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

1
2 DISCLAIMER

3

4

5 UNITED STATES NUCLEAR REGULATORY COMMISSION'S

6 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

7

8

9 The contents of this transcript of the

10 proceeding of the United States Nuclear Regulatory

11 Commission Advisory Committee on Reactor Safeguards,

12 as reported herein, is a record of the discussions

13 recorded at the meeting.

14

15 This transcript has not been reviewed,

16 corrected, and edited, and it may contain

17 inaccuracies.

18

19

20

21

22

23

24

1 UNITED STATES OF AMERICA

2 NUCLEAR REGULATORY COMMISSION

3 + + + + +

4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

5 (ACRS)

6 + + + + +

7 ABWR SUBCOMMITTEE

8 + + + + +

9 THURSDAY, MAY 20, 2010

10 + + + + +

11 ROCKVILLE, MARYLAND

12 The Subcommittee convened at the Nuclear

13 Regulatory Commission, Two White Flint North, Room

14 T2B1, 11545 Rockville Pike, at 8:30 a.m., Dr. Said

15 Abdel-Khalik, Chairman, presiding.

16 SUBCOMMITTEE MEMBERS PRESENT:

17 SAID ABDEL-KHALIK, Chair

18 J. SAM ARMIJO

19 MARIO V. BONACA

20 CHARLES H. BROWN, JR.

21 MICHAEL CORRADINI

22 MICHAEL T. RYAN

23 WILLIAM J. SHACK

24 JOHN D. SIEBER

25 JOHN W. STETKAR

1 NRC STAFF PRESENT:

2 PETER WEN, Cognizant Staff Engineer and Designated

3 Federal Official

4 MARK TONACCI

5 GEORGE WUNDER

6 STACY JOSEPH

7 FRANK TALBOT

8 DINESH TANEJA

9 GARY HOLAHAN

10 ADRIAN MUNIZ

11 JACK ZHAO

12 LAURA DUDES

13 ED HACKETT

14

15

16

17

18

19

20

21

22

23

24

25

1 ALSO PRESENT:
2 SCOTT HEAD
3 STEVE CASHELL
4 STEVE BLOSSOM
5 GREG SWANNER
6 ED BROWN
7 CHRIS CREFELD
8 TIM HURST
9 AKIRA FUKUMOTO
10 TOSHIFUMI SATO
11 JAY PHELPS
12 CAL TENG
13 ERIC FREDRICKSON
14 BOB QUINN
15 JERRY MAUCK
16 COLEY CHAPPELL
17
18
19
20
21
22
23
24
25

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

AGENDA ITEM PAGE

Opening Remarks 5

NR0/STPNOC Staff Introductions 7

STP COLA FSAR Chapter 14 35

STP COLA FSAR Chapter 7 50

Public Comment 244

Subcommittee Discussion and Closing

Remarks 245

Adjourn

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

2 8:28 a.m.

3 OPENING REMARKS

4 CHAIR ABDEL-KHALIK: The meeting will now

5 come to order.

6 This is a meeting of the ABWR Subcommittee

7 of the Advisory Committee on Reactor Safeguards. I'm

8 Said Abdel-Khalik, chairman of the subcommittee.

9 ACRS members in attendance today are Jack

10 Sieber, Charlie Brown, John Stetkar, Sam Armijo, Mike

11 Corradini, Bill Shack, Michael Ryan and Mario Bonaca.

12 Mr. Peter Wen is the designated federal

13 official for this meeting.

14 The NCR staff review of the STP Combined

15 License Application is generating safety evaluation

16 reports with open items by chapters. In our last

17 meetings on March 2nd and 18th we discussed the COLA

18 FSAR and the corresponding SER with open items for

19 chapters one, four, five, eight, 11, 12, 15, 16, 17

20 and 18.

21 In today's meeting we are scheduled to

22 discuss chapters seven and 14.

23 We have scheduled additional ABWR

24 subcommittee meetings through June, followed by a

25 meeting of the full committee in the middle of the

1 year. the agenda goes chapter by chapter, I expect
2 today's discussion to be issue-centric although,
3 related to the technical issues in the COLA and the
4 SER.
5 The rules for participation in today's
6 meeting were announced in the Federal Register on May
7 18, 2010, for an open/closed meeting. Parts of this
8 meeting may need to be closed to the public to protect
9 information proprietary to Toshiba or other parties.
10 I'm asking the NRC staff and the applicant to identify
11 the need for closing the meeting before we enter into
12 such discussion to verify that only people with the
13 required clearance and need to know are present.
14 We have a telephone bridge line for the
15 public and stakeholders to hear the deliberations.
16 The line will not transmit any signal from this end
17 during the closed portions of this meeting. Also to
18 minimize this service the line will be kept in listen-
19 only mode until the last 10 minutes of the meeting.
20 At that time we will provide an opportunity to members
21 of the public joining us through this bridge line to
22 make a statement or provide comments.
23 Since the meeting is being transcribed, I
24 request that the participants in this meeting use the
25 microphones located throughout this room when

1 addressing the subcommittee. Participants should
2 first identify themselves and speak with sufficient
3 clarity and volume so that they can be readily heard.
4 We will no proceed with the meeting, and I
5 call on Mr. Mark Tonacci of NRO to begin the
6 presentation.
7 NRO/STPNOC STAFF INTRODUCTIONS
8 MR. TONACCI: Good morning, and thank you
9 for hearing our presentations this morning. I have no
10 introductory remarks. However there are a few for
11 George Wunder the lead project manager.
12 MR. WUNDER: Good morning. I'm George
13 Wunder. I'm the lead project manager for the South
14 Texas combined license review. Today we are going to
15 be presenting two chapters, Chapters 14 and 7. We
16 have elected to do them in that order because we
17 anticipate the presentation on 14 will be briefer, and
18 because of the interest that has been generated on
19 Chapter 7 we thought that that might expand.
20 There is one thing that is not on your
21 agenda; it's kind of a late-breaking issue. Gary
22 Holahan, our deputy office director, will be making
23 some brief remarks. We anticipate that he'll be done
24 here about 10:30. And so if all goes according to
25 schedule we would like him to make those remarks just

1 before the presentation begins on Chapter 7.

2 For Chapter 14 today the staff will be

3 represented by project manager Stacy Joseph and Frank

4 Talbot of the quality and vendor branch, and the

5 presentation for Chapter 7 will be done by project

6 manager Adrian Muniz and Dinesh Taneja of the INC

7 branch.

8 CHAIR ABDEL-KHALIK: Thank you.

9 At this time I guess we will begin with

10 the applicant's presentation. And Mr. Scott Head will

11 begin the presentation.

12 INTRODUCTIONS

13 MR. HEAD: Good morning. Thank you for

14 this opportunity to brief the ACRS on Chapter 14.

15 Look forward to the discussions today.

16 As to the agenda, this is our standard

17 agenda, introduction of the speakers, summary, detail

18 and the contents, departures, pretty much our standard

19 agenda that we have used. And then at the very end we

20 will have a discussion, short discussion, on the flow-

21 induced vibration with respect to Unit 3.

22 Participating today is Steve Blossom, our

23 Construction, Startup and ITAAC Manager for STP 3 and

24 4. And Mr. Miyamoto-san from Toshiba is joining us

25 today also. He has extensive experience in startup

1 operations, starting up seven BWRs and three ABWRs, a
2 crucial member of our team.
3 Jay Phelps is also here with us today,
4 who's presented in the past, previous chapters, our
5 operations manager, and Steven Cashell, who presented
6 tech specs recently, is also with us here today.
7 I'm going to go ahead and turn it over to
8 Steve.
9 MR. CASHELL: Thank you, chairman and
10 members.
11 The summary of Chapter involves an Initial
12 Test Program in ITAAC. The Initial Test Program
13 includes all the testing activities conducted
14 following completion of construction, going all the
15 way through to the startup of commercial operations.
16 ITAAC defined the activities that we take
17 to verify that the as-built system conforms with the
18 design features and characteristics that are in the
19 design description for that system.
20 Contents, Chapter 14.1 was the old PSAR
21 information. It's no longer applicable, so we added a
22 14.1S for the applicable regulations and Reg Guide.
23 14.2 are all the test descriptions for the Initial
24 Test Program. We supplemented that 14.2S, and we'll
25 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

1 DCD, so we have to take care of that.

2 9.5-1 says simply a change in the Reg

3 Guide status for a couple of the descriptions.

4 11.2-1 and 11.4-1 we changed quite a bit

5 of the liquid and solid rad waste process equipment.

6 So we had to change the TIS (phonetic) descriptions

7 for those. 14.2-1 is a CRD friction test at rated

8 pressure. We have about four different ways of doing

9 this friction test now with the fine motion control

10 rod drive that we have, so we can now do this test at

11 cold pressure. If it passes at cold it will pass at

12 heated, since things come into alignment as the vessel

13 heats up.

14 Then finally standard department of

15 vendor, throughout the test descriptions, GE Hitachi,

16 the NSSS vendor, specifically all over the place. So

17 we changed that to a more generic NSSS vendor.

18 And there are these six departures, Tier 1

19 departures, that affect ITAAC.

20 Tier 12.2-1 is rod control and information

21 system power supply testing. There is two UPS,

22 uninterruptible power supplies, and redundant

23 controllers. Only we can lose one and still

24 everything should work. So we are testing one and one

25 to make sure that it all still works.

1 Tier 12.4-1 we increased spent fuel
2 cooling by adding a third RHR look, RHR-A, to the
3 spent fuel pool, so we are testing all the
4 connections, and making sure that all works right.
5 Tier 12.4-3 RCIC turbine testing, we have
6 new RCIC pumps, and turbines, so we are testing that -
7 or have an ITAAC for this, sorry.
8 Tier 12.12-1, shop testing of - oh, the
9 DCD specified minimum and maximum voltage testing for
10 all electrical components. We are doing a lot of that
11 in the shop now, the minimum and maximum, and
12 correlating that with what we find in the field. So
13 that is a departure. But the Tier 12.14-1, hydrogen
14 recombiner elimination, again, and our old friend,
15 Tier 13.4-1 that affects almost everything, the I&C
16 nomenclature, and architecture.
17 In doing all this we had to supplement the
18 Chapter 14 quite a bit. We wrote a startup
19 administrative manual that describes how we are going
20 to do testing, and then these chapters here, 14.2S.1
21 is organization and training in support of the initial
22 test program. 14.2S-1 is a first of a kind systems.
23 14.2S-3, overlap of the Unit 3 test program with the
24 Unit 4 test program. 14.2S-4, testing required to be
25 completed prior to fuel load. 14.2S-12, site-specific

1 test descriptions. So we have several site specific
2 tests that we had to add. And 14.3S is the selection
3 criteria for the site-specific systems, emergency
4 planning, and security ITAAC.
5 COL License Information Items, we have
6 nine, items one, two and three are accommodated by a
7 commitment we made to provide the site-specific pre-op
8 and test specs six months prior to the start of the
9 initial test program.
10 Item four involves two additional
11 commitments, one to supply the pre-op test procedures,
12 and the other to supply the startup test procedures 60
13 days prior to the fuel load or prior to the start of
14 the program.
15 And then items 5, 6, 7, 8 and 9 are all
16 accommodated within the startup administrative manual.
17 And that delineates that processes that we are going
18 to use to administer the initial test program.
19 For ITAAC now, there is a separate
20 section. Section 9 contains all the ITAAC, and ITACC
21 were scattered all throughout the DCD. However, the
22 selection criteria is in Chapter 14.3 and 14.3S.
23 The selection criteria methodology that we
24 have chosen to use, is what was provided in 14.3, so
25 we utilizing that for all the site-specific things,

1 and also for emergency planning and physical security
2 hardware. And the physical security and emergency
3 planning ITAAC, they conform with the guidance in Reg
4 Guide 1.206.
5 And now I'd like to turn it over to Steve
6 Blossom -- he is our construction/startup and ITAAC
7 manager - to go over the implementation of the test
8 program.
9 MR. BLOSSOM: Thanks, Steve.
10 As Scott and Steve said, I am the
11 construction/startup and ITAAC manager. And I'll tell
12 you a little bit about why I'm in the position that
13 I'm in. I'm approaching 40 years experience in
14 nuclear. I used to count the years. Now I just round
15 it up to 40.
16 I've been at South Texas for 22 years on 1
17 and 2 until three years ago I came to the new units as
18 maintenance manager. Outage management, I was the
19 steam generator replacement implementation manager
20 back in 2000 and 2002. I've done work in work
21 control, and prior to coming to South Texas in '88 I
22 did multiple startups. I started up a fast breeder
23 reactor, five PWRs, two boiling water reactors, and
24 then I did a restart at a DOE reactor at Savannah
25 River, a K Reactor. So I never thought I'd get an

1 opportunity to start up another one and I'm very
2 excited about it.
3 The initial test program, very similar to
4 what we did in the `70s and `80s, just divided up into
5 very distinct phases. Construction test phase,
6 sometimes referred to as component testing, which
7 include things such as flushing and hydro, initial
8 calibrations on equipment, wiring checks, initial
9 valve stroke, initial energization. Essentially what
10 this phase does is get the system ready for pre-op
11 testing.
12 Pre-operational testing will be pre-fuel
13 load testing to verify that the systems operate in
14 accordance with the design. Also during that phase we
15 will collect baseline data for use as the plant moves
16 forward. We will run in equipment to shake it out. We
17 will evaluate system performance on an integrated
18 basis with respect to other systems, and then we will
19 have a strong effort in that phase to train personnel
20 in both engineering and operations, so that as the
21 plant moves forward, people are equipped to operate it
22 like that.
23 And then the startup test phase, that is
24 the fuel load, the commercial ops, refuel and shut
25 down power level testing, nuclear heat up, the NOP/NOT

1 testing, from the 5 percent to the 100 percent
2 plateaus, divided up into three phases, low power, mid
3 power and high power testing, and all culminating in a
4 warranty run, and then declaration of commercial ops.
5 Next slide shows how we've laid out our
6 test program using Reg Guide 1.68 as our bases, our
7 procedures, and organization are tailored around the
8 same requirements as you will see in 1.68, very
9 typical standard to what you saw back in the `70s and
10 `80s also. And that gives us the structure that we
11 need.
12 I want to talk a little bit about the
13 startup organization with respect to you've got your
14 EPC, engineering procurement constructor contractors,
15 who in our case are Toshiba, Fleur, Westinghouse and
16 Sargent & Lundy make up the engineering procurement
17 construction team, and they are responsible - the EPC
18 startup manager who will be a Toshiba person,
19 Mayamoto-san (phonetic) or one of his compadres, will
20 be responsible for the day-to-day activities in the
21 pre-op test group. Startup, EPC startup manager will
22 be responsible for a smooth interface between the -
23 our plant, the STP plant staff, and the testing
24 organizations.
25 We will have the Joint Test Group in place

1 that will approve all pre-operational test procedures,
2 test results, test exceptions, and things that occur
3 during the pre-op testing, and in my organization STP
4 will provide oversight throughout this process, and
5 will also supplement the EPC organizations to get that
6 training we need to move the personnel forward.
7 Next slide, turnover. The process is
8 broken down into - we will have two distinct
9 turnovers. The first one will be internal to the
10 engineering and procurement and construction teams.
11 And that will be from construction to the pre-
12 operational test groups. They will do pre-operational
13 testing, and then there will be a final turnover from
14 the EPC organization to STP, pre-fuel load. So that
15 will allow us to move forward. And we will also use
16 some configuration of a construction completion
17 organization to work off exceptions throughout those
18 turnovers, but I have made it very clear that the bar
19 is very high for exceptions; don't want to take
20 systems like we did back in the `70s and `80s and then
21 your construction completion effort was very painful.
22 So I've set the bar very high, and we are going to be
23 very very picky as to what we will take as an
24 exception, and almost nothing in the final turnover.
25 Next slide talks about ITAAC and the

1 relationship to the initial test program. ABWR, we
2 have 939 ITAAC, approximately 38 percent will be
3 completed during construction, and pre-operational
4 test phases. The completion of the ITAAC,
5 particularly given the back -end loading, will require
6 very close coordination between the test organization
7 and the ITAAC completion organization, and I'm sure
8 you remember one of my titles is also the ITAAC, so
9 I'm - I'll be overseeing this effort as well and
10 providing oversight.
11 And the bottom bullet there is the 52.99
12 and the 52.103(g) process. And that is the process
13 that is tailored around any NEI 08-01, and as a
14 project and myself the person, I've had significant
15 input into the development of NEI 08-01, with respect
16 to ITAAC closure and ITAAC maintenance. So I think we
17 will be well positioned to meet our obligations with
18 respect to ITAAC closure maintenance.
19 Next slide, fuel load. I'll assume the
20 responsibility as the startup manager for fuel load
21 and commercial ops. I will be responsible for day-to-
22 day operations in interface between all the various
23 organizations. At that point in time we'll have a
24 plant ops review committee in place that will also
25 approve test procedures in that phase, exceptions,

1 test results. I'll provide technical direction for
2 plant startup activities via use of test directors.
3 But again EPC will be very involved in it; they'll be
4 more in an advisory capacity at that point in time.
5 As again in an operational environment the
6 operational staff will be under the leadership of the
7 operation shift supervisor, and with respect to the
8 direction of tests and data collection and all that,
9 that will be administered out of my organization,
10 people out in the field collecting data.
11 The next slide reflects Toshiba's
12 experience with ABWR construction and initial testing.
13 As you can see they've got three ABWR here identified.
14 Scott introduced Miyamoto-san, in addition to starting
15 up these three ABWRs in Japan, he has also started up
16 seven BWRs in Japan. So Toshiba has significant
17 experience associated with ABWR startups, and to
18 capitalize on all this experience we have created a
19 very comprehensive lessons learned process where we
20 have taken NUREG-1055 and INPO and Okiluto and right
21 now we are translating the lessons learned from the
22 ABWR startups in Japan and loading them into our
23 database so that we capitalize on that experience as
24 well.
25 And slide #21, you see kind of an outline

1 of the preoperational and startup test phases. Right
2 now we are tracking to our preoperational test window
3 is going to be approximately nine months in duration
4 followed up by fuel load and startup testing which is
5 seven months in duration. So a very aggressive
6 schedule but doable.
7 MEMBER SIEBER: I have a question. To
8 what extent or what separation is there between Units
9 1 and 2 plant organization and Unit 3 startup?
10 MR. BLOSSOM: The Unit 1 and 2
11 operations were completely separate.
12 MEMBER SIEBER: And management also?
13 MR. BLOSSOM: Yes.
14 MEMBER SIEBER: So basically these are
15 independent units on a single site?
16 MR. BLOSSOM: Correct. Now we have
17 interface arrangements where if we are doing work on 3
18 and 4 we have a process to evaluate the impacts --
19 MEMBER SIEBER: Impacts, right.
20 MR. BLOSSOM: -- on the operating units,
21 and mitigate those. But no, the organizations are
22 distinctly different. The only time they become
23 common is at our chief executive office.
24 MEMBER SIEBER: Okay. Again, will it
25 stay that way after commercial operation?

1 MR. BLOSSOM: I think that is a little
2 bit unknown with the ownership situation. I think the
3 ABWR, the boiling water side and the pressurized water
4 side will be separated to some extent.
5 MEMBER SIEBER: Yes, you will have dual
6 licenses.
7 MR. BLOSSOM: But I can't predict what
8 the ownership of 1 and 2 and 3 and 4 will be seven
9 years. So.
10 MEMBER SIEBER: Well, that is not all
11 that complex. At site BP where we had three units
12 with three totally different ownerships; it works.
13 MR. BLOSSOM: It will complement each
14 other.
15 MEMBER STETKAR: Steve, thanks for the
16 good overview. I went back to the ITAAC, especially
17 with regard to what we are going to be talking about
18 later today. Could you give us a - it's on slide 17 -
19 could you give us any general idea of what fraction of
20 those 939 ITAAC or 356 during construction and pre-op
21 involve design acceptance criteria in particular? And
22 I'm not talking about pipe hangers or things like
23 that. I'm more interested in digital INC, either the
24 reactor trip or SFAS (phonetic) functions. Because
25 I've reads that indeed you know the process is

1 invoking the concept of DAC in terms of the digital
2 INC, and I was just curious how much of that is
3 getting carried through into the ITAAC process versus
4 closeout at the COL issuance phase.
5 MR. BLOSSOM: I'm not sure I know the
6 answer with respect to percentage of the 38 percent.
7 Perhaps Craig, would you?
8 MR. CASHELL: I see an audience member
9 that knows.
10 MR. SWANNER: Hi, my name is Craig
11 Swanner. I'm working with Toshiba America through
12 NPR. I've been associated with the INC team for the
13 last two years or so for the - I've been working with
14 ComFerdet on the DAC effort, pilot effort here with
15 STP.
16 There are - for INC there are seven design
17 acceptance criteria specified during Section 3.4(b),
18 and they are in table 3.4, item seven through 14.
19 There are specifically seven through 11 are from the
20 hardware and software development process.
21 MEMBER STETKAR: Those are - I'm glad you
22 mentioned that. Those - I've read those, those tend
23 to be programmatic. I was more interested in terms of
24 actual verification of the design itself and how it
25 functions.

