KHALIK: Let's just give him a chance to answer.

MEMBER BROWN: He's thinking.

MR. BROWN: No, actually he's going to

pass it on to me to give you a little more information about the way the Common Q processor in communication works. The Common Q processor is not a general purpose computing machine. It is a controller that is designed to buffer a safety function processor from external events, including communication events and network events from the interdivision network.

Within the controller there are actually two separate microprocessors with separate memory.

MEMBER BROWN: Beyond the 630s or something like that, 640s, I don't know.

MR. BROWN: 646 is correct. So the processor section reads everything as data. It does have an external interrupt, that is a real time clock tick, that sets the periodicity functions for that processor.

MEMBER BROWN: That's the task schedule, the interrupt service routine, I am familiar with that, or I know it's there.

MR. BROWN: Right. For information that is communicated by high speed link, that's done in a second processor. That processor handles only communications, and can only pass data through a dual-ported shared memory to the safety-function calculator. It cannot pass anything other than data, and the data types that it can pass are restricted.

MEMBER BROWN: To?

MR. BROWN: Certain types in certain divisions. For example, the entire maximum message has limitations on the types of data that you can include in the message. So if we wanted the number of bits, we could say we have so many long integers. And those would represent the bits for the status bits. Receiving station would expect those bits. In the communication processor, it strips the header. It is only expecting one message, and it strips the header, does the CRC check, and takes the data and puts it into the dual-ported memory. The only thing the function processor does is to read that data and use it in a calculation.

MEMBER BROWN: For this, I'm trying to understand what you said, so that if you are only sending for the voting logic and the voting logic process represented does nothing else except take ones and zeroes, it accepts no other type of data. That is not stated anywhere in here, in the descriptions. And I understand the dual-ported RAMS that it passes. If the header is stripped, and you say it does a CRC on it, it seems to me that since you are only expecting a one or a zero, there is only -- two states of a CRC that you should even expect, would that be correct, because the headers and the tail end also involved in the CRC calculation? I thought they were.

MR. BROWN: Yes, but the data in between can be a varied set of ones and zeroes, since it's a safety function status of all of the safety functions from the EPM.

MEMBER BROWN: So there is more than one -- it's more than just a one or zero in this case.

MR. BROWN: Right, it is a clean set.

MEMBER BROWN: Okay, that's a problem.

MR. BROWN: So if there are 16 analog values that the EPM is going to implement, we need to actuate these functions. There is a set of ones and zeroes that determine the actuation status of the various safety functions.

MEMBER BROWN: So they are only transmitted once for all the --

MR. BROWN: Yes.

MEMBER BROWN: -- in that division.

MR. BROWN: Yes.

MEMBER BROWN: In other words, in the processing unit, back in the DTM, it sends its stuff through -- over to the transmittal, but it's looking for multiple messages. If there are multiple pieces of data that are going to be compacted into one --

MR. BROWN: Right.

MEMBER BROWN: -- one message each time?

MR. BROWN: The DTM function processor will put all those status messages together, and put it -- store it to the dual-ported memory, and when it stores something in the dual-ported memory, it generates an interrupt, the communication section.

MEMBER BROWN: Then it gets the last, when it's finished.

MR. BROWN: When it's finished, the communication section then takes that, formats the message. Now it also includes redundancy. It takes the data, it also generates the inverse of the data. For a complete message.

MEMBER BROWN: In ones complement, in other words.

MR. BROWN: Yes, then puts the CRC check on it, then transmits it.

MEMBER BROWN: All that does is mean the data looks the same at the end as it did at the beginning. That's all those checks do. They don't make the combination of ones and zeroes.

MR. BROWN: No, they just help you make sure the message has a reasonably probability of being correct.

MEMBER BROWN: Okay, if it's generating a set of ones and zeroes for the various protection functions, how do you prevent -- you have a field of ones and zeroes here that are being serially transmitted. If it is 16, and I don't recall in bits, either one can be a one or a zero, I know there is not a combination of those that gets through, but when they are taken up on the other line and sent into the processing unit won't compromise that voting unit.

MR. BROWN: Okay, because they are treated only --

MEMBER BONACA: Could you please speak into a microphone? We can't hear you.

MR. BROWN: It is treated only as data. The processing unit at the beginning of the task of two-out-of-four voting reads the input signals, so it will read the communication signals and it will take that and do a combination logic, Boolean logic, to determine do I have a coincidence of two or more signals. If you have one set of data, it will be part of that computation, but it will not stop it from functioning.

MEMBER BROWN: So your point, your argument is -- I don't mean argument in the sense of an argument, is that the -- there is no combination of units, ones and zeroes, in that 16 bit serial stream that when they are passed now into the processing unit for looking at each -- I'm going to ask another question about the voting units -- that will corrupt or could lock up or stop the processing in any particular voting platform.

MR. BROWN: Right, because of each of the states is a valid state, either one or zero. All zeroes, the functions are not tripped; all ones, the functions are tripped.

MEMBER BROWN: Okay, I got that, let me get to the next point to keep this going here. Is that packet represents all functions, how does -- if there are 16 protection parameters, or eight, or whatever it is, I guess it would be 16 in this case, how does it know which of the bits corresponds to which function? In other words if it's a low pressure or a high temperature or a low flow or a high power whatever, do you want to tell me how that is done?

MR. BROWN: The position of the bit is always the same for the same function so that the processor knows which one of those bits in that data word is the one for high pressure core flood or injection, leak detection system, RHR actuation.

MEMBER BROWN: So it's the placement with the field string that gives you that information?

MR. BROWN: Yes.

MEMBER BROWN: So when the processor gets it it takes the first bit and it says, okay that is a low pressure; the second bit is a vector, and that is a predetermined process?

MR. BROWN: Right.

MR. FREDRICKSON: Every SLF voter function is not necessarily looking at all 16 bistable parameters, it's only looking at the ones it needs for its overall function.

MEMBER BROWN: That was my next question. I was presuming that when you -- I've got four sets of data coming, I've got my own and three other divisions worth of data coming in. And they are all asynchronous, but as long as they are positionally located, it doesn't really matter.

My next question and I think I got this out of the reading is that you all's tripping is not just two out of four in any protection function, if it's unlike, it's all like, in other words it takes all the pressures -- I got that from one of the other logic diagrams, the one you had in there.

MR. FREDRICKSON: Yes, correct, when it

is doing the vote confirmation it is looking at only the like parameters from all four divisions. For example for leak detection it is looking at low water level from all four division sensing and high drywell pressure and it ignores all the rest of them.

MEMBER BROWN: Well, the other --

MR. FREDRICKSON: Yes, it ignores the other parameters because that SLF is only worried about leak detection. The high pressure core flooder SLF will be worried about its parameters. The RHR SLF loader will be worried about its parameters.

MEMBER BROWN: Each one of those is a control module within what they call it.

MR. FREDRICKSON: Right, and that is why there is six SLFs per division, because they are each looking at individual things for its own system, they are not all combined into one vote for Division 1.

MEMBER BROWN: Okay. You wanted to ask the next question of you all?

CHAIR ABDEL-KHALIK: Just go ahead, Charlie.

MEMBER BROWN: All right, you've answered that one satisfactorily, thank you.

On the aspect of being deterministic -- is the mike picking this up now? Can you hear me? The task schedule is in that service routine that operates in the Common Q thing?

MR. BROWN: Yes.

MEMBER BROWN: I think it is a two millisecond cycle time or something like that.

MR. BROWN: Yes.

MEMBER BROWN: And it picks up control modules, executes them, and then they go I guess to the copy task, the transmit and the receive functions are then all spread out after that. So all the control modules have separate priorities, they can't have the same at least according to the topical report. And so high priority module will always interrupt a lower priority -- it'll stop it.

MR. BROWN: Yes, it's preemptive multi-tasking.

MEMBER BROWN: Yes, what did you call it, preemptive multitasking, fine. Then when it comes back to it if it is now the right program it will come back to that task. The transmit cycle, the data transmission, is an event driven thing, in other words, you don't send anything until you get a collection of the last message that has been clicked through the DPRAM into the processor, the transmit, the communication processor.

MR. BROWN: Right.

MEMBER BROWN: So I've got three processors in a row here, let's just use two of them for the trip operation, I guess all three. And I've got a task schedule which is an interrupt function with different control modules that have different priorities. I've got an event-driven interrupt, and then a trend. So I've got almost an indeterminate in my opinion at least at this point response in terms of being able to say everything is going to happen in a predetermined, predictable and repeatable timeframe. Because if you look at the way at least the topical report came across, not all control modules get processed in the -- necessarily in the same order, because they may be interrupted and another one could take it's place. So you could even be in a position that a particular control module is being processed that happens to be needed for an accident consideration that is in process, but another module sits up there, it's time schedule says, oh, I've got to run this module, it pops down, stops that one, does that, and then it comes back -- maybe. It might come back to another one. And your action goes on, and the act is important and it does not get processed until too late, or in other cycles. So I'm trying to come to grips with why nonrepetitive control module execution scheme where every line is just done lockstep one right after another within a fixed cycle time and then just repeated, instead I'm putting myself in a circumstance where important modules may or may not be allowed to execute in a timeframe that is suitable for some particular transient.

In other words the problem with this is it's nonpredictable and nondeterministic. And the Common Q platform topical report recognizes that, if you go back in the deterministic description of it, it talks about you have to keep the burden on this interrupt driven process below I think they said 70 percent -- that seemed kind of high -- but below 70 percent, and only make sure you didn't have overruns, in which case I couldn't find out what happens if you have an overrun, whether it stops and recycles and starts all over again.

MR. BROWN: It goes to a default trip state.

MEMBER BROWN: Okay, so it was not clear how I really had a system that is both predictable and repeatable from input out through the observation and trip functions to all three of the microprocessors.

MR. BROWN: Okay, let me try to clear it

up a little bit because the topical report talked about the capabilities of the entire machine in a number -- which is used in a number of applications. You would not necessarily use all those capabilities to do a function like the -- let's take the DTF function for example. And the typical way the protection processor works is it reads all of its data input at the beginning of execution, it executes, and at the end of execution transmits its outputs. So --

MEMBER BROWN: Want to say that again?

MR. BROWN: Okay, the typical way the controller functions --

MEMBER BROWN: In the Common Q platform.

MR. BROWN: -- in the Common Q platform, the program starts and reads its data first, and this is the dataset for that calculation -- it completes the calculation, the program set of modules and then it outputs its information. When it inputs its information it reads data from IL cards if they are local. Data is already at the IL cards converted, and reads the data back. It may also read data from the support system if it's a support system function, but if it's a DTF it will not.

It will take in all of its analog sensor data during the beginning and then will calculate each one of the protection functions. At the end of that it will provide an output to the HSLs. Now all of the interrupt with communications are in the second processor, so the only thing we are getting in the first processor is the real time tick, and agree, the loading is kept at 70 percent, because loading could vary by different data, there is always that possibility. So that guarantees that you will always get cyclic information.

When you go to the communication section and you transmit that first piece of data, that is cyclic because it is tied to the cyclic nature of the execution of the program that is tied to the clock interrupt. That will always be a cyclic transmit, and it's received from a cyclic task. So if you look at a processor, it has two potential serial inputs, and one potential serial output. And these are independent, all three are independent. So there is a receive buffer for Serial Link 1, there is a receive buffer for Serial Link 2, and then there is a transmit buffer. So when Serial Link 1transmits, fills its buffer, Serial Link 2 transmits, fills its buffer, then the application task can be dumping into the buffer three. What happens when the first message is done, that interrupt keeps that first serial message processor from reading it once it is stored into a part of RAM, second serial message the same thing, put into dual-ported RAM. So those don't interrupt each other.

And then finally the transmission task. The way you assure that these interrupts can be properly serviced is that the amount of time available to the service the interrupts is very long with respect to the amount of time that either the program periodicity or the communication time. So there is a majority of dead time in they communications processor. It's mostly waiting for activity, and it can perform all three basic tasks it has Receive Link 1, Receive Link 1, and transmit output without ever having a situation where it could be overloaded. Since those are all cyclical tasks, it is driven to become deterministic because it is keyed to deterministic tasks that either starts the transmission, read by deterministic task that executes the data, and then the transmission to the next tier down, which would be the two-out-of-four voter, is periodic, and predictable.

MEMBER BROWN: In the Common Q report, topical report, I think I understood everything you said, it also made the comment that for each application you need to do a timing analysis in order to confirm that you are really not deterministic -- I understand what you are saying, what you are doing, you are forcing yourself not to overload the internal communications structure, so that you don't get into circumstances where you are not getting just a lot of wait time; I mean that is fundamentally the scheme of what you are doing. I don't want to argue about that right now.

But the --- I didn't see that requirement it's part of the design requirements, so like a timing analysis and the acceptance test for the ITAAC, the sole thing for determinism says a report will be issued that says it's deterministic. It doesn't say how they are going to do it. It doesn't replicate what the Common Q platform says you need to do in order to ensure that in order to meet this quote metric that they have in there.

MR. BROWN: But there is an ITAAC that says the platform has to be demonstrated to be deterministic, and that would be the test.

MEMBER BROWN: You are talking about a time response test?

MR. BROWN: Yes.

MEMBER BROWN: Well, I built a system

out of interrupts, okay, and you end up having to do a lot of tests statistically to get -- if it's deployed -- to get a good feel. So when you want to do a time-response test, you are not going to get the same number every time in these systems.

MR. BROWN: Oh, absolutely, there is a band of acceptable values.

MEMBER BROWN: And so you also run a number of tests in order to make sure you come into the bandwidth, come into the band. But that is why you don't want to end up at the end -- I'm talking about the design process now and then the test, there was no timing analysis shown, and I can probably accept this, I think, I'm going to have to think about what you told and look back at the report again. But without some type of looking at the application what you all have got in a number of modules and what you demonstrate, and the assumptions, and there is no requirement for that to be done, other than -- the only thing that would be required to be done is in the full operational test that you do a time response test, and that was the only place I saw a test. But that in itself is not conclusive, depending on how it's run.

MR. BROWN: If you read the topical test, there is a requirement for us to do --

MEMBER BROWN: In the topical report?

MR. BROWN: Yes, there is a requirement for us to do that complete timing analysis and provide it.

MEMBER BROWN: The topical report doesn't require you, it just says it needs to be done. It says it will be done, but are you all subsuming that under the guise of your design that you all then have to do that that.

MR. BROWN: Yes.

MEMBER BROWN: Even though it is not called out as an acceptance criteria in the ITAAC for the qualification part of this system.

MR. BROWN: We will do that as a basis for establishing the ITAAC deterministic tests. I mean that is the logical solution. We will do that timing analysis to satisfy ourself the system meets its performance requirements. It is required for us to submit that --

MEMBER BROWN: And within the time response needed by --

MR. BROWN: Most demanding accident?

MEMBER BROWN: -- most demanding accident, okay. I'll cut that off right here. Thank you.

CHAIR ABDEL-KHALIK: You have one last slide, I guess, your conclusion slide. Please proceed.

MR. MURRAY: In the conclusions we feel that the FSAR provides a complete set of licensing basis and the requirements for the I&C systems, as well as the 3&4 departures provide the design advancements to eliminate obsolete equipment to utilize current technology control systems. And that was our last slide.

CHAIR ABDEL-KHALIK: Thank you very much. At this time we can switch to the staff's presentation.

MR. HEAD: Mr. Chairman, if I could, I would to propose that we had some questions earlier, and if we have time after the staff finished we would --

CHAIR ABDEL-KHALIK: We will get to them. Thank you.

MR. WUNDER: Mr. Chairman, Mr. Holahan is being called, he's on his way down, and we thought that this would be a good time for him to deliver his remarks. Could we possibly just take a four or five minute recess until he gets down here?

CHAIR ABDEL-KHALIK: Well, we can answer --

MR. HEAD: No, no, people next door are finalizing our responses. So I will just tell you we had planned on getting back to you on some of those today.

CHAIR ABDEL-KHALIK: But later?

MR. HEAD: Yes.

MR. WUNDER: I'm just told that he will be here in about five minutes.

CHAIR ABDEL-KHALIK: Okay, we will take a five minute break.

(Whereupon, at 1:49 p.m., the proceeding in the above-entitled matter went off the record and resumed at 1:54 p.m.)

REMARKS BY THE DEPUTY DIRECTOR OF THE OFFICE OF NEW REACTORS

CHAIR ABDEL-KHALIK: Okay, we are back in session.

Mr. Holahan, would you like to make a statement?

MR. HOLAHAN: Thank you. My name is Gary Holahan. I'm the deputy office director with the office of new reactors, and Mike Johnson, our office director, is also interested with the committee, and I think that his calendar just gotten a little tied up because we were prepared for this morning.

I want to make three points which I hope will be helpful to the committee in getting through not only this one but the digital I&C issues for each of the other design certifications as well.

First is, the staff does recognize that digital I&C is a very important issue. In some ways maybe it's the most important issue for the new reactor designs. Digital systems can enhance safety and reliability, but they bring with them new and different issues and concerns, and we need to deal with those. We take these issues very seriously, we take the ACRS' concerns of these issues very seriously. We won't always agree on all the details and it's going to take a fair amount of dialog, but we take the ACRS issues seriously. We intend to address them, we have a very good I think working relationship with the committee, and certainly with the committee staff.

We meet with committee staff every single week. They are invited to our staff meetings on Monday mornings, and I think it's produced a very good working relationship.

The second issue I want to put is, there's been a lot of discussion as to how and what the decision-making process is, and what I want to emphasize is that the review and approval of digital I&C systems, like other safety systems in the new reactor designs, is really a licensing activity, and needs to take place, needs to be done, needs to be done well, as part of the design certification and COL process. Not as part of the field inspections. We will do field inspections, we will do inspections of digital I&C issues, we will involve our technical digital I&C experts, but that is not a substitute for making the licensing and safety decisions as part of the design certs and the combined license process.

That's not just a legal issue. Clearly as part of Part 52 calls for a safety decision to be made as part of the design cert and COS. But we also have experience with trying to inspect safety and quality into systems in the field, and it doesn't work? It doesn't work well. This has been one of the characteristics of fire protection issues for decades. Inspection needs to be clear in its role, inspection activities need to be based on a clear licensing basis to ensure that what is assured through the inspection activities is based on a good technical evaluation done as part of the licensing process.

And I know there has been a lot of discussion about the role of inspection in these activities, but I would encourage the committee to focus on the design cert system a the most logical place to make safety findings on digital I&C and other systems. Combined licenses, where necessary, where issues don't get fully closed at the design cert stage, and not to try to use the inspection process as a second level of review.

I think we with the committee's advice need to come to a position on a good enough licensing basis to make the final safety determinations in the licensing process itself.

The third point I'd like to emphasize is the staff, the ACRS, and the Commission has struggled with digital I&C as a difficult topic for more than a decade. We have been through this topic in each design cert in the 1990s. It is continuing, and I suspect for a long time it will continue to be a challenging issue.

We think that the staff of the Commission, and at least the ACRS in the past, and I know that one of the values of having a new committee is that you can raise issues that may have been missed before, and I think those are good things to address.

In the past the staff, the Commission, and the ACRS came to what we think is a practical approach for assuring the safety of plants with -- based on digital technology. And that is really with two major aspects to the review. One is assuring that the design itself is a good design, that it's based on up to date and state of the art standards, that it is done through a well planned and structured process, that it's tested to the extent that systems can be tested, and it's checked for things like independence and communication between channels and between various parts of the system, all of these things are normally done.

But we also recognize, and maybe this is an inherent characteristic of digital systems, that it is really hard to come to a conclusion that the system is without flaw. The systems are complex, the software is getting more complicated I think all the time, and recognizing how difficult it is to make a determination that a digital-based system is inherently reliable, the Commission took a position, and I think it was a very practical position to say, we need to push the systems to the state of the art that they should be as good as we know how to make them; they should not have any identifiable design flaws, and I think that our interactions with the committee and with the applicant are very good ways to identify areas of concern; but ultimately none of these systems will be good enough that it doesn't need some kind of diverse -- either diversity within the system or a backup system.

And that decision that especially because of concerns over common cause failures of software that we cannot now and maybe we could never get to the point of saying that these digital safety systems don't need a backup. A backup that is diverse, independent, and in itself reliable.

We chose this as a practical way of dealing with all the residual concerns that we have with digital systems. So we don't want a system that we know has weaknesses, it's overly complex or it has communications, we are not comfortable with it, fair enough, and we are going to deal with those.

But we think, and I would encourage the committee to think, about the value that the backup system brings to the overall decision-making process. The residual concerns, you can't quite get to the point of saying there are no flaws in some of the code, thousands of lines of code. I'm not sure how we would ever get to make such a determination.

Diversity, either inside or as a backup to the protection system, goes a long way in giving the staff comfort that the unknown unknowns in digital systems are reasonably well covered.

It's an area that we focus our review, and we recognize that some of the designs that are under review -- and I don't want to speak to the ESBWR, our experts are here to do that this afternoon, but we are concerned about communication interactions within the protection system. We are certainly concerned about interactions, communications, between the protection system and its independent and diverse background, so I think what you will see on the part of our review, we are addressing residual concerns by convincing ourselves that the backup capability his solid, its independent and diverse on the protection system, and this combination of reviewing it, reviewing the system to be high quality plus a reasonable backup is the balanced approach to digital I&C.

Those are basically the messages I wanted to leave you with. Our staff is here to cover the details this afternoon. We interacted with your committee and your staff on these issues. If you need more management attention or you are not getting what you need to resolve any of these issues, we are available to address such concerns, and let me leave it with that.

CHAIR ABDEL-KHALIK: Thank you very much.

We will proceed with the presentations.

STPCOLAR FSAR - CHAPTER 7 - STAFF PRESENTATION

MR. MUNIZ: Good afternoon, my name is Adrian Muniz, and the staff is going to be presenting the finding on the SER with open items for Chapter 7, instrumentation and controls. Here with me is Dinesh Taneja, the lead reviewer for the review of the Chapter 7, and he will be in charge of the technical discussion.

Some of the topics that we are going to be discussing are the Tier 1 departure, the Tier 1 3.41 that addresses obsolete data communication technology, and digital I&C platform selection. We will also be discussing the digital I&C platforms and the Tier 2* departure, and get changes or put the design compliance with foreign regulations codes and standards.

We will also be discussing the DAC/ITAAC process for implementing the digital I&C design details. And also as part of our review we reviewed in Chapter 7 the Setpoint Methodology Technical Report that was omitted by the applicant, to resolve the bracketed items in the technical specifications.

Members of ACRS identify some items of interest, and we prepared some slides to discuss those topics. We are prepared to discuss them in detail. However in the interests of time we propose that we treat those slides as backup slides and if you have specific questions we will refer to those in addressing your questions.

CHAIR ABDEL-KHALIK: Much of this material was covered by the applicant, but if necessary we will revisit the issue as appropriate. Thank you.

MR. MUNIZ: And just an update, in the SER we identify four open items, all of them are being closed and are being tracked right now confirmatory items. Also since the SER was written one new open item was identified in the area of the instrument setpoint methodology, and we will provide details as to what that open item is.

So with that I will turn it over to Dinesh.

MR. TANEJA: Good afternoon. I am Dinesh Taneja. I'm in the Office of New Reactors, engineering division, and I'm the lead reviewer of this South Texas COL application. I've been at this task for the last about two years now, and I've had a good supporting cast of characters in our branch, that have supported review of this application. And I personally have been with the Agency now over three years; spent one year in Office of Research and the rest of the time in the Office of New Reactors. And prior to that since 1981 I have been involved in the nuclear field in various capacities, I& C engineering, startups, operations, electrical engineering, supervision. So there is considerable experience that came into reviewing this application.

And Jack Zhao that helped me in this review has significant experience with digital technologies, and PLCs and DCS equipments, and that was a great asset in trying to review these applications.

Primarily, the change that drew this application was the obsolescence of this communication system that is in the certified design. So this is an example of an idea. If that technology wasn't obsolete, it could have been implemented as is. Because of the change, the way the applicant chose to address that is, they couldn't use their technology, so what they did was, the used the platforms that have data and communication capabilities. So they removed the data communication by addressing it by each individual platform with inherent capability built into it. And the original design was based on shared sensor, it was a multiplex system, and it was based on the FDDI technology which was discussed this morning.

MEMBER BROWN: My two questions are done, so you can based on other people's interest.

CHAIR ABDEL-KHALIK: When the time comes we'll get to it.

Please proceed.

MEMBER BROWN: Just wanted to let you know that.

MR. TANEJA: The one thing that is to notice is that the Tier 1 sections on neutron monitoring system, the reactor protection system and core cooling systems, the functional requirements that are required in those sections, so there is no impact to those sections because of this departure. So the conclusion that we came to that the functionality of the I&C is still the same, it's just how that function is accomplished is being done a little differently. But what it does is exactly the same thing.

MEMBER STETKAR: I'm a little curious, Tanesh, because they've changed a few things. They've made active decisions -- when you say functionality, yes, in the broad sense that if I get low level and high drywell pressure I am supposed to do something. But how they have implemented those functions, and I'll ask you the questions that I asked the applicant this morning. They've changed how they implement for example alternate rod insertion. They have changed coincidence logic to two out of two coincidences from separate SLFs within a division to one out of one in many cases.

I'm curious how you conclude that there are basically no changes.

MR. TANEJA: No, no, the functionality as described in these systems, core cooling system, right, is essentially saying that the system, needs to respond to these events a certain way, right, that these pumps need to start if you have a low level condition in the reactor vessel, right. System performance requirements are identical. The reactor needs to trip if you have high drywell pressure or low level, right? Those requirements at that level did not change.

MEMBER STETKAR: It's a very high level.

MR. TANEJA: Exactly.

MEMBER STETKAR: It's a very high level.

MR. TANEJA: Right, now how you

accomplish that -- now your question on two out of two, right, this was one of our review concerns. We had a number of our eyes on that topic, and essentially from the regulatory compliance side of it, right, we have basically regulations which states that you have redundant systems that are independent and safety systems so you really address an issue of single random failure. Redundant I&C systems. So if you look at it, there are three trains in safety systems, three pumps, three trains, three RHR pumps and three, you know. So you need one out of three to do the safety function, correct. So you have basically four divisions of I&C which take four different readings, and they come up to a decision to start one of the pumps. So I can essentially have a single failure that can take out a whole division, but I still have the other division that is going to perform the function, right?

MEMBER STETKAR: Two out of two versus one out of two?

MR. TANEJA: I believe the whole decision of the design is to improve reliability of the system from the point of view that the two out of two logic will prevent any inadvertent actuations.

MEMBER STETKAR: Now let me stop you

right there.

MR. TANEJA: Okay.

MEMBER STETKAR: That's what you believe personally. I believe that I can't understand why they made the specific decisions for some signals and some decisions for other signals; that's what I believe. And I believe that preventing a rare spurious actuation in many cases may be worse than reducing the reliability of something under conditions when it's required to act. That is what I believe. Now that is my belief. We are not regulating the nuclear power industry based on your belief or my belief. We are regulating the nuclear power industry based on a determination of adequate safety.

MR. TANEJA: Right.

MEMBER STETKAR: And if I see someone making a change to a design, I want to understand why they made that change, and I want to understand that indeed the reasons for that change and the way it was implemented are indeed at least safety neutral or safety improvement, not reliability improvement in terms of availability of the plant to produce electric power, not nuisance neutral in terms of nuisance to operators for spurious signals, I want to make sure that indeed they improved or at least did not reduce safety.

MR. TANEJA: The philosophy of the design is maintained. The reactor protection system is a fail-safe system.

MEMBER STETKAR: I'm not talking about reactor protection. I'm talking about emergency core cooling actuation.

MR. TANEJA: And that system is a fail-as-is system, right?

MEMBER STETKAR: That is a fail-as-is, and energized to actuate system.

MR. TANEJA: Correct. So when you have a two out of two, a redundancy within a division, right, that is really installed to prevent inadvertent actuations.

MEMBER STETKAR: That's right.

MR. TANEJA: Right. Now a lot of concern, and I have the same concern, that would rather have an actuation than not have an actuation, because that is a safe state, correct. The way this logic is designed is if you have a failure of one of those SLFs, then it goes to one-of-one logic. It does not sit there on two-out-of-two logic, that one gets thrown out.

MEMBER STETKAR: That's not what I saw in the logic, and I'd like to have the applicant confirm that, because I felt that I needed a positive output from both of those to actually actuate the device.

MR. TANEJA: Self-diagnostic, if you take one out, then you are at one out of one.

MEMBER STETKAR: If it's in bypass under some of those logics that's true, and in most of them I believe if one of the SLF fails -- but let's let the people who designed the system answer that.

MR. TANEJA: But that was the concept of the certified design which was carried over.

MR. MURRAY: Would you like us to answer that question?

MEMBER STETKAR: Yes, I would actually.

CHAIR ABDEL-KHALIK: Yes, please.

MR. BROWN: Okay, my name is Ed Brown, I'm from Westinghouse. For the two out of two designs, there is -- there are two types of bypasses. One is an automatic output bypass which when a failure is detected online from one of the SLF processing logic channels, the logic is changed to one out of one. There also is a manual capability to perform that SLF bypass also. So most of the failures are detectible by online diagnostics, so when that failure is detected, there is an automatic bypass of a failed select processor channel, that changes the logic from two out of two to one out of two -- one out of one, I'm sorry.

MR. TANEJA: And that was the last certified design which was carried over.

MEMBER STETKAR: That is certainly not apparent in any of the schematic diagrams that are available in the FSAR, because those schematic diagrams seem to indicate serial connections of the output devices from the individual SLFs, which is not -- is not quite consistent from what I just heard.

MR. BROWN: I believe in Section 7 it is described in words. And it is also described in the ITAAC as things that will be testable.

MEMBER STETKAR: Okay, let me cut to the chase here. In the SER I see words that are parroted back, the same words that are parroted back from the FSAR. They are very high level words. I see references to figures, in Chapter 16, the same figures that are referred to this morning. I do not know how any of the equipment indeed is aligned to any of those logics, nor which are deferred to one out of one, or which starts with one out of one. And I come to a final conclusion that says, the staff found the applicant's response to RAI 07-9 acceptable. For a detailed technical evaluation of this ESF design concept and its regulatory compliance refer to Section 7.3 of this SER. I read it, it doesn't say much. Verification of the implementation of these ESF design concepts described above will be performed via Tier 1 Section 3.4 DAC ITAAC inspections.

I just thought that we heard that we are making licensing decisions based on safety at this stage, not into ITAAC DAC inspections. An inspector can indeed confirm that something is wired up on a two-out-of-two logic or a one-out-of-one logic; that's what I would expect them to do. I would expect the staff at this stage to be answering questions about, why did you change this from a one out of one -- or I'm sorry, a two out of two to a one out of one. I didn't see any of those questions. I read the RAI.

MR. TANEJA: That was a question that we asked. Jack, there was a specific RAI on that question, correct.

MR. ZHAO: This is Jack Zhao, New Reactor Office. I know there was one.

MEMBER STETKAR: Did you get an answer to that in terms of a list and the reasons why they changed each one?

MR. ZHAO: I didn't hear that. What I

hear is that the response I've seen -- I have been away from this project for six months, but I cannot remember exactly.

MEMBER STETKAR: I'd be interested to see that detail.

MR. TANEJA: What I recall in the response to that RAI was, what was said this morning that the ECCS components and the containment isolation components would be using redundant buses, okay. The functions that are not -- you know the consequences of that function actuation is not critical, those would use single buses. That was one of the responses. And the other thing I recall that it made a reference to some table in Chapter 16 for a list of components.

MEMBER STETKAR: I couldn't find that table, so if it exists I'd really be thrilled to see that table. It doesn't refer to a table; it refers to five figures.

MR. TANEJA: Well, I think we had asked that question, which components would be part of the two, and which components would be, you know, on a single bus.

MEMBER STETKAR: I'd love to see that, because for the life of me I can't understand why a two-out-of-two logic is required for low pressure injection, for example.

CHAIR ABDEL-KHALIK: Would the applicant --

MEMBER STETKAR: I asked them this morning. That is one of the things that is on the table.

MR. MURRAY: Right, that is one of the follow up questions.

MEMBER STETKAR: What I'm trying to do is to find out how deeply the staff has probed into these changes in a design at this stage of the licensing process, because they are changes to a design.

MR. TANEJA: Yes, those are -- that is one of the departure issues, and basically the way we understood that change was that that actually was simplifying the design and taking some complexity out of it rather than making it more complex. See, two out of two logic makes things complicated; it's not a simple thing. See, if you already have four divisions, okay, one out of four to actuate two out of four is what the existing plant -- if we looked at the SRP guidance which is our regulation there is no regulation that states that we must have a two-out-of-two within a division. We do not require that.

MEMBER STETKAR: Correct.

MR. TANEJA: If you look at 603 there is no requirement for that. It is - -basically addresses the issue of inadvertent actuations to prevent -- it's basically an aide to make a better operation of a plant, not really to make it safer. Safe would be to start the pump regardless of whether you need it or not.

MEMBER STETKAR: Not necessarily.

MR. TANEJA: Not necessarily, right, but the way the regulations, fail safe means, you know if a condition occurs, my safe condition is to go into that safety mode. So we actually do not have any specific regulation that requires that you must have a redundant feature within a division, so we cannot really say that they don't meet a certain regulatory requirement if they don't do it. I couldn't find one, unless you know of something. I'd love to hear that.

MEMBER STETKAR: I'm not talking about a regulatory requirement; I'm talking about understanding a change in a design and the impact of that change on fundamental plant safety. Have I improved plant safety by making that change to the design? Have I maintained the same level of safety as the original certified design? Or perhaps because of an inadvertent oversight have I reduced the level of safety? Based on that change? I'm only talking about the change. I'm not talking about philosophical --

MR. TANEJA: Let's say two out of two for containment isolation functions, that's critical, all right. Now if I'm just taking -- I don't want the list of components. All containment isolation functions. They are very well defined. I can't inspect -- I know which ones have containment isolation values. When I go to inspect them, or an inspector goes to inspect, containment isolation is a very well defined component. It's not like you know that we have to sit there and decipher, is there a containment isolation or not, right?

ECCS components, clear cut, we know what ECCS components are. They are part of the ECCS system. From my experience with BWR, E-21s, E-41s, HPCI, RCIC, ECCS. Clear cut. You know, from the power sources to my inventory of suction, where I'm taking the suction from, and where I'm pumping to, and what drywell you need to line up that system, that makes up the ECCS system.

So for us when we looked at it, you know, yes, we wanted to have a list, but we didn't see a whole lot of value in having an inventory of components clearly identified. I thought those systems were adequate for that purpose.

CHAIR ABDEL-KHALIK: The applicant will follow up with that information, so please proceed with your presentation. Thank you.

MR. TANEJA: Sure.

MEMBER STETKAR: Dinesh, I'm sorry, I was searching for a reference here. You have to be careful, because I am going to try to keep people precise. And what I was searching for is the reference I finally found. In the FSAR in Section B.3.3.1.4 of the technical specifications, they make reference to a non-two-out-of-two coincidence, something that has been changed to a one-out-of-one, specifically for containment isolation. That is all it's called out is containment isolation. So in this area where you are talking about two of two for containment isolation, that is one area where they made a change. I just wanted to get that on the record. Thanks.

MR. TANEJA: Okay, on this slide this is from the DCD. This figure comes out of the DCD, which really shows the function of the obsolete data communication multiplexing system. And as you can see from this figure that communication is shared by RPS and ECCS. If you lose that communication, basically you render the whole division inoperable. And this change, going to the next figure, which also shows the figure out of DO-1, it shows the block diagram of the SSLC logic and where you can see that the social multiplexing system is used both for the inputs, which are shared by the ESFs and the RPS modules, and the outputs that go out of the CM use to RM use, you know, is done on the EMS system. . Now that portion of it on the outputs is strictly for the ESFs, because I think the RPS even on the existing, the old certified design, was hardwired. But these common weakness on the design that we certified was on the EMS side, and that was a weakness. And that's why there was a lot of attention given in the design certification on the EMS system, because it was very critical to the functionality of the complete division.

So the applicant on their design when they were addressing this obsolescence they basically elected to divide up the SSLC system into three very distinct platforms. They separated out the ELCS, NMS and RTIS, and I think we heard a lot of that discussion this morning on that one, and I believe we had a good presentation on their communication capability, which is inherent to each of the platform, it's all built into. So this is what really replaced the obsolete data communication capability of the SSLC.

And this is a simplified block diagram that shows the new design which essentially shows that all the -- for the RPS, the RTIS function, you -- all your inputs are hardwired. There is no -- there is no communication used there. Everything is hardwired into the DTS. They do not share any of the inputs with the ELCS or the ESF systems, so the ESF systems are basically using the -- that is a Common Q platform so it's using the communication capabilities to get the remote data into the DCFs.

And the Note 5, which basically says that each function may be accomplished by the multiple processor to minimize any hardware or software complexity or operational impact. And I think that one is basically on the loading of the processors. And like it was mentioned this morning, the Common Q SER has these plant specific action items. If you are to use a Common Q platform for a given plant the licensee must address those specific action items in order to use that platform. And one of the action items as described this morning was the form of timing analysis for that application to demonstrate that the timing would be within the bounds of the Chapter 15 analyses. All the event analysis. So that becomes a requirement for the design if that platform is to be used in this application, then that would become a requirement, and our -- and our lifecycle development phase, in the requirement phase we expect to see all those requirements identified even at that phase.

Not until this thing is built, we want to see those things right there. That that requirement is identified, and it's being designed to those requirements. That is our expectation.

MEMBER BROWN: When is that going to be done?

MR. TANEJA: Well, that is part of the post-COL activity because the applicant has chosen to go that route, and based on our Part 52 license, they have the option to either do it as part of the COL application, or do it after they get the COL.

MEMBER BROWN: Who is going to review that report?

MR. TANEJA: Who is going to review that report?

MEMBER BROWN: Yes, who is going to do the final -- if they are required to do it, who is going to execute the review to see if it was done satisfactorily?

MR. TANEJA: Well, it is part of the DAC ITAAC activity, right. It's in the 3.l, there's a DAC that requires those work to be done. Implementation of the software/hardware development is a DAC item. And that requirement is -- it's on a targeted ITAAC list so the staff is going to inspect it.

MEMBER ARMIJO: But not review it? I have a big problem with this inspect/review. Is there going to be an equivalent of a design review, a licensing review at that stage or not? The answer I get is, yes, we are going to inspect it, but I don't know if that means the same thing.

MS. DUDES: No, the answer to that question for the Part 52 process is that the safety decisions have been made in licensing, and that it will be an inspection targeted inspection, but it will be an inspection to verify compliance with the licensing basis. Sorry, this is Laura Dudes.

MEMBER ARMIJO: Yes, I understand.

MEMBER BROWN: So let me amplify what Laura just said. So the ESR for the Common Q platform becomes an integral part of the licensing basis?

MR. TANEJA: Well, the SER for the --

MEMBER BROWN: The action item from the SER becomes a -- it's effectively an inspection item.

MR. TANEJA: Right.

MEMBER BROWN: If I'm wrong, you just said that, and in order to verify that it was done correctly, somebody has to review it.

MR. TANEJA: Correct.

MEMBER BROWN: Who is going to do that review? Is it -- you say staff.

MR. TANEJA: Well it is part of the -- it is part of the DAC inspection process, because this work is now implemented. It's implementation of that platform. It's an implementation.

MEMBER BROWN: Okay, let me ask the question another way. You get the report.

MR. TANEJA: Right.

MEMBER BROWN: There's two ways. As an inspector, I say, hey, I got a report. They tell me the number is 69. Check. Okay, I'll put the thing aside. This is like taking a micrometer and measuring the diameter of a pipe. It doesn't work for this. How do you know they did the timing analysis correctly?

MR. TANEJA: Let's not say that it's that simple of an inspection.

MEMBER BROWN: Come on, I'm trying to give the thought process.

MR. TANEJA: Thought process --

MEMBER BROWN: This is not the same in terms of complexity or difficulty of what I would call standard site inspection.

MR. TANEJA: That is the reason, that is the very reason, over these questions, is why there is that pilot program that is being implemented at this stage to figure out exactly what needs to be done in those inspections.

MS. DUDES: Excuse me, this is Laura Dudes again. Again, we understand that an I&C inspection may be a little bit more complicated, and in fact we do have staff and inspectors who can actually go beyond the measuring of a pipe, and we -- we as NRO and our counterparts in the Inspection Program Branch understand that there is the complexity of that type of inspection, and for those implementation activities within the Common Q SE, which are specific -- I mean we made our safety determination on the platform, and wrote the safety evaluation based on the Common Q platform with specific items for which we will verify implementation of that via another regulatory activity beyond licensing, which is inspection, develop inspections that will cover satisfactorily verifying that the licensing basis established in the safety evaluation report is in fact what is being implemented in the plant.

CHAIR ABDEL-KHALIK: We have heard your message. We have heard Mr. Holahan's message. And I think the committee will address this issue from a generic philosophical approach, and the committee will make its opinions known to the commission and to the staff. Thank you. So this is not the place to debate this issue now. So please proceed.

MR. TANEJA: All right, next slide. I think we have seen this one already. This was actually a better picture. This came out of the application; these guys had a nice color picture of it. So basically that is a layout of the architecture. Now next slide, these are the specific items of interest coming out of this departure. We basically started our review of the application at the stage of acceptance review. And during the acceptance review, you know, we had a number of meetings with the applicant, and we came out with a number of changes to the application at the acceptance review process. And the review of the application actually was deferred to Rev. 2 by the time we actually started to review the application, because there was significant additional information hat got added from initial to middle to the Rev. 2 stages. And since then we have written a number of RAIs, and gone through a number of meetings to get to where we are today to make the conclusion that we are here with the Phase 2 phase of the SER review.