1 MR. SWANNER: There are ITAAC in 3.4
2 which are one through six which verify the
3 functionality of the design as installed. But the
4 program and process ones are seven through 11.
5 MEMBER BROWN: So seven through 11 - yes
6 I went through those also. They are not listed, they
7 are just listed as ITAAC, there is no cryptic word
8 like DAC stuck in there. So you are saying seven
9 through which, 14?
10 MR. SWANNER: Seven through 14 - in NUREG
11 1503, ABWR DCD SER it identifies DAC for 3.4 as the
12 ITAAC-associated with Section 3.4(b). Those are seven
13 through - and let me correct myself - it seven through
14 15, not seven through 14, I am sorry.
15 MEMBER STETKAR: Seven through 15.
16 MEMBER BROWN: Okay, again I'm just
17 reiterating John's comment. Those are very very
18 general, and they say almost nothing. I mean I hate
19 to be blunt, but there is just so little detail it's
20 tough to figure out what is being verified. So there
21 are a few other ones that are pulled out of ITAAC in
22 Tier 1, Section 2.7.5, excuse me, and I will probably
23 bring it up later, but I'll bring it up now. For
24 example, when you talk about evaluating the
25 deterministic behavior of the system, it just says

1 that the report will be issued showing it's
2 deterministic. That is the acceptance criteria, which
3 is not exactly soul satisfying when you look at the
4 pre-COL licensing determination, particularly relative
5 to the Common Q platform, the FPGA when it is a little
6 bit - it's different, since you have got two different
7 platforms you are dealing with.
8 I guess I would have looked for a little
9 more detail on what somebody was going to do as far as
10 the DAC relative to timing analysis, relative to
11 stackup or microprocessors in series, the
12 interrelation of the event-driven communications from
13 microprocessor to microprocessor as opposed to a fixed
14 period. I'm just iterating that from the standpoint
15 of design acceptance criteria this - both the FSAR and
16 the DCD original, if you go back to where you pull out
17 - only four sections changed when we went from the DCD
18 to the FSAR, I think it was 3, 4, 12 and 13 or
19 something like that, so it had some changes to it.
20 So the rest is back in the original setup, the
21 original plan for DAC.
22 So anyway you've just confirmed what I
23 think John and I both in looking at this.
24 MR. BLOSSOM: A preview of the
25 discussion this afternoon, maybe?

1 MEMBER BROWN: Indeed, just wanted to
2 ask.
3 MEMBER STETKAR: Another question,
4 relating to the ITAAC or pre-op testing for the
5 digital INC or safety systems called SSLC logic
6 control. In the pre-op test description it says
7 something to the effect that operability of the system
8 from input sensor to driven equipment shall be
9 demonstrated during a series of overlap testing, and
10 then it pulls out some examples of verification that
11 is going to be performed. That leads me to believe
12 that there won't be any end-to-end functional testing
13 where you actually go out to the sensor, trip it, or
14 insert a signal depending on which it's supposed to
15 do, verify that indeed the signal goes through all the
16 analog to digital processing stuff, that the digital
17 stuff does everything that it wants to do, that the
18 output devices function, and indeed eventually the
19 valve opens or closes and the pump starts.
20 Are you going to do any of that end-to-end
21 functional testing?
22 MR. BLOSSOM: My intent would be to do
23 that.
24 MEMBER STETKAR: It doesn't say that you
25 are going to do that. That's why I was asking. I

1 see descriptions saying, well, you are going to test
2 the intermediate stuff to make sure that the
3 microprocessors all work, that you are going to test
4 the analog to digital converters, you are going to
5 check to make sure that the calibrations are correct,
6 you are going to make sure that the equipment works
7 given an actuation signal. But I didn't really see
8 anything that says, you are going to make sure the
9 whole system works.
10 MR. BLOSSOM: Let me take an action and
11 get back with you on that.
12 MEMBER STETKAR: I'd appreciate, because
13 it's something that --
14 MEMBER SIEBER: Won't that sort of happen
15 automatically during cold functionals and hot
16 functionals?
17 MEMBER STETKAR: Not necessarily.
18 There's been examples in the existing fleet where
19 people test bits and pieces.
20 MEMBER SIEBER: You have protection
21 systems, unless you intentionally test those every
22 track you may not get those, but the regular flood
23 control --
24 MEMBER STETKAR: Oh, regular, no, but I'm
25 talking about the protection, SFAS, reactor protection

1 and safeguards actuation from the process sensor.

2 MEMBER SIEBER: You're right on that,

3 that has to be tested.

4 MR. CASHELL: All surveillance

5 requirements in the technical specifications will have

6 to have been met when we startup, so that will cover

7 those systems.

8 MEMBER STETKAR: Well, except those

9 surveillances can be done without doing an end-to-end

10 function.

11 MR. CASHELL: Well, the way we've

12 designed our functional test is an end-to-end, and we

13 have also specified verification of setpoint during

14 those, so I think you will see that those particular

15 systems will be tested.

16 MEMBER BROWN: Yes, but doing a setpoint

17 check you can do with a test device or some input

18 device or a laptop feeding into a microprocessor

19 checking it. I mean it's a software setpoint.

20 MR. CASHELL: Functional software,

21 itself is a --

22 MEMBER BROWN: Yes, the only thing I

23 found when looking at this was in the original DCD

24 section, I guess the reactor protection pre-op test,

25 and in that particular test there is what you call a

1 channel response time check, which goes from the
2 process variable to the de-energized state of the
3 SCRAM pilot valve solenoids. So I think that might be
4 an example, is that an example of what you are looking
5 for? That was in Chapter 14 of the original Rev. 4
6 of the DCD.
7 MEMBER STETKAR: Yes, I'm reading Chapter
8 14 of the --
9 MEMBER BROWN: Of the FSAR.
10 MEMBER STETKAR: Of the COL FSAR.
11 MEMBER BROWN: Yes, which is - but this
12 part wasn't changed. Regardless of the change in
13 platforms. But other than that in terms of other
14 response, of linear responses, did anything - did
15 everything get installed as it's supposed to? I mean
16 did you do multiple point checks? That is not the
17 only thing you should put in a signal, check that it
18 trips and ends up tripping something else. I don't
19 disagree with that. That is a good thing to do. But
20 typically you would expect in a preoperational test if
21 you go back through and say here is a range of inputs
22 from the bottom of the scale to the top of the scale.
23 All my indicators, my plant displays, all respond in a
24 satisfactory manner. Yet that is not in this - there
25 are very general words, proper system operation will

1 be demonstrated.

2 MEMBER STETKAR: I think in particular

3 what bothered me if you want a reference, it's Section

4 - here we go - 14.2.12.1.11, which talks about STD or

5 standard departure T13.4-13(b) which is engineered

6 safety features actual system tests, so there is a

7 reference. It says, it specifies three tests. It

8 says setpoint validation using input simulation and

9 automatic self-test feature. Trip logic test of SLF

10 using input simulation and automatic self test

11 feature, and equipment operation using input

12 simulation or manual. That to me sounds like separate

13 tests of the sensors, the intermediate processing

14 logic, and input signal to the final output device

15 separately, not in an integrated end-to-end test. And

16 that's what I'm asking about in particular.

17 MR. HEAD: May I suggest that we might be

18 able to answer that in more detail this afternoon.

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

20 then.

21 MR. HEAD: Any other questions for Steve

22 at this point?

23 CHAIR ABDEL-KHALIK: Let's continue with

24 the presentation.

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

1 just want to have a quick briefing on flow-induced
2 vibration. Our plan here is to provide a briefing on
3 the technical aspects in our Chapter 3 discussion that
4 we did want to inform the ACRS that STEP had
5 originally was going to be a non-prototype, relying on
6 K-6 as being the prototype. As we reviewed the
7 expectations with respect to Rev. 3 and some other
8 questions, we've decided to designate ourself as the
9 prototype plant in accordance with the Reg Guide 120,
10 Rev 3. And this will involve performing STP-specific
11 predictive analysis. We will use K-6 to form our
12 scope and expectations, and the STP will then be a
13 Category 1 non-prototype plan.
14 So the approach we'll be using will be
15 similar to what's done for extended power uprates on
16 operating BWRs.
17 CHAIR ABDEL-KHALIK: Just for reference
18 what is the steam line velocity for this plant vis-à-
19 vis some of the plants that have gone extended power
20 uprates?
21 MR. HEAD: Do we have anyone who could
22 answer at this point?
23 We may not be able to answer that, but we
24 will get that answer I think today.
25 CHAIR ABDEL-KHALIK: Okay.

1 MR. HEAD: And certainly in the Chapter 3
2 briefing I would have expected us to give the answer
3 to that.
4 With respect to this change that we have
5 made, the last bullet is the deliverables there were
6 in support of the COL review, and the dates that those
7 will be provided, including - well, there will be a
8 testing program that will be a part of that that the
9 NRC will be able to witness, and the dates that are
10 there will support our COL review schedule.
11 And as I said we will have a more detailed
12 technical discussion on invocations of this change we
13 will be able to provide in our Chapter 3 discussions.
14 Any questions for me at this point?
15 MEMBER ARMIJO: What is the experience of
16 the steam dryers in the K-6 and K-7 units? Did they
17 have problems that lead you to expect you might have
18 problems with STP Unit 3?
19 MR. HEAD: No, sir.
20 MEMBER ARMIJO: So this is kind of
21 confirmatory work?
22 MR. HEAD: No, this is really quite
23 frankly a regulatory strategy for the Rev 3, the
24 changes that came with Rev 3, between K-6, and today
25 there were other issues with dryers that may be some

1 of the expectations are different than they were
2 originally envisioned when the DCD was licensed. And
3 then overarching all of that there is the potential
4 that we are going to do an uprate for Unit 3, and that
5 would - it would meet its own expectations with
6 respect to the testing program. So all of that
7 combined together just made the idea of becoming a
8 prototype for the rest of what we hope is an ABWR
9 fleet, domestic fleet, it just seemed like reasonably
10 good idea for us.
11 MEMBER ARMIJO: Okay, thank you.
12 CHAIR ABDEL-KHALIK: Now the flow-induced
13 vibration test associated with the fuel itself, and
14 right now you are sort of going with the GE7 fuel, and
15 eventually you will change to a more modern fuel. Is
16 that part of the amendment when you sort of decide to
17 change the fuel? Is that part of the acceptance of
18 the new fuel design?
19 MR. HEAD: When we do the amendment, for
20 the fuel --
21 CHAIR ABDEL-KHALIK: Right.
22 MR. HEAD: -- then aspects of the ABWR
23 for the current ABWR, and if we do an extended power
24 uprate, it will have to be considered as part of that
25 amendment if there are any aspects that have to be

1 addressed.

2 I don't know if I have answered your

3 question.

4 CHAIR ABDEL-KHALIK: Not quite, but we

5 will get to that issue I guess at the appropriate

6 time.

7 MEMBER BROWN: I have one other - well,

8 one more question, anyway, whatever it leads to. In

9 going through the list of testing, you had a table, in

10 the old DCD, which is then amplified or modified in

11 the FSAR based on the changes, you do have a specific

12 reactor protection system preoperational test, it runs

13 through a whole series of things. There are - you

14 refer in the rest of all the text, in Chapter 7 and 8,

15 to the ELCS, which is the Engineered Safeguards Logic

16 Control system I think. But when I went and looked at

17 where is the test of that overall system, there is not

18 even - ELCS is not even used anywhere in the chapter.

19 It is absent. So I searched and searched, could not

20 find an equivalent test for the overall engineered

21 safeguards system, the logic control system testing at

22 all. Now some of those - and it's been comprised of I

23 don't know, two hands full with various systems under

24 various accident type scenarios. For instance under a

25 LOCA there are a number of systems that come into play

1 that have to play in a certain either sequence or
2 manner based on certain signals coming in through the
3 progress of a transient. And there is no mention of
4 any type of testing that tests that type of an
5 integrated beginning to end equivalency for those - an
6 integrated application of all those various systems.
7 They are all tested individually but not on a - sort
8 of piece wise, and whether this is piece wise or
9 linear or not, I don't know, but I guess what I'd be
10 familiar with is if you had an integrated system test
11 of the overall safeguards systems under the various
12 accident conditions under which it is supposed to
13 operate. Now whether it is subsumed somewhere else in
14 the safety logic system pre-op test is another -
15 really deals with a set of either FPGA or
16 microprocessor based logic blocks, whether they are
17 digital trip functions or trip logic functions, or
18 whatever. They didn't seem to apply to the overall
19 test. That seemed to be absent. Just an
20 amplification of the previous discussion of the
21 overall integrated testing.
22 MR. HEAD: Someone in this room I think
23 will be able I think to address that this afternoon.
24 MEMBER BROWN: Okay.
25 CHAIR ABDEL-KHALIK: Now the models and

1 the analyses that will be performed to support the
2 steam dryer qualification will be completed I see by
3 the middle of December, and I suspect the subcommittee
4 would like to look at those reports. So we will work
5 with the staff on scheduling when we would have an
6 opportunity to evaluate these reports.
7 (Off the record comments.)
8 MR. HEAD: And I think that was our
9 presentation on Chapter 14.
10 CHAIR ABDEL-KHALIK: Thank you. At this
11 time the staff will make their presentation.
12 STP COLA FSAR CHAPTER 14
13 MS. JOSEPH: Good morning. My name is
14 Stacy Joseph, and I am project manager for the staff's
15 review of Chapter 14 in South Text project
16 application. I am joined today by Frank Talbot, from
17 the Quality and Vendor Branch, who is the lead
18 reviewer for the initial plant testing portion of
19 Chapter 14.
20 In addition to Frank's contribution to
21 Chapter 14, reviewers listed on this slide were also
22 contributors to the technical review of this chapter.
23 Today we are going to be discussing the
24 staff's review of Chapter 14 verification programs.
25 Frank Talbot will be discussing the staff's findings

1 in Section 14.2 which covers initial plant testing.
2 Section 14.2's review of Tier 1 and Tier 2 departures,
3 several COL licensing information items, and startup
4 administration manual.
5 Next, I'll be discussing Sections 14.3 and
6 14.3S of the staff's SER. I will be discussing our
7 review strategy for Tier 1 departures presented in
8 Section 14.3S, and we will be presenting a summary of
9 the ITAAC review discussed in Section 14.3 of the SER.
10 With that I'll turn it over to Frank.
11 MR. TALBOT: Hello, my name is Frank
12 Talbot, I'm in the Quality and Vendor Branch A of the
13 Office of New Reactors.
14 For STP 14.2 I reviewed the FSAR in
15 accordance with NUREG 0800, SRP 14.2, and Reg Guide
16 1.206, and also in accordance with Reg Guide 1.68 and
17 the other 18 Reg Guides that are referenced in Reg
18 Guide 1.68.
19 The section 14.2 of the DCD was
20 incorporated by reference with several departures.
21 The staff reviewed three Tier 1 departures and 9 Tier
22 2 departures affecting FSAR Section 14.2, and we also
23 reviewed COL information items and the startup
24 administration manual. The staff issued 13 requests
25 for additional information on STP Units 3 and 4 FSAR

1 Section 14.2. Next slide, please.

2 We had the two open item issues, and the

3 issues related initially to STP not taking credit for

4 Japan K-6 as the prototype plant for STP Units 3 and 4

5 has a nonprototype category one plant related to the

6 flow induced vibration assessment program. Recently

7 on April 20th, 2010, STPNOC informed the staff that STP

8 Unit 3 would now become the prototype plant, and STP

9 Unit 4 would be the nonprototype Category I plant.

10 STPNOC plans to submit revised responses to the

11 two open items we have related to RAI 14.2-06 and

12 14.2-08 regarding the flow induced vibration program

13 test abstracts. The flow induced vibration program

14 test specs for Unit 3 prototype plant is already

15 provided in the ABWR DCD Section 14.2 The revised

16 flow induced vibration assessment program for STP Unit

17 4 which is the nonprototype category I plant will be

18 evaluated in the STPNOC update to FSAR Sections 3.9.2

19 and 14.2 to identify what flow induced vibration tests

20 are needed for Unit 4.

21 MEMBER BROWN: Why would they be

22 different? I understand the prototype match, but I

23 presume the design is the same. I mean there is no

24 variation. So all you are looking for is a subset.

25 MR. TALBOT: Well, if you look at Reg

1 Guide 1.20 --

2 MEMBER BROWN: I didn't, so I'll give you

3 the benefit of doubt.

4 MR. TALBOT: Yes, Reg Guide 1.20

5 basically specifies what you test for prototype

6 plants. And then for a non-Category I --

7 MEMBER SIEBER: It's a subset.

8 MR. TALBOT: -- it's a subset of what it

9 is for the prototype plants. And you don't have to do

10 as much testing before the --

11 MEMBER BROWN: I understand that. I

12 don't disagree with it. But since I'm not familiar, I

13 hate to tell you this, but I'm not familiar with 1.2.

14 I'm an electrical geek, not a mechanical geek.

15 MR. TALBOT: Right.

16 MEMBER BROWN: But does it bound the

17 conditions? I mean is there some type of requirement

18 in there that you bound the conditions, that you test

19 endpoints or something like that, so that you at least

20 know what you got on the beginning and at then end?

21 MR. TALBOT: Oh, yes, you would take your

22 bounding conditions for the prototype plant, and then

23 what you can take credit for on the prototype plant,

24 or the nonprototype plant Category I there may not be

25 as many testing requirements for the nonprototype

1 Category I plant to meet the guidance in Reg Guide
2 1.20.
3 MEMBER BROWN: Okay, thank you.
4 MEMBER ARMIJO: I'm still a little
5 confused. By designating Unit 3 as the prototype
6 instead of K-6 does that require that STP perform more
7 testing than they would have done otherwise?
8 MR. HEAD: Yes, extensive testing.
9 MEMBER ARMIJO: You have made a big
10 commitment on much more testing?
11 MR. HEAD: Yes, sir, we have made a very
12 big commitment, and we feel like it's an appropriate
13 thing to do, and will set the stage for --
14 MEMBER ARMIJO: Other things.
15 MR. HEAD: Yes.
16 MR. TALBOT: Scott, you may want to talk
17 about for the dryer that you have more testing related
18 to this information.
19 MR. HEAD: Yes, the predictive analysis
20 will be extensive, and we are using previous
21 approaches that the NRC has already reviewed, and then
22 the analysis will obviously be confirmed as part of
23 the testing, the pre-op testing, and then the testing
24 throughout the startup phase, and then operational
25 phase also. So as you look at it it's a very big

1 commitment, and that then will set the stage for a
2 more limited process with respect to Unit 4.
3 MEMBER SHACK: Have you chosen the people
4 who will be doing the analytical model for the
5 acoustic expectation?
6 MR. HEAD: You mean the predictive
7 analysis?
8 MEMBER SHACK: Right.
9 MR. HEAD: Which company is that?
10 MR. HEAD: It's being led by
11 Westinghouse. And it's similar to the AP1000 approach
12 that has already been reviewed. So it's --
13 MEMBER SIEBER: And how will you
14 establish the acceptance criteria for the prototype
15 testing results? Are you just going to say it didn't
16 fall apart?
17 MR. HEAD: Oh, no, it's much more exotic
18 than that. The expectations will be defined with
19 respect to stresses and --
20 MEMBER SIEBER: So you don't have any of
21 that at this point? What the criteria will be, how it
22 will be based?
23 MR. HEAD: I think those are really a
24 Chapter 3 type discussion, that we will be more than
25 prepared to do in Chapter 3. I think today was more

1 really from a testing standpoint, sort of our coming
2 out, that we are making this change.
3 MEMBER SIEBER: You got this group and
4 they are going to do these things.
5 MR. HEAD: Exactly, we have large number
6 of people who are creating this product to support the
7 schedule that you saw in here.
8 MEMBER SIEBER: Well, as you can probably
9 tell this is an area of great interest to us.
10 MR. HEAD: Yes, sir, and it is to us, and
11 that is part of the reason the decision, while
12 important and far reaching, it was relatively easy for
13 us to do, because we recognized how important this
14 issue is, and how much has changed since the original
15 certified design.
16 MEMBER SIEBER: Correct.
17 CHAIR ABDEL-KHALIK: As I said earlier,
18 we will have the opportunity to review those models
19 once the reports are completed. Thank you.
20 MEMBER BROWN: Can I ask one question?
21 CHAIR ABDEL-KHALIK: Yes, sir.
22 MEMBER BROWN: You commented that you are
23 going to use the same method or the same approach used
24 on AP 1000, and this is an education question, so
25 excuse me gentlemen, that's a PWR, this is a boiling

1 water reactor, and I would think that the flow
2 regimes, the velocities, the mechanical configuration
3 are different. Am I right or wrong? The
4 extrapolation of a model from a PWR to this, it's not
5 hard?
6 CHAIR ABDEL-KHALIK: It's not an
7 extrapolation.
8 MEMBER BROWN: Sounds like it. I don't
9 know, when I do that in the electrical world things
10 blow up. (Laughter)
11 MR. HEAD: Obviously pressures and flows
12 and stressed will be different, but the process that
13 you go through to get the predictive analysis has been
14 defined, and we are in essence using that as a model
15 to go through. And so it's really our statement that
16 some people have been through this before, and now we
17 are going to be repeating that is really what that
18 says. Clearly for the ABWR the results, flows and
19 everything else, will be different.
20 MEMBER BROWN: Okay, like I said it was
21 an educational question. I'm half educated now.
22 (Laughter)
23 MR. HEAD: That's better than I normally
24 do.
25 MEMBER SIEBER: Well, maybe just as an

1 extension, and maybe this is too detailed for this
2 stage, but steam dryers, steam separators in BWRs have
3 been noteworthy in drawing attention to their
4 construction and operation and durability, but the
5 rest of the BWR internals has had a host of
6 historical problems, a lot of which are materials
7 related, some of which are flow related and so forth.
8 Are you going to do anything more than has been done
9 with the current generation of BWRs to ensure that the
10 whole core internals will satisfy lifetime objectives
11 for durability and performance?
12 MR. HEAD: I believe we will be. I mean
13 we obviously are factoring in all the experience that
14 you alluded to and the current, which we think is of
15 significant benefit is that before we are operational,
16 for pre-op testing, the Japanese plants will have
17 continued to operate. So that is one of the - that's
18 one of the things that we -- even though we are not
19 using K-6 as a prototype, we clearly are going to use
20 K-6 as both the testing and any results that come out
21 of that in this intervening period to our advantage,
22 and so that's close to answering your questions.
23 Probably there will be some more detailed discussions
24 maybe on some of those failures you are alluding we
25 will talk about in the Chapter 3 discussion.