I think the response to RS 07-6, we talked about that, that added a new supplemental section, 7.1S to the COLA. 7.9S is another supplemental section that was added to the DCD FSAR to elaborate on the communication capabilities, both the safety and the nonsafety side. The PDN was discussed in there, and how the system is different and independent from the safety communication networks.

And that is really described in 7.9S, and the RAI 07-9 is where the clarification on the ELCS function was provided. That was the RAI where we were talking about this two out of two versus one out of two, and I think that is the RAI where we got into that discussion to try to figure it out a bit. Next page.

The Common Q platform like we've talked about it is already qualified and reviewed by the NRC, and the same platform is being used in the AP1000 designs and their safety applications. The associated design for the STP 3 & 4, it conforms to the ISG-04, and it also conforms to all the current regulatory guidance standards on data, in today's date. The certification was based on for example IEEE 279. And then it was certified. One of the biggest changes that was made was that any new I&C platform that is being added will conform to the IEEE 603 requirements.

We used the current version of the SRP Chapter 7 to do these evaluations, of the application. And basically the design that we saw for the SSLC in the application, it offered significant enhancements for what was certified for the ABWR.

So in conclusion to this section, the South Texas I&C design that was in the COLA, and including some of the RAI responses which still is a confirmatory item, it adequately addressed all the applicable licensing basis, and is in compliance with the applicable regulation, regulatory guides and standards.

The SLC design I&C platforms including inherent data communications capability are in compliance with current regulations, regulatory guides, and standards. Specifically IEEE 603 and its companion standard 7-4.3.2, 2003 version.

All open items have been resolved that

were related to this departure, and all the proposed COLA changes are being tracked right now as a confirmatory item.

The Tier 2* Departure, essentially this departure is where they address compliance to the current regulatory guides for the INC design. And based on this departure, the safety related I&C systems on all three of the platforms now conform to 603-1991 and the current versions of the applicable reg guides, and the NUREG-0800, the SRP and the Branch Technical Positions.

So those really are the things that give us confidence that the design is going to be at this level, and these are all the requirements.

And in response to one of our RAIs, the applicant provided supplemental tables, 1.9S-1, and 1.9S-1A, these two tables were added which identify the IEEE standards and the related regulatory guides that are specific to developing software. And these reg guides came into place after the design was certified, so these were added to the COL application.

So in conclusion I have to say that the design now complies with the current regulation, regulatory guides and standards, and all open items have been resolved, and we are basically tracking these are confirmatory items.

And for the interest, I guess I added these two tables to our backup slides, just to -- these were part of the RAI response. They are not in the application; for your interest. Basically it points to all the very recent regulatory guides, for example, 1.168 through 1.173, all these reg guides are very specific to the development of these software and hardware systems. And their companion IEEE standards are on 1.9S-1D.

Configuration management software test documentation, software requirement specification, software unit testing, V&V. So that is really what is our BTP 7-14, which these folks are complying to for developing these platforms. So that really is the guidance that is most up to date right now that we are following for getting these designs built to a good quality standard.

MEMBER BROWN: I want to make one observation. You state the Common Q platform was approved and has been evaluated for use and found suitable for use. The difficulty is when you put them into a specific application they can be applied in a manner which is not satisfactory. So the fact that the platform is functionally okay, but you can execute it such that it doesn't give you the end result. So you are going to review, at least I will, any of these applications to see that the application of that platform -- if you notice in my comments I didn't argue about the platform so much as how it was utilized in the specific system. And how it's characteristics were used to try to ensure that you got the satisfactory performance, that was the point.

So my point being is that using that is an argument for why everything is okay is like telling me why a Motorola 68000 is okay because we've used it before. It doesn't matter if it is not used -- I just wanted to make sure you understood that, because I've heard that comment before that this has already been approved. It makes it sound like why are you asking. Because the way it's done. You don't have to say any more.

MR. TANEJA: Yes, I agree with you.

MEMBER BROWN: Because we need to on with it. But I just wanted to make sure you understood that point.

MR. TANEJA: It's the same. It's very relevant thinking, so I agree with you on that one, but it needs to be applied very judiciously for its safety application.

MEMBER BROWN: Appreciate that.

MR. TANEJA: I believe.

CHAIR ABDEL-KHALIK: I believe the comments made on slides #17 - #19 have been made several times today, and I would recommend that we move on to slide #20;.

MR. TANEJA: The setpoint methodology document is actually one of those DAC ITAAC item that was originally the intent of the applicant was to actually treat that as a full COL activity. And under a separate activity that was trying to address the bracketed items for the tech spec, the applicant elected to use the option where they were going to go with the setpoint control program. And part of the setpoint control program was to promote the setpoint determination methodology.

So we received that document and we reviewed it as part of Chapter 7, and our evaluation of that as SCP's setpoint methodology is captured in Chapter 7.1-4 I think it is.

And we've completed our review -- next slide -- the basic couple of items of interest is that this report was prepared by Westinghouse for this ABWR application, and that methodology is very very similar to what we have received for AP1000 which was already reviewed and approved by the staff, the AP1000 methodology. And we had primarily one significant RAI on this one, which was adequately responded to, and the rev one of the methodology was issued incorporating all the response to that RAI, and then we were reviewing the Rev 1 item, and there was one minor reference that we found that basically references to a topical report on stability analysis for the OPRM setpoints, and that topical report is intended to be part of the fuel amendment which is like a beyond COL activity. So right now we have identified that, and we have initiated an RAI on that one, and we are tracking that one as an open item at this stage.

CHAIR ABDEL-KHALIK: What do you expect the answer to be? Is it related to GE7 fuel, or is it to whatever fuel they are going to have after that amendment?

MR. TANEJA: Have you guys figured out anything? Right now we felt that that was not -- the COL application right now assumes IBR, right. So when you see this application referring to that, can we take that? The question is, you know, how can you reference something that does not exist, or does not exist in this application? And that was our question.

So I only heard that resolution.

MR. MURRAY: The question was which fuel is it based on.

MR. QUINN: Yes, Bob Quinn, Westinghouse Licensing, been involved in nuclear power and nuclear fuel for about 30 years now. Our strategy at this point going forward is we are going to remove the reference to the topical report from the setpoint methodology report, and we will be bringing in an actual calculated value for OPRM, based on the stability option 3 from the BWR owners group, and we will be applying the uncertainty analysis as documented in the current technical report, and we will actually be providing that, that sample value, in the report. So for GE7 fuel we are going to stick with the approved approach, which is approved in the DCD FSER for the BWR stability option three approach to OPRM, calculating the setpoints.

MEMBER ARMIJO: And what happens when you put the real fuel in the SVEA, whatever it is? Are you going to redo that analysis?

MR. QUINN: Yes, we --

MEMBER ARMIJO: Will the staff review that again?

MR. QUINN: The setpoint -- I'm sorry,

the stability topical report is going to be submitted next month as part of a number of topicals related to the fuel amendment which we'll, be doing after COL, so we'll be redoing the calculation for the stability setpoints, as part of that, and we will be using that topical, which we hope to have approved at that time, as the basis for doing it.

CHAIR ABDEL-KHALIK: Let's move on.

MR. TANEJA: So essentially because of this one open item we are unable to finalize our conclusions on the setpoint methodology.

Now these next few slides are on the items that the members were interested in finding out more on, and if you like I will go through them.

CHAIR ABDEL-KHALIK: I will defer to Charlie at this point. You heard -- or have you received sufficient information from the applicant regarding your questions?

MEMBER BROWN: We didn't spend a whole lot of time on this, but I didn't have any questions on this. The diverse systems I think we probably agree, I think they were diverse. And they were redundant.

CHAIR ABDEL-KHALIK: How about the issue of determinism?

MEMBER BROWN: They were analog. My memory is failing at this point. They were hardwired analog, if I remember. They were not FPGAs even were they? Okay, my memory is failing me; thank you.

MEMBER ARMIJO: I think you have a typo on your slide #23. I don't think I've ever seen the certified US ABWR at this time. You have a certified ABWR design. I'm just wondering what do you mean by that?

MR. TANEJA: I have seen it both ways in Appendix A.

MEMBER ARMIJO: Is it in the DCD?

MR. TANEJA: Yes, it's in Part 52, Appendix A.

MEMBER ARMIJO: It seems that the U.S. has dropped out so many times, that sounded like a mix-up with some other certified design.

CHAIR ABDEL-KHALIK: That's fine. Are there any questions for the staff at this point?

MEMBER BROWN: One question on diversity applications. It's not on the specifics, but for the analysis used in this project for the diverse systems, is their response based on the same conservative casualty analysis or accident analysis that your primary systems are based on?

MR. TANEJA: What we found on that one is that these -- on slide #26 is the summary of the assumptions made for making that diversity analysis. They used the worse case postulated common mode failure of the safety system, concurrent with each of the design basis event. That's in Chapter 15. The analysis, they used a realistic modeling values as opposed to the licensing, the worse case values.

MEMBER BROWN: Okay, that is what I missed.

MR. TANEJA: These were the three key things that I picked up when I was going through that. Essentially they have to not remove shutdown system has capability to -- which is independent of --

MEMBER BROWN: Yes, that is manual.

MR. TANEJA: All manual, right?

MEMBER BROWN: Yes.

MR. TANEJA: So that has full capability of bringing the plant to full shutdown. So essentially I think one of the conditions was that you cannot go there for at least an hour, so you have to be in the control room doing everything within an hour. So that was one of the -- and I think the digital failure that was assumed in this analysis was the multiplexing system because that took down the whole division. That was the worst failure that was assumed.

MEMBER BROWN: I'm done with that, thank you.

CHAIR ABDEL-KHALIK: All right.

MR. TANEJA: And I think, John, your question was whether the change of the platform had any impact to this diversity implementation. Basically the platform and its architecture. And I think this figure that 7C, one figure in the application, this figure, in the shaded areas, that the worst features that are added, so you can see that they really bypass everything that is digital that go straight to the components.

MEMBER STETKAR: That helped a lot.

MR. TANEJA: Yes.

MEMBER BROWN: I was satisfied with that one when I saw it, no problem.

CHAIR ABDEL-KHALIK: Are there any other questions for the staff?

Okay, thank you very much.

Let me just try to catch up on the action items. There is an action item related to the documentation for each ESF component, as to how the SLF coincidence logic is implemented, its actuation.

This is one of the issues raised by John. And we --

MR. HEAD: And that was from this morning.

CHAIR ABDEL-KHALIK: Right. We essentially have it for the ADS, but for nothing else.

MR. HEAD: That is one of the ones we are supposed to be talking about here in just a minute.

CHAIR ABDEL-KHALIK: There was a need for follow up on departure 7.2.2, departure 7.2.6, and 7.3.9.

MR. HEAD: 7.2.6, the zero pressure?

CHAIR ABDEL-KHALIK: Yes.

MR. HEAD: And 7.2.9 was the --

CHAIR ABDEL-KHALIK: 7.3.9, 7.3.9 was the shutdown cooling.

MR. HEAD: All right, okay.

CHAIR ABDEL-KHALIK: Do you have responses for any of these or any of the other follow up items that we identified prior to that with regard to Chapter 14?

MR. HEAD: I believe we are poised to give you an answer on those four, but begging your indulgence, I'd like to take a break and just make sure I know where we are, and then we'd come back and answer.

CHAIR ABDEL-KHALIK: Okay, we will take a 10 minute break. We will reconvene at 10 after 3:00.

(Whereupon, at 2:57 p.m., the proceeding in the above-entitled matter went off the record and resumed at 3:09 p.m.)

CHAIR ABDEL-KHALIK: We are back in session.

At this time STP would like to provide answers to some of the questions that were raised earlier today.

MR. HEAD: Exactly, I am going to turn over the first one to Craig Swanner, if you will identify which one we are talking about specifically.

MR. SWANNER: Do we want to do the Chapter 14 one first?

MR. HEAD: Yes, go ahead.

MR. SWANNER: There was a question when we were going through Chapter 14 regarding I&C and it was on whether preoperational testing -- or there was any preoperating testing of ELCS, because one of the committee members asked, looked through the chapter and couldn't find any mention of the acronym ELCS. The answer to the question is, ELCS is part of the overall SSLC system, and preoperational testing of SSLC is described in Chapter 14.2.12.1.11 of the application, and in there it has a parts referring to ESF, and the requirements ESF go to ELCS. So the acronym doesn't appear in the chapter, but it is covered.

MEMBER BROWN: So RPS is also part of the --

MR. SWANNER: That's correct.

MEMBER BROWN: -- safety -- and it has its own separate section. So there is a little dichotomy there in terms of I guess ELCS is not as important as the RPS, tongue in cheek? The RPS was very -- I won't say very detailed, but it's got a listing, whereas the SSLC when it's a little bit more --

MR. SWANNER: Generic.

MEMBER BROWN: -- generic.

MR. SWANNER: That's correct.

MEMBER BROWN: So it's a little hard to connect the dots between one needs -- can be generic and the other can't. I got the answer. I'm not so sure I like it.

MR. SWANNER: That is the answer.

MEMBER BROWN: Okay.

MEMBER STETKAR: Is that the only answer regarding Chapter 14? Because it really didn't answer the question that I asked.

MR. SWANNER: Can you repeat the question, please?

MEMBER STETKAR: My question was, is there a preoperational test of whatever acronym you want to use, ELCS, SLLC, let's focus on ELCS, that tests the function from what I call end to end, in other words if I had a sensor out in the plant that is supposed to sense reactor vessel level and eventually starts a high pressure core flooder that indeed a functional test is performed where I insert a low level signal which I can do at the sensor itself, verify that indeed the combinatorics -- the full combinatorics is processed through the digital I&C system and that indeed the pump starts. In a single test, not a piecemeal three level overlapping test which is indicated in Chapter 14.

MR. SWANNER: If there is -- as part of the tech spec, there is a surveillance for each of the ESF functions that is a full comprehensive function test, end to end, specified tech spec, Able 3.3.1.4-1. and that is to be performed on a refueling outage basis.

CHAIR ABDEL-KHALIK: Could you repeat that number, please?

MEMBER STETKAR: I was asking for a preop test though, because I would really like to understand before I start up this plant that it is going to work on day one, not find out that two years later that maybe it had a problem.

MR. SWANNER: We can take that and figure it out.

MEMBER BROWN: That was the question.

MR. HEAD: Where was the more comprehensive testing? That was in the tech specs?

MR. SWANNER: That was in the tech specs.

MEMBER BROWN: But that's a surveillance issue.

MR. HEAD: We would know that we are in that condition before we start the plant up. I understand your question. Before that we are going to know that answer.

MEMBER STETKAR: In pre-op would be a good time to find out if there was a bug.

MEMBER BROWN: Same applies to the protection system.

CHAIR ABDEL-KHALIK: So is this issue going to be followed on?

MR. HEAD: Yes.

MEMBER BROWN: So for the RTIS as well,

or RPS, whatever.

MR. HEAD: The basically logic control, safety logic control system.

MR. MAUCK: My name is Jerry Mauck. During one of the ITAAC's has that the system has to be shown to be functional, as part of the ITAAC closure once the system is in, and also as part of the site acceptance testing you do an end to end test on it then.

MEMBER STETKAR: I just didn't see it specified in that way that you are saying it orally right now. Because in writing, the acceptance criteria specifies, it's where that ITAAC sits, it specifies under acceptance criteria -- in the FSAR now --

CHAIR ABDEL-KHALIK: Is the answer as simple as providing us this ITAAC, a reference to that ITAAC, then that would be adequate. If not, we are going to --

MEMBER STETKAR: Sure. It specifies a full end-to-end test.

CHAIR ABDEL-KHALIK: Right. Okay, thank you. Please proceed.

MR. SWANNER: Sure. And then the first question that you had on Chapter 7, moving on to --

CHAIR ABDEL-KHALIK: There is a question about the steam line velocity.

MR. HEAD: That will be Chapter 3.

CHAIR ABDEL-KHALIK: Okay, that's fine.

MR. SWANNER: Moving on to the four questions that you had for Chapter 7, the first one as I understood it, please correct me if I'm misstating the question, but it's where in the application are there are required ESF actuation logic redundancy specified?

MEMBER STETKAR: I am not sure whether you stated the question correctly. That's not what I asked, but let's see what you answered.

MEMBER BROWN: Just tell him your question.

MEMBER STETKAR: What I'm interested in is seeing where in the FSAR I can find the information that we were discussing earlier with respect to coincidence logic within a single division, for actuation of ESF equipment. So if that is what you are -- because I know I can find different divisions for equipment.

MR. SWANNER: That is what I am trying to answer.

There have been several RAIs on this issue as you are well aware. The first one was our response to 07.03-1, which you may have in front of you. The other one was a response to 07-9, and both of those -- one of the RAIs describes the list of tech spec functions for ESF, and describes which one is -- has required redundancy in the division, and which one goes to one-out-of-one voting, and then in 07-9, it describes the I guess criteria for how we selected the redundancy for each of the functions. That information resides, and I think you located the place in the FSAR, it is again in the tech spec bases, it's in the description for 3.3.1.4, and then as well it's shown in the figures B.3.3.1.4.-1, through 5. And it's only shown as a system level, like for example, 3.3.1.4-4 shows the ADS logic; 3.3.1.4.-3 shows the HPCF C logic. 3.3.1.3-2 shows the remaining ECCS logic, things like low pressure flutter, RCIC and HPCF and then the 3.3.1.1 -- or 3.3.1.4-1 shows the remaining systems that are actuated by ESF.

MEMBER STETKAR: And that is literally the way to interpret those figures, such that every piece of equipment which is associated with low pressure flooding divisions B and C, for example, apply the logic that is shown in 3.3.1.4-2.

MR. SWANNER: That is correct.

MEMBER STETKAR: Would apply to that. Okay. That probably -- that's the way to interpret that, then that would satisfy what I'm interested in, because someone could indeed go confirm that indeed that equipment was actuated that way. Behind all of this is actually a deeper question regarding why the redundant design -- as I understand it, the redundant -- I won't call it redundant -- the two out of two coincident logic has been removed from the certified design for whatever the set of equipment that is controlled under B.3.3.1.4-1 which is containment isolation and a number of what you call ESF support functions, which I have to go look at, which there are some cooling water systems in there, ventilation, things like that. So there is apparently a rationale behind that.

MR. SWANNER: There is, and that is described in the responses to 7.3-1 and 07-9.

CHAIR ABDEL-KHALIK: Okay.

MEMBER STETKAR: Okay.

CHAIR ABDEL-KHALIK: Proceed.

MR. SWANNER: The next one is I believe on standard departure 7.2-2, and that would be on backup SCRAM.

MR. CHAPPELL: My name is Coley Chappell

with STP 3 and 4 setpoint licensing, and I had the pleasure to address ACRS on a number of earlier occasions, and I'm glad to be here again today. I will handle a couple of questions. The first is, on the departure 7.2-2 it's a standard departure, this cleared up a description in Tier 2 that shows that the backup relays are energized. The backup relays, in order to energize a SCRAM, they are energized in a logic that is two out of two, so two channels coincident, that would then energize a relay, and they are redundant channels. So therefore no single failure can prevent or cause an actuation of the backup SCRAM function.

The description that is provided on the figure shows on the left hand side for a normal SCRAM that the relays are open. On the right hand side it shows the relays closed. And it's a power distribution system, but that shows what a trip condition is on the relays. That is based on the DCD information as shown on that data.

MEMBER STETKAR: You are going to have to walk me through that again. I'm sorry, I hate to be really dense about it, but you are going to have to walk me through it again.

MR. CHAPPELL: The description is correct in that it describes an energized to actuate backup SCRAM function.

MEMBER STETKAR: Energize to actuate backup SCRAM function?

MR. CHAPPELL: That is correct.

MEMBER STETKAR: Okay.

MR. CHAPPELL: So the logic is that two out of two, coincident channel, will energize the relay, will energize the solenoid, close the relay.

MEMBER STETKAR: Close the relay.

MR. CHAPPELL: And then will energize the solenoid valves that will then vent the SCRAM air header.

MEMBER STETKAR: Got you.

MR. CHAPPELL: There are redundant channels, so if one channel has a failure in it, the redundant channel will actuate those valves.

MEMBER STETKAR: Okay, I understand that. I am still not clear -- I am looking at a figure 7.2.8 in the FSAR that shows the relay contacts in a -- I'm an electrical engineer so look at normally closed contacts as the thing when the coil is deenergized. And it shows a bunch of normally closed contacts as energizing the SCRAM solenoid valve, which is, and I will quote from the design DCD, this is from the design DCD Section 7.2.1.1.4.1, normally closed relay contacts are arranged in a SCRAM logic circuitry between the air header dump valve solenoids and the air header dump valve solenoid 125 volt DC power source such that when in a trip state, parenthesis, coiled deenergized, the relays will cause energization of the air header dump valve solenoids, air header dump initiation.

So that says in the original design it was as it is shown as an electrical engineer, I would understand this figure such that when you deenergize the relays you would energize the solenoid and dump the air, and from what I understood you to say is that it has now been changed to energizing those coils to energize. So that is a change in the way that those interface relays work.

A point to the staff now, staff's SER concludes that indeed this is acceptable because -- let me see -- I can't find the quotation. They essentially did that all they did was clear up and make the way the system operates consistent with the way it's shown on the drawing. That is not true. It was changed.

MR. CHAPPELL: I may comment on that and simply say that in the way that the description is written, the way it's described on a normal SCRAM, the way it is described for a backups SCRAM.

MEMBER STETKAR: I'm not arguing about the normal SCRAM. I'm going to keep focus over here on the backup SCRAM.

MR. CHAPPELL: I also, sort of used to looking at the prints in a certain way. This print is confusing to me in the sense that I have to compare both left-hand and right-hand sides because it is described as a power distribution. It's showing on the power, on the left-hand side the normal SCRAM, those contacts are normally closed.

MEMBER STETKAR: That's right, the relays are normally energized. I'm an electrical engineer. I understand how those A contacts work.

MR. CHAPPELL: Right, and so what it's shown is, on that print it's shown in trip condition.

MEMBER STETKAR: Yes.

MR. CHAPPELL: And on the right-hand side those contacts are shown closed, which would not be a trip condition under a description -- well, if the description in the DCD were correct is what I would say. And the description in the DCD compared to the design that is provided in the COL with the departure 7.3.9. 3.

MEMBER STETKAR: Let me see if I -- I am probably being too dense here. In the original DCD design, was it necessary to energize a SCRAM, a backup SCRAM air header dump valve solenoid to dump the air? Did I need to actually apply voltage across the solenoid coil for the dump valve, for the solenoid valve, in the original design, yes or no?

MR. CHAPPELL: I can't answer that question, and the reason I can't answer that question is because I looked at this one issue, this one paragraph, but not at the extended condition.

MEMBER STETKAR: Okay, because if I read the words and I look at the drawing, again, this is from the DCD, it says -- I hate reading this stuff -- when in a tripped state -- they are talking about -- I don't want to quote the whole thing again -- when in a tripped state coil deenergized the relays will cause energization of the air header dump via solenoids. That is a pretty clear statement that seems consistent with the drawing that I'm staring at.

So it seems like the original design was an energize to dump the back SCRAM air header -- energize the solenoid valve.

MR. CHAPPELL: Right.

MEMBER STETKAR: And what I've heard you

say that that is still the case, I still need to energize those solenoids to dump the backup --

MR. CHAPPELL: You still energize --

MEMBER STETKAR: Energize the solenoids.

MR. CHAPPELL: It's still energize to actuate.

MEMBER STETKAR: Right, so now the question is, how do those relays in between work? Because in the original design I used to remove power from the relay coil to get the output contacts to close to apply power to the solenoid. And what I heard you say -- and I might be wrong -- but from what I heard you say I now need to apply power to the relay coil to close the output contacts from that relay to apply power to the solenoid. Is that correct?

MR. CHAPPELL: It does apply power -- it does require power application to the relay to cause the contact to close is my understanding.

MEMBER STETKAR: So you've changed the way those relays operate from the design, from the certified design?

MR. CHAPPELL: That is my understanding.

MEMBER STETKAR: Okay.

CHAIR ABDEL-KHALIK: Is the documentation adequate?

MEMBER STETKAR: Yes, well, it's -- I am not sure that an electrical engineer will look at the drawing and understand the way it works, which is why I raised the question initially. It's not clear to me that the staff had a full understanding that that part of the design had been changed.

Now is it an important change in the design? I'm not going to the issue of value judgment. But it is a change in the design, and it fundamentally changed a failure mode, a deenergize to actuate the safe condition for those relays, to an energize to actuate the safe condition of those relays. So it's not something that is simply clearing up the potential misinterpretation of a drawing; it seems to be an actual change to the design. I don't know why the change was made, but it seems to be a change unless I am misinterpreting something.

MR. CHAPPELL: Fundamentally the normal SCRAM function is a deenergize to actuate, so a loss of power --

MEMBER STETKAR: I'm not arguing about the normal SCRAM function.

MR. MURRAY: Have we made an actual change, is the --

MEMBER STETKAR: I am only talking about

the backup SCRAM function. As best as I can tell there has been absolutely no change in the normal SCRAM function, and I understand the verbal description of that, and I can look at the electrical drawing, and I can see how that works.

Look at Figure 7.28 and how the system now works, and see whether or not those contacts make sense.

CHAIR ABDEL-KHALIK: STP will clarify this.

MR. HEAD: And we will have an interaction with the staff on whether there needs to be additional clarification, an update of some sort.

CHAIR ABDEL-KHALIK: Okay, thank you.

MR. MAUCK: Let me add one point to that. The name is Jerry Mauck. I'm with STP I&C. That ARI SCRAM system is there only to meet the ATWS rule 10 CFR 50.62, which is never deenergize to actuate; it's always energize it to actuate. So it meets the ATWS rule.

MEMBER STETKAR: It does, and the final end device, the solenoid, has always been -- they solenoid valve to dump the air header pressure has always as best as I can tell been an energize to actuate. It's just how I get that thing energized seems to have changed.

MR. TONACCI: Excuse me, this is Mark Tonacci, why don't we take an IOU on this one?

CHAIR ABDEL-KHALIK: Thank you.

MR. SWANNER: And I apologize a little bit for backtracking to the first one where we talked about the ITAAC and the ITAAC that were mentioned, the two ITAAC that are relevant in that case is Table 3.4-1, ITAAC No. 2 -- excuse me, Table 3.4 ITAAC 2, and in the case of reactor protection it's Table 2.2.7, ITAAC No. 2, and if you go and follow the systems, for example ESF and neutron monitoring you will find similar comprehensive tests, end-to-end tests, in ITAAC in each of them.

MEMBER STETKAR: Thanks, that's -- that will at least point us toward a reference.

MR. HEAD: But they don't say end to end, they say --

MEMBER STETKAR: They don't. They say comprehensive.

MR. SWANNER: Yes.

MEMBER BROWN: You said 2.2.7?

MR. SWANNER: 2.2.7 is for RPS, and 3.4 is for general SSLC. It's somewhat repetitive, I agree.

MEMBER BROWN: I went through 3.4, let me tell you, it was number what?

MR. SWANNER: Tests will be performed --

MEMBER BROWN: Didn't change in the SR?

MR. SWANNER: Yes, tests will be performed on as-installed SSLC, using simulated input signals. System outputs will be monitored to determine operability of function -- of safety-related functions.

MEMBER STETKAR: But again that is pretty general.

MEMBER BROWN: That's high level, that is so general it could be anything. Somebody could --

(Simultaneous speaking.)

MR. SWANNER: 2.2.7.

MEMBER BROWN: I had that one. Item which?

MR. SWANNER: Item two.

MEMBER BROWN: I don't have that layout.

MR. SWANNER: I can read that one as well,

MEMBER BROWN: Get those iPods moving, right?

MR. SWANNER: Tests will be conducted using simulated input signals for each process variable to cause trip conditions in two, three and four instrument channels of the same process variable of the RPS. The acceptance criteria: the RPS load drivers, change their states to interrupt electrical power to SCRAM solenoids, RPS backup SCRAM relays close and RCIS relays close to provide signals to RCIS.

MEMBER STETKAR: That is a little more comprehensive.

(Simultaneous speaking.)

MEMBER STETKAR: That is pretty clear. That is pretty clear.

MEMBER BROWN: We can buy that one.

MR. SWANNER: And I haven't looked at the ones for ESF. They are in section 2.3 of Tier 1.

CHAIR ABDEL-KHALIK: If you could follow up on that?

MR. SWANNER: Okay, moving on quickly, there was another question regarding standard Departure 7.2-6, and that was regarding the high drywell pressure, there appeared to be a change that the range in the instrumentation was set above -- above the normal atmospheric value, and so you couldn't get that indication. I believe this is just somewhat of an interpretation problem in the COLA. If you go back and look at Table 7.2-1, there are some strikeout beside this value range, and that strikeout is a solid line, and then the next value is 15 KPAG, but if you look close at the 15 KPAG, there is actually a negative sign beside it. So it's negative KPAG to 30 KPAG --

MEMBER STETKAR: Hokey smokes. That is "hokey smokes" for the recorder. Thank you.

CHAIR ABDEL-KHALIK: Okay, thank you.

MEMBER STETKAR: So thank you.

MR. SWANNER: And the last one was on 7.3-9, and that is on shutdown cooling, and I will turn that over to Coley.

MR. CHAPPELL: So I'll continue discussion on the follow-up items on Standard Departure 7.3-9. First of all I want to clarify the description of the design. The suction isolation valves inboard and outboard isolation valves on RHR shutdown cooling receive isolation signals from Level 3 drywell pressure, high drywell pressure, and lead detection. There is another suction isolation valve that is interlocked, closed, with an ECCS initiation signal. The purpose of this isolation valve is to align the RHR system in a low pressure flutter mode upon initiation of ESF. That initiation can be from

Level 1, or it can be from high drywell pressure. But the signal actually comes from the ESF initiation, so it's not a direct Level 1 initiation signal that is confirmatory or anything for a shutdown cooling isolation valve, and it's a different set of valves. The actual containment isolation valves are isolated by a Level 3; that has not changed. So the intent of the departure was to clarify this description. I think we will maybe take a look at that and make sure that we have done so.

MEMBER STETKAR: I was writing notes. Just run it by me quickly again.

MR. CHAPPELL: Okay, effectively there are three valves.

MEMBER STETKAR: Yep.

MR. CHAPPELL: There are two inboard -- there's an inboard and outboard isolation valves.

MEMBER STETKAR: Right.

MR. CHAPPELL: That receive a Level 3 isolation signal among others. There is a third shutdown cooling suction valve whose purpose is to align the RHR system to low pressure flutter mode. It does that upon an ECCS initiation signal of which are included Level 1 and hydraulic pressure. So the design has not changed.

MEMBER STETKAR: Has not changed, I was trying to clarify which valves are actuated by which station.

MR. CHAPPELL: Which of the valves are repositioned. All of the valves are normally closed.

MEMBER STETKAR: Yes, okay, thank you.

CHAIR ABDEL-KHALIK: So I guess the question that was raised in much simpler terms, do we get a low pressure safety injection if the Level 3 signal failed?

MR. CHAPPELL: If -- well, those valves are normally closed, and the overriding condition -- the reason those valves are closed is in order to ensure that you don't drain the vessel, and the overriding function is to inject. So there is no interlock back from those valves that would present an injection if those -- if those valves were closed, but that signal failed, those valves would still be closed, and the suppression of the suction valves would still be --

MEMBER STETKAR: I was thinking -- I try to think about safety across all operating modes, so I was thinking in low pressure cooling conditions, if you had a loss of coolant, indeed, when you were lined up for shutdown cooling, and those valves would be opened, I don't know when your protection -- do you keep your protection system enabled during --

MR. CHAPPELL: In all modes you are required to maintain the minimum number of operable systems. So if you have -- if all the valves are open that would be inoperable for the low pressure flooder, because the suppression pool cooling suction is interlocked closed.

MEMBER STETKAR: If those valves are open. On the other hand if they get a signal to close from a Level 3 and they close, you should be able to initiate an injection?

MR. CHAPPELL: There are a number of factors, but that seems logical.

MEMBER STETKAR: Okay. I think the fundamental point is, I don't think they have changed the design here. I think it's partly my misinterpretation of the wording and not being able to fight through the logic diagrams, quite honestly. From what I heard you say it hasn't really changed.

MR. CHAPPELL: Correct.

MEMBER STETKAR: Thanks.

CHAIR ABDEL-KHALIK: Is there anything else that we need to follow up on, or that completes the list of items?

MR. HEAD: That completes our feedback for the day.

CHAIR ABDEL-KHALIK: And I guess there are follow-up to the follow-up items that you will come back to us and to the staff?

MR. HEAD: Yes.

MEMBER STETKAR: And by the way, as critical as I am, thanks a lot. I know you guys did a lot of quick searching, so I really appreciate that.

CHAIR ABDEL-KHALIK: Thank you very much.

MR. HEAD: We appreciate the opportunity to provide the feedback today.

CHAIR ABDEL-KHALIK: Thanks.

PUBLIC COMMENT

CHAIR ABDEL-KHALIK: At this time on our schedule we are to provide an opportunity for public comments, and therefore I've asked our staff enable this phone line for any member of the public who has joined us in this meeting to make any statements or comments.

Is the phone line open? Are there any members of the public who wish to make a comment?

(No response.)

Let's just verify that the phone line is open before we terminate this process.

MR. HACKETT: The line is open.

CHAIR ABDEL-KHALIK: Is there any member of the public who wishes to make a comment?

(No response.)

The answer is none, so let's proceed to the next item on the agenda, which is the closure, subcommittee discussion ands closing remarks.

SUBCOMMITTEE DISCUSSION AND CLOSING REMARKS

CHAIR ABDEL-KHALIK: I would like to just go around the table and see if the people have any additional comments or questions or closing remarks.

Charley.

MEMBER BROWN: I think mine got answered at this point other than the one open item still on the site and security, whenever we see that, so I'll hold that one in abeyance. I've still got to think about the deterministic discussion that we had; that was a good discussion, but I need to go integrate some of that.

CHAIR ABDEL-KHALIK: Thank you. John.

MEMBER STETKAR: My only comment is a fairly general comment, and that is because of the importance of instrumentation and control, I'll stay away from the digital aspect of that, I think it's very important that the documentation in the FSAR at the COL stage contains consistent and enough detailed information such that when those ITAAC inspections are performed, the inspectors indeed have sufficient information so that they can confirm that the design is actually implemented according to at least the functional logic. So that's my only -- the reason I was asking several of these questions was to try to examine that level of detail, and to try to highlight areas where it may not be quite as clear in the FSAR, thinking from the perspective of somebody who is going to go out and actually try to verify that the design is installed in the way that it is supposed to be. That -- I've gotten some assurance that that information is available. I'm not quite there yet on some of the other stuff.

CHAIR ABDEL-KHALIK: Okay, Sam?

MEMBER ARMIJO: No comment.

CHAIR ABDEL-KHALIK: Bill?

MEMBER SHACK: For a nonprofessional, I just want to say I thought it was a very helpful discussion today.

MEMBER RYAN: No additional comments, but thanks for everybody's participation.

CHAIR ABDEL-KHALIK: Mario.

MEMBER BONACA: I share John's views on a number of items, and you know I wonder if there is more there of the same type, which is not necessarily a misrepresentation but an inconsistency between what is in the text of the FSAR and the plant as built. So I'm sure that with time we will get a better understanding, but in general I learned quite a bit today.

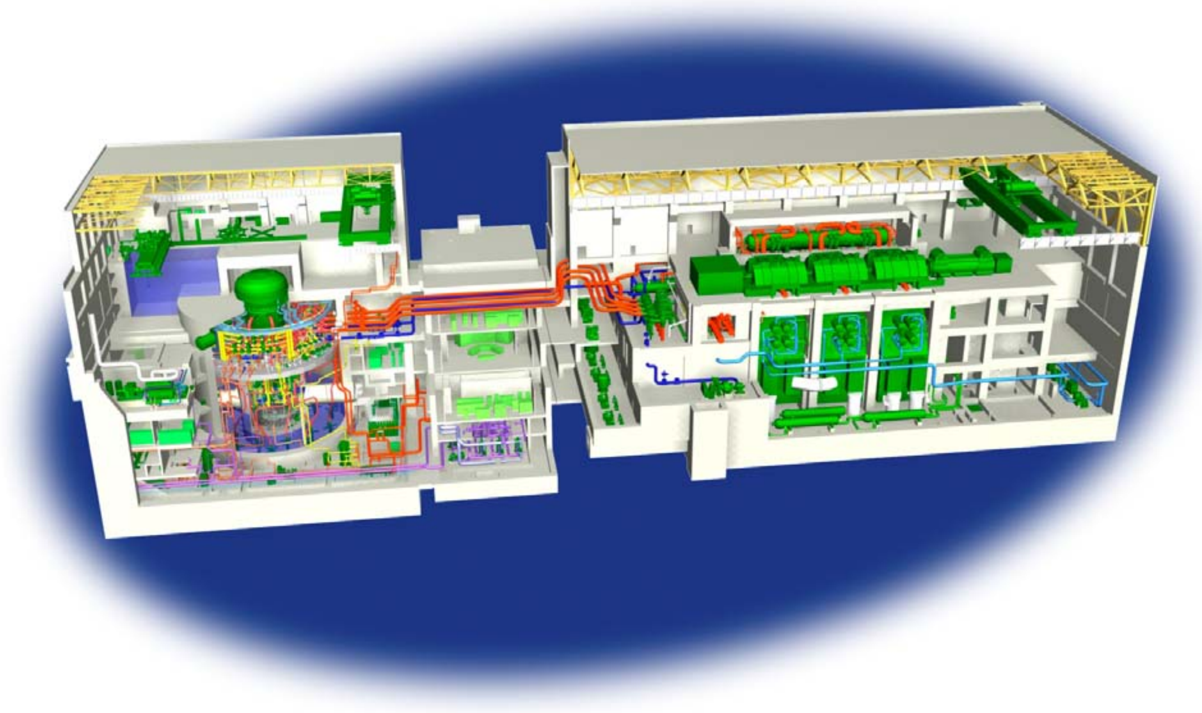
CHAIR ABDEL-KHALIK: Okay, thank you. Well, let me express the committee's appreciation to STP and the staff for a really informative presentation today. Thank you very much.

Meeting is adjourned.

(Whereupon, at 3:47 p.m., the proceeding in the above-entitled matter was adjourned.)

South Texas Project Units 3 & 4 Presentation to ACRS Subcommittee

Chapter 14
Initial Test Program



Agenda

- Introduction
- Summary
- FSAR Chapter 14 Contents
- Departure Information
- COL License Information Items
- Site-Specific Supplements
- ITAAC
- Initial Test Program Implementation
- Flow Induced Vibration
- Conclusion

Attendees

Scott Head	Regulatory Affairs Manager, STP 3&4
Steve Blossom	Construction/Startup/ITAAC Manager, STP 3&4
Chikashi Miyamoto	Pre-Operation & Startup Test Group, Toshiba
Jay Phelps	Operations Manager, STP 3&4
Steve Cashell	Licensing, STP 3&4

Chapter 14 Summary

- The Initial Test Program (ITP) includes the testing activities that will be conducted following completion of construction and extends through to the start of commercial operation.
- The ITAAC define activities that will be undertaken to verify the as-built system conforms with the design features and characteristics defined in the design description for that system.

Chapter 14 Contents

Departures - Test Descriptions

- STD DEP T1 2.4-3
  - RCIC pump/turbine design changes
- STD DEP T1 2.14-1
  - Hydrogen recombiner elimination
- STD DEP T1 3.4-1
  - I&C architecture and nomenclature changes
- STD DEP 4.6-1
  - CRD performance testing equipment (CRD pump vs. separate pump)
- STD DEP 8.3-1
  - Plant medium voltage design changes
- STD DEP 9.1-1
  - Fuel storage and handling equipment changes

Departures - Test Descriptions

- STD DEP 9.5-1
  - RG 1.108 withdrawn in August 1993, replaced by RG 1.9.
- STD DEP 11.2-1
  - Liquid radwaste process equipment changes
- STD DEP 11.4-1
  - Solid radwaste process equipment changes
- STD DEP 14.2-1 (Table 14.2-1)
  - CRD friction test at rated pressure eliminated
- STD DEP Vendor
  - Replaces the reference to GEH as the NSSS vendor with the generic term “NSSS vendor.”