1 MEMBER SIEBER: Thank you.

2 MR. TALBOT: Okay, the last issue that we
3 have is related to license conditions, next slide.
4 And STPNOC proposed three COL commitments - proposed
5 COL commitments to address post-COL license
6 information items. The staff has identified that the
7 commitments should be license conditions to meet
8 52.79(a)(28) and Reg Guide 1.206 Regulatory Positions.

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

24 CHAIR ABDEL-KHALIK: Thank you.

25 MS. JOSEPH: All right, the next section

1 of the staff's SER evaluates - 14.3 of the FSAR
2 identifies the Tier 1 selection criteria and
3 processes. This section of the FSAR is completely
4 incorporated by reference. Chapter 14.3 of the
5 staff's SER is basically a summary of the Tier 1 and
6 Tier 2 departures - sorry, Tier 1 and Tier 2*
7 departures identified in revision three of the COLA.
8 This section of the SER does not contain
9 any technical evaluations, but instead simply provides
10 a roadmap to identify where in the SER each of these
11 Tier 1 and Tier 2* departures are evaluated.
12 Section 14.3S of the staff's SER evaluates
13 the inspections test analysis and acceptance criteria
14 proposed by FTP in Part 9 of the application. Part 9
15 contains changes to the design certification ITAAC.
16 Site specific ITAAC, emergency planning ITAAC, and
17 physical security ITAAC. There are six Tier 1
18 departures in Revision 3 of the COLA that affect
19 changes to the ITAAC identified in Tier 1 chapters two
20 and three of the DCD.
21 The staff reviewed changes to the ITAAC in
22 conjunction with changes to the design in the Tier 2
23 chapters, and determined that the changes made to the
24 ITAAC are consistent with the changes made to the
25 design and are acceptable at this time. There are no

1 open items related to design certification ITAAC for
2 those identified in Revision 3 of the FSAR.
3 The site also reviewed site specific ITAAC
4 proposed in Part 9. In general the site specific
5 ITAAC were developed to address the interface
6 requirements identified in Tier 1, Chapter 4, of the
7 DCD. Evaluations of the site specific ITAAC
8 identified on this slide are located within the
9 evaluation of that design and in another section of
10 the SER.
11 Evaluation of offsite power ITAAC,
12 breathing air ITAAC, and structural evaluations for
13 the site specific ITAAC are located in Section 14.3S
14 of the FSAR.
15 There are two open items identified in
16 Section 14.3S related to the structural evaluation of
17 the site-specific ITAAC. These two open items deal
18 with general process for - general process question
19 for performing structural analysis ITAAC, and also
20 there is a request for an addition of ITAAC for the
21 diesel generator fuel oil storage.
22 Since publication of the SER with open
23 items, STP has responded to the staff's request, and
24 the staff has determined that the response has
25 adequately addressed those concerns.

1 Therefore for the evaluations provided in
2 this section of the SER, there are no open items, and
3 the staff determined that the ITAAC will ensure that
4 the systems perform in accordance with the design.
5 Finally in Part 9 of the COLA contains
6 ITAAC for emergency planning and physical security.
7 The emergency planning ITAAC is evaluated in Section
8 13.3 of the staff SER, and the evaluation for physical
9 security ITAAC is ongoing and will be provided in the
10 SER with no open items at a later time.
11 And in summary, as Frank stated, because
12 of the open items in Chapter 14, and in the related
13 design chapters, staff cannot finalize their
14 conclusions at this time.
15 CHAIR ABDEL-KHALIK: Are there any
16 questions for the staff? Yes, sir.
17 MEMBER BROWN: Yes, the other thing - I
18 guess I wanted to just backtrack a little here, not
19 too much though. But in going through there was a
20 mention and I can't remember where it was in the FSAR,
21 on cybersecurity relative to all the plant data and
22 network or whatever it's called, that this would all
23 be addressed later. I mean it was very very sparse,
24 and when I looked, I would be thinking that maybe it
25 doesn't sound like it's site specific but it appeared

1 to me to be a big whole relative to the expectations.
2 I mean like there has been no thought process at all.
3 Is that true?
4 MR. HEAD: No, we have responded to the
5 NRC on that I think what is there is what present at
6 the time. We just submitted an amount of information
7 provided to the staff about cyber security. So we
8 could again discuss that in more detail this afternoon
9 if you like.
10 MEMBER BROWN: Okay, no, that's fine,
11 it's not a critical comment. I just noticed the
12 absence in the listing of the ITAAC of addressing how
13 does cyber security work. Can you attack it? Can you
14 get past firewalls, whatever.
15 MR. TONACCI: This is Mark Tonacci. The
16 cyber security reviews were postponed until later in
17 our SER development. They are going to be done as
18 part of Chapter 13. They aren't quite ready yet. But
19 Chapter 13 will be coming to you I think later on this
20 month, but that portion for cyber was deferred because
21 of rulemaking activities in the security office. So
22 we will look into that, but it's not going to be this
23 cycle of SER reviews.
24 MEMBER BROWN: But let me backtrack again
25 slightly, even though it is addressed there, isn't

1 there - wouldn't there have been some need to have
2 ITAAC associated with cyber security reflected in
3 Chapter 14, or at least --
4 MR. TONACCI: I really cannot answer
5 that. I can take that as a lookup, but they have not
6 proposed any at this time to us, but they are not
7 finished with their reviews either.
8 CHAIR ABDEL-KHALIK: We may have to
9 revisit this.
10 MEMBER BROWN: That's fine. It's just an
11 absence of information, and I couldn't find it
12 anywhere else.
13 MS. JOSEPH: All the reasons for
14 planning ITAAC is in the evaluation of Chapter 13
15 anyway.
16 MEMBER BROWN: So is that considered
17 emergency planning, cyber security?
18 MS. JOSEPH: I guess not. Sorry.
19 (Laughter)
20 MEMBER BROWN: That would be a real
21 emergency.
22 (Off the record comments.)
23 CHAIR ABDEL-KHALIK: Before we end our
24 discussions let me just try to capture the action
25 items. STP has an action item with regard to end-to-

1 end functional testing.

2 MEMBER BROWN: Including the ELCS system

3 which seems to be absent.

4 CHAIR ABDEL-KHALIK: Okay, they also

5 provide comparison of steam line velocities versus

6 plants that have extended power uprates. And I guess

7 we'll work with the staff on scheduling the time the

8 committee will hear the analyses when they are

9 completed by the end of December?

10 MR. TONACCI: Yes, that will go obviously

11 out into next year, first quarter, probably.

12 CHAIR ABDEL-KHALIK: Are there any other

13 action items or open items that we need to keep track

14 of?

15 MR. TONACCI: None.

16 CHAIR ABDEL-KHALIK: Okay, at this time

17 we are way ahead of schedule, and rather than taking a

18 break, if the applicant is ready, we can move on with

19 Chapter 7, and then we will take a break at an

20 appropriate time.

21 (Off the record comments.)

22 STP COLA FSAR CHAPTER 7

23 CHAIR ABDEL-KHALIK: Is the applicant

24 ready to proceed with the presentation?

25 MR. HEAD: Let us do a maneuver here and

1 we'll be there.

2 CHAIR ABDEL-KHALIK: Thank you.

3 (Off the record comments.)

4 MEMBER STETKAR: Our reporter will take

5 care of you if you don't.

6 MR. HEAD: Okay, we will go ahead and get

7 started on Chapter 7. We appreciate the opportunity

8 because there is a lot to discussion this topic.

9 The attendees today, myself, we have Mike

10 Murray who has presented before on Chapter 18.

11 Joining us also today is Kyle Dittman. Mr. Ikeda-san,

12 vice president with TANE, Craig Swanner, you've

13 already heard from earlier this morning. And Dr.

14 Fukumoto-san, a senior fellow from Toshiba is here

15 today to help us with the presentation. And Mr. Mr.

16 Fredrickson from Westinghouse.

17 Also joining us today in preparation for

18 this discussion are other people who could be

19 available to hopefully answer questions that we will

20 either get or that we have already received. So this

21 is an important topic, and in preparation for this we

22 have attempted to obviously get ready for today's

23 presentation.

24 With that I'm going to turn the discussion

25 - oh, I missed the agenda?

1 MR. MURRAY: Michael Murray, I'm the
2 manager of the I&C platforms at the STP #3 and #4,
3 thank you. If you follow through the agenda, a lot of
4 the first up front is bookkeeping discussions of what
5 we have changed. I think a lot of the interesting
6 discussions I would say will be when we get into the
7 I&C protection system basic architecture. And there
8 are time when I say, can we hold that discussion,
9 because what we will have there are some pictures and
10 diagrams that we will be able to talk through some of
11 the questions better.
12 So that - you may hear me say that, and I
13 will ask your help in that.
14 Chapter 7 summary, we've listed a few of
15 the sections there, the controls and instrumentation
16 section, the control panel section, we listed it
17 because there are a lot of changes there. That is
18 where the demultiplex changes came from that we will
19 describe later. And the 3.4 which is the main
20 instrumentation and controls system for the ABWR.
21 The COLA incorporates by reference the
22 ABWR DCD information, functionality and logic, that is
23 being incorporated by reference. Departures are taken
24 - are for incorporation of the advances in technology
25 as well as provide clarification. We found a number

1 of places where clarification was required to better
2 describe the functionality of the design. Next slide.
3 The chapters in it is the introduction,
4 7.1, 7.1Sierra, which is instrumentation control
5 platforms. 7.2, which is the reactor protection trip
6 system, and then the 7.3 which is the engineered
7 safety feature system. 7.4, which is the systems
8 required for safe shutdown. 7.5, information systems
9 important to safety. 7.6, all other instrumentation
10 required for safety, 7.6 Sierra, interlock systems
11 important to safety. 7.7, control systems not
12 required for safety, and examples of those would be
13 rod control systems, the recirc flow control system,
14 important systems but not for safety.
15 7.8, the COL licensing information,
16 diverse instrumentation and control systems which will
17 be in 7.8Sierra, and in 7.9Sierra, data communication
18 systems, 7Alpha, 7Bravo and 7 Charley, defense in
19 depth, Appendix R, and implementation of hardware and
20 software development.
21 We'll start into discussions on
22 departures. We will cover some of it, will actually
23 be repetitive as we get more detail on it. Our
24 departures are driven - and I'll keep my paper away
25 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.

1 MR. MURRAY: Some of the changes were
2 nomenclature changes to improve our standardization.
3 For example the original DCD had terms that were more
4 fitted for the platform that was being applied, like
5 trip logic unit, which was a component within the
6 platform. We have used some generic terms for that to
7 facilitate standardization of that. We will use the
8 term, trip logic function, for example.
9 MEMBER BROWN: I take it those are
10 algorithms. Data comes in, and there is a function
11 that processes data and develops the trip or
12 something?
13 MR. MURRAY: The trip logic function --
14 MEMBER BROWN: Software.
15 MR. MURRAY: The voter hardware -
16 MEMBER BROWN: There's processing and
17 then there is software voting?
18 MR. MURRAY: That's correct. And it's
19 the function and not necessarily --
20 MEMBER BROWN: But implemented by
21 software.
22 MR. MURRAY: That is correct, or hardware
23 in the case of the FBGA.
24 So next slide. Again, advances in
25 technology. The final platforms we selected, we then

1 had to implement into the design. Incorporation of -
2 we have also incorporated the generic boiling water
3 reactor I&C enhancements, the adoption of the boiling
4 water generically approved oscillation power range
5 monitors, so we have incorporated that into the
6 design.
7 And we had discussed at a previous meeting
8 that we had eliminated the main steam high radiation
9 trip and main steam isolation. That was supported by
10 safety evaluation reports, and generic owners' group
11 work with the staff.
12 Departure clarification: we did a lot of
13 clarification in Tier 2 specifically. A couple of
14 examples here of some clarification on the automatic
15 depressurization system logic. It wasn't clear how
16 the timers were being used, how they were functioning
17 within the logic, and also the logic between for
18 example Reactor Vessel Level 1, and the high drywell
19 pressure. What we did there was we made sure it was
20 clear that we were - the functional requirements that
21 we were implementing. So we did clarification there;
22 that's on example.
23 Another example in the Residual Heat
24 Removal system, suppression pool logic was not as
25 clear as it needed to be for what the functionality

1 that was being done, and also residual heat removal
2 shut down cooling, so we did clarification there of
3 those functions that were not the primary functions
4 but secondary functions for residual heat removal to
5 make sure it was clear how those functions were being
6 implemented.
7 MEMBER STETKAR: Mike?
8 MR. MURRAY: Yes, sir.
9 MEMBER STETKAR: We've had enough
10 discussions in the past to know that I'm a kind of
11 detail oriented guy. So tell me when in your
12 presentation you'd like to discuss specific details
13 about some of these changes. Do you want to get more
14 into kind of an overview first, and how the --
15 MR. MURRAY: Why don't we get through the
16 overview, see if we --
17 MEMBER STETKAR: I don't want to
18 interrupt kind of a stream of consciousness by putting
19 specific questions.
20 MR. MURRAY: Well, let's see if we can
21 answer some of the questions as we go, and then the
22 specifics on the change you ask, and I'll have people
23 that can help and we'll be able to answer the
24 questions.
25 MR. MURRAY: I just want to know when is

1 the best time to sort of start that discussion?

2 MR. MURRAY: I'd like to get through the

3 technical discussions on the platforms, and I think at

4 that point we will see if we can answer some of the

5 questions you've got and then continue, if that is

6 okay.

7 MEMBER STETKAR: No, that's fine.

8 MR. MURRAY: Again a little more detail

9 on the Tier 1 departures: control system changes,

10 input test, hardware. We had a Tier 1 departure

11 because it impacted the Tier 1 test requirements. And

12 rod control and information system, we read the

13 original requirements. It made it look like the power

14 supplies were not independent, that either power

15 supply would take down the entire system; actually

16 they are redundant. So we had to clarify that so that

17 when we tested it it would be tested properly for

18 further design, which is much more robust than I was

19 defining the test.

20 Again, the deletion of the mainstream

21 isolation closure trip, we have discussed that

22 previously.

23 And then in the Tier 1, 3.4-1, and this is

24 where we'll have a lot of discussion later, we

25 eliminated the data communications technology, the

1 obsolete technology, unnecessarily inadvertent ESF
2 actuations, we'll discuss that further also, and we
3 got that covered.
4 Have you got questions on that, I guess.
5 MEMBER STETKAR: Now is the time on that
6 one.
7 MR. MURRAY: Now is the time on that one,
8 that's correct.
9 MEMBER BROWN: On which one?
10 MR. MURRAY: This would be the second
11 bullet which is the unnecessary inadvertent ESF logic.
12 MEMBER STETKAR: Detail question: how
13 many - you call them - I can't read it with my glasses
14 on, I can't read with my glasses off - safety system
15 logic functions is the terminology which is used in
16 the FSAR, SLF like Frank. I don't know whether those
17 are microprocessors or what they are. They are little
18 boxes on the drawing. How many of those exist in each
19 division? Two, 20, 30?
20 MR. MURRAY: Ed Brown, introduce
21 yourself, please, he'll be able to answer those
22 detailed questions. Now this is - what we'll be
23 answering first with Ed would be in the ELCS, or ESF
24 logic and control system. Is that where your question
25 comes from?

1 MEMBER STETKAR: Exactly, I'm interested
2 in ELCS, that's right.
3 MR. BROWN: My name is Ed Brown. I work
4 for Westinghouse.
5 I have 41 years of experience in nuclear
6 power plant I&C. I am a technical adviser to the
7 director of safety monitoring systems, and I'm
8 assigned full time to the ELCS system for South Texas
9 Project #3 and #4.
10 The question if I understand it correctly
11 was how many safety logic functions are there within
12 the ELCS in each division.
13 MEMBER STETKAR: That's correct.
14 MR. BROWN: Okay, the COLA describes that
15 there is a minimum of two and they are segmented by
16 function, low pressure injection functions, and high
17 pressure injection functions. So there is a mode of
18 functional diversity that is required by the COLA. We
19 have further segmented the functions to provide for
20 basically additional fault tolerance, so we have now
21 six SLFs per division, and that is per each one of the
22 three divisions of engineered safeguards. The SLFs
23 that have very important functions like ECCS are
24 duplicated --
25 MEMBER STETKAR: Let me, before we get to

1 that, one statement you made was that the SLFs were
2 segregated by high pressure and low pressure
3 functions, and unfortunately the only information I
4 have is Figures 7.1-2 in the FSAR. And it wasn't at
5 all clear to me, looking at the actual allocation of
6 functions on that figure that indeed they are
7 allocated strictly between high pressure and low
8 pressure. For example in one division I see a diesel
9 generator start allocated to high pressure core flood,
10 which seems to make sense because you need the diesel
11 for that function, but in another division I don't see
12 the diesel allocated to high pressure core flood. So
13 I'm curious about how those allocations actually exist
14 and whether there is a very explicit documentation of
15 how they are actually made. Or whether there were
16 active decisions about why some things that don't seem
17 to be high pressure are with low pressure, and things
18 like that. I got a little confused.
19 MR. MURRAY: Could we have Mr. Swanner
20 provide more information.
21 MR. SWANNER: Hi, my name is Craig
22 Swanner. I previously introduced myself.
23 The statement that Ed Brown is referring
24 is in 7.1S.2, where we have a detailed description of
25 the ELCS system, the ELCS platform. And that section

1 has been revised, and Revision 1 to our response to
2 RAI A7-6.
3 MEMBER STETKAR: I have that material
4 here with me, and I still couldn't figure out how the
5 high pressure and low pressure are allocated among the
6 SLFs, because it doesn't tell me that. I have the
7 text. I have read it.
8 MR. SWANNER: There is a statement in
9 there that identifies that.
10 MEMBER STETKAR: It says the same words
11 that we heard this morning. I'm looking at a drawing
12 that doesn't seem at all clear that it supports those
13 words. So I'm curious whether the drawing - whether
14 I'm misinterpreting something on the drawing or
15 whether the drawing isn't correct. I'm looking for an
16 explicit list so that I can indeed confirm that
17 statement that is in the text. This is sort of
18 verifiability of something that is stated in a text
19 with something that can indeed be checked when I'm
20 looking at the actual functioning of the system.
21 MR. MURRAY: I would like to take that
22 back after the break if we can.
23 MEMBER STETKAR: Take it back, because it
24 could be some just rearranging - the drawing may not
25 replicate what is actual, but on the other hand if the

1 drawing does there must have been some active
2 decisions made, and I'd like to really understand what
3 those decisions were.
4 MR. MURRAY: We will discuss that at the
5 break and we will follow that up. The question is the
6 allocation --
7 MEMBER STETKAR: The question is the
8 allocation of the high pressure versus low pressure in
9 terms of the basic functional allocation between those
10 redundant processors, if you want to call them that.
11 Sorry to interrupt you. Now we can get to the
12 redundancy of individual SLFs for a particular
13 function, which is where you started when I
14 interrupted.
15 MR. BROWN: You had I think a question.
16 That is the topic, I wondered what the question you
17 might have concerning that.
18 MEMBER STETKAR: Okay, the question I had
19 is that looking at the - I tried to understand where
20 the coincidence logic, if I can call it that, is
21 applied to specific components and functions in the
22 design, and I read through several of the RAIs and the
23 responses, and in the technical specifications,
24 background documentation, I was finally pointed to
25 that, there are a set of five figures that show

1 difference schemes of implementing coincidence logic,
2 serial versus - two out of two coincidence logic, to
3 prevent spurious operation of some equipment, single
4 actuation for other things where you are apparently
5 not so worried about spurious actuations.
6 I was curious about where I could find in
7 the documentation which specific equipment is applied
8 - to which specific equipment are each of those five
9 different actuation schemes applied? Again, what I'm
10 trying to do is verify something in the design that
11 will point me to an actual logic that is applied to
12 something that could later be verified.
13 And I couldn't find it. I can find it for
14 ADS, so ADS, don't give me ADS as an example, because
15 that is the one place where I could find it. I'm
16 interested in other things like RCIC or specific
17 containment isolation valves or things like that.
18 MR. SWANNER: This is Craig Swanner
19 again. Did you - just a question for you - did you
20 just look at the figures and the bases, or did you
21 look at the text that introduces the figures as well?
22 MEMBER STETKAR: I did both. But the
23 text --
24 MR. SWANNER: I understand.
25 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

1 documentation in the FSAR. Essentially the equivalent
2 of functional logic diagrams for the individual
3 actuated equipment to show me where that two out of
4 two voting versus that single point actuation is
5 implemented. And the reason, for example, low
6 pressure core flood is not something that I'd be
7 particularly concerned about spuriously actuating
8 during power operation, because it isn't going to do
9 anything. On the other hand, if you implemented a
10 serial two out of two coincidence logic requirement
11 you've doubled the likelihood for failure of that
12 function during the conditions when you need it to
13 operate, at least as far as the availability of those
14 SLF logic modules are concerned.
15 So I'm curious about what type of
16 integrated thought process went through when you made
17 the decisions to retain a two out of two voting logic,
18 which as I understand the original design was strictly
19 two out of two for everything. So you have made the
20 decision to remove that for some functions and retain
21 it for others, and I'm curious about what criteria
22 were used, and I can't even infer the criteria by
23 necessarily looking at the design because I can't see
24 the details of the design.
25 MR. MURRAY: Ed, do you need time on

1 that, or can you handle that now?