Tier 1 Departures affecting ITAAC

- STD DEP T1 2.2-1
  - RCIS power supply testing to verify Operability with 1 UPS
- STD DEP T1 2.4-1
  - Testing of additional third RHR loop to spent fuel pool
- STD DEP T1 2.4-3
  - RCIC turbine testing for new design
- STD DEP T1 2.12-1
  - Shop testing of min & max voltage vs. field testing
- STD DEP T1 2.14-1
  - Hydrogen recombiner elimination
- STD DEP T1 3.4-1
  - I&C architecture and nomenclature changes

Site-Specific Supplements

- Startup Administrative Manual
- 14.2S.1 - Organization and Training in Support of the ITP
- 14.2S.2 - First of a Kind Systems
- 14.2S.3 - Overlap of Unit 3 Test Program with Unit 4 Test Program
- 14.2S.4 - Testing Required to be Completed Prior to Fuel Load
- 14.2S.12 - Site Specific Test Descriptions
- 14.3S - Selection criteria for site-specific systems, Emergency Planning and Security ITAAC

COL License Information Items

- Items 1, 2 and 3 - The site-specific Preoperational and Startup Test Specifications, containing testing objectives and acceptance criteria, will be provided to the NRC at least 6 months prior to the start of the Initial Test Program. (COM 14.2-2)
- Item 4 – The approved preoperational test procedures will be available for NRC review approximately 60 days prior to their intended use but no later than 60 days prior to fuel loading (Subsection 14.2.3) (COM 14.2-3).
  The approved startup test procedures will be available for NRC review approximately 60 days prior to fuel loading (Subsection 14.2.3) (COM 14.2-4)
- Items 5, 6, 7, 8 and 9 - The Startup Administrative Manual has been submitted, which delineates the processes that will be used to administer the Initial Test Program.

ITAAC

- The selection criteria and methodology provided in Section 14.3 of the reference ABWR DCD for the certified ABWR design were utilized as the site-specific selection criteria and methodology for inspections, tests, analyses, and acceptance criteria (ITAAC) including those applicable to the emergency planning and physical security hardware.

- The emergency planning ITAAC conform to the guidance provided in Sections C.I.14 and C.II.1 of Regulatory Guide 1.206, as modified to reflect the design and specific emergency planning program requirements.

- The security ITAAC conform to the guidance in Appendix C.II.1-C of Regulatory Guide 1.206, as modified to reflect the design and site-specific security requirements.

Initial Test Program Implementation

- Steve Blossom
  - Construction / Startup / ITAAC Manager

Initial Test Program Test Phases

- The Initial Test Program consists of the following distinct phases:
  - Construction Test Phase
  - Preoperational Test Phase
  - Startup Test Phase

Preoperational and Startup Test Procedure Content and Format

- Test procedure content and format will follow guidance of Reg. Guide 1.68 with the following key sections:
  - Purpose
  - Acceptance Criteria
  - Precautions
  - Initial Conditions/Prerequisites
  - Test Procedure
  - Analysis and Evaluation
  - Data Collection
- Additional Reg Guides used in the development of the ITP are listed in Section 14.2.7

Startup Organization –
Construction and Preoperational Test Phases

- Engineering, Procurement and Construction (EPC) contractor responsible for developing the test program:
    - EPC Startup Manager responsible for day-to-day activities of Preoperational Test Group.
    - EPC Startup Manager responsible for ensuring smooth interface between STP Plant Staff and Testing organization.
    - Joint Test Group review and approval all preoperational test procedures and test results.

System Turnover Process

- **System Turnover**: Jurisdictional transfer of systems, subsystems or equipment from Construction to the Testing organization and from the Testing organization to STP.
  - EPC Construction team responsibility for outstanding construction work on released systems/equipment prior to final turnover to STP.
  - Internal system turnover: EPC Construction to Preoperational Test group for construction and preoperational testing.
  - Final turnover to STPNOC after preoperational testing and prior to fuel load and the Startup Testing phase.

Completion of Inspections, Tests, Analysis and Acceptance Criteria (ITAAC)

- All ITAAC (Tier 1 and Site Specific) completed prior to Initial Fuel Load (approximate per unit)
  - 939 ITAAC for the ABWR (including site-specific ITAAC).
  - 356 ITAAC or ~ 38% completed during the Construction and Preoperational Test Phases.
  - Completion of testing ITAAC requires close coordination between EPC Testing organization and EPC ITAAC Completion Organization (ICO).
  - STP Startup/ITAAC Manager provides oversight of the EPC ICO.
  - 10 CFR 52.99(a) and 10 CFR 52.103(g) processes.

Startup Organization –
Startup Test Phase

- At fuel load, STP Startup Manager assumes responsibilities of EPC Startup Manager including:
  - Startup Test Group day-to-day activities.
  - Responsibility for ensuring smooth interface between STP Plant Staff and Testing organization.
  - The Plant Operations Review Committee (PORC) will be responsible for review of safety related operating procedures, test procedures, test results and other startup test documents, as instructed by the Plant General Manager.

Completion of Startup Testing Following Initial Fuel Load

- STP Startup Manager provides technical direction of plant startup activities.

- STP operations staff under the leadership of the Operations Shift Supervisor responsible for the operation of the plant.

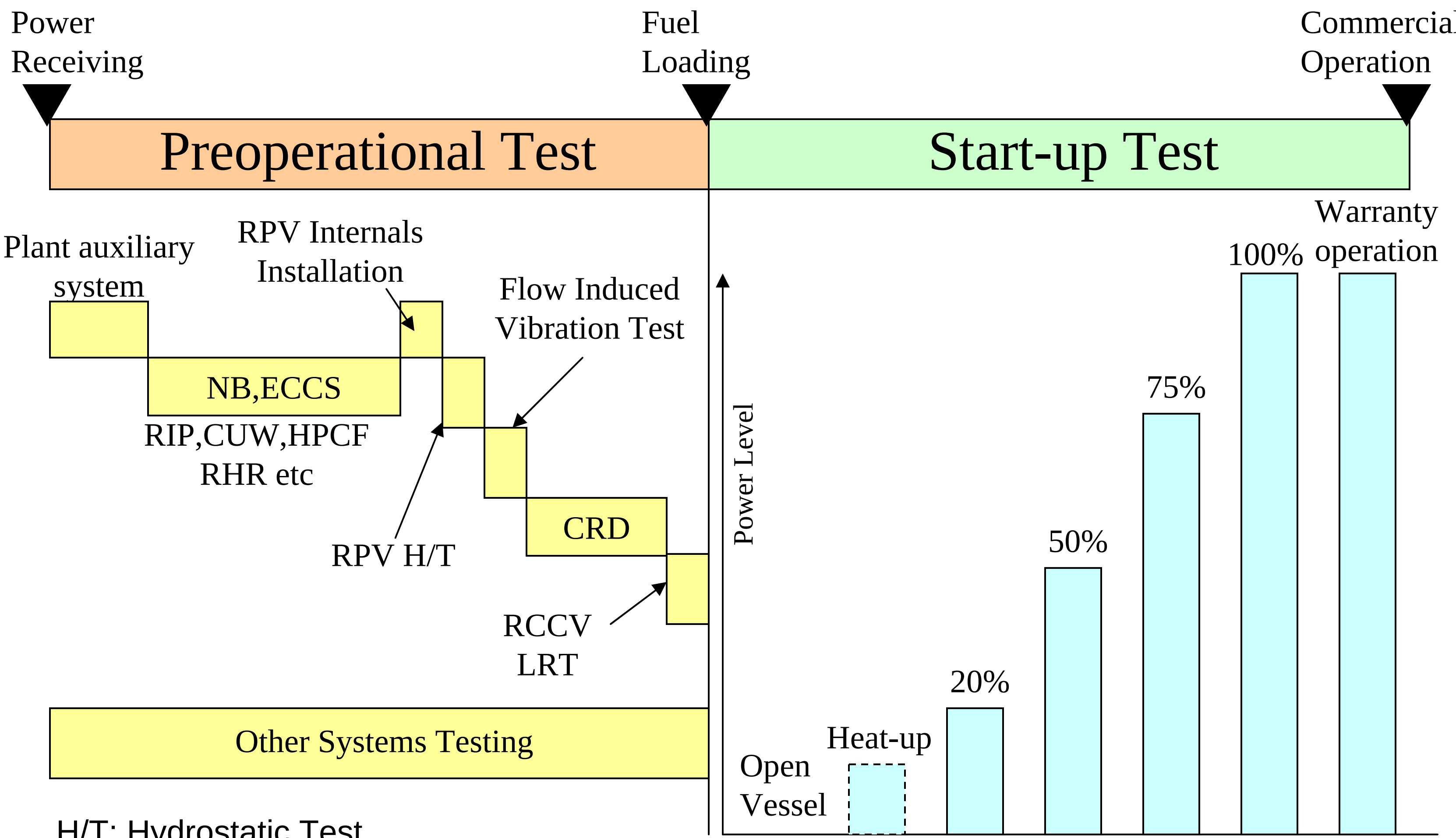
- Startup test performance and data collection done by members of the Startup Test Group as directed by STP Startup Manager.

Toshiba experience in ABWR Construction and Initial Test Program

Plant	Rated power (MWe)	Construction period (months) Note 1	Preoperational test period (months) Note 2	Start up test period (months) Note 3	COD	ITP Lead	Nuclear Island (NI) Constructor	Turbine Island (TI) Constructor
Kashiwazaki-6 (K-6)	1356	51	10	11	1996/Nov	**Toshiba**	**Toshiba**/GE	Hitachi/GE
Kashiwazaki-7 (K-7)	1356	51.5	12	9	1997/Jul	Hitachi	Hitachi/ GE	**Toshiba**/GE
Hamaoka-5 (H-5)	1380	56	13 Note 4	11	2005/Jan	**Toshiba**	**Toshiba**	Hitachi

Notes:
1. Bedrock inspection to Commercial Operation Date (COD)
2. Initial power receiving to Fuel Loading
3. Fuel Loading to COD
4. Includes non-technical delay, effective test period is ~10 months

Outline of Preoperational and Startup Tests



H/T: Hydrostatic Test

LRT: Leakage Rate Test

Flow Induced Vibration

- STP Unit 3 is designated as a prototype plant in accordance with the guidance of RG 1.20, Rev. 3
    - STP-specific predictive analysis
    - Using K-6 test results to inform scope of STP-3 program
    - STP-4 will be “Category I non-prototype”
- Approach similar to dryer qualifications for EPUs at operating BWR plants
- Deliverables in support of COL will be reports that summarize the analytical models, validation, and predictive analysis results for the steam dryer and the remaining reactor internals, including a summary of the instrumentation and inspection plans
    - Initial Acoustic Screening report 1-June
    - MSL /Steam Dryer subscale testing report 30-Sep
    - FIV assessment program report 15-Dec
    - Steam Dryer High Cycle Fatigue report 15-Dec

Chapter 14
Initial Test Program

Questions and Comments

Presentation to the ACRS Subcommittee

South Texas Units 3 and 4 COL Application Review

SER/OI Chapter 14
"Verification Programs"

May 20, 2010

Staff Review Team

- **Project Managers**
  - George Wunder, Lead Project Manager, DNRL/NGE2
  - Stacy Joseph, Chapter Project Manager, DNRL/NGE2

- **Technical Staff Reviewers**
  - Frank Talbot, CQVA
  - Dinesh Taneja, ICE2
  - Bhupendra Bhatia, Amar Pal, EEB
  - David Jeng, SEB2
  - Yuken Wong, EMB2
  - George Thomas, SRSB
  - Raj Goel, SBCV
  - Steven Williams, Robert Kellner, CHPB

Summary of Technical Discussion Points for South Texas COL Chapter 14

FSAR Section		Summary of Information Reviewed
14.2	Initial Plant Test Program	Tier 1 and Tier 2 Departures COL License Information Items – Proposed License Conditions Open Items
14.3	Tier 1 Departures	Brief description explanation of Review Strategy
14.3S	ITAAC	Design Certification Departures Site Specific ITAAC

Summary of Information Reviewed in STP Units 3 and 4 SER 14.2, Initial Test Program

- Reviewed Section 14.2 using the guidance in:
  - NUREG-0800, SRP 14.2
  - Regulatory Guide (RG) 1.206, C.I.XIV
  - RG 1.68, and 18 other RGs (e.g., RG 1.20) referenced in RG 1.68
- Section 14.2 Incorporated by reference with the exception of:
  - (3) Tier 1 Departures
  - (9) Tier 2 Departures
  - COL License Information Items
  - Startup Administrative Manual
- The staff issued 13 Requests for Additional Information (RAIs)
- Two remaining Open Items

Open Items

- STPNOC originally cited Japanese Reference ABWR as prototype for Flow Induced Vibration Assessment Program (FIVAP)
- STPNOC now using STP Unit 3 as the prototype plant and STP Unit 4 is the non-prototype category I plant.
- STPNOC plans to submit revised responses to RAIs regarding the FIV preoperational and startup test abstracts.
- FIV test abstracts for STP Unit 3 (prototype) will be incorporated by reference.
- The revised FIVAP for Unit 4 non-prototype category I plant will be evaluated in Sections 3.9.2 and 14.2.

License Conditions

- STP proposed 3 post COL commitments to address COL License Information Item for "Test Procedures/Startup Administrative Manual"

- The staff identified that the commitments should instead be license conditions

- The staff proposed five post COL license conditions for STP Units 3 and 4 ITP in the following areas:
    - Preoperational and Startup Test Specification and Test Procedures
    - Startup Administration Manual
    - Startup and Power Ascension Test Phase Results
    - Test Program Schedule
    - Test Changes

- The staff sent RAI requesting applicant inform the staff if the above proposed license conditions are considered appropriate

14.3 Tier 1 Selection Criteria and Processes

- Chapter 14.3 of FSAR incorporated by reference
- Chapter 14.3 SER is a summary of the 12 Tier 1 Departures and 1 Tier 2* Departure reviewed in Revision 3 of COLA
- Chapter 14.3 SER points to the evaluation of each Tier 1 and Tier 2* departure in the respective Tier 2 chapters

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

14.3S Inspections, Tests, Analysis and Acceptance Criteria

- Design Certification ITAAC (6 departures to Tier 1 DCD Chapters 2 and 3)
  - Staff concluded that the proposed ITAAC will ensure that the system will perform in accordance with its design
  - No open items
- Site Specific ITAAC (developed to correspond with the interface requirements identified in DCD Tier 1 chapter 4)
  - Ultimate Heat Sink (evaluated in 9.2.5)
  - Offsite Power System
  - Makeup Water Preparation System (evaluated in 9.2.8)
  - Reactor Service Water System (evaluated in 9.2.15)
  - Turbine Service Water System (evaluated in 9.2.16)
  - Circulating Water System (evaluated in 10.4.5)
  - Backfill Under Category 1 Structures (additional evaluation in Chapter 2)
  - Breathing Air System

14.3S ITAAC

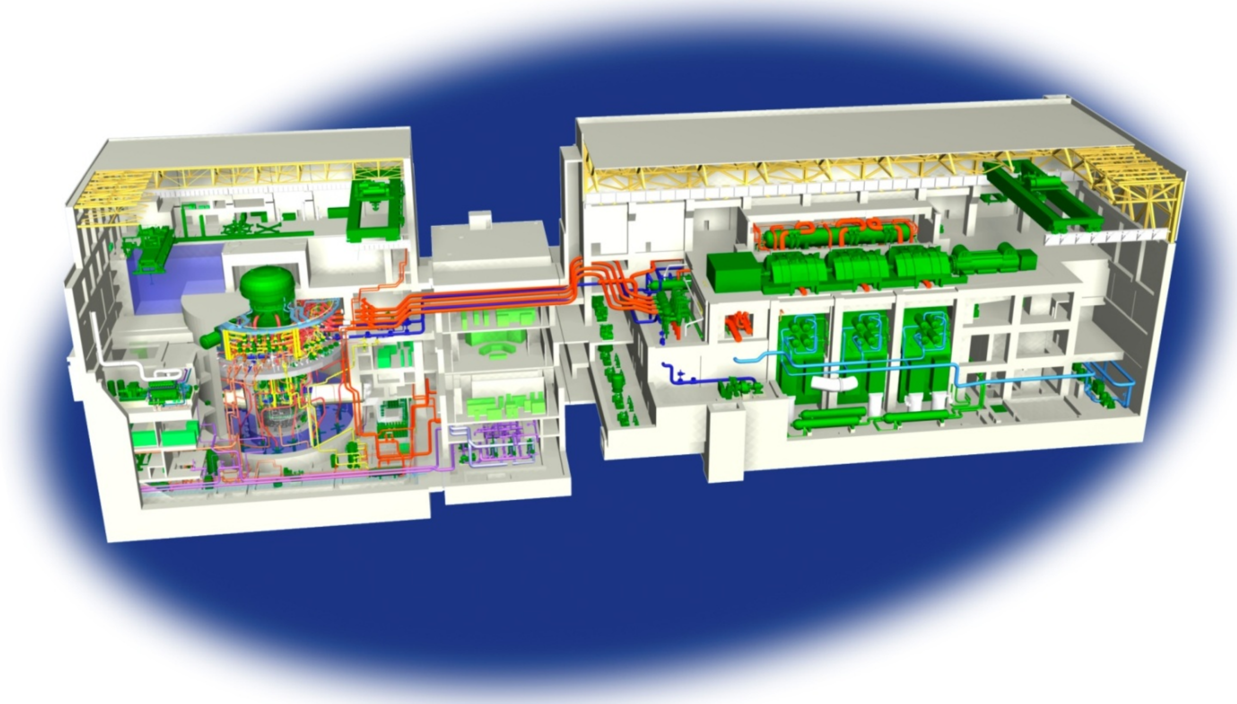
- Site Specific ITAAC - Continued
  - The structural aspects of the site-specific ITAAC are evaluated in the 14.3 SER
  - Two open items in SER are now considered closed
    - General question regarding process for performing structural analysis ITAAC
    - Requesting addition of ITAAC for Diesel Generator Fuel Oil Storage Vaults
- Emergency Planning ITAAC (evaluated in Chapter 13 of the SER)
- Physical Security ITAAC (evaluation will be added to SER during Phase 4)

Questions and Answers

- Questions
- Follow-up actions

South Texas Project Units 3 & 4 Presentation to ACRS Subcommittee

Chapter 7 Instrumentation and Control Systems



Agenda

- Introduction
- Summary
- Contents of Chapter 7
- Departure Information
- COL License Information Items
- Supplemental Sections
- I&C Protection Systems Basic Architecture
- Conclusion

Attendees

Scott Head	Manager, Regulatory Affairs, STP 3&4
Mike Murray	Manager, I&C Engineering, STP 3&4
Kyle Dittman	Supervisor, I&C Engineering, STP 3&4
Jun Ikeda	Vice President, I&C Engineering, TANE
Craig Swanner	Licensing, TANE (MPR)
Dr. Akira Fukumoto	Senior Fellow, Toshiba
Eric Fredrickson	Project Manager, Westinghouse

Attendees (cont'd)

Tim Hurst	I&C Engineering, STP 3&4
Jerry Mauck	I&C Engineering, STP 3&4
James Cook	Licensing, STP 3&4
Steve Cashell	Licensing, STP 3&4
Hiroshi Sakamoto	I&C Engineering, Toshiba
Tadashi Miyazaki	I&C Engineering, Toshiba
Toshifumi Sato	I&C Manufacturing, Toshiba
David Herrell	I&C Engineering, TANE (MPR)
Bradley Mauer	Licensing, Westinghouse
Robert Quinn	Licensing, Westinghouse
Ed Brown	I&C Engineering, Westinghouse
Chris Crefeld	I&C Engineering, Westinghouse
Cal Tang	I&C Engineering, Westinghouse
Bobby Bakshi	I&C Engineering, Westinghouse
Steve Frantz	Morgan Lewis

Chapter 7 Summary

- Tier 1 Sections 2.2, 2.7 and 3.4 and Tier 2 Chapter 7 describe the instrumentation and control (I&C) systems for STP 3&4.
- COLA incorporates by reference ABWR DCD information regarding functionality and logic of the I&C systems and components.
- Departures from the certified design taken to incorporate advancements in technology and provide clarifications.

Contents of Chapter 7

Contents of Chapter 7 (cont'd)

Departure Information

- Advances in Technology
  - Updated I&C Architecture
    - Replaced obsolete Fiber Distributed Data Interface (FDDI) multiplexer communication technology with current data communication technology
    - Simplification of Safety System Logic and Control (SSLC) design by separation into Reactor Trip and Isolation System (RTIS) and ESF Logic and Control System (ELCS)
  - Nomenclature changes improve standardization
    - Changed equipment description to functional description

      Examples include:
      - Trip Logic Unit (TLU) to Trip Logic Function (TLF)
      - Process Computer System (PCS) to Plant Computer Function (PCF)

Departure Information

- Advances in Technology (cont'd)
  - Selection of Final Controls Platforms
  - Incorporation of generic BWR I&C Enhancements

    Examples include:
    - Adoption of BWR generically approved Oscillation Power Range Monitor (OPRM)
    - Adoption of BWR generically approved removal of main steam high radiation Main Steam Isolation Valve (MSIV) closure trip

Departure Information

- Clarification of Content

  Examples include:

  - Expansion of the discussion of Automatic Depressurization System (ADS) initiation logic to improve understanding of bypass timer operation
  - Expansion of the discussion of the Residual Heat Removal (RHR) Suppression Pool Cooling (SPC) logic to enhance understanding of automatic and manual operations

Departure Information

I&C Systems Modified by Tier 1 Departures

- **STD DEP T1 2.2-1**, Control Systems Changes to Inputs, Tests, and Hardware
  - Rod Control and Information System (Test Clarification)
- **STD DEP T1 2.3-1**, Deletion of MSIV Closure and Scram on High Radiation
  - Reactor Protection
  - Process Radiation Monitoring
- **STD DEP T1 3.4-1**, Safety-Related I&C Architecture
  - Eliminate obsolete data communication technology
  - Eliminate unnecessary inadvertent ESF actuation logic
  - Clarification of digital control nomenclature and systems
  - Final selection of platforms
  - Testing and surveillance changes

Tier 2 Departures requiring NRC approval

Examples of departures impacting Technical Specifications include:

- **Standard departures STD DEP 7.7-10 and STD DEP 7.7-18**
  - Rod Control and Information System (RCIS) updated to comply with current design installed in operating ABWRs
  - Minor clarifications in Technical Specification bases
- **STD DEP 16.3-100, Setpoint Control Program Implementation**
  - Implements approach (Option 3) specified in Interim Staff Guidance (ISG-08)
    - New Technical Specification, 5.5.2.11, “Setpoint Control Program”
    - Project Document U7-PROJ-J-GDD-0018, “South Texas Project Advanced Boiling Water Reactor Instrument Setpoint Control Program Plan”
    - Setpoint Methodology based on WCAP-17119-P “Methodology for South Texas Project Units 3 & 4 ABWR Technical Specification Setpoints”

Tier 2 Departures NOT requiring prior NRC approval

Numerous Tier 2 departures not requiring prior NRC approval:

- All departures were evaluated based on the 10 CFR Part 52 process
- Typically used for clarification of content in I&C design
- Advances in design, for example
  - Average Power Range Monitor (APRM) and Oscillation Power Range Monitor (OPRM) trip signals separated

COL License Information Items

- **7.1 Cooling Temperature Profiles for Class 1E Digital Equipment**
  - Addressed by ITAAC Table 3.4 Item 14(b).
- **7.2 APRM Oscillation Monitoring Logic**
  - The APRM oscillation logic is implemented in accordance with the BWR Owners Group Stability Option III and described in Tier 2 Subsection 7.6.1.1.2.2.
- **7.3 Effects of Station Blackout on the HVAC**
  - Addressed by commitment COM 7.8-1.
- **7.4 Electrostatic Discharge on Exposed Equipment Components**
  - Addressed by ITAAC Table 3.4 Item 12.
- **7.5 Localized High Heat Spots in Semiconductor Materials for Computing**
  - Addressed by commitment COM 7.8-2.

Supplemental Sections

7.1S Instrumentation and Control Platforms

Provides information on the safety-related I&C systems:

- Reactor Trip & Isolation System (RTIS)
  - Provides the primary functions of Reactor Protection System (RPS), Main Steam Isolation and Suppression Pool Temperature Monitoring (SPTM)
- Safety-related Neutron Monitoring System (NMS) functions
  - Provides nuclear power related trips of RPS
  - Local Power Range Monitor (LPRM), Average Power Range Monitor (APRM), Oscillation Power Range Monitor (OPRM), and Startup Range Neutron Monitor (SRNM) functions
- Systems implemented in a non-rewritable Field Programmable Gate Array (FPGA) based platform

Supplemental Sections (cont'd)

7.1S Instrumentation and Control Platforms (Cont'd)

- Engineered Safety Features Logic and Control System (ELCS)
  - Provides the automatic actuation and control, manual control, and operator interface functions for the Engineered Safety Features (ESF) systems
  - Provides display of safety-related information from other platforms
  - System implemented in a microprocessor based controls platform

Supplemental Sections (cont'd)

7.6S Interlock Systems Important to Safety

- Section added to comply with RG 1.206.
- Refers to information already provided in DCD Section 7.6.1.3.

7.8S Diverse Instrumentation and Control Systems

- Section added to comply with RG 1.206.
- Refers to DCD Section 7C.5 where the subject information is addressed.

7.9S Data Communication Systems

- Section added to comply with RG 1.206.
- Describes both the essential (safety-related) and non-essential (non-safety-related) data communication functions that are part of or support the I&C systems
- Includes data communication between systems and between divisions within a system

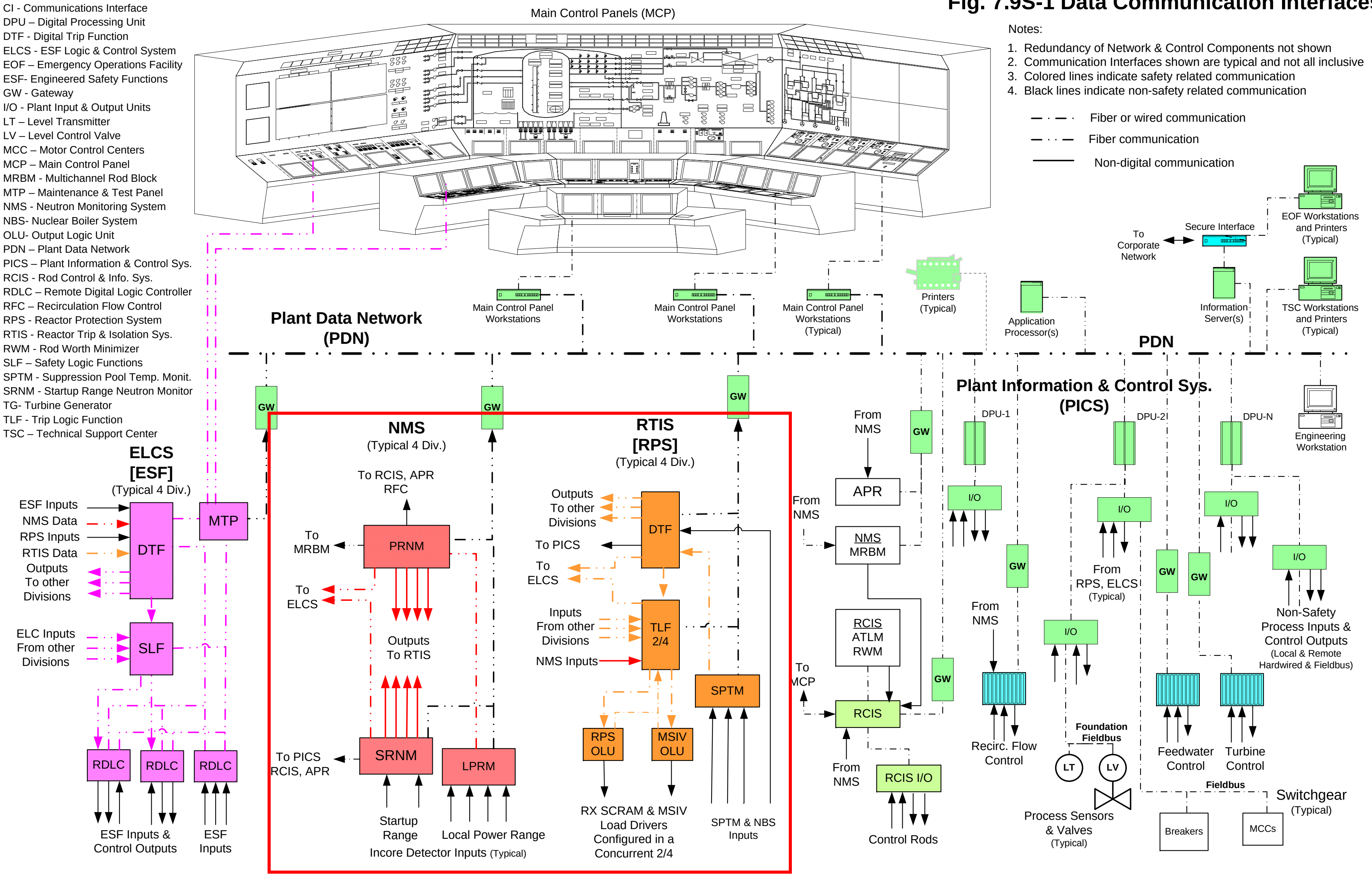
Japanese ABWR Main Control Room

Features of Safety System Design

- ABWR DCD SSLC implements RPS and ESF using a common essential multiplexer system (data highway)
- STP 3&4 departs from DCD using clear division of safety functions
  - RTIS and ELCS are functionally independent
  - Simplifies and reduces complexity
  - Reduces likelihood of common cause failure
- RTIS/NMS and ELCS implemented on diverse platforms
  - RTIS/NMS uses FPGA based platforms
  - ELCS uses microprocessors based platform
  - Also reduces likelihood of common cause failure
- Non-safety functions are performed by Plant Information and Control System (PICS)
  - Separate and diverse microprocessor based platform from safety systems
  - Primary Operator Interface for non-safety systems
  - Historian functions
  - Bypass and inoperable status determination
  - Alarm processing, logging and display

Legend:
APR - Auto Power Regulator
APRM – Average Power Range Monitor
ATLM – Auto. Thermal Limit Monitor
CI - Communications Interface
DPU – Digital Processing Unit
DTF - Digital Trip Function
ELCS - ESF Logic & Control System
EOF – Emergency Operations Facility
ESF- Engineered Safety Functions
GW - Gateway
I/O - Plant Input & Output Units
LT – Level Transmitter
LV – Level Control Valve
MCC – Motor Control Centers
MCP – Main Control Panel
MRBM - Multichannel Rod Block
MTP – Maintenance & Test Panel
NMS - Neutron Monitoring System
NBS- Nuclear Boiler System
OLU- Output Logic Unit
PDN – Plant Data Network
PICS – Plant Information & Control Sys.
RCIS - Rod Control & Info. Sys.
RDLC – Remote Digital Logic Controller
RFC – Recirculation Flow Control
RPS - Reactor Protection System
RTIS - Reactor Trip & Isolation Sys.
RWM - Rod Worth Minimizer
SLF – Safety Logic Functions
SPTM - Suppression Pool Temp. Monit.
SRNM - Startup Range Neutron Monitor
TG- Turbine Generator
TLF – Trip Logic Function
TSC – Technical Support Center

Fig. 7.9S-1 Data Communication Interfaces



Features of communication design (FPGA)

- Safety function communication
  - Deterministic
  - Isolated (fiber optic based)
  - Point to point communication
  - No handshaking

Communication in RTIS

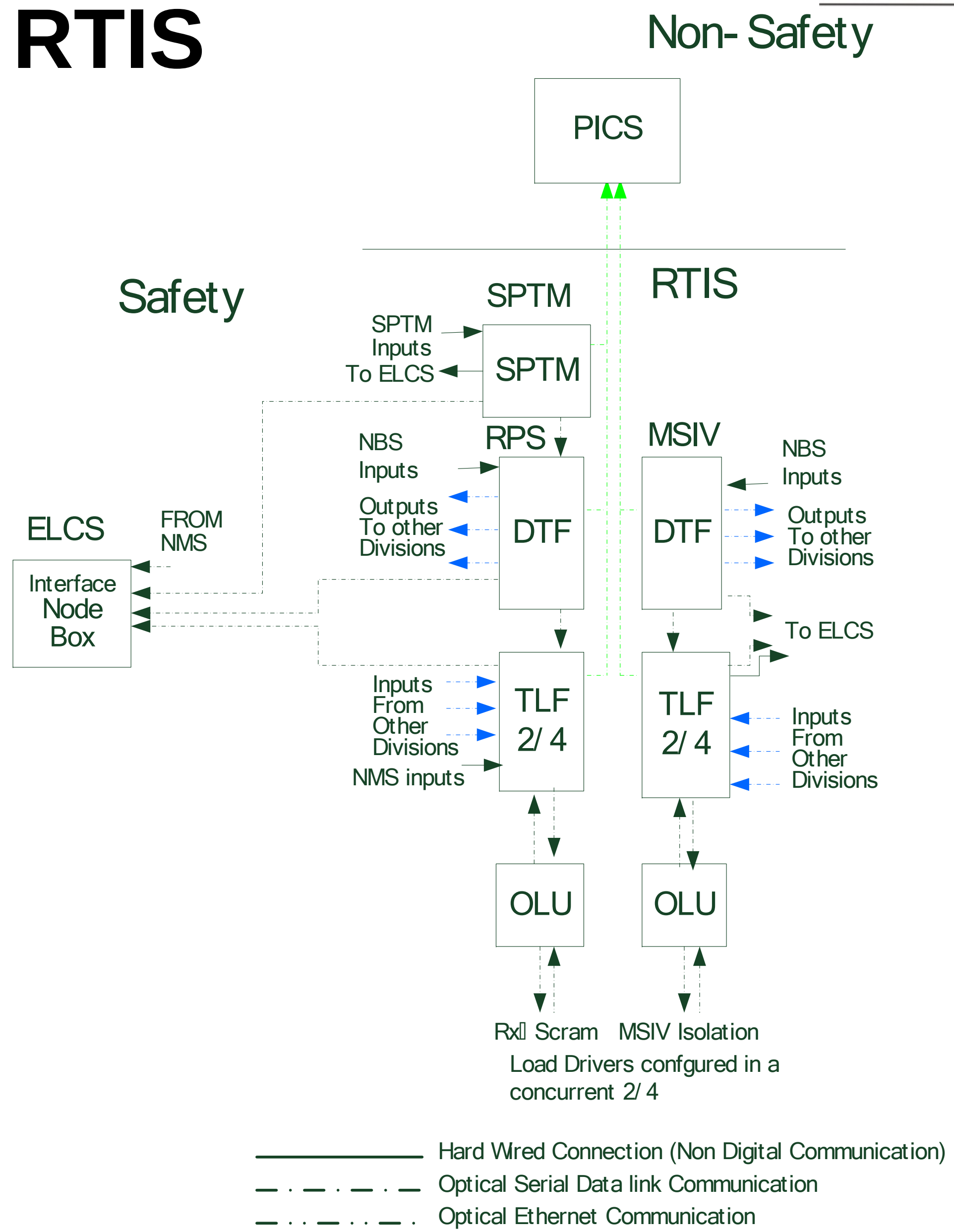
- Interdivision

  -Optical serial link to/from other divisions
  -One-way, no handshake

- Intra-division
  -RTIS to ELCS for display
  -Optical serial link to ELCS
  -One-way, no handshake

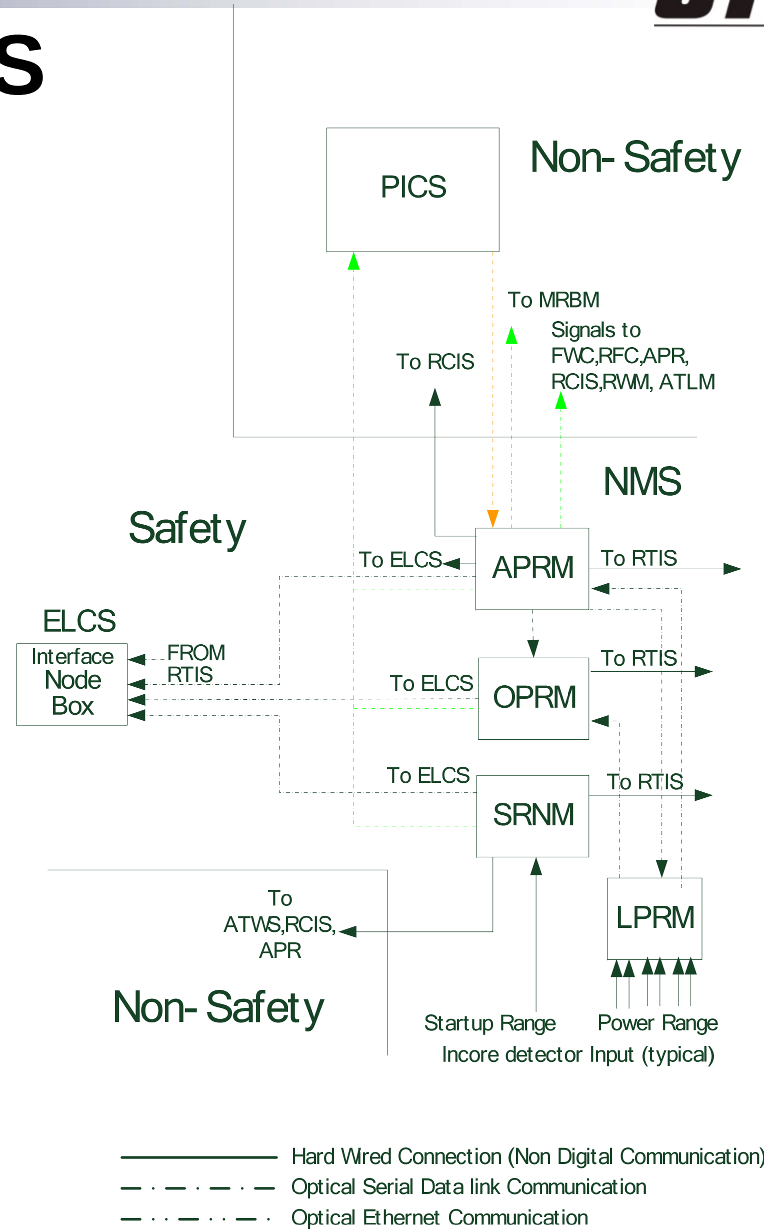
- Safety to non-safety
  -RTIS to Non-Safety
  -Optical serial data link to PICS
  -One-way, no handshake

- Non-safety to safety
  -There is no non-safety to safety communication



Communication in NMS

- Interdivision
  -There is no interdivision communication
- Intra-division
  -NMS to ELCS for display
  -Optical serial data link to ELCS
  -One-way, no handshake
- Safety to non-safety
  -NMS to non-safety systems
  -Optical serial data links
  -One-way, no handshake
- Non-safety to safety
  -Calibration function
  (See next slide)

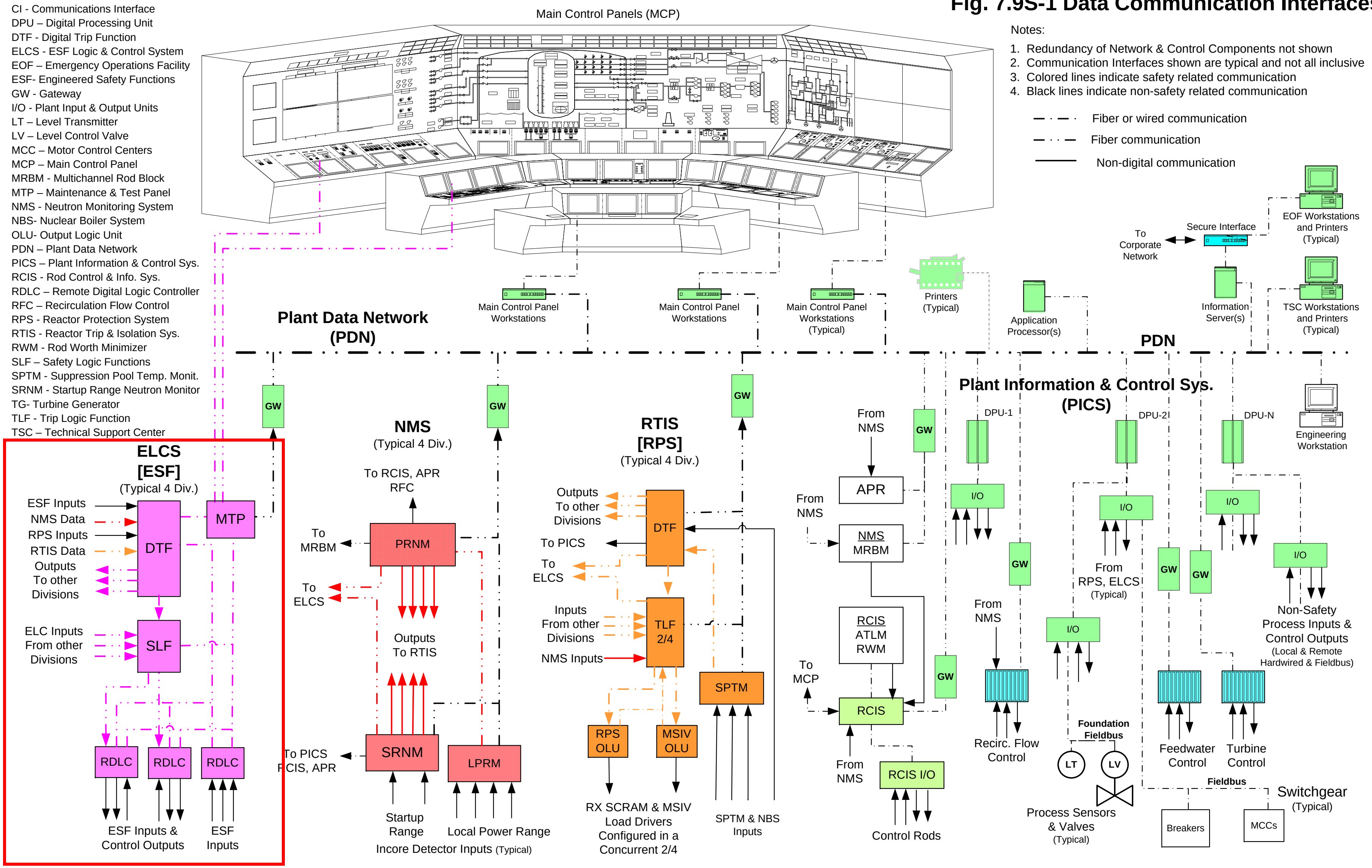


Non-Safety to Safety Calibration Communication in NMS

- A method is provided to support offline calibration activities that allow the transfer of calibration data from PICS to the NMS.
- When NMS is operable (not bypassed), data transfer to the NMS from the non-safety system is prohibited (blocked) by a key lock switch.
- The transfer is controlled by the following process
  1. The NMS division desired to receive the information must first be Bypassed and placed in an Inoperative status by the control room operator.
  2. The key lock switch for the division must be physically enabled to allow the data transfer.
  3. Only a limited data set, in a predefined format, is accepted by the NMS.
  4. Manual verification and acceptance of all data is required prior to returning the channel back to service.