2 MR. BROWN: No, I think I can elaborate

3 now. And basically it was picking up that the very

4 important functions, the ones that were highlighted in

5 the DCD dealing with ECCS would remain with duplicate

6 SLFs and two out of two redundancy. That was the

7 design principle. The containment isolation system,

8 because that would have an inadvertent effect on

9 operation if that were not duplicated.

10 The systems that are selected for one out

11 of one are typically ventilation type systems or of

12 the supporting systems, some of which do not even

13 receive an actuation signal. In HPN2 is an example.

14 Some of the cooling water control functions, some of

15 the - say are the less critical functions where an

16 inadvertent actuation really wouldn't be indicating

17 either cause plant damage or a transient that would

18 cause or degrade safety function. That was the

19 philosophy.

20 MEMBER STETKAR: Okay, I hear that

21 philosophy, and at one level it sounds fine. I think

22 I was asking was, where in the FSAR can I find

23 documentation to show how it was implemented. You are

24 talking generalities about, well, for some of the

25 cooling water functions, and for containment

1 isolation. I'm looking for something like a list of
2 every safeguards actuated compound, with a reference
3 to which of these particular logic coincidences, and
4 there are five of them, applies. So that for example
5 if I was looking at the design as it is finally
6 implemented in the plant, you see where I'm going,
7 implemented in the plant, I can actually verify that
8 indeed that design philosophy, if I understand the
9 design philosophy, at this stage of the licensing
10 process and agree with the philosophy, I can actually
11 verify that it was implemented when the plant was
12 constructed. And at the moment I don't have that
13 second part of the check. I can't even figure out the
14 first part of the check at this time.
15 MR. MURRAY: I think we will have to take
16 an action to get back on that, but I understand your
17 question.
18 MEMBER STETKAR: Thanks, that's all I
19 had.
20 MR. MURRAY: I'm glad we had a discussion
21 on that topic. That's why I paused. Again, I'm back
22 on slide 11, and we've covered the top two bullets.
23 We will cover the first one in more detail later,
24 under 3.4-1.
25 Clarification of the digital control

1 nomenclature and systems. We've done that as well as
2 final selection of platforms. We've specified these
3 final platforms, as well as testing and surveillance,
4 some of the testing and surveillance changes would
5 have been, originally there was a very complicated
6 automatic surveillance test controller. We have
7 simplified that. For example in the ESF logic and
8 control system we'll do all blind testing and bypass,
9 manually initiated automation. We are maintaining the
10 automation, but we are not doing it continuous
11 automated testing, it's very complex strategy with
12 that.
13 And in the - yes, sir.
14 MEMBER BROWN: Did you - I guess I lost
15 that, because in reading the - I thought in reading
16 the FSAR that you had retained the end process
17 testing, did you - I guess I lost that, because in
18 reading the - I thought in reading the FSAR that you
19 had retained the end process testing, certain types,
20 and it looked like there was a restriction, in other
21 words you weren't trying to trip things, but yet
22 operation from input to output of a particular
23 processor you were running a set of automated tests to
24 see that all of its functions were performing. Now it
25 didn't - I mean it might take a half an hour to do

1 them, because you are going through whatever the
2 cycles are. So I guess I don't understand your
3 comment that you have eliminated the process testing.
4 MR. MURRAY: Let me clarify it then I'll
5 have Ed give even more clarification on it. My
6 comment was that the auto surveillance test controller
7 function, we are not using that function.
8 MEMBER BROWN: In other words, a separate
9 test?
10 MR. MURRAY: Yes, but we are using an
11 automatic test function that you just understood and
12 described.
13 MEMBER BROWN: There are self diagnostics
14 within the process?
15 MR. MURRAY: That is correct. So Ed, why
16 don't you make sure that Mr. Brown has the clearest
17 picture on that.
18 MR. BROWN: Okay, this is Ed Brown again
19 from Westinghouse. We have retained the online
20 diagnostics, which gave a comprehensive fault
21 monitoring during the operation of the system while
22 it's online; that means it's not bypassed and it's
23 operating at power. This extends through all of the
24 processor modules, the communication links, and
25 everything, including the final voting element, but it

1 doesn't not actuate.

2 The self - the original self-test

3 controller was doing signal injection, and was

4 bypassing components during operation, and it was

5 coordinating these tests between divisions, so to make

6 sure that self test did occur. This type of test

7 significantly increases the complexity of the

8 software, significantly increases the difficulty of

9 assuring you will not get a spurious function.

10 What we have done based on experience with

11 other installations has relied on the self diagnostics

12 for plant power operation. Then there are the

13 technical specifications which require sets of tests

14 to be performed at intervals.

15 MEMBER BROWN: Those are operator-

16 initiated tests?

17 MR. BROWN: Those are technician or

18 operator-initiated tests.

19 MEMBER BROWN: And the plant will be in

20 some controlled mode of operation, shutdown or

21 whatever.

22 MR. BROWN: No, the plant will be - it

23 has to be performed online.

24 MEMBER BROWN: Okay, I got it. So for

25 example where we have a fourfold redundancy of the

1 digital trip functions, we will go to a sensor bypass
2 and then operator will put the system in bypass, the
3 operator must follow if there is a manual interlock to
4 request the test mode, the bypass must be present.
5 Then he performs a series of automated
6 tests for the test controller makes a test panel, and
7 the processor associated with that, injects software
8 signals as close to the sensor, and tests all of the
9 logic for the DTF. That would like a Phase I. The
10 second phase we take credit for the diagnostics
11 between - this is what is called overlap testing. The
12 diagnostics which run continuously on the
13 communication link for sending data between a digital
14 trip function and the two out of four voter.
15 MEMBER BROWN: That's the TLF, in other
16 words, the trip logic function.
17 MR. BROWN: Well, they call it an SLF in
18 the in the ECCS.
19 And then for the SLF, you would then go to
20 an SLF bypass, you would bypass the SLF and the same
21 signal injection into the two out of four logic in
22 that one division would occur. The division would
23 remain operable, and then you would test the down
24 portion. The final test which tests the actuation of
25 the device is performed on refueling interval basis.

1 There actual sensor signals are injected through
2 multiple divisions, and components are allowed -
3 components that can be actuated in a particular mode
4 of operation will be actuated, but they are typically
5 not actuated during normal plant operation.
6 MEMBER BROWN: Okay, I understand.
7 MR. MURRAY: Now the field-programmable
8 gate array systems are similar in that we do offline
9 testing and bypass. There is diagnostic continually
10 running as well. And we test and check strategies for
11 surveillance testing.
12 Next slide. Examples of departures for
13 technical specifications, these departures required
14 NRC approval. The first one there which is on the
15 rod control and information system, it was - the
16 reason it required the changes, there was some
17 discussion on the bases, so that drove us to requiring
18 NRC approval. Other than that in this departure what
19 we did was, we clarified the functions of the rod
20 control system as it is applied in the operating
21 current ABWR in Japan, the rod control information
22 system. We clarified such terms as in the design the
23 DCD, it had single rod, rod gain, step, continuous, in
24 and out. The current technology uses similar
25 controls, but uses terms such as step, notch,

1 continuous, insert, withdraw. So we aligned those
2 terms, clarified how those functions were performed.
3 So that was a lot of what we did with that particular
4 departure.
5 And then the setpoint control program is
6 another area where we did a standard departure as
7 well. We implemented the approach in the ISG-08, and
8 we elected option number three, for the setpoint
9 control program.
10 There are two aspects of that, and that is
11 the program itself as well as the setpoint methodology
12 for it. We have listed there the documents. We've
13 got those implementing documents prepared, and the
14 setpoint methodology is based on a similar methodology
15 that is used by Westinghouse in PWRs, so we looked
16 carefully at those differences in those, and had a
17 good understanding. We used the setpoints that are
18 used in existing plants to do comparison of whether
19 our results were as we expected when we went through
20 that process, and gained confidence that the approach,
21 the Westinghouse approach to setpoint methodology,
22 would be suitable, and also the staff is familiar with
23 that methodology.
24 Any questions on that?
25 CHAIR ABDEL-KHALIK: If you can tell me

1 when would be an appropriate point in your
2 presentation to take a break?
3 MR. MURRAY: This would be a good place.
4 I think this is a good place, because we will start
5 getting into - not long we'll be in more detailed
6 discussions.
7 CHAIR ABDEL-KHALIK: So why don't we take
8 a break at this time. We will reconvene at 10:30.
9 (Whereupon at 10:10 a.m. the proceeding in
10 the above-entitled matter went off the record and
11 resumed at 10:28 a.m.)
12 CHAIR ABDEL-KHALIK: We are back in
13 session.
14 Please continue.
15 MR. MURRAY: Okay, we had completed Slide
16 12 discussion of setpoint program. And Slide 13, I
17 use the word, numerous, because instrumentation and
18 controls as you've reviewed it, it covers a lot of
19 areas, and that is the nature of the equipment. We had
20 just a few of the departures listed. These are not
21 requiring prior NRC approval. They were all addressed
22 and reviewed in the Part 52 process, typically again
23 for clarification of content, and advances in design.
24 For example, one of the examples is, on the average
25 power range monitor, and the oscillation power range

1 monitor, the trip signals are separated. That just
2 gave us some - it reduced the potential for
3 inadvertent trips out of that. And just made a much
4 simpler design. And we did that in Tier 2 changes.
5 MEMBER STETKAR: Is it the appropriate
6 time to insert a long interruption on a few examples
7 on these?
8 MR. MURRAY: Yes, sir , if you have
9 questions specifically.
10 MEMBER STETKAR: First question I had,
11 one of these examples for reference it's Department
12 7.2-2, has to do with the SCRAM - it's called SCRAM-
13 actuating relays, but indeed the change I think is the
14 backup SCRAM relays. And the departure as it's listed
15 seems to describe a fundamental change in the way that
16 those backup SCRAM relays are actuated from the
17 drawing in the FSAR which is Figure 7.2-8, which has
18 not changed from the design certification FSAR to the
19 COL FSAR. Those backup SCRAM relays are shown as if I
20 can call it a deenergized actuate, in other words the
21 output signal from the reactor protection line
22 deenergizes the relay, when the relay is deenergized a
23 normally closed coil - a normally closed contact
24 closes which in sub - which subsequently through a two
25 out of four logic energizes the backup SCRAM

1 solenoids. If anybody is following that.

2 It seems like the logic has been changed

3 such that those relays now, the interfacing relays,

4 are normally deenergized and the output of the reactor

5 protection logic now energizes those relays and a

6 normally open contact closes through a two out of four

7 logic to energize the backup SCRAM solenoids.

8 Is that - first of all I want to make sure

9 that I understand that the change actually is as I

10 just described it.

11 MR. DITTMAN: I am Kyle Dittman, I

12 supervise I&C at South Texas. This departure was as

13 you described it. The backup ultimate rod insertion

14 SCRAM solenoids are changed from a normally energized

15 to normally deenergized, to spend their life and

16 prevent --

17 MEMBER STETKAR: These are the relays

18 themselves?

19 MR. DITTMAN: Yes, these are the coils,

20 the actual solenoid valves will be the --

21 MEMBER STETKAR: Well, the solenoids, I

22 thought the solenoids were always deenergized.

23 MR. DITTMAN: Okay, on the backup, in the

24 DCD in this design they were energized.

25 MEMBER STETKAR: The solenoids themselves

1 were continuously energized.

2 MR. DITTMAN: The ARIs were normally

3 energized. We are changing it to normally

4 deenergized, which is consistent with existing BWRs I

5 used to work at here in the United States with backup

6 ARI solenoids. Now the primary solenoids are only

7 energized, the SCRAM solenoid valves. They will

8 continue to be.

9 MEMBER STETKAR: I am not talking about

10 the primary SCRAM, the change as I understand it is

11 only the backup, the ARI.

12 MR. DITTMAN: The ARI.

13 MEMBER STETKAR: It's the air dump off

14 the accumulator.

15 MR. DITTMAN: Dump air header blocked in

16 blowdown.

17 MEMBER STETKAR: I really don't - okay.

18 You are going to have to explain it to me again,

19 because what you explained didn't come through in my

20 understanding of the description of the change in the

21 FSAR or in the departures report, and I couldn't

22 rationalize the description of the change with the

23 unchanged functional schematic drawing. The

24 description in the FSAR says, if I can find the right

25 one --

1 MEMBER BROWN: Are you looking at the
2 standard departure or the FSAR?
3 MEMBER STETKAR: I'm trying to find me -
4 I have too many notes, so bear with me for a second.
5 STP 3 and 4 FSAR subsection has revised the wording of
6 the relay logic contact status from normally closed to
7 normally open, and clarified that the trip state is
8 when the coil is energized. That is relay coil, it
9 doesn't say anything about the actual SCRAM valve
10 solenoids. I was under the impression that they had
11 always been deenergized. This is talking about the
12 interfacing relays that make up the two out of four
13 coincidence logic to either energize or deenergize the
14 solenoids, which I'm not sure what it does anymore.
15 You were talking about a change to the solenoids
16 themselves. This seems to be related to a change in
17 the relays. But the drawing still shows normally
18 closed contacts. I couldn't figure out exactly what
19 the change was, and whether it's consistent with the
20 drawing, and if indeed it's a change from normally a
21 deenergized to actuate to an energize to actuate, I'm
22 curious why that is a very simple thing that doesn't
23 change how the system operates. Because it sounds
24 like it changes the way the system operates. I'm kind
25 of a PRA guy, and I'm worried about failure to open,

1 I'm worried about what happens when I lose power for
2 example, in the old design if I lost power I would get
3 a signal from that one division for which I lost
4 power. If it's now an energize to actuate, I don't
5 get that signal. So I'm struggling to understand what
6 that change actually is now, and even more so.
7 MR. DITTMAN: Maybe we can get some
8 clarification.
9 MEMBER STETKAR: Do we have anybody was
10 involved in that.
11 MR. MURRAY: We will get somebody --
12 MEMBER STETKAR: Okay, take it away for
13 this afternoon. Maybe I can bring up another one
14 here.
15 MR. DITTMAN: Let me make sure I can say
16 it correctly.
17 MEMBER STETKAR: Yes, because the
18 description seems to talk about the interfacing relays
19 if you look at the drawing.
20 MR. DITTMAN: I may have been incorrect
21 in clarifying that.
22 MEMBER STETKAR: The reason I was
23 assuming that the solenoids themselves were
24 deenergized even in the original DCD is every BWR I've
25 seen is alternate rod insertion, is an energized to

1 actuate.

2 MR. DITTMAN: It's an energize to

3 actuate.

4 MEMBER STETKAR: To energize the

5 solenoids themselves.

6 MR. DITTMAN: To dump their header on.

7 MEMBER STETKAR: That's right.

8 On - here is a simple one, I hope, and

9 this one is STD departure 7.2-6. And it's simply a

10 change in the instrumentation range for dry wall high

11 pressure instrumentation, and the original DCD had a

12 range of zero to 0.036 mega-pascals gauge, and for

13 those of us who think in psig, that is zero to 5.22

14 psig. The change revises that range from 15.0 to 30.0

15 kilo-pascals gauge, which for those of us who think in

16 psig is 2.18 to 4.35 psig.

17 The ABWR drywell is normally inerted, so

18 it's normally at some pressure. Is there safety

19 related instrumentation now that extends the pressure

20 range available for display to the operators down to

21 zero kilo-pascals or zero psig? In other words there

22 used to be instrumentation that at least displayed

23 pressure down to zero. That is important to me as an

24 operator if I've got inerted containment that is

25 normally pressurized to know whether I have leaks or

1 things like that. I'd like to really know if I have
2 positive pressure in that containment during normal
3 operations, a lot of other issues.
4 MR. MURRAY: Cal, can you help us with
5 that? You don't know the answer. Okay.
6 MEMBER STETKAR: So better take that.
7 The question is, do I have safety? Since I have
8 changed the range on the safety-related drywell
9 pressure instrumentation that feeds into my protection
10 logic, do I still have some type of safety-related
11 instrumentation that provides indication to the
12 operator down to zero pressure?
13 MR. MURRAY: I understand the question.
14 MEMBER STETKAR: The third one I had, and
15 this one is STD Departure 7.3-9, and it has to do with
16 shutdown cooling operation. This one I may not have
17 fully understood the change. So you will have to help
18 me on this.
19 As I understand it the original design had
20 - let me set the stage first for context. Talking
21 about signals to close the shutdown cooling suction
22 valves, shutdown cooling suction valves being the
23 suction from the reactor coolant system to the RHR,
24 some normal RHR cooling suction valves. As I
25 understand it the original design had a signal to

1 close those valves on level three, and it's been
2 retained, and it, I think, had a confirmatory signal
3 to close those valves on Level 1, Level 1 being the
4 safety related signal that starts low pressure
5 injection of low pressure coolant.
6 The change seems to have removed the Level
7 1 confirmatory signal. Is that correct?
8 MR. DITTMAN: I don't know if I would say
9 it was confirmatory. The change was essentially a
10 signal from Level 3 that shut down cooling isolation
11 valves, and the Level 1 signal was just redundant to
12 that. It tried to shut valves already shut, so they
13 removed that.
14 MEMBER STETKAR: Called a confirmatory or
15 redundant. But there was a Level 1 signal?
16 MR. DITTMAN: Yes, it was, but they
17 removed it because --
18 MEMBER STETKAR: In the current design if
19 that Level 3 signal fails will I ever get low pressure
20 injection? When level gets to Level 1? I would have
21 in the old design. If the valve for some reason
22 hadn't closed under the Level 3 signal.
23 MR. DITTMAN: If you weren't isolating
24 all three, it would be important if more than one
25 train failed.

1 MEMBER STETKAR: That is correct. My
2 point is a designer at one time installed that Level 1
3 signal as a confirmatory backup because the designer
4 apparently thought that it was really important to
5 have low pressure injection available even if the
6 Level 3 signal failed as a backup. A decision was
7 made for whatever reason to remove that, and I'm
8 curious about what is the rationale for that decision.
9 It's a change. It was a multi-division Level 3 safety
10 related signal in the old design. A decision has been
11 made to remove that.
12 MR. MURRAY: That should be documented in
13 our departure report. We just don't have it --
14 MEMBER STETKAR: Yes, I couldn't find -
15 it's not documented. The departure report only says
16 what you said, that the valve should already be closed
17 from Level 3, but it should have been closed from
18 Level 3 in the original design.
19 And one more just as an example. And this
20 one I literally ran out of gas last night, so - this
21 one is 7.3-13 is the departure and it's on the
22 containment spray logic. Is - I got confused and I
23 didn't have enough time to try to trace everything
24 back - is drywall spray automatically initiated under
25 any conditions in the current design?

1 MR. MURRAY: The answer is no.
2 MEMBER STETKAR: No? Was it in the
3 previous design?
4 MR. MURRAY: No. Cal, can you help us
5 with that? The answer is no, the previous design and
6 current design.
7 MEMBER STETKAR: Fine. As I said, I ran
8 out of gas, and there were words about manual and
9 automatic. Thanks.
10 MR. MURRAY: The original certification.
11 MEMBER STETKAR: It was just clarifying
12 that there is a manual override that has been changed
13 a little bit.
14 MR. MURRAY: Yes, there was clarification
15 of that. The override.
16 MEMBER STETKAR: This was more just a
17 point of information, because I literally didn't have
18 enough time to trace it. Those are enough examples.
19 Thanks for bearing with me.
20 MR. MURRAY: We've got some follow up
21 with you. We've got do we have a safety related
22 instrument that resends zero pressure in the drywell,
23 and also some more discussion on the normal energized,
24 normally deenergized on the contacts for the ARI
25 circuit as well as the discussion more on the Level 1

1 shutdown cooling.

2 MEMBER STETKAR: If we have more time

3 later this afternoon I have more examples, but I don't

4 want to bog down the - those are the top three or four

5 that I came across.

6 CHAIR ABDEL_KHALIK: Please continue.

7 MR. MURRAY: Slide 14, please.

8 These are the COL licensing information

9 items, cooling temperature profiles for the 1E digital

10 equipment. We've got that addressed in ITAAC table

11 3.4 item 14Braveo. APRM oscillation monitor, we've

12 included it in Section 7.2 The effects of station

13 blackout on the heating, ventilation and air

14 conditioning, we've got commitment tracking there, we

15 will do an analysis on temperature rises.

16 Electrostatic discharge, exposure of equipment and

17 components, that's addressed by ITAAC 3.4, item 12,

18 and that's also included in our EMC plan.

19 Localized heat spots in semiconductor

20 materials for computing, that is addressed by

21 commitment 7.8. We will do that with purchase order

22 information as well some where appropriate will have

23 continuous monitoring of equipment for that, and we'll

24 be doing testing during all the factory tests.

25 MEMBER BROWN: I didn't understand that

1 too much. Are you literally talking about a chip
2 heat, or are you talking about the physical location,
3 and it's located in a high heat area?
4 MR. MURRAY: Ed is our subject matter
5 expert somewhat on that. I think it is more localized
6 heating in areas, chips in areas of the panel.
7 MEMBER SIEBER: Like for a CPU.
8 MEMBER BROWN: I understand CPUs, but all
9 the stuff is fan cooled anyway, isn't it?
10 MR. MURRAY: Not all is fan cooled, no,
11 sir. Some equipment is fan cooled, some is natural
12 convection.
13 MEMBER BROWN: That was one of my
14 questions that I hadn't gotten to yet.
15 MR. MURRAY: ELCS equipment is fan
16 cooled, is that correct, E d? And the FPGA is
17 convection cooled.
18 Are we answering your question there, or
19 are there still questions?
20 MEMBER BROWN: Let me rephrase it. With
21 all microprocessors as well as FPGAs, the more dense
22 they get the hotter they operate. Is that the issue
23 you are trying to address or evaluate in this
24 application.
25 MR. MURRAY: Ed, can you help us?

1 MR. BROWN: Ed Brown from Westinghouse.
2 Let me make one other clarification: typically the
3 desire is, the harder you drive them functionally,
4 they will also, there is a range of frequencies at
5 which your clocks can operate. The higher, you get
6 more data throughput, more bandwidth, all that good
7 stuff, but the harder you push them the hotter they
8 operate. So there is normally a design to push it
9 down as low as you can and still meet the overall
10 requirements.
11 MEMBER BROWN: Now I'll let you try to
12 answer my kind of obvious question.
13 MR. BROWN: Okay, Ed Brown, Westinghouse.
14 The original DCD had commitments to calculate
15 temperature rises because the equipment had not been
16 designed or built yet. This section now has
17 descriptions of the type of cooling used for the
18 systems because, for example, for ELCS, it's a well
19 proven platform, heat dissipation is known, the clock
20 speeds are known. The area of interest is the heat
21 profile in the capsule added to find the ambient
22 temperature. So what we've done for the ELCS for
23 example is to find the external ambient consistent
24 with the Chapter 3 analysis of the ambient condition
25 of the drums. Then we allow for a designed

1 temperature rise, which we then confirm during
2 qualification testing, and they are in factory
3 acceptance testing.
4 Because we are using forced air
5 convection, we have added a temperature --
6 MEMBER BROWN: You just used a magic
7 word. He said one is convection, the other one is fan
8 cooled. I mean obviously forced cooling is
9 convection.
10 MR. BROWN: Right.
11 MEMBER BROWN: I think one is non-fan
12 cooled convection.
13 CHAIR ABDEL_KHALIK: Natural convection.
14 MEMBER BROWN: Natural convection.
15 MR. MURRAY: That is the term.
16 MEMBER BROWN: Okay, so the FPGAs, the
17 LPS is going to be just natural convection. And the
18 other ones are the forced convection.
19 MR. MURRAY: Forced convection.
20 MR. BROWN: Forced convection. And
21 because they are forced convection, we thought it
22 prudent to add a temperature monitoring device in each
23 cabinet that would monitor local temperature and
24 provide an alarm in case there was a rise that was
25 unexpected, which could be indicative of a forced

1 cooling problem. And that is a commitment - that
2 commitment we are tracking there is to do those things
3 provide those tests.
4 MEMBER SIEBER: And that is permanently
5 installed?
6 MR. BROWN: Permanently installed, yes.
7 MEMBER SIEBER: Well alarmed.
8 MR. BROWN: Well alarmed.
9 MEMBER SIEBER: What is the operator
10 supposed to do?
11 MR. BROWN: Well, he would send -
12 dispatch a technician to find out -- he would go down
13 and probably fix the failed alarm.
14 MR. MURRAY: That would be an alarm
15 response procedure, and it would have the verification
16 and notifications and responses required for that
17 alarm. And being an engineer I would get the call.
18 MEMBER BROWN: Is this going to be in
19 both the natural and the forced convection design?
20 MR. BROWN: No, it's in the forced
21 convection.
22 MEMBER BROWN: It's only the forced?
23 MR. BROWN: The original DCD did not have
24 that in because it was originally all convection
25 cooled. So when we changed the ELCS to forced

1 cooling, we added the temperature diagnostic.

2 MEMBER BROWN: As opposed to putting just

3 two fans in?

4 MR. BROWN: There is more than one fan.

5 MEMBER BROWN: There is more than one

6 fan? They all blow in the same direction?

7 MR. BROWN: Yes.

8 MEMBER BROWN: So they are there to

9 assist each other?

10 MR. BROWN: Yes.

11 MEMBER BROWN: That leads to the next

12 question: do you detect loss of a fan? In other

13 words, are they supposed to work okay with just one

14 fan in place, but you have two?

15 MR. BROWN: If there is the loss of a

16 fan, we are not monitoring the fan itself.

17 MEMBER BROWN: Just the temperature?

18 MR. BROWN: Just the temperature in the

19 cabinet, which is really the critical issue. Because

20 it could also change due to unexpected ambient

21 temperature rises due to failed cooling devices

22 externally.

23 MEMBER BROWN: Okay.

24 MR. BROWN: So we set that limit below,

25 well below, our qualification temperature limit so

1 that there is a warning.

2 MEMBER BROWN: Okay. Glad I asked the

3 question though. Thank you.

4 MR. MURRAY: Any other questions in that

5 area?

6 MEMBER SIEBER: It makes you feel better.

7 MEMBER BROWN: It makes me feel better.

8 MR. MURRAY: Okay, any other questions on

9 slide 14.

10 Go to slide 15. Supplement sections

11 continued in 7.1Sierra instrument controls. What we

12 found in this area, and the staff also addressed this

13 in REI 07-06 was that the Tier 2 should define well

14 what is supplied in Tier 1, and the detail that -

15 there wasn't as much detail as was necessary to

16 support the Tier 1 function. So we added this

17 section, 7.1Sierra to provide that detail of the

18 implementing platforms to support Tier 1. And we did

19 that for the reactor trip isolation system as well as

20 the safety-related neutron monitoring system. And we

21 also explained that we would be implementing the -

22 using non-rewritable Field Programmable Gate Arrays

23 for the neutron monitoring system and reactor trip

24 isolation system.

25 MEMBER BROWN: Now the RAI that you

1 answered provided the additional, another two or three
2 pages over and above the two pages of very high level
3 information in the original.
4 MR. MURRAY: That is correct, put more
5 detail into the supporting information.
6 MEMBER BROWN: It would have been helpful
7 if you had more drawings with more definition, because
8 a thousand words don't integrate well. It's still
9 hard to understand what is going on.
10 MEMBER STETKAR: Can I ask a question?
11 MR. MURRAY: On Slide 15?
12 MEMBER STETKAR: Finish 7.1 Sierra and
13 then I'll ask a question.
14 MR. MURRAY: On 7.1Sierra, slide 16, we
15 also clarified the - more additional information yet
16 on the engineered safety features logic system, ELCS,
17 provided - we provided the automatic actuation manual
18 control operator interface descriptions, and that also
19 explained that it provided the displays on safety
20 related information on the other platforms. For
21 example the reactor trip and instrumentation system
22 and the neutron monitoring system, the operator -
23 operations information was needed to support safety
24 related indications goes up through the ELCS system
25 and uses the display drivers there, division to

1 division, not across divisions, and provides that
2 information to the operators in the control room. And
3 that system we explained was implemented in a
4 microprocessor-based control system.
5 Any questions on slide 16?
6 MEMBER STETKAR: Yes, let me stop here.
7 It's not particularly on slide 16, but part of the
8 additional information in that section, it's under
9 ELCS, discusses a maintenance and test panel, MTP.
10 Could you - it's described simply as the maintenance
11 and test panel will be used for technician
12 surveillance, maintenance and test functions for each
13 division. The MTP provides the means for operator or
14 technician to change setpoints and certain remove
15 bypasses for periodic testing and display detailed
16 system diagnostic messages. It also notes that the
17 MTP communication interface to the nonsafety systems
18 provides for communication isolation to assure that
19 data flows in a unidirectional manner from the ELCS to
20 the nonsafety systems. Could you explain a little
21 bit more what these MTPs are? It sounds - I first
22 thought that they were some type of standby panel
23 where people could perform testing and diagnostics and
24 make changes to software and things like that, but it
25 sounds like they are an actual online functioning

1 system if they are porting the communications from the
2 safety related to unsafety related parts of the
3 instrumentation.
4 MR. MURRAY: That is one of the
5 functions. That is located - Ed, again, can answer in
6 great detail. The way you've got it pictured is
7 correct. There are multiple functions for that
8 particular panel, but the isolation also in that panel
9 performs that isolation and communication safety, one
10 way, to nonsafety, to be able to utilize the
11 information out of the system. Ed, give us more.
12 MEMBER BROWN: Before he answers that,
13 can I expand just a bit? Because when I read the
14 stuff between the plant data network I thought - and I
15 guess I didn't understand this well either until he
16 asked the question - I had presumed that this was
17 literally allowing the operator to see what somebody
18 was doing at the maintenance test panel as opposed to
19 the normal operational data that was sent,
20 unidirectional, out to the consoles or other
21 operational stations. So if you can answer that
22 question in that context.
23 MR. BROWN: Yes, let me describe the
24 general - my name is Ed Brown from Westinghouse. Let
25 me describe the general functions of the maintenance

1 and test panel. The system is centered on basically
2 it is not involved in the safety actuation functions
3 of the ELCS system. It is provided to support the
4 safety functions. It is a safety-related system, the
5 software safety rated, but it is not in the actuation
6 path, and it's failure would not prevention actuation.
7 It is continuously connected, a piece of equipment
8 that is fully qualified. Now the maintenance and test
9 panel, they are associated as two associated pieces of
10 computing equipment. One is called a node box, and
11 that node box has a display functionality for the
12 maintenance technician. That node box also contains
13 the interface card that allows us to speak to the
14 external nonsafety system. We have two communications
15 functions within ELCS, one is high speed serial link
16 system we will talk about later that is directly
17 supporting system actuation functions. We also have
18 an interdivision network which is totally contained
19 within the division that supports other safety
20 functions that are not directly associated with the
21 reactor trip functions.
22 MEMBER BROWN: You mean intradivision?
23 MR. BROWN: Within the division. Only
24 within the division.
25 MEMBER BROWN: Okay, intra not inter? I

1 just wanted to make sure I understood.

2 MR. BROWN: Now, the status information

3 and the diagnostic information is communicated on this

4 intra-division network to allow it to be collected and

5 displayed at the operator display stations in the main

6 control board and at the maintenance and technician

7 panel.

8 MEMBER BROWN: So it goes both places?

9 MR. BROWN: Both places. That allows the

10 technicians to see all the alarms, to basically look

11 and interrogate the system in a passive way. It also

12 collects the information that is desired to be passed

13 to the nonsafety related systems for further

14 processing.

15 MEMBER BROWN: Such as?

16 MR. BROWN: Such as process values and

17 the nonsafety system will do like a multiple division

18 comparison. The nonsafety system will do things like

19 bypass an inoperable status calculations, so the more

20 complex calculations, especially things that you want

21 to see done between divisions, are done in the process

22 computer system. And that way the design is

23 simplified. It minimizes the amount of interdivision

24 data that is sent within a safety system. So each

25 division has this MTP system, and it performs this

1 function of collecting the plant data from this
2 intradivision network, then buffers it, and then
3 transmits it out through a separate card,
4 unidirectionally, to the plant information control
5 system, so that it's available for nonsafety
6 processing. It's a design subject to buffering that
7 it cannot receive data cross this fiber optic link,
8 and it cannot be used as anything other than data; it
9 cannot receive instructions and things of this nature.
10 So it performs that buffering.
11 It also performs the functions that allow
12 the operator - the operation staff to change
13 setpoints. This requires that we have switch
14 interlocks that are required and the support of
15 administrative controls to access where these other
16 functions which are alarmed in the operator's control
17 room. And there you can enter a setpoint. It will be
18 sent to the appropriate processor, and then it would
19 be reported back to the technician interface on the
20 MTP for confirmation.
21 MEMBER BROWN: When that's being done,
22 the control room operator knows it's being done.
23 MR. BROWN: Yes.
24 MEMBER BROWN: I think you said that.
25 MR. BROWN: Yes, the program operator

1 knows it's being done, and that division for - it has
2 to be a division of censored bypasses because we
3 cannot change setpoints with the system online. So it
4 must be bypassed for that operation.
5 MEMBER STETKAR: Are the bypasses enabled
6 also in the same panel?
7 MR. BROWN: No, for the ABWR, the
8 bypasses are controlled by hard switches in the
9 control room.
10 MEMBER STETKAR: Okay.
11 MR. BROWN: The standard bypasses. If it
12 were necessary to go through and do something
13 extraordinary similar to what would be a wire jumper,
14 you may be able to do that through the console
15 depending on the function. But that is not currently
16 a planned function for the ABWR.
17 MEMBER STETKAR: So if I'm hearing you
18 correctly, although this panel provides the facility
19 for people to input changes to setpoints, that
20 facility must be enabled through separate switches
21 that only exist in the control room? I'm worried
22 about whether faults in this panel can lead to
23 spurious input, changes to setpoints that nobody would
24 know about this.
25 MEMBER BROWN: Let me, can I amplify that

1 a little? My question to amplify, my understanding at
2 this point is, in order to do any of these you have to
3 manually engage a switch contact which allows access
4 to the operation of the protection system, or the ELCS
5 in this case, which we are talking about. Or is it
6 online and energizes a safety switch that says, okay,
7 start communicating in some way as opposed to a hard
8 open contact break. If it's not called out one way or
9 the other in either the DCD or the SER. Or at least I
10 didn't find it.
11 MR. BROWN: To change any configuration
12 which would be setpoints, the hard switch in the main
13 control room does division of sensors bypass. You
14 must bypass that division.
15 MEMBER BROWN: I understand the sensor
16 bypass part of that, but now you have got to connect
17 into the processor with whatever you are going to do
18 to change the setpoint in the software.
19 MR. BROWN: Right.
20 MEMBER BROWN: Is that continuously
21 connected and all you are doing is bypassing the
22 sensors, or is there another contact that now connects
23 the maintenance and test panel to that specific
24 division's process?
25 MR. BROWN: The maintenance and test

1 panel is always connected, but the functions to change
2 things are not enabled.
3 MEMBER BROWN: By what, a software block?
4 MR. BROWN: No, a hard switch that goes
5 into software.
6 MEMBER BROWN: So there is not - it does
7 not close that contact between the maintenance and
8 test panel and the division cabinets.
9 MR. BROWN: Right, but if you don't have
10 the division sensors bypass enabled you will not be
11 able to update that setpoint because it can tell that
12 that division is not bypassed.
13 MEMBER BROWN: I understand but the
14 processor is connected all the time. If you had a
15 software failure and started sending data, even if the
16 bypass switch is not enabling it, you've got a hard
17 connection, that's the way you phrased it.
18 MR. BROWN: Right.
19 MEMBER BROWN: So there is a data path.
20 And yes, I agree, if you got your pressure going up
21 and down or whatever it is you are trying to modify,
22 you are going to have a hard time doing it. Now I've
23 got a sensor feeding it and I've got the test panel
24 putting in data. Which one does it believe? What
25 kind of conflict do you get on the inputs? On the A

1 to D converters or whatever.

2 MR. BROWN: Let me go through a few more

3 steps. It takes multiple steps to change a setpoint.

4 So it would be very unlikely that software - software

5 doesn't really fail; it's either right or wrong. But

6 a hardware failure or software problem to initiate

7 setpoint change, because it takes multiple steps in

8 the computing device. But in any case if you

9 nonmechanistically proposed that single failure, and

10 yes, you could fail a portion of that division,

11 whatever setpoint we're changing. That's your one

12 failure. You then have the four other sensor

13 divisions, which are voted two out of three then.

14 MEMBER BROWN: No, I understand that, but

15 it's not clear that you would know that that had an

16 internal failure that started pumping data, so you

17 can't count that - you still have to consider another

18 failure.

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

20 MEMBER BROWN: I'm just gathering that,

21 it's not clear.

22 MR. BROWN: When we talk about the

23 communications later for this bus, we will discuss how

24 the communications work.

25 MEMBER BROWN: Okay, that's fine.

1 MR. MURRAY: And the sensor bypass
2 switch, by title, it actually bypasses the division,
3 does it not?
4 MR. BROWN: It bypasses the division.
5 MR. MURRAY: So it's not just the
6 sensors. I just - you were using a term, and I just
7 wanted to make sure we are clear on that, that said,
8 like the sensor was only being bypassed, and it
9 actually bypasses the division.
10 MEMBER BROWN: No, no, that's fine, I
11 understand that.
12 MR. MURRAY: Correct.
13 MEMBER BROWN: But if the switch doesn't
14 get turned, and you had this other internal failure
15 still permanently connected, you've got an output bus
16 connection indirectly, and you can't consider that the
17 single failure if you had an internal failure that is
18 not protected, because you are trying to force this
19 one channel. Now you have to - that channel may not
20 respond, and now you've got another - now I've got two
21 failures, after the single failure, there was an
22 incipient failure that is not detected.
23 MR. MURRAY: I understood that portion of
24 your question.
25 MEMBER CORRADINI: And it's not that -

1 you've operated that way for awhile.

2 MR. BROWN: We will speak to

3 detectibility in the communications section.

4 CHAIR ABDEL-KHALIK: Okay, let's continue

5 please.

6 MR. MURRAY: Okay, the interlock systems

7 important to safety, that is 7.6Sierra, these

8 sections, we added those sections to comply with Reg

9 Guide 1.206. And it refers to information already

10 provided, basically the information was already there,

11 we just made the pointers to it.

12 7.8 Sierra, diverse instrumentation and

13 control systems. A section was added to, again, meet

14 the requirements of 2.206, and the Section 7C.5 had

15 that subject material addressed, so it was again, it

16 was required that there was a pointer.

17 Then data communication systems, we will

18 also talk about these - we have a slide on the

19 diversity that we will talk about a little bit more

20 when we get into the technical discussions, more

21 detailed technical discussions. But on the data

22 communication systems, basically it describes both

23 essential and nonessential is what was there, and we

24 have corrected that for the data communications

25 function which was in our departures. And includes

1 data communication between systems and between
2 divisions within the systems. And we will have slides
3 that discuss that in more detail.
4 Any discussions?
5 (Pause)
6 MR. MURRAY: Mr. Chairman, we are getting
7 into a transition area where we are going into the
8 detailed discussions on what we discussed before, we
9 will get into communications. And with that I'll turn
10 this over to Kyle Dittman to lead that discussion.
11 MR. DITTMAN: My name is Kyle Dittman.
12 I'll give you some of my background. BSEE, been in the
13 nuclear industry for almost 22 years now. I started
14 at Clinton Power Station in 1988, was there 10 years,
15 I was what they called a managing employee, so I got
16 sent to a lot of different - maintenance, quality,
17 licensing. I became an STA, went on shift for five
18 years as a part of the operating crew, as a shift
19 technical adviser. And I came off shift five years
20 and went to system engineering, and then I switched,
21 or I actually changed and went up to Point Beach
22 Nuclear Power Plant, and I was at Point Beach for 10
23 years, and I started out there as an I&C and
24 electrical designer there. It was supposed to be just
25 I&C. I did that for many years, and I slowly evolved

1 into - became the I&C and electrical design supervisor
2 before I left. And just prior to leaving Point Beach
3 I was actually the project supervisor for different
4 projects, project designs. That is my background.
5 What you are seeing here is a Japanese
6 typical - or I shouldn't say that - it's a Japanese
7 ABWR main control room. This is what our control room
8 is going to be based on. We are upgrading it or
9 changing it based on the human factors engineering
10 that is being done. Also we are going to be
11 incorporating operating experience from the Japanese
12 ABWRs. We actually got feedback from the operators
13 and stuff, so we are using that.
14 Also numerous or several STP people had
15 gone over and had partaken in the simulator training
16 that is offered over in Japan, and had provided
17 feedback, so that type of feedback will be
18 incorporated in this design step.
19 MR. MURRAY: Kyle and I both have been
20 through the simulator training in Japan at the boiling
21 water training center; quite beneficial.
22 MEMBER ARMIJO: Is that a K-6, K-7, or
23 Hamaoka.
24 MR. DITTMAN: This is actually a Hamaoka
25 5 simulator is what you're seeing here.

1 MEMBER ARMIJO: That's the simulator?

2 MR. DITTMAN: Yes, this is actually their

3 simulator. There have been some upgrades on this. If

4 you would see like the K-6 simulator, the screen

5 layouts are a little different on the front panel, the

6 operating panel. It has split screens, and they did

7 upgrades to the Hamaoka design. The other thing that

8 we are incorporating in this is, also we are going to

9 incorporate technical advances like flat panel

10 displays and stuff like that, so there will be some

11 differences. But the basic layout is going to be

12 similar.

13 The original certified design used an

14 essential multiplexing system for RPS and ESF systems.

15 And ESF are essential safety functions which covers

16 ELCS, RTIS, stuff like that, is the original term for

17 the safety systems.

18 In three and four we are departing from

19 that type of communication to more of a clear division

20 of the safety functions. Specifically, RTS and ELCS

21 are going to be partially independent with their own

22 communication system. They are not going to have

23 that one common communication per division. This

24 simplification will help reduce the likelihood of the

25 common cause failures. So there are advantages to

1 that.

2 Also the RTIS and NMS is being implemented

3 by FPGA platform, and ELCS is being implemented by a

4 microprocessor-based platform, so this also reduces

5 the probability of common - common mode type failure.

6 We also tried - and the whole idea is the

7 simplification of these safety systems. So we also

8 kept the nonsafety functions off the safety system,

9 which Ed alluded to earlier, is like the bypass inop

10 status determination, alarm processing, logging

11 display, historian functions are going to be

12 maintained on the PICS which is plant information peer

13 system.

14 MEMBER BROWN: A data logging system, is

15 that what you mean that?

16 MR. DITTMAN: Yes, data logging system.

17 It's for long term history. We will be on PICS. And

18 PICS itself is a separate and diverse microprocessor

19 based platform from the safety systems, and PICS is

20 our primary operator interface for operating plant

21 normal operations.

22 Next slide, please.

23 MEMBER BROWN: Are you going to talk

24 about that a little bit more in terms of the PICS?

25 Are you going to talk about the PICS? You made the

1 magic word: is your primary plant operation function -
2 -
3 MR. DITTMAN: I don't have any slides to
4 talk about it more later, but if you want to talk
5 about it now.
6 MEMBER BROWN: It's a nonsafety system.
7 Therefore it is not necessarily redundant, so I'm
8 interested in the --
9 MR. DITTMAN: It's not redundant but it's
10 another diverse operating system --
11 MEMBER BROWN: I understand diverse just
12 means different stuff that is used in the boxes. Do
13 you have multiple stations which are independent
14 within the PICS, that if any particular station fails
15 the other ones - or is there a neck-down point when
16 all the communications, when the operator wants to do
17 something, has to go through one machine?
18 MR. MURRAY: Let me handle that. The
19 design of PICS is a redundantly based type computer
20 system. Each box, the boxes have redundancy. You
21 have one box, that the function is redundant. The
22 operator interface in the main panel, and you can see
23 in this picture here it shows the displays in the main
24 panel and there are some displays in the back, those
25 displays are set up such that if one fails you can go

1 for one right next to it and call up the same
2 functionality and perform the same functionality from
3 it. So we don't have where it's a direct control from
4 that one display.
5 MEMBER BROWN: Well, is PICS - something
6 has to feed the data out to all those displays. Do
7 they all have their own feed? Do they all have their
8 own little data processing computer that feeds each of
9 the different display stations?
10 MR. MURRAY: Chris, if you will, help us
11 with that. It's a distributed control system so it's
12 going to do the standard --
13 MEMBER BROWN: Is my question clear?
14 MR. CREFELD: Yes. My name is Chris
15 Crefeld, and I work for Westinghouse on the PICS
16 system. The PICS platform is the Ovation platform
17 which is Emerson technology, Emerson process
18 management. The controllers on PICS, it's a
19 distributed control system, the controllers are all
20 redundant. The network of PICS is also redundant.
21 And the work stations for certain critical
22 applications are also redundant. For operator
23 functions they are duplicated or multiple, as Kyle was
24 explaining. There's multiple operator work stations
25 in the main control room, and if one becomes disabled,

1 the same functions are duplicated on another work
2 station that the operator can access from they main
3 control.
4 MEMBER BROWN: I am trying to look at the
5 little picture down here with a couple of boxes. I
6 see things that are called DPU-1 and DPU-2 and DPU-N.
7 That means nonsafety based on the other little stuff
8 in there. Now DPU-1, is that identical to DPU-2
9 functionally and in all operations? Does it feed
10 certain stations?
11 MR. CREFELD: It's a security control
12 system, so any operator work station can access the
13 data from any of the controllers. So if you want to
14 be a redundant pair of controllers that have certain
15 plant functions assigned to them.
16 MEMBER BROWN: Okay, stop right there.
17 Do they send their data out on separate buses?
18 MR. CREFELD: No, they --
19 MEMBER BROWN: So they all dump into the
20 same bus?
21 MR. CREFELD: Correct.
22 MEMBER BROWN: So when a work station
23 accesses DPU-1, or 2, or N, he selects that, but all
24 the data is going through one what I would call a
25 local area network bus?

1 MR. CREFELD: One redundant bus, network.

2 MEMBER BROWN: Okay, by redundant you

3 mean there's two --

4 MR. CREFELD: Fully redundant in switches

5 and --

6 MEMBER BROWN: Okay, but do you access it

7 via - so you select the bus you go on?

8 I'm just trying to gain some understanding

9 based on the lack of definitive detail in the drawings

10 as to how you achieve the ability to not lose all of

11 the process and control data with one thing. You say

12 it's on the dual redundant bus, I guess that's what

13 you're calling it, I added a word, you said it was a

14 dual bus - what did you say?

15 MR. CREFELD: Fully redundant.

16 MEMBER BROWN: Fully redundant, and I'm

17 trying to make it clear that those buses are separate,

18 they run separate. Does somebody have to select the

19 bus.

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

21 MEMBER BROWN: So the bus decides whether

22 it's working or not and shifts to another bus? You

23 can't have data coming in - the same data coming in

24 two places and ask the station, the work station, to

25 figure out what you are getting. It's a decision

1 process somewhere.

2 MR. MURRAY: Tim, can you help explain

3 that, please?

4 MR. HURST: My name is Tim Hurst. I'm

5 with STP. The system is designed to be fully

6 redundant. From any point where you bring multiple

7 signals together. It generally starts at the control

8 processor, all the way through the network

9 communication, and then to the work stations. Each

10 device whether it be a control processor or a work

11 station or a server can see both networks at all

12 times. They can each look at and determine is there

13 proper communication on that network. Am I

14 communicating to the piece of equipment or finding the

15 piece of data that I need. If not it will immediately

16 go over and look at the other network for the data.

17 So having the system fully redundant gives us a very

18 high availability, and keeps all of the system - the

19 system once it comes up will never be shut down, both

20 in normal operation, refueling, it's designed to be

21 modified online; because it's an important system

22 throughout the plant life.

23 MEMBER BROWN: The word never is an

24 interesting word to use. All right, I guess I'll let

25 us go on here. It's not absolutely clear to me how

1 this is connected. I understand the word, redundancy.
2 It's a matter of a wiring diagram that shows that
3 redundancy in a manner that is understandable. Right
4 now it's just one line for everything.
5 MR. HURST: The diagram does not show the
6 redundancy. Every one of the lines you see on there
7 is redundant.
8 MEMBER BROWN: The DPU-1 has two
9 redundant lines going to every work station.
10 MR. HURST: Essentially it does. It's
11 not physical lines. You go into a network.
12 MEMBER BROWN: Okay, let's go on.
13 MEMBER ARMIJO: Well, Charlie, is that
14 level of detail available now in drawings?
15 MEMBER BROWN: No, it's not in here, at
16 least I didn't see it. This is even more than it's in
17 the SR or in the DCD. So it just raised the question
18 I looked at it. I couldn't get this out of reading
19 the PICS discussion.
20 MEMBER ARMIJO: I understand the thought
21 process. It sounds like Toshiba has got a lot more
22 information available here from the description, from
23 the design. I'm not quite sure, why don't we have
24 it?
25 MEMBER BROWN: The interesting point is

1 between RTIS, NMS and the ELCS. All these feed into
2 this common redundant bus also. So this bus has to be
3 a pretty robust bus, and all LAN buses when you start
4 dumping tons of information into them, you may or may
5 not - you've got to make sure you've got the bandwidth
6 for it. And if you run a bandwidth that gives you, I
7 don't know, call it deterministic, but it's not
8 because it's not on a LAN. You just don't know when
9 the information is going to get there, and in my
10 experience, we used to run stuff around one or two or
11 maybe maximum of about 5 percent of the bandwidth, and
12 for the most part, data packages don't run into each
13 other. There is no discussion of the bandwidth or how
14 far they loaded up in any of this discussion. It's
15 just, a dual redundant bus, and that's about it. So
16 it's just a concern about the nature of the bus, how
17 it's utilized, and there is nothing that addresses it
18 from an ITAAC or DAC standpoint, at least that I could
19 find. So to me that is kind of an open item to make
20 sure we got a clear picture of how all this data gets
21 to the operators in a manner that it doesn't get
22 conflicted.
23 That's all I can say.
24 CHAIR ABDEL-KHALIK: It's an open --
25 MEMBER BROWN: I would consider it open

1 right now to get some more information in terms of
2 how we make sure this redundant bus actually operates,
3 and to ensure the data gets there under some failure
4 modes, whatever runs the buses.
5 MR. TONACCI: This is Mark Tonacci. I
6 understand your questions well. What I don't quite
7 get is, where is the nexus to safety? Where is that
8 coming in?
9 MEMBER BROWN: Well, the operator has got
10 to control something, so I guess it's a good idea for
11 them to be able to get information.
12 MR. TONACCI: For economic benefit I
13 understand completely, but for safety is where I'm
14 coming from.
15 MEMBER BROWN: I guess I'm not supposed
16 to be concerned about the operators having information
17 available to them about what the plant looks like or
18 the control functions? That's a safety issue to me if
19 you don't know where the plant is.
20 MR. TONACCI: I wanted to make sure I
21 understood the nexus to safety or operation of the
22 plant.
23 MEMBER BROWN: Yes, operation of the
24 plant requires knowledge of what the parameters are.
25 If I'm off base - I thought displaying information was

1 important.

2 MR. TANEJA: One piece of information

3 that we are not paying attention to, each safety

4 division has two operator interface consoles which are

5 safety related and which are independent of PICS.

6 MEMBER BROWN: Nobody said that until

7 you just said it. It just goes into a big bus; that's

8 all it says.

9 MR. MURRAY: We are going to get there.

10 Okay let's do some clarification here.

11 MEMBER BROWN: That's fine, we can go on.

12 It just goes into a big bus, and they said they had a

13 dual redundant thing that goes into it.

14 MR. MURRAY: I'd like to do some

15 clarification then.

16 CHAIR ABDEL-KHALIK: Please continue.

17 MR. MURRAY: Let's do the clarification

18 on this particular - when we say it does go into the

19 plant data network into the bus, that is the signals

20 that are used for - these same signals, the same

21 equipment - or excuse me, statuses that are going into

22 that bus are available in the safety related

23 indications to the controller. In those displays that

24 Craig is pointing out there.

25 MEMBER BROWN: And they are on a separate

1 bus?

2 MR. MURRAY: They are on buses that are

3 safety related.

4 MEMBER BROWN: So it's independent on the

5 PICS bus?

6 MR. MURRAY: Absolutely.

7 MEMBER BROWN: Okay, why didn't you just

8 do that?

9 MR. MURRAY: We didn't understood the

10 question.

11 MEMBER BROWN: I thought I was asking the

12 question, but I didn't get there. I'm sorry. I'm

13 happy.

14 CHAIR ABDEL-KHALIK: Let's continue.

15 MR. MURRAY: And I think if we had gone

16 through the communication processes you would have

17 seen that. What I could have done is say this part is

18 nonsafety. And what we are going to discuss next is

19 RTIS and Internet safety section of the red bus in the

20 red box, and discuss communication. This stuff right

21 here is the PICS that we were just talking about on

22 the nonsafety bus, which supplies for the normal

23 operation of the plant, normal operator interface in

24 the plant. That's where I should have added on, the

25 safety interface to the plant comes up through these

1 dedicated one -- you know, there's dedicated for
2 division.
3 MEMBER BROWN: That's just the ELCS. The
4 RTIS goes into this --
5 MR. DITTMAN: We'll get into
6 communication in the next slide, and it does
7 communicate and I'll show you how that works.
8 For RTIS it uses - this is the high level
9 communication that RTIS uses - is RTS, NMS, they use
10 the dedicated data links, which are deterministic.
11 They are isolated electrically, and you use fiber
12 optic base way to do that. They are point to point,
13 and they use no handshaking.
14 MEMBER BROWN: Okay, but isolated
15 electrically does not equal deterministic.
16 MR. DITTMAN: That's right.
17 MEMBER BROWN: Okay, just wanted to make
18 sure.
19 MR. DITTMAN: They are deterministic,
20 yes, I understand that.
21 MEMBER BROWN: It also doesn't make them
22 independent.
23 MR. DITTMAN: I just wonder what your
24 question --
25 MEMBER BROWN: We'll get into that. I'm

1 just saying, if you are trying to send a message, that
2 makes them independent, it doesn't.
3 MR. DITTMAN: There are four types of
4 communication paths in RTIS, and we are going to go
5 RTIS, NMS and ELCS. The first is interdivisional,
6 which is between divisions. It's an optical serial
7 link to and from the other divisions. This is the two
8 on port voters. It's one way and no handshaking,
9 okay. This is - so this is the communication between
10 divisions, and we are pointing out where those go. So
11 it leaves the DTF, the digital trip functions, goes to
12 the other divisions. You can see the 2R4 voltage that
13 comes back into the implementing divisions for
14 reboarding.
15 MR. MURRAY: It should be noted only one
16 division is shown here.
17 MR. DITTMAN: Yes, this is only one
18 division. For intra-divisional internal to the
19 division RTIS communicates to ELCS so it can display
20 on those screens we were just talking about the status
21 from RTIS, so the operator will be able to see status
22 on safety-related screens for this division. So if
23 this is Div 1, the Div 1 ELCS screen will display the
24 status of RTIS. And that is - that data communication
25 is a serial link. It's optically isolated, it's one-

1 way no handshake.

2 MEMBER BROWN: This shows - that's

3 interesting - this shows an interface node box. Is

4 there an interface node box for every division?

5 MR. DITTMAN: That's correct. Every

6 division has an interface node box.

7 MEMBER BROWN: It depends on the ELCS

8 node box for the RTIS communication to the operator;

9 is that correct?

10 MR. DITTMAN: That is correct.

11 MEMBER BROWN: Okay, so RTIS - I want to

12 say this a different way - -RTIS and ELCS do not have

13 independent communications for their own systems to

14 the operators? They all - each division, each RTIS

15 division depends on a node box for each ELCS division.

16 Even Division 4, which does not - I think it's

17 Division 4 which is not performing --

18 MR. DITTMAN: There's no equipment,

19 actually, since we only did four equipment --

20 MEMBER BROWN: -- the SFAS function. It

21 doesn't do an SFAS function.

22 MR. DITTMAN: But it does, the RTIS 4 -

23 Div 4 communication through the node box to ELCS for

24 display on the panels.

25 MR. MURRAY: Within a division.

1 MR. DITTMAN: Within that division. So
2 each division has their own panels.
3 MEMBER BROWN: I am listening.
4 MR. DITTMAN: And there are actually two
5 safety-related panels, one in the front panel - this
6 was in the previous slide, but the front panel then
7 the back by the large panel display. So for each
8 division there are two separate safety-related
9 displays in the control room.
10 The next type of communication path is we
11 have safety to nonsafety, and this is where feeds to
12 our PICS or Plant Information Computer System, and
13 other places. But it's optical in a serial data link
14 to PICS is one-way no handshake. It's has the 1E and
15 non-1E isolation.
16 Then the last type of communication you
17 could have is nonsafety to safety. In this case there
18 is no nonsafety communication to the safety division
19 for RTIS. We don't have it.
20 Any other questions on this?
21 MEMBER BROWN: I'm not sure yet.
22 MR. DITTMAN: Okay, we'll go on to the
23 next slide.
24 MEMBER BROWN: I don't know what message
25 we had - I don't know whether we are there yet.

1 MR. MURRAY: By the time we are through
2 with these slides you will see the big picture.
3 MEMBER BROWN: I am giving you some
4 latitude here to finish these, and then I will ask my
5 questions.
6 MR. MURRAY: That I think that will be
7 perfect.
8 MR. DITTMAN: Okay, the next slide I
9 wanted to talk about is the same type of communication
10 but with NMS. In NMS there are again four types of
11 communication that we have: interdivisional which is
12 between divisions. In this case NMS does not
13 communicate between divisions. It feeds its trip
14 signals down to RTIS which does the interdivisional
15 communication for two out of four voting.
16 MEMBER BROWN: Let me backtrack to this
17 previous slide. Okay this is a picture still
18 basically high level.
19 MR. DITTMAN: Yes, it's a simplified
20 diagram for one division.
21 MEMBER BROWN: Very simplified.
22 MR. DITTMAN: Yes.
23 MEMBER BROWN: Okay, very simplified,
24 there are other issues that aren't identified in it.
25 I guess one of my questions is how does this

1 configuration get translated into design, since it's
2 not - the schematic, a pictorial of it, a block
3 diagram, is not displayed in either the original DCD,
4 it's not in the FSAR, the COL. Where does this
5 definition get kind of locked in in terms of what the
6 design is supposed to look like?
7 MEMBER SIEBER: That probably comes
8 first.
9 MEMBER BROWN: No, this is how they are
10 supposed to do the design. But it's not in --
11 MR. DITTMAN: This Figure 7.9S-1 is in
12 the COLA, and what that is, you can basically take --
13 MEMBER BROWN: That was in Chapter 7?
14 MR. DITTMAN: It's in 7.9S, this figure
15 is.
16 MEMBER BROWN: Not that one, I'm talking
17 about this one.
18 MR. DITTMAN: That is basically taking
19 the RTIS portion of this figure, and we added a little
20 more detail for discussion purposes in this meeting.
21 MEMBER BROWN: You said it's in 7.9S?
22 MR. DITTMAN: This, the one that's
23 presented right now is in 7.9S.
24 MR. SWANNER: This figure is slightly
25 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

1 better picture of what four divisions look like.

2 MR. DITTMAN: That was the purpose of

3 this was to try to break this up for discussion.

4 MEMBER BROWN: I'm just trying to say how

5 does that get reflected - how do you end up with this

6 in the end, that is part of the design, the DAC

7 process, which is not very clear.

8 You can move on. I'm just haranguing you

9 right now.

10 MR. SWANNER: One other note just on

11 these figures, it does indicate like for safety to

12 non-safety on this one figure, it is in green, so

13 these green arrows, unfortunately it appears the way

14 this got converted to a PDF that shows almost a solid

15 line which would lead you to believe that it is

16 hardwired, but the description over here is actually

17 correct. It is an optical serial data link, so just

18 to make sure that that is not confusing anyone.

19 MEMBER BROWN: Well, the printout shows

20 it's dotted.

21 MR. SWANNER: That's good.

22 MR. DITTMAN: That's just the way of

23 projecting here.

24 MR. SWANNER: The projection is maybe not

25 fine enough, I don't know, but I just wanted to make

1 sure there was no confusion.

2 MEMBER STETKAR: The colors are a lot

3 more vivid in your display.

4 (Simultaneous speaking.)

5 MR. SWANNER: I understand.

6 MR. DITTMAN: Okay, NMS. That's back

7 here where I left off. I did intradivisional

8 internal, again NMS has a serial data link to ELCS

9 which is, again, one-way no handshaking, and it

10 supplies information to the panels in that division.

11 The next type of path is the safety to

12 nonsafety. Again this leads mainly to PICS, and it's

13 again optical serial, it's one-way, no handshaking,

14 make sure we have the 1E to non-1E isolation.

15 And the last type is a nonsafety to

16 safety. We do have one very specific nonsafety to

17 safety communication path which is purely used for

18 calibration functions of the ELCS LPRMS with the gain

19 adjustment factors. And if you would go to the next

20 slide.

21 MEMBER BROWN: What is MVS? In slide 22.

22 Oh, got it.

23 MR. DITTMAN: It's the instrumentation.

24 Okay, this specific path, communication

25 path, is a method to provide the off-the-line

1 calibration activities that allow to transmit
2 calibration PICS. Basically this is the same path or
3 same calibration as the existing BWRs did, where they
4 will run the TIPS system, get the information, it
5 would be verified, and they would manually input it
6 into the ELCS LPRMS to do the gain adjustment factors.
7 This system is going to have the
8 capability through use of a key lock switch, because
9 normally now when this division is operational the key
10 lock switch blocks this through contact.
11 MEMBER BROWN: The calibration function?
12 MR. DITTMAN: This calibration function.
13 MEMBER BROWN: It's in a separate
14 cabinet?
15 MR. DITTMAN: Well, it's --
16 MEMBER BROWN: Separate set of hardware?
17 Say that again, I'm sorry I interrupted
18 you.
19 MR. DITTMAN: The key lock switch is with
20 the EPRM cabinet, EPRM equipment. So it's in that
21 cabinet, so it blocks that signal coming into the
22 APRs.
23 And the process that - there is a basic
24 process that would be followed for this is, the
25 division that you would be doing the calibration on

1 you would put it in bypass, and then the next step you
2 would take the key lock switch to enable, which would
3 connect this communication path, and then the dataset
4 that comes down is limited, and it's predefined, I
5 mean it's very specific, this dataset, and it's
6 accepted by NMS. And prior to returning that division
7 to service, there is manual verification and
8 acceptance at each LPRM of this data that - this
9 calibration data, this gain adjustment, for each LPRMS
10 its own gain adjustment factor, and it will be
11 verified before we return. Each one will be verified
12 for the whole division before we return it to service.
13 Any questions on this?
14 (No response)
15 MR. DITTMAN: Okay, then the next system
16 I want to discuss is the communication path through
17 the ELCS system, which is our ESF system. ELCS - and
18 Ed Brown commented on this. There are two types of --
19 MEMBER BROWN: Are you every going to
20 talk about the communication systems for the RTIs, or
21 is it just because it's FPGA it's assumed to be okay?
22 MR. DITTMAN: It's FPGA, and it's all
23 these dedicated serial data lines between all the
24 modules. Could we back up a slide? Here. Every one
25 of the communications between each module is a serial

1 link between each module.

2 MEMBER BROWN: I'm not worried about the

3 - what's in the intradivisional, it's the

4 interdivisional communications.

5 MR. DITTMAN: Okay, between the

6 divisions.

7 MEMBER BROWN: Yes.

8 MR. DITTMAN: Okay, it's the same type of

9 single link to digital trip function, we send that

10 information over to the other division for it to do

11 two-out-of-four. So like here the other division will

12 bring the two-out-of-four in from the other division

13 and do a two-out-of-four.

14 MEMBER BROWN: Is it a continuous signal?

15 MR. DITTMAN: It would be data packets.

16 Serial data link has data packets. Actually let's get

17 Akira to help discuss this with you.

18 MR. FUKUMOTO: I am Akira Fukumoto. I am

19 (Unintelligible) Eastern Nuclear (Unintelligible).

20 And I have 20 years experience for developing of I&C

21 systems in Japan. And let me ask you to repeat your

22 question. You are asking is --

23 MEMBER BROWN: I'm trying to - let me

24 state it again or try to. This is for the RTIS. I

25 realize it's FPGA but you are going from the data trip

1 function, and I understand it's burned in, hard logic,
2 it's like combinational logic, take little circuits
3 and you make - it's like take a hardwired computer as
4 opposed to software controlled, but you still have to
5 send data of some sort from division to division to
6 accomplish the trip function. So when is that a - I
7 already got one answer, it's a serial data link so
8 that means there is a continuous set of data packets
9 going over, and it's going into a preprogrammed logic,
10 the TLS, in each of the divisions, and then that data
11 is taken and it's voted on, and it's a hardwired
12 voting logic. But - and I'm not an FPGA expert - but
13 the point being, and I'll bring this up again with the
14 ELCS system because it's different - when you send
15 that serial data in you've got four channels. You've
16 got you own channel feeding in, you've got three other
17 channels feeding in, and that logic has to be
18 processed. So you've got the data packets coming in,
19 and if you get a corrupt data packet, okay, then it
20 goes into the voting logic, this is my understanding
21 of how you would do this, and little AND and OR case,
22 okay, which may be wrong. And in that configuration
23 when it's one single unit of little voting units or
24 voting logic, one set of data can come in and you can
25 possibly corrupt all three; the other three coming in.

1 So what I'm trying to figure out is can a
2 corrupt data packet, okay, and now I'm not trying to
3 deal with parity checks, checksums, or cyclic
4 redundancy checks or anything of that nature. All
5 that those do is say, the data that leaves the DTF is
6 the same as the data that arrives at the TLF. It
7 doesn't say it's good data. It doesn't say it's not
8 data that can't compromise the entire voting logic.
9 And on a microprocessor based system with an algorithm
10 it very clearly can do that, in an FPGA system, I'm
11 trying to wrap my head around, because it is a
12 hardwired logic function, how you prevent one set of
13 corrupt data packets from compromising every division,
14 two out of four data configuration.
15 MR. FUKUMOTO: I do have some questions
16 because I have some communication problems.
17 MEMBER BROWN: I speak too fast.
18 MR. FUKUMOTO: How do we avoid the data
19 corruption?
20 MEMBER BROWN: Yes.
21 MR. FUKUMOTO: Between the --
22 MEMBER BROWN: Well, no, not prevent it.
23 I'm assuming corrupt data arrives - in other words,
24 the DTF for some reason, don't ask me why, it just
25 happens, it says, here is a data packet, I'm going to

1 send it, it's corrupt. It generates a checksum, a
2 cyclic redundancy check, parity, whatever you use for
3 that, it gets transmitted, it arrives at the other
4 place, still the same, didn't get changed; it's still
5 the same old crummy corrupt data packet. So it gets
6 passed on through to the voting logic section. And my
7 point being is, in the FPGA system can that corrupt
8 data packet compromise the voting logic - because it
9 goes to all four divisions, it goes to all three of
10 the other divisions, so it can disable its own and it
11 can disable all three of the others, and what I'm
12 looking for is, can it, number one, because of the
13 logic configuration of the chips, so I was hoping
14 somebody could show me that, and if the answer is yes,
15 have you taken some action to prevent that. I'm not
16 sure what it would be, but that is my concern with the
17 serial data issue. It's a different issue - it's the
18 same issue in the ELCS system where it's obvious you
19 can corrupt and block up every one of them. But in
20 this one, in the FPGA system, it's not. So I didn't
21 understand that. I couldn't get it out of here when
22 it talks about compromise of independence. Because it
23 only said, number one, I'm isolated, and I can do
24 parity checks or keep alive checks, that just says the
25 line is open, or cyclic redundancy as it checks, et

1 cetera. So that was my question.

2 MEMBER SIEBER: It sounds like you want

3 to know how do you detect?

4 MEMBER BROWN: No, I want to know if the

5 data packet arrives and it goes into the voting logic,

6 can it corrupt and stop the voting logic in the

7 division from operating?

8 CHAIR ABDEL-KHALIK: Let's give them a

9 chance to answer, please.

10 MR. FUKUMOTO: So first of all I have to

11 say we have some detection guidance, as you said. We

12 can (Unintelligible) in (Unintelligible) is located in

13 (Unintelligible), it's in the logic card. So that

14 detects some data coming, or realize --

15 MEMBER BROWN: That's a different issue.

16 MR. FUKUMOTO: So first are you talking

17 about here if the transmitter send across data to the

18 receiver and it goes through all three divisions --

19 MEMBER BROWN: It will, yes.

20 MR. FUKUMOTO: -- and in that case, how

21 can we handle, how do you detect --

22 MEMBER BROWN: Will it corrupt the voting

23 logic in each other division?

24 MR. FUKUMOTO: That will not corrupt --

25 MEMBER BROWN: Now why?

1 MR. FUKUMOTO: You know, what do you
2 request? The logic?
3 MEMBER BROWN: To stop the voting logic
4 from operating.
5 MR. FUKUMOTO: Okay.
6 MR. MURRAY: Akira, what we need to
7 explain is what we discussed yesterday is that if a
8 failed signal or a corrupted or bad signal, came in to
9 the reactor equipment isolation signal, we know that
10 it comes in, can that affect its ability to see the
11 other three divisions and perform its function? And
12 that's what - that and some data swap, and we
13 discussed that yesterday. Just go through how that
14 communication works and how it's sensed --
15 MR. DITTMAN: How do we ensure that the
16 data that comes across can't be interpreted as a
17 command that can cause the two-out-of-four vote to do
18 something bad?
19 MEMBER BROWN: To lock up, not transmit a
20 trip.
21 MR. DITTMAN: How do we prevent that?
22 MR. FUKUMOTO: The logic FPGA in the
23 transmission and receiving LPGA works synchronously
24 with, independent of the clock. So it's synchronous.
25 MEMBER BROWN: I understand it's a

1 synchronous.

2 MR. FUKUMOTO: And so if you have a

3 corrupt data in Division 2, and the Division 2 looks

4 at that data, that data comes from Division 1,

5 Division 2 - 3 treat that transmission as Division 1.

6 MEMBER BROWN: How does it know it's

7 fatal?

8 MR. FUKUMOTO: You do a survey.

9 MR. SATO: Toshifumi Sato, 26 years

10 experience, and I have been (Unintelligible). So we

11 intentionally used the short length fixed format for

12 the transmission.

13 MEMBER BROWN: Fixed what?

14 MR. SATO: Fixed format, format.

15 MEMBER BROWN: Format? Okay, thank you.

16 MR. SATO: So we can detect the parity

17 error, (Unintelligible) error easily by - even by

18 their FPGAs.

19 MEMBER BROWN: All that does is say, the

20 parity checks, checksums, and all that, all that says

21 is that the data that got sent from the DTF and the

22 data received at the other end are identical. It

23 doesn't mean it's good; it doesn't mean it's bad; it

24 just says it's a packet of data. That's all it does.

25 The question is, does it - it sends the - the DTF

1 generates corrupt data. No good. It generates a
2 parity bit or a checksum, or a cyclic redundancy
3 check algorithm number. It sends it. The other side
4 duplicates that, says, oh it's fine, passes it on
5 through. It's going to have to because that is the
6 nature of parity checks, checksums, so all that does -
7 that doesn't tell anybody. Now that corrupt data
8 that doesn't represent reality, can that bad data
9 compromise the two-out-of-four voting logic once it
10 gets passed on in. That is the question?
11 MR. FUKUMOTO: As Sato-san says, we have
12 fixed deterministic data format in the serial bus
13 pipe. Any of it shows which division tripped, this
14 kind of thing. That serial data go into a hardwired
15 LPGA buffer in the (Unintelligible), so looking at
16 each function of (Unintelligible) and those kinds of
17 thing those are just ones and zeroes, binary data. So
18 just one-zero there is no --
19 MEMBER BROWN: Serial data is a one or a
20 zero. A series of ones and zeroes.
21 MR. FUKUMOTO: So one zero means a trip
22 or no trip or those kind of things, just a digital
23 communication. So you can see if one turns to the
24 other that should be corrupt data for one trip. But
25 in that case that data fed into the trip, that is

1 true. But in that case we saw to it, logic, trip that
2 data as a (Unintelligible).
3 MEMBER BROWN: Well, if it's a one or a
4 zero, that is just fine.
5 MR. FUKUMOTO: There is no volume data --
6 MEMBER BROWN: So there is no other
7 combination of data that gets transmitted. Therefore
8 when it goes in - each division feeds into its other
9 buffer? Or is it a common buffer for all divisions?
10 Which way? I gave you two points: one buffer for
11 every set of data coming in from each division or --
12 MR. FUKUMOTO: Each signal in a data
13 buffer.
14 MEMBER BROWN: Independent buffer within
15 each TLF? So each division's TLF has an independent
16 buffer for each set of data coming in?
17 MR. FUKUMOTO: That is correct.
18 MEMBER BROWN: And there are only two
19 states in which the data can be exhibited in this - in
20 the way you all are transmitting the data, as a one or
21 a zero?
22 MR. FUKUMOTO: Yes.
23 MEMBER BROWN: And then once it gets out
24 of the buffer it obviously goes into a series of
25 logic.

1 MR. FUKUMOTO: That is correct.

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

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

7 MEMBER ARMIJO: I had an easier
8 question.

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

24 MEMBER ARMIJO: My question was on your
25 safety calibration. When you input the new

1 calibration data and then you turn that division to
2 service, or at least for some period of time you get
3 two divisions operating, one with the old calibration
4 data, one with the new calibration, how do you handle
5 that?
6 MR. MURRAY: That is a technical
7 specification. Jay.
8 MR. PHELPS: Calibration frequencies.
9 MEMBER ARMIJO: You have to come up.
10 Do you immediately input the new data to
11 the other divisions?
12 MR. DITTMAN: Yes, typically in an IT in
13 the operating plant - I'll let Jay in a second - is
14 you build one division and then the next. You do one
15 and you build the next one. I'll let Jay.
16 MR. PHELPS: This is Jay Phelps, I'm the
17 operation manager on STP #3 and #4. The calibrations
18 that they are discussing are the frequency based
19 identified in the technical specifications. So as
20 they specify we will, go through and do a channel
21 calibration on the frequency identified, whatever the
22 parameter identified in the technical specifications,
23 and if a calibration is required in the case of the
24 maintenance test panel, that would be usually
25 setpoint, not being able to reach out to the actual

1 instrument that provided that input. But if a
2 setpoint required changes, that's how you do it, one
3 channel at a time, return it to service, just like we
4 do in the existing plants, if you go out and calibrate
5 an instrument in a division you will do one of those,
6 return it to service, do the next one, return it to
7 service, on whatever frequency is required.
8 MEMBER ARMIJO: My question is --
9 MR. DITTMAN: Can I restate your
10 question?
11 MEMBER ARMIJO: Do you understand my
12 question?
13 MR. DITTMAN: Can I restate it? You are
14 asking, I calibrated one, now I did two and did three
15 and did four, and calibrate, how do I account for that
16 they are now in a calibrated position that may have a
17 little different information on it --
18 MEMBER ARMIJO: The system has got two
19 sets of data for some period of time. I just wanted
20 to make sure you understood my question.
21 MR. DITTMAN: And you do gain adjustment
22 factors, and I'll go off my experience from operating
23 an ABWR, you go on the duties, gain adjustment
24 factors, for like Div 1. You are not going to be
25 doing huge changes to these gain adjustment factors.

1 This is minor. Changes to the gain due to the burn on
2 the detectors, the LPRM detectors. And it's done in a
3 frequency enough that the changes aren't huge. So
4 they did one, and once that is done and they are okay
5 with the calibration, and they bring it back into
6 service, there is not that much different than the
7 other divisions. Then you move on, you would do
8 again - all four divisions are driven by tech specs.
9 MEMBER ARMIJO: So you do them one right
10 after another?
11 MR. DITTMAN: One right - then you move
12 on to 2, and then you move on to 3, then 4.
13 MEMBER SIEBER: But things like
14 temperature and pressure you don't do it when you are
15 online because you have no way to vary the parameters.
16 MEMBER ARMIJO: No, I didn't say that.
17 MEMBER SIEBER: Like channel alpha q
18 block, you bypass with a key, it's a manual operator
19 action. Then you can get into the plant information
20 system to change setpoints or whatever it is you want
21 to do to check that and then return it to service by Q
22 block.
23 MR. MURRAY: We are talking hours, not
24 months. I think that is your question.
25 MEMBER ARMIJO: Yes, it just seems

1 confusing to have two sets of calibration data on
2 independent divisions. At some point -
3 (Simultaneous speaking.)
4 MEMBER STETKAR: The fact of the matter
5 is, we have that now. This is not different. We have
6 that now.
7 CHAIR ABDEL-KHALIK: Let's continue,
8 please.
9 MR. DITTMAN: Next slide, 26 I believe.
10 This talks about, Ed alluded to it
11 earlier, ELCS has two types of internal communication
12 which is the actuation communication.
13 MEMBER BROWN: Actually do you want me to
14 ask the other question on the FPGA system for the RTIS
15 before we get on to --
16 MR. DITTMAN: Yes.
17 MEMBER BROWN: Is that okay?
18 I guess my next question is, and again I
19 probably need help from you gentlemen, probably, you
20 got - the way I see this being hooked up, you have a
21 multiple set of FPGAs, you've got a set for the DTF
22 function, hard wired, you've got another set or
23 another FPGA for - I'm presuming this now, it's not
24 all in one - for the trip logic function. And then
25 I'm trying to remember the drawing or the block

1 diagram, I think out of the trip logic function that
2 is an analog style signal that goes to your load
3 drivers or something; is that correct? That's what I
4 got out of the major block diagram.
5 MR. FUKUMOTO: This is Akira. I need
6 help from Sakamoto-san. He is responsible for our
7 RTIS engineering. But from our view --
8 MEMBER BROWN: After the TLF.
9 MR. FUKUMOTO: That one discrete signal -
10 -
11 MEMBER BROWN: A discrete signal.
12 MR. FUKUMOTO: -- transmitted by fiber.
13 MEMBER BROWN: That's fine, and it goes
14 to OLU, which is an analog, but what is that, is that
15 another FPGA?
16 MR. FUKUMOTO: OLU, it's a hardwire, so
17 it's safe.
18 MEMBER BROWN: Okay, it's semiconductors
19 wired -- and tell me what the OLU.
20 MR. FUKUMOTO: Output Logic Unit.
21 MEMBER BROWN: Logic Unit, right. But
22 that -- you are now generating, that's -- you have
23 already generated a trip, haven't you? There is an
24 OLU in each division.
25 MR. FUKUMOTO: Yes.

1 MEMBER BROWN: But from the picture it
2 only showed the TLF from one division feeding the OLU
3 in one division.
4 MR. FUKUMOTO: Right.
5 MEMBER BROWN: And then the OLU, it looks
6 like all that does is convert your one or your zero
7 into a signal that drives the driver of some kind.
8 MR. FUKUMOTO: -- what is the contents of
9 your signal transmitted from OLU to the rod driver,
10 rod driver is not shown here, I think that is --
11 MEMBER BROWN: The OLU output is a state
12 -- I'm just trying to understand -- some type of a
13 state signal that triggers a driver. It can be
14 optically coupled. It's given enough power to drive
15 the actuator.
16 MR. FUKUMOTO: Yes.
17 MEMBER BROWN: Is that the output of an
18 OLU?
19 MR. FUKUMOTO: Can I translate? Sorry.
20 MEMBER BROWN: Go ahead, keep talking.
21 MR. FUKUMOTO: (Speaking in Japanese.)
22 Sorry. What you are saying is like, this is
23 transmitted, the state signal, the trip signal, from
24 OLU to rod driver. But the state is driven by
25 frequency, the light frequency.

1 MEMBER BROWN: Fiber optic.

2 MR. FUKUMOTO: Frequency is very short,

3 it's a zero --

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

5 MR. FUKUMOTO: One or zero.

6 MEMBER BROWN: From the OLU to the

7 driver.

8 MR. FUKUMOTO: To the rod driver.

9 MEMBER BROWN: Okay, there is a reason

10 for not using the TLF to do that?

11 MR. FUKUMOTO: We need some -- like a on-

12 off type of state. This is a frequency high or low.

13 So that's why we need to put it to --

14 MEMBER BROWN: Now that I understand that

15 I'll ask my question, okay. My question is relative

16 to the timing on the deterministic behavior. You make

17 the statement that this is deterministic. You've got

18 two FPGAs in series, each driven by a clock obviously

19 because that's how the data gets stepped through the

20 various logic gates. How --

21 MR. FUKUMOTO: You are talking about the

22 response-time issue?

23 MEMBER BROWN: Well, my issue is

24 deterministic performance of -- I mean I built from

25 LPGS systems back in my previous existence; it's been

1 15 years.

2 (Simultaneous speaking.)

3 MEMBER BROWN: It's been a long time

4 since I did some of these, and I've just forgotten the

5 details. My previous understanding is, it was

6 deterministic performance, but now I don't remember

7 what, with the FPGAs, and I thought because I had --

8 it was both predictable and repeatable. That is my

9 definition of deterministic behavior. And I'm trying

10 to understand now with the multiple sets of FPGAs how

11 do I get my timing such that I get both a predictable

12 and a repeatable performance. I did a little reading,

13 and my conclusion from the reading, which was not very

14 good, is that if you don't get the timing right

15 between FPGAs, when using them in series, that you may

16 not get the right results; in other words you get real

17 variability. Now am I correct with that?

18 MR. FUKUMOTO: Yes.

19 MEMBER BROWN: So my question is, how do

20 you make that happen in the right manner and such that

21 I can analyze and say the time response ought to be X,

22 and when I test it I will get an X plus or minus some

23 very small amount. How do you do that and keep it

24 fixed? They are both operating asynchronously.

25 MR. FUKUMOTO: Yes.

1 MEMBER BROWN: Okay.

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

7 MR. DITTMAN: Functional element.

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

20 MEMBER BROWN: Okay, I got that.

21 MR. FUKUMOTO: So based on that
22 knowledge, we assume the response time from the very
23 bottom to the top, assuming the maximum time response
24 to that. For example you can assume that two cycles
25 for a single response time. And each cycle is very

1 short, milliseconds' order.

2 MEMBER BROWN: Okay.

3 MR. FUKUMOTO: So --

4 MEMBER BROWN: Okay, so you got a clock

5 in each FPGA and they are asynchronous, and they will

6 vary. Do you account for the uncertainty, for the

7 variability of the clock, as it's operating? No

8 matter how good your clock the frequency is going to

9 vary somewhat.

10 MR. FUKUMOTO: Yes, yes, we assume that

11 but, again we verify that in the testing arena, our

12 testing and the variation test.

13 MEMBER BROWN: All right, thank you, I

14 appreciate that. That's fine, sorry.

15 CHAIR ABDEL-KHALIK: Okay, thank you,

16 let's continue, please.

17 MR. DITTMAN: Yes, thank you.

18 As we talked about a little bit earlier,

19 there are two types of communication in ELCS,

20 specifically internal. One is the first type of

21 communication is the actuation communication. It's

22 unidirectional point-to-point, serial link,

23 deterministic, isolated, and it's a dedicated single

24 function communication links between the logic and

25 final actuated component.

1 What I mean by that is, it works its way
2 through the logic. You got the transducer, goes to
3 the DTF, you get the digital trip function, which
4 trips all that, which then goes directly to the two-
5 out-of-four voter, and out of the two-out-of-four
6 voter it goes to the system level actuation. So it's
7 a very specific pathway for this communication.
8 This actuation communication is where the
9 actual, the manual initiation like a high pressure
10 core flood, and the auto initiation of a high pressure
11 core flood, is actually -- this is the pathway that
12 does that, okay.
13 Then there is the intra-division network,
14 which is the division communication. It's a bus
15 mastered network, and it is internal to each division.
16 It is deterministic, because you use a bus master type
17 setup. The thing is, a failure of this network will
18 not affect the actuation communication. The
19 actuation communication will continue to run if this
20 network goes down. The main purpose for this network
21 is to display the information to the operators on the
22 flat panel displays. It also is for if the operators
23 want to manipulate from the displays, they want to
24 manipulate like a valve or a starter pump, shutdown
25 pump, as communicated through this network. It also

1 communicates the diagnostic information for ELCS, and
2 it's connected to the maintenance panel for
3 maintenance test support. Next slide please.
4 Again, I'll go through the four types of
5 different communications for ELCS. For
6 interdivisional, and this is between divisions again,
7 it's again point to point, serial, deterministic, one-
8 way, no handshake.
9 Intra-divisional, we just covered that.
10 It's basically the two networks, so you got safety
11 actuation, and then the intra-divisional network
12 before getting to the displays, giving the displays
13 data, stuff like that.
14 Then the safety and nonsafety type of
15 communication is isolated, one way, no handshake, and
16 basically goes through PICS, okay.
17 And the last type of communication is
18 nonsafety to safety, and again in this case, in ELCS,
19 there is no case of that. We do not communicate from
20 nonsafety to safety in ELCS.
21 Any more questions?
22 MEMBER BROWN: It depends on how long you
23 want to spend.
24 MEMBER STETKAR: Let me ask a quick one
25 before Charley rolls out.

1 MEMBER BROWN: We'll be here until 2:00
2 o'clock.
3 MEMBER STETKAR: We'll hopefully get this
4 one done before lunch. This is just kind of a mundane
5 question. In the figure that you have there, you show
6 a DTF RDLC, that is characterized at least on this
7 display as an interface device with what is called ESF
8 inputs that feed into the DTF. Can you give me an
9 example of what those might be? I thought I
10 understood how the system worked in terms of
11 processing -- is -- oh, I'm sorry, I guess I'm reading
12 that wrong, is that my actual sensor inputs coming in
13 through that?
14 MR. DITTMAN: Correct.
15 MEMBER STETKAR: Okay, never mind. I
16 told you it was quick.
17 CHAIR ABDEL-KHALIK: My intent is to
18 break for lunch as close to 12:30 as possible. So if
19 there is a good point to stop at this time. Or if you
20 can finish. We can revisit those after lunch.
21 MEMBER BROWN: We can come back. I am
22 happy to go on.
23 MR. DITTMAN: Okay, we will go on to the
24 next slide, and come back to this.
25 The next area I'd like to discuss is

1 diversity and defense in depth, otherwise known as D3.
2 In our case we incorporate our D3 design by reference,
3 we did not depart from it. All the AWBR DCD diverse
4 features have been retained including, for example,
5 the manual reactor SCRAM, the manual switches, or the
6 switches, the high pressure core flood Charlie, the
7 diverse manual control, the diverse display and
8 specific process parameters that were in DCD were
9 retained, and the diverse hardwired controls, they go
10 directly to the components and bypass the digital
11 platforms.
12 Any questions?
13 MEMBER STETKAR: You say they go directly
14 to the components, that is directly to the circuit
15 breaker?
16 MR. DITTMAN: That is correct.
17 MEMBER STETKAR: Having not lived through
18 them, I'm just stalling for time here to wait for
19 Charlie, having not lived through the ABWR design
20 certification process, is there some reason why only
21 high pressure core flood Charlie, and I don't care
22 about the division of high pressure cores, what I'm
23 interested in is why only one high pressure core flood
24 division was selected for D3, and not for example one
25 division of low pressure core flood. And/or one

1 division of ADS. In other words, why only the high
2 pressure core flood function was selected
3 MR. DITTMAN: I understand, you are
4 asking why that function?
5 MEMBER STETKAR: Why not also the ability
6 to depressurize and get low pressure.
7 MR. DITTMAN: I'm going to let Cal Teng,
8 knows D3 pretty well, so I'll let him respond to that.
9 MR. TENG: Yes, my name is Cal Teng. I'm
10 with Westinghouse I&C engineering, and I did look
11 through the ABWR certification, so I have a background
12 I can share with you. At the time you were discussing
13 D3 with NRC, the analysis, I think, we can read from
14 Appendix 7 Charley, it was -- discusses the fact that
15 NRC did not let the applicant at that time take credit
16 for the feedwater control system, and the question is
17 asked, what else can you offer up to have the high
18 pressure system that can inject water into the HPCF
19 Charley was chosen for that.
20 MEMBER STETKAR: But I mean basically in
21 terms of my question, the history is that it was
22 strictly related to diverse method of reactor SCRAM,
23 and a diverse method for high pressure cooling without
24 a consideration of any low pressure cooling functions.
25 That is essentially I think whatever --

1 MR. TENG: In addition to the HPCF
2 Charlie, the condensate pump was taking credit for
3 being able to inject water in the reactor condensate
4 pump is a relatively low pressure system. And that is
5 taken credit for in the PRA analysis. So we basically
6 have a low pressure condensate pump, and a high
7 pressure safety related PCF Charlie that can --
8 MEMBER STETKAR: Okay, thanks.
9 CHAIR ABDEL-KHALIK: Next slide is
10 conclusions, and Charlie would like to get back to
11 slide #27, is that correct?
12 MEMBER BROWN: Yes.
13 CHAIR ABDEL-KHALIK: So and your
14 discussion will likely take more than five minutes.
15 So what I would like to do is break for lunch at this
16 time, reconvene at 1:15. And we will take Charlie's
17 discussions at that point.
18 (Whereupon, at 12:22 p.m., the proceeding
19 in the above-entitled matter went off the record and
20 resumed at 1:15 p.m.)
21 CHAIR ABDEL-KHALIK: We are back in
22 session.
23 I guess we will get back to where we
24 stopped on slide #27, and Charlie has some questions.
25 MEMBER BROWN: Okay, let me start with

1 the first one I guess, and this is on -- and the DTF
2 and the SLF both consist of maybe the other SLF RDLC
3 also, but I think I'm -- is that third one down there
4 also a common Q platform?
5 MR. BROWN: Each one of those devices are
6 built around -- each one of those boxes is built
7 around a Common Q platform. There may be other
8 ancillary equipment in there.
9 MEMBER BROWN: That's fine, the Common Q
10 platform is the fundamental platform for the CPU
11 process or whatever?
12 MR. BROWN: That is correct. Yes.
13 MEMBER BROWN: Okay, thank you.
14 I guess my question here is that if you
15 look in the FSAR and the DCD and the others -- well,
16 not the DCD, but the FSAR and the other supplements
17 you sent, the evaluation of these as being independent
18 is solely based again on the fact that the data is
19 sent over a fiber optic link and therefore it is
20 electrically isolated from -- this is interdivision,
21 not within a division, this is interdivision
22 communication. So in other words this transmission of
23 the DTF trip signals to the LFF for the two-out-of-
24 four voting, and then whatever process sends that
25 voting signal to the SLF RDLC which then also

1 generates some outputs. So that's three of them in a
2 row. And that's reflected in one of the figures, I
3 forget, 3.4b or something like that, Tier 1, 3.4.b, or
4 b. Now and so the statement is they are independent,
5 yet in each of these circumstances -- this is
6 literally a high speed serial data link, in other
7 words, it's generating a packet of data that gets sent
8 from the DTF to the SLF for the voting. The voting
9 unit is a software voting unit, not like the FPGAs,
10 where it is a set of combinational logic, digital
11 hardware gates. And it goes from one to every one of
12 the other ones.
13 So when you are unplugging a set of
14 serial data from division one, pick one, to two, three
15 and four, into that ESLFs, and therefore that one
16 packet, same question, one packet of corrupt data can
17 go over and it can literally in this case lock up the
18 computer.
19 MR. MURRAY: Eric or Ed, would you try to
20 address that? What we are trying to get to is your
21 confidence that a single corrupt data packet cannot
22 halt basically the other --
23 MEMBER BROWN: The other three
24 microprocessors.
25 MR. MURRAY: Right.

1 MR. FREDRICKSON: I am Eric Fredrickson,
2 Westinghouse, eight years, nuclear Navy, and 2-1/2 at
3 Westinghouse as the project manager for ELCS. Very
4 similar to the FPGA case, the data packet that is sent
5 over to the voter function consists of bi-state
6 status, it's a bi-state of status zero/one type of
7 bit, and does not include instructional information.
8 So on the other end, on the SLF side, when it receives
9 that it puts it into a memory location and the SLF
10 logic will then look to that memory location to get
11 the zero and one bit. It can't go there to get
12 independent instructions. So there is nothing that
13 could corrupt the functionality of the SLM vote
14 function that would have come across the HSL or the
15 high speed link.
16 MEMBER BROWN: Does that include the lead
17 -- I'm trying to understand the function of the
18 buffer. I presume that input is a buffer,
19 effectively, to hold in place. So there has got --
20 normally it's more than just a one or a zero that is
21 sent. You normally have a lead header and a -- I call
22 it a header, but some packet identifier that is at the
23 beginning, and another part at the end. And you are
24 saying those two pieces in no way can -- those are
25 read by the processing section. I understand your

1 one/zero point on this, but there is a part of those
2 data packets that are read in the TLF processing unit,
3 and so I understand your point, it's similar to the
4 FPGA, but it is not exactly the same. So -- and
5 because this is an interrupt-driven system all the way
6 along, particularly on the data transmit and the data
7 receive functions, and that comes from the Common Q --
8 I went and looked at those in the Common Q category,
9 it's unpredictable from that standpoint relative to
10 the -- I mean as long as you are reading all that
11 stuff, you are now putting extraneous data -- FPGA,
12 you are putting a one or a zero, that is very clear,
13 that one is easy. But here you have got to read that.
14 It's got to say, this is what it is, and that data in
15 itself could end up corrupting the voting function
16 process for that, or at least it's probably difficult
17 to prove a negative in this circumstance. But it is
18 still a circumstance, where you are putting in place a
19 potential to have those processes, if it's bad enough
20 to corrupt one it'll do the same thing to the other
21 ones. And that is one of my major concerns.
22 CHAIR ABDEL-KHALIK: Let's just give him
23 a chance to answer.
24 MEMBER BROWN: He's thinking.
25 MR. BROWN: No, actually he's going to

1 pass it on to me to give you a little more information
2 about the way the Common Q processor in communication
3 works. The Common Q processor is not a general
4 purpose computing machine. It is a controller that is
5 designed to buffer a safety function processor from
6 external events, including communication events and
7 network events from the interdivision network.
8 Within the controller there are actually
9 two separate microprocessors with separate memory.
10 MEMBER BROWN: Beyond the 630s or
11 something like that, 640s, I don't know.
12 MR. BROWN: 646 is correct. So the
13 processor section reads everything as data. It does
14 have an external interrupt, that is a real time clock
15 tick, that sets the periodicity functions for that
16 processor.
17 MEMBER BROWN: That's the task schedule,
18 the interrupt service routine, I am familiar with
19 that, or I know it's there.
20 MR. BROWN: Right. For information that
21 is communicated by high speed link, that's done in a
22 second processor. That processor handles only
23 communications, and can only pass data through a dual-
24 ported shared memory to the safety-function
25 calculator. It cannot pass anything other than data,

1 and the data types that it can pass are restricted.

2 MEMBER BROWN: To?

3 MR. BROWN: Certain types in certain

4 divisions. For example, the entire maximum message

5 has limitations on the types of data that you can

6 include in the message. So if we wanted the number of

7 bits, we could say we have so many long integers. And

8 those would represent the bits for the status bits.

9 Receiving station would expect those bits. In the

10 communication processor, it strips the header. It is

11 only expecting one message, and it strips the header,

12 does the CRC check, and takes the data and puts it

13 into the dual-ported memory. The only thing the

14 function processor does is to read that data and use

15 it in a calculation.

16 MEMBER BROWN: For this, I'm trying to

17 understand what you said, so that if you are only

18 sending for the voting logic and the voting logic

19 process represented does nothing else except take ones

20 and zeroes, it accepts no other type of data. That

21 is not stated anywhere in here, in the descriptions.

22 And I understand the dual-ported RAMS that it passes.

23 If the header is stripped, and you say it does a CRC

24 on it, it seems to me that since you are only

25 expecting a one or a zero, there is only -- two states

1 of a CRC that you should even expect, would that be
2 correct, because the headers and the tail end also
3 involved in the CRC calculation? I thought they were.
4 MR. BROWN: Yes, but the data in between
5 can be a varied set of ones and zeroes, since it's a
6 safety function status of all of the safety functions
7 from the EPM.
8 MEMBER BROWN: So there is more than one
9 -- it's more than just a one or zero in this case.
10 MR. BROWN: Right, it is a clean set.
11 MEMBER BROWN: Okay, that's a problem.
12 MR. BROWN: So if there are 16 analog
13 values that the EPM is going to implement, we need to
14 actuate these functions. There is a set of ones and
15 zeroes that determine the actuation status of the
16 various safety functions.
17 MEMBER BROWN: So they are only
18 transmitted once for all the --
19 MR. BROWN: Yes.
20 MEMBER BROWN: -- in that division.
21 MR. BROWN: Yes.
22 MEMBER BROWN: In other words, in the
23 processing unit, back in the DTM, it sends its stuff
24 through -- over to the transmittal, but it's looking
25 for multiple messages. If there are multiple pieces

1 of data that are going to be compacted into one --

2 MR. BROWN: Right.

3 MEMBER BROWN: -- one message each time?

4 MR. BROWN: The DTM function processor

5 will put all those status messages together, and put

6 it -- store it to the dual-ported memory, and when it

7 stores something in the dual-ported memory, it

8 generates an interrupt, the communication section.

9 MEMBER BROWN: Then it gets the last,

10 when it's finished.

11 MR. BROWN: When it's finished, the

12 communication section then takes that, formats the

13 message. Now it also includes redundancy. It takes

14 the data, it also generates the inverse of the data.

15 For a complete message.

16 MEMBER BROWN: In ones complement, in

17 other words.

18 MR. BROWN: Yes, then puts the CRC check

19 on it, then transmits it.

20 MEMBER BROWN: All that does is mean the

21 data looks the same at the end as it did at the

22 beginning. That's all those checks do. They don't

23 make the combination of ones and zeroes.

24 MR. BROWN: No, they just help you make

25 sure the message has a reasonably probability of being

1 correct.

2 MEMBER BROWN: Okay, if it's generating a

3 set of ones and zeroes for the various protection

4 functions, how do you prevent -- you have a field of

5 ones and zeroes here that are being serially

6 transmitted. If it is 16, and I don't recall in bits,

7 either one can be a one or a zero, I know there is not

8 a combination of those that gets through, but when

9 they are taken up on the other line and sent into the

10 processing unit won't compromise that voting unit.

11 MR. BROWN: Okay, because they are

12 treated only --

13 MEMBER BONACA: Could you please speak

14 into a microphone? We can't hear you.

15 MR. BROWN: It is treated only as data.

16 The processing unit at the beginning of the task of

17 two-out-of-four voting reads the input signals, so it

18 will read the communication signals and it will take

19 that and do a combination logic, Boolean logic, to

20 determine do I have a coincidence of two or more

21 signals. If you have one set of data, it will be part

22 of that computation, but it will not stop it from

23 functioning.

24 MEMBER BROWN: So your point, your

25 argument is -- I don't mean argument in the sense of

1 an argument, is that the -- there is no combination of
2 units, ones and zeroes, in that 16 bit serial stream
3 that when they are passed now into the processing
4 unit for looking at each -- I'm going to ask another
5 question about the voting units -- that will corrupt
6 or could lock up or stop the processing in any
7 particular voting platform.
8 MR. BROWN: Right, because of each of the
9 states is a valid state, either one or zero. All
10 zeroes, the functions are not tripped; all ones, the
11 functions are tripped.
12 MEMBER BROWN: Okay, I got that, let me
13 get to the next point to keep this going here. Is
14 that packet represents all functions, how does -- if
15 there are 16 protection parameters, or eight, or
16 whatever it is, I guess it would be 16 in this case,
17 how does it know which of the bits corresponds to
18 which function? In other words if it's a low pressure
19 or a high temperature or a low flow or a high power
20 whatever, do you want to tell me how that is done?
21 MR. BROWN: The position of the bit is
22 always the same for the same function so that the
23 processor knows which one of those bits in that data
24 word is the one for high pressure core flood or
25 injection, leak detection system, RHR actuation.

1 MEMBER BROWN: So it's the placement with
2 the field string that gives you that information?
3 MR. BROWN: Yes.
4 MEMBER BROWN: So when the processor gets
5 it it takes the first bit and it says, okay that is a
6 low pressure; the second bit is a vector, and that is
7 a predetermined process?
8 MR. BROWN: Right.
9 MR. FREDRICKSON: Every SLF voter
10 function is not necessarily looking at all 16 bistable
11 parameters, it's only looking at the ones it needs for
12 its overall function.
13 MEMBER BROWN: That was my next question.
14 I was presuming that when you -- I've got four sets of
15 data coming, I've got my own and three other divisions
16 worth of data coming in. And they are all
17 asynchronous, but as long as they are positionally
18 located, it doesn't really matter.
19 My next question and I think I got this
20 out of the reading is that you all's tripping is not
21 just two out of four in any protection function, if
22 it's unlike, it's all like, in other words it takes
23 all the pressures -- I got that from one of the other
24 logic diagrams, the one you had in there.
25 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

1 task schedule is in that service routine that operates
2 in the Common Q thing?
3 MR. BROWN: Yes.
4 MEMBER BROWN: I think it is a two
5 millisecond cycle time or something like that.
6 MR. BROWN: Yes.
7 MEMBER BROWN: And it picks up control
8 modules, executes them, and then they go I guess to
9 the copy task, the transmit and the receive functions
10 are then all spread out after that. So all the
11 control modules have separate priorities, they can't
12 have the same at least according to the topical
13 report. And so high priority module will always
14 interrupt a lower priority -- it'll stop it.
15 MR. BROWN: Yes, it's preemptive multi-
16 tasking.
17 MEMBER BROWN: Yes, what did you call it,
18 preemptive multitasking, fine. Then when it comes
19 back to it if it is now the right program it will come
20 back to that task. The transmit cycle, the data
21 transmission, is an event driven thing, in other
22 words, you don't send anything until you get a
23 collection of the last message that has been clicked
24 through the DPRAM into the processor, the transmit,
25 the communication processor.

1 MR. BROWN: Right.

2 MEMBER BROWN: So I've got three
3 processors in a row here, let's just use two of them
4 for the trip operation, I guess all three. And I've
5 got a task schedule which is an interrupt function
6 with different control modules that have different
7 priorities. I've got an event-driven interrupt, and
8 then a trend. So I've got almost an indeterminate in
9 my opinion at least at this point response in terms of
10 being able to say everything is going to happen in a
11 predetermined, predictable and repeatable timeframe.
12 Because if you look at the way at least the topical
13 report came across, not all control modules get
14 processed in the -- necessarily in the same order,
15 because they may be interrupted and another one could
16 take it's place. So you could even be in a position
17 that a particular control module is being processed
18 that happens to be needed for an accident
19 consideration that is in process, but another module
20 sits up there, it's time schedule says, oh, I've got
21 to run this module, it pops down, stops that one, does
22 that, and then it comes back -- maybe. It might come
23 back to another one. And your action goes on, and the
24 act is important and it does not get processed until
25 too late, or in other cycles. So I'm trying to come

1 to grips with why nonrepetitive control module
2 execution scheme where every line is just done
3 lockstep one right after another within a fixed cycle
4 time and then just repeated, instead I'm putting
5 myself in a circumstance where important modules may
6 or may not be allowed to execute in a timeframe that
7 is suitable for some particular