Legend:
APR - Auto Power Regulator
APRM – Average Power Range Monitor
ATLM – Auto. Thermal Limit Monitor
CI - Communications Interface
DPU – Digital Processing Unit
DTF - Digital Trip Function
ELCS - ESF Logic & Control System
EOF – Emergency Operations Facility
ESF- Engineered Safety Functions
GW - Gateway
I/O - Plant Input & Output Units
LT – Level Transmitter
LV – Level Control Valve
MCC – Motor Control Centers
MCP – Main Control Panel
MRBM - Multichannel Rod Block
MTP – Maintenance & Test Panel
NMS - Neutron Monitoring System
NBS- Nuclear Boiler System
OLU- Output Logic Unit
PDN – Plant Data Network
PICS – Plant Information & Control Sys.
RCIS - Rod Control & Info. Sys.
RDLC – Remote Digital Logic Controller
RFC – Recirculation Flow Control
RPS – Reactor Protection System
RTIS - Reactor Trip & Isolation Sys.
RWM - Rod Worth Minimizer
SLF – Safety Logic Functions
SPTM - Suppression Pool Temp. Monit.
SRNM - Startup Range Neutron Monitor
TG- Turbine Generator
TLF – Trip Logic Function
TSC – Technical Support Center

Fig. 7.9S-1 Data Communication Interfaces



Features of Communication Design (ELCS)

- Actuation communication
  - Multiple, unidirectional, point-to-point serial links
  - Deterministic
  - Isolated (fiber optic based)
  - Dedicated single function communication links between trip logic and final actuated component
    - e.g. input signals to DTF, DTF channel actuation to 2/4 vote, voter output (system level actuation) to component actuation
- Divisional communication (Intra-division network)
  - Bus master network per division
  - Deterministic
  - Failure will not affect actuation communication
  - Functions:
    - Information for display
    - Manual control of a single component
    - Diagnostic information
    - Maintenance and test support

Communication in ELCS

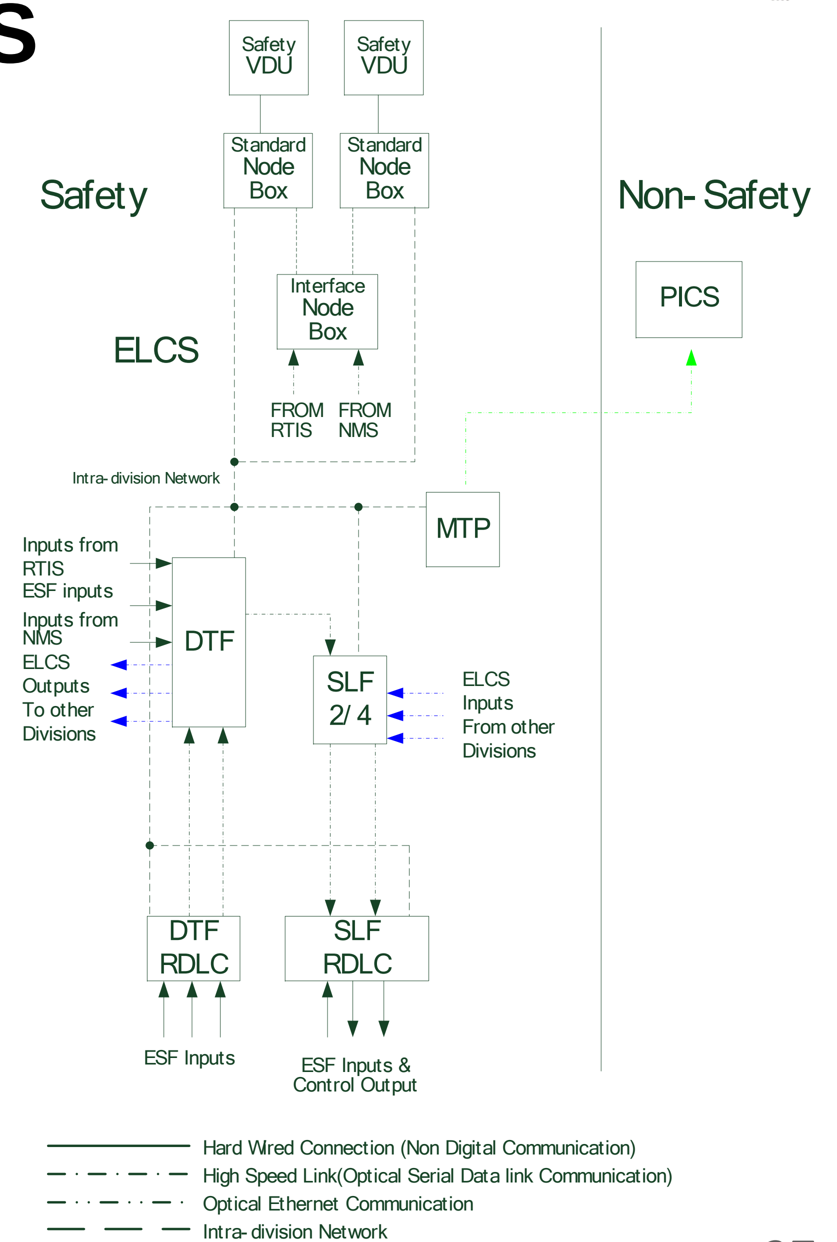
- Interdivision

  Unidirectional serial links
  - Point to point, serial, deterministic
  - One-way, no handshake
- Intra-division

  Intra-division Network
  - Deterministic protocol
  - Display, manual component control and diagnostics/test

  Safety Actuation
  - Point to point, serial
  - Deterministic
  - One-way, no handshake
- Safety to non-safety

  Maintenance and Test Panel Interface
  - Isolated (fiber optic)
  - One way, no handshake
- Non-safety to safety
  - There is no non-safety to safety communication



Diversity and Defense-in-Depth (D3)

- D3 design is incorporated by reference from ABWR DCD
- No departures impact D3
- All ABWR DCD diverse features have been retained including:
  - Manual reactor scram
  - HPCF C diverse manual is hard wired
  - Diverse display of specific process parameters
- Diverse hard wired controls go directly to the controlled component

Conclusion

- FSAR provides a complete set of licensing basis requirements for the I&C systems
- STP 3&4 departures provide design advances to eliminate obsolete equipment and utilize current technology control systems

Chapter 7
Instrumentation and Control Systems

Questions and Comments

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

Presentation to the ACRS Subcommittee

South Texas Units 3 and 4 COL Application Review

SER/OI Chapter 7
"Instrumentation and Controls"

May 20, 2010

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Staff Review Team

- **Project Managers**
  - George Wunder, Lead Project Manager, DNRL/NGE2
  - Adrian Muñiz, Chapter Project Manager, DNRL/NGE2

- **Technical Staff**
  - Dinesh Taneja, Reviewer, DE/ICE2
  - Jack Zhao, Reviewer, DE/ICE2
  - 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

Tier 1 Departure T1 3.4-1	This departure changes the I&C architecture & related nomenclatures to address obsolete data communication technology & digital I&C platform selection.
Digital I&C Platforms	**SSLC** (safety system logic and control) encompasses the logic and controls associated with safety-related systems and utilizes **RTIS** (reactor trip & isolation systems), **NMS** (neutron monitoring system), and **ELCS** (ESF logic & control system) platforms.
Tier 2* Departure 1.8-1 – Codes, Standards, & RG Edition Changes	SSLC design compliance with current regulations, codes, standards, and regulatory guidance documents.
DAC/ITAAC	DAC/ITAAC process for implementing the digital I&C design details.
Setpoint Methodology Technical Report	Setpoint methodology technical report is a part of Setpoint Control Program (SCP) established to resolve bracketed items in the Technical Specifications and is evaluated in this chapter.

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

ACRS Items of Interest	•Diversity and Defense-in-Depth •Independence of Data Communication Functions •Deterministic Features of Data Communication Functions •Simplicity of I&C Design
Open Items	All of 4 open items in the SER with OI (Phase 2) have been closed and are being tracked as confirmatory items. One new open item identified after SER issuance.

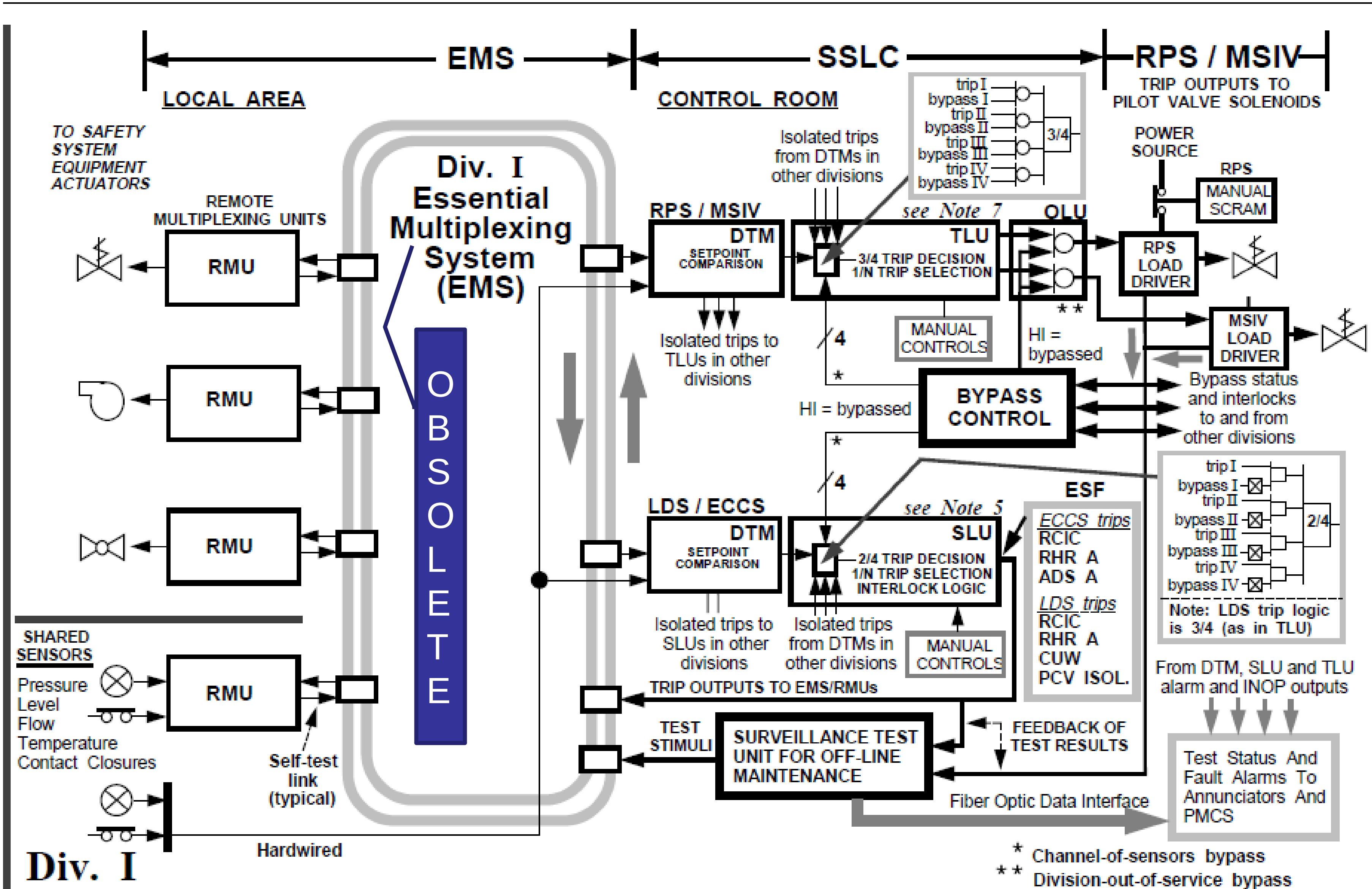
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Tier 1 Departure T1 3.4-1

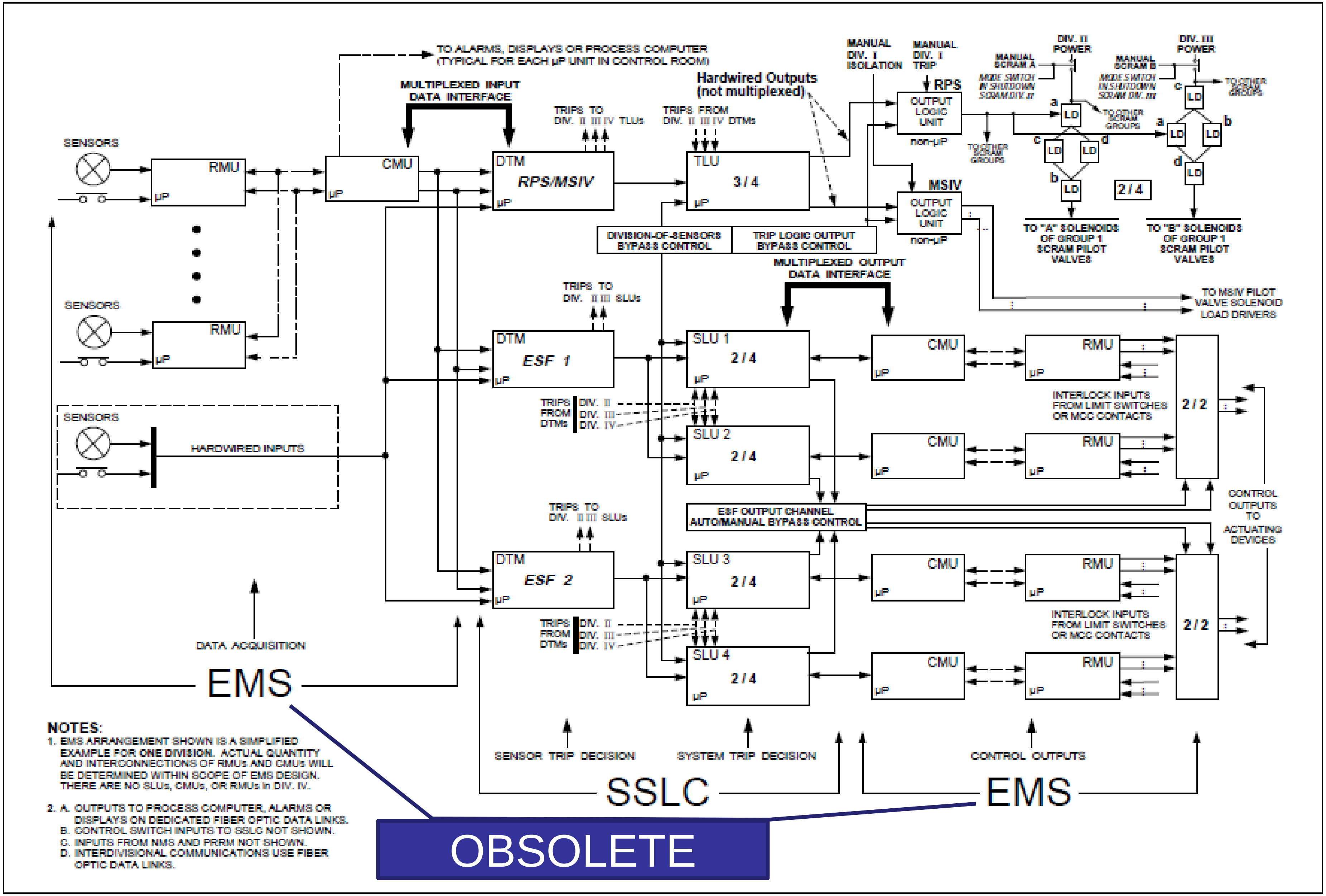
- Brief description
  - I&C design for STP 3 & 4 incorporates by reference the certified ABWR DCD with one significant . This departure primarily resolves issues associated with obsolete data communication technology used in the certified ABWR Safety System Logic and Control (SSLC) design. Tier 1 departure STD DEP T1 3.4-1.
  - The certified ABWR SSLC design is based on:
    - Shared sensor
    - Time multiplexed plant protection systems
    - Employ a common essential multiplexing system (EMS)
    - EMS is based on obsolete ANSI ASC X3T9.5 Fiber Distributed Data Interface (FDDI) technology

Tier 1 Departure T1 3.4-1

- Brief description (continued)
  - This departure <u>does not change</u> any of the SSLC functional requirements:
    - Tier 1, Section 2.2.5, “Neutron Monitoring System” – No Impact
    - Tier 1, Section 2.2.7, “Reactor Protection System” – No Impact
    - Tier 1, Section 2.4, “Core Cooling Systems” – No Impact



ABWR DCD Figure 7A-1 SSLC



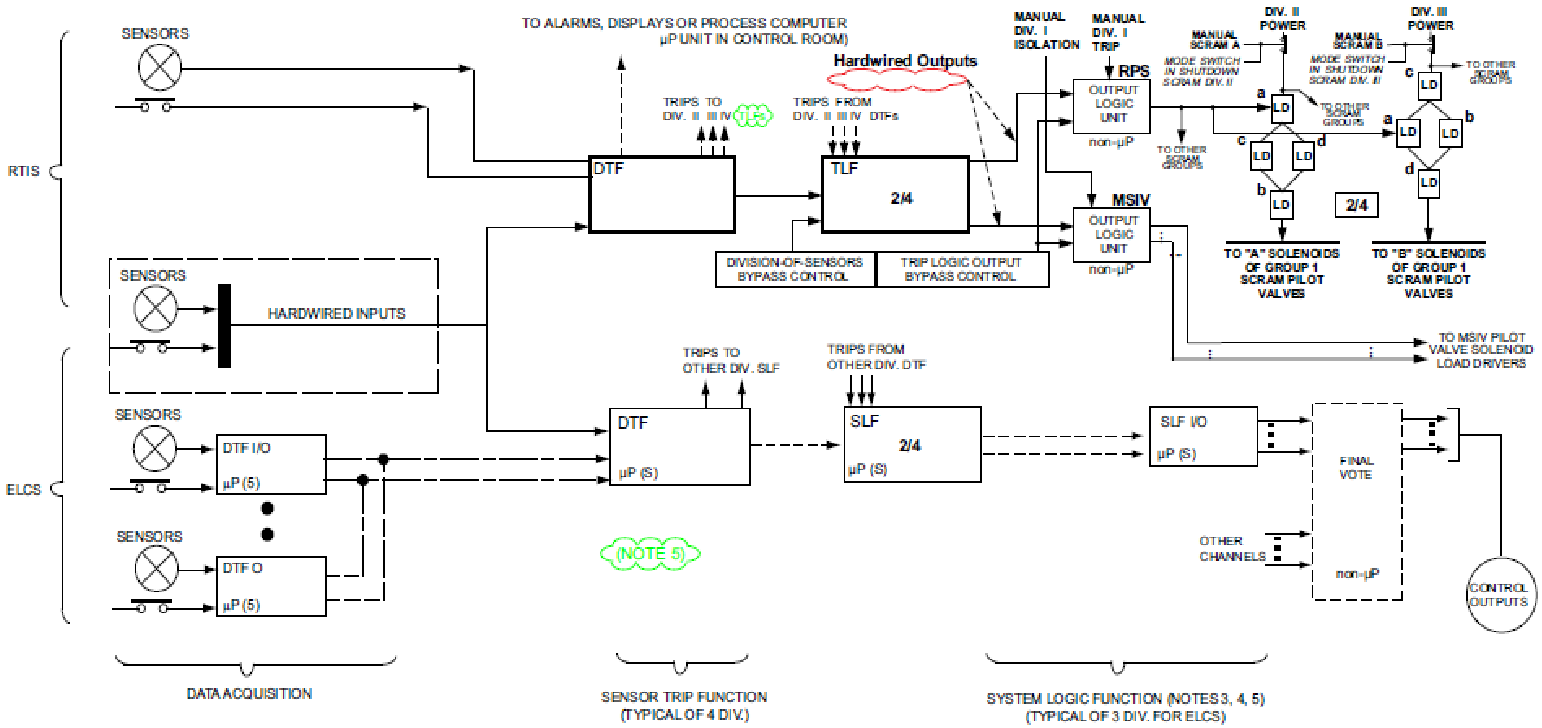
ABWR DCD Figure 3.4b SSLC Block Diagram

Tier 1 Departure T1 3.4-1 (continued)

- Brief description (continued)
  - –In STP 3 & 4 SSLC, data communications is achieved by:
    - •Elimination of obsolete EMS used in certified ABWR design
    - •Use of digital I&C platforms with inherent communications capabilities
    - •SSLC has been segregated into three distinct digital I&C systems:

	DI&C System	Platform
SSLC	RTIS (Reactor Trip & Isolation System)	Toshiba – NRW-FPGA (Non-Rewritable Field Programmable Gate Array)
	NMS (Neutron Monitoring System)	Toshiba – NRW-FPGA (Non-Rewritable Field Programmable Gate Array)
	ELCS (ESF Logic and Control System)	Westinghouse – Common Q (Microprocessor based)

- •Data communication functions of digital I&C platforms are:
  - – Separate and independent from each digital I&C system
  - – Separate and independent from each division within the system



NOTES

1. ARRANGMENT SHOWN IS A SIMPLIFIED EXAMPLE FOR ONE DIVISION

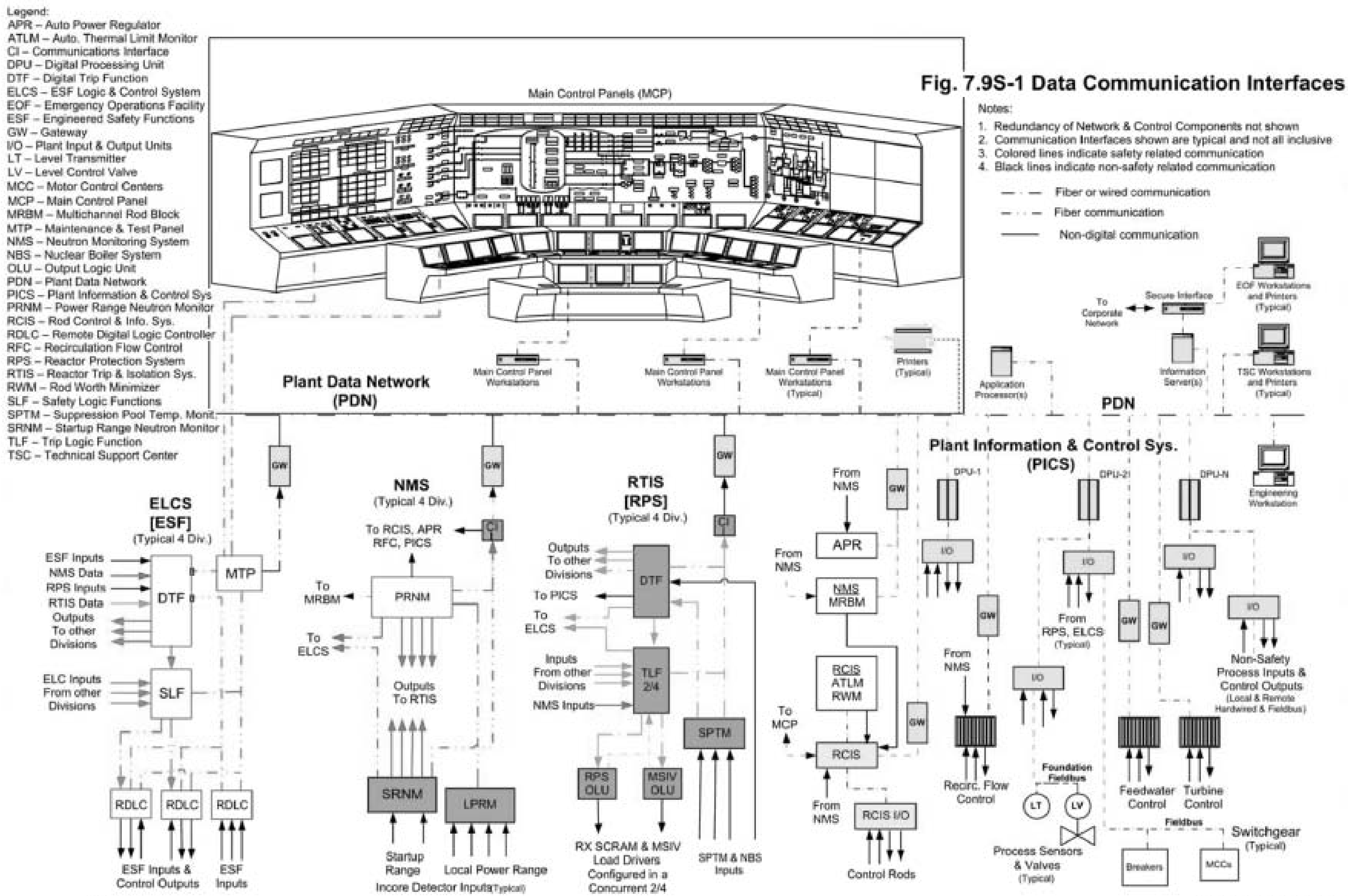
2. A. NOT ALL CONTROL SWITCH INPUTS SHOWN.
   B. INPUTS FROM NMS AND PRM NOT SHOWN.
   C. INTERDIVISIONAL COMMUNICATIONS USE FIBER OPTIC DATA LINKS.

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



COLA Figure 7.9S-1 Data Communication Interfaces

Tier 1 Departure T1 3.4-1 (continued)

- Specific items of interest
  - Through use of the acceptance review and the RAI process, applicant revised significant portions of the COLA to address I&C design information and licensing basis.
  - In response to RAI 07-6, the applicant provided a new supplemental FSAR Section 7.1S, which provides design information on the digital I&C platforms for safety-related I&C systems, including their inherent data communications capabilities.
  - Supplemental FSAR Section 7.9S provides design information on the STP 3 & 4 data communications functions.
  - In response to RAI 07-9, the applicant provided clarifications on design criteria for ELCS functions.

Tier 1 Departure T1 3.4-1 (continued)

- Specific items of interest (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)
  - AP1000 also uses Common Q platform in safety application.
  - STP 3 & 4 SSLC design conforms to current regulations, standards, and regulatory guidance, including DI&C-ISG-04.
  - Current version of the SRP Chapter 7 was used in evaluating the departed STP 3 & 4 SSLC design, including the inherent data communications capabilities.
  - STP 3 & 4 SSLC design offers significant enhancements over the certified design.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Tier 1 Departure T1 3.4-1 (continued)

- Conclusion
  - STP 3 & 4 digital I&C design information in the COLA (including RAI responses) adequately addresses all applicable licensing basis, and is in compliance with applicable regulations, regulatory guidance, and standards.
  - SSLC digital I&C platforms, including inherent data communications capabilities, are in compliance with current regulations, regulatory guides, and standards (e.g., IEEE Std 603-1991, IEEE Std 7-4.3.2-2003).
  - All open items have been resolved
  - All proposed COLA changes are being tracked as confirmatory items.

Tier 2* Departure 1.8-1
Codes, Standards, & RG Changes

- Brief description
  - Departure 1.8-1 identifies Tier 2* items in Tier 2 FSAR Tables 1.8-20 and 1.8-21, which are being updated to current revisions/editions.
- Specific items of interest
  - This departure updates the SSLC conformance to regulatory requirements, RGs, and industry standards to current revisions and editions.
  - Based on this departure, the safety-related I&C systems (e.g., ELCS, NMS, and RTIS) now conform to IEEE Std 603–1991[1] (a 10 CFR 50.55a(h) regulatory requirement), current revisions of applicable RGs, industry standards, and NUREG–0800 (SRP), and the BTPs.

1. The criteria contained in this standard establish minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power generating stations.

Tier 2* Departure 1.8-1
Codes, Standards, & RG Changes (continued)

- Specific items of interest (continued)
  - In response to early meetings and RAIs, supplemental FSAR tables 1.9S-1 and 1.9S-1a were added, which identify IEEE standards and related Regulatory Guides applicable digital I&C design.
- Conclusion
  - SSLC design complies with current regulations, regulatory guidance, and standards (e.g., IEEE Std 603-1991 & IEEE Std 7-4.3.2-2003).
  - All open items have been resolved.
  - All proposed COLA changes are being tracked as confirmatory items.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DAC/ITAAC

- Brief description
  - Design acceptance criteria (DAC) is a set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies in making a final safety determination to support a design certification.
  - In ABWR DCD, digital I&C DAC are identified as inspections, tests, analyses, and acceptance criteria (ITAAC) in Tier 1 Table 3.4.
  - In accordance with 10 CFR 52.63, certified designs, including ITAAC have finality.
  - Applicant has elected the option to use DAC process for implementing the digital I&C design details.
  - This option allows DAC resolution after COL is issued.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DAC/ITAAC (continued)

- Specific items of interest
  - COLA incorporates by reference (IBR) all I&C DAC, and other I&C related ITAAC with minimal changes resulting from departed I&C architecture.
  - In accordance with SRP 14.3 guidance, the staff evaluated the impact on I&C DAC and other I&C related ITAAC resulting from I&C departures.
  - In response to RAI 14.03.05-8, the applicant reevaluated the impact of I&C related departures on Tier 1 ITAAC in accordance with SRP 14.3 and 14.3.5 guidance and concluded that the ITAAC described in the DCD remain completely applicable and valid, and changes to I&C ITAAC are not required. The staff found applicant’s response acceptable.
  - Under a <u>separate **(post COL)** activity</u>, the staff is developing DAC/ITAAC inspection process.

DAC/ITAAC (continued)

- Conclusion
  - The staff finds the I&C DAC and other I&C related ITAAC in the COLA to be adequate, such that when DAC/ITAAC activities are performed and the acceptance criteria are met, the facility would have been constructed and will operate in conformance with the design basis stipulated in COL and the applicable regulations.

Setpoint Methodology Technical Report

- Brief description
  - The applicant's original intent was to develop the setpoint methodology after COL issuance (Tier 1 Table 3.4 ITAAC Item 13).
  - The applicant has chosen to resolve the bracketed items in the Technical Specifications (TS) using the Setpoint Control Program (SCP) in conformance with the regulations on TS (see DC/COL-ISG-8).
  - In support of the SCP, the setpoint methodology technical report was submitted as part of the COL application.
  - Evaluation of the SCP is documented in Chapter 16, and the setpoint methodology report is evaluated in Chapter 7.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Setpoint Methodology Technical Report (continued)

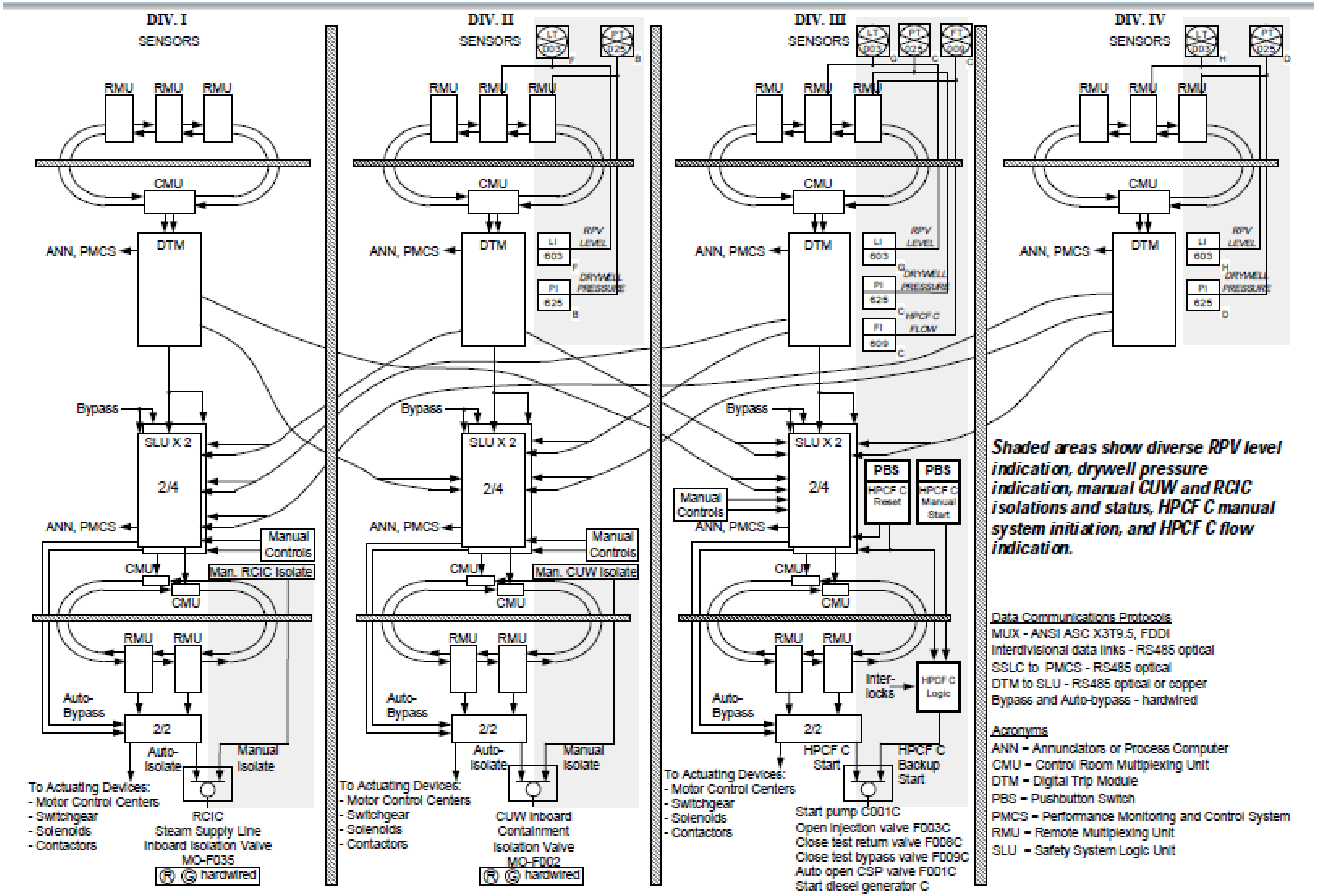
- Specific items of interest
  - This technical report is prepared by Westinghouse for STP 3 & 4 to document the instrument uncertainty calculations for the RPS and ESF functions for the ABWR plant.
  - This STP 3 & 4 ABWR setpoint methodology is similar to the AP1000 setpoint methodology topical report.
  - In the setpoint methodology report (WCAP-17119-P, Rev. 1), a reference is 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 is not relevant to the COL application. An RAI has been initiated on this issue and is being tracked as an open item.

Setpoint Methodology Technical Report (continued)

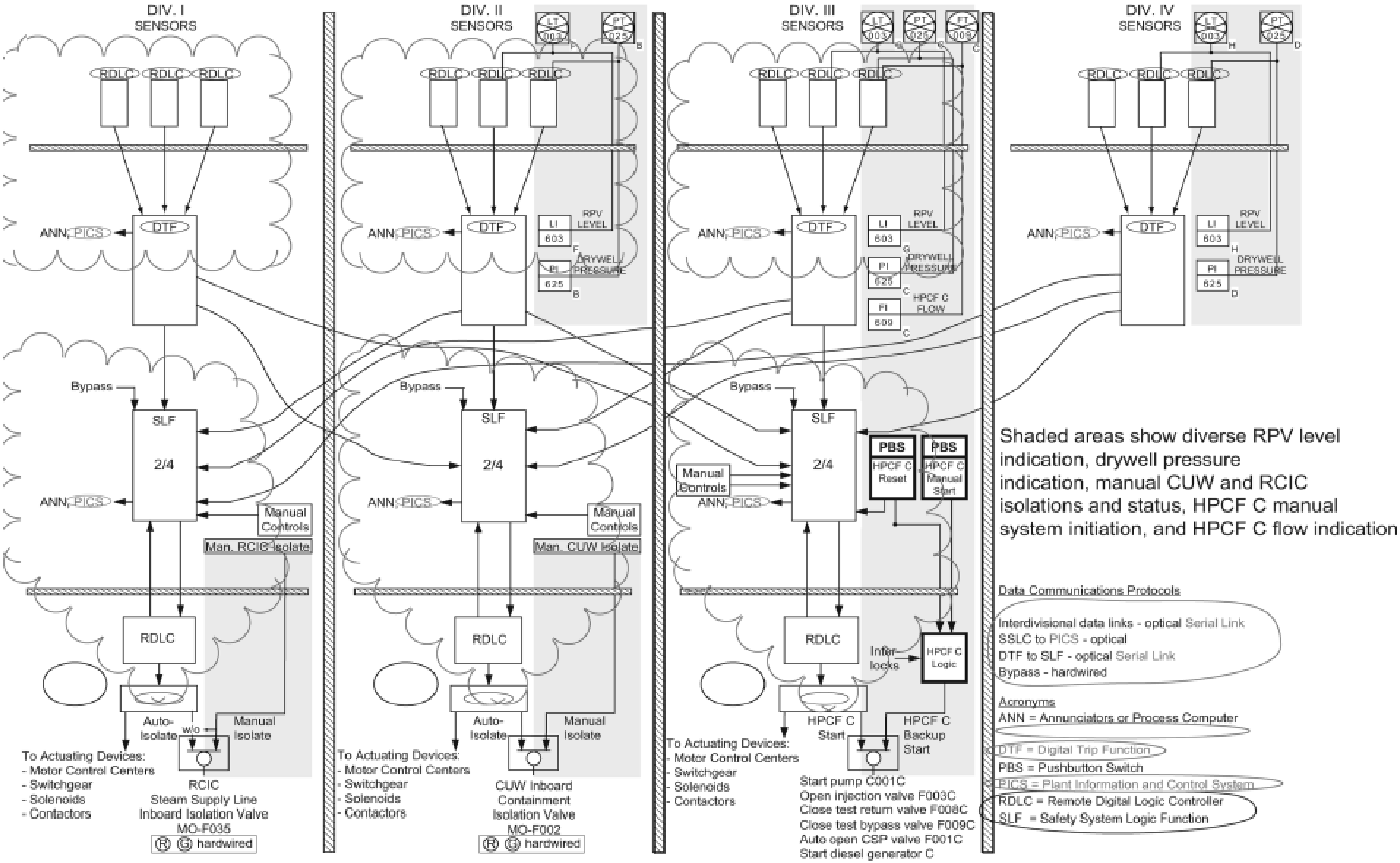
- Conclusion
  - As a result of one open item identified above, the staff is unable to finalize its conclusions relating to “Instrument Setpoint Methodology” in accordance with the NRC requirements.

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.

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.

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.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

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.

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.

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.

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.

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.

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.

Overview of STP RCOL Chapter 7

Discussion/Committee Questions

Backup Slides

Table 1.9S-1 Site-Specific Conformance with RG

No.	Title	Rev.
Division 1		
1.47	1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems	0 (1973)
1.53	1.53 Application of the Single-Failure Criterion to Safety Systems	2 (11/03) 0 (1993) for ELCS[1]
1.62	Manual Initiation of Protection Actions	0 (1973)
1.75	Independence of Electrical Safety Systems	3 (2/05) 2 (1978) for ELCS[1]
1.100	Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants	2 (1988)
1.118	Periodic Testing of Electric Power and Protection System	3 (1995) 2 (1978) for ELCS[1]
1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	2 (2006) 1 (1996) for ELCS[1]
1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	1 (2004) 0 (1987) for ELCS[1]
1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.173	Developing Software Life Cycle Process for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.180	Guidelines for Evaluating Electromagnetic and Radio- Frequency Interference in Safety-Related Instrumentation and Control Systems Instrumentation and Control Systems	1 (2003) 0 (2000) for ELCS[1]
1.209	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants	0 (2007) for ELCS see note 2

Table 1.9S-1a IEEE Standards Applicable to STP 3 & 4 Platforms

IEEE No.	Category	Rev.
IEEE 7-4.3.2	Digital Computers and Software	2003 1993 for ELCS[1]
IEEE 323	EQ	2003 1983 for ELCS[1]
IEEE 338	Periodic Testing	1987
IEEE 344	Seismic	1987
IEEE 379	Single Failure	2000 1994 for ELCS[1]
IEEE 384	Independence	1992
IEEE 603	I&C	1991
IEEE 828	Configuration Management	1990
IEEE 829	Software Test Documentation	1983
IEEE 830	Software Requirements Specifications	1993
IEEE 1008	Software Unit Testing	1987
IEEE 1012	V&V	1998
IEEE 1028	Software Reviews and Audits	1997
IEEE 1042	Software Configuration Management	1987
IEEE 1074	Software Life Cycle Processes	1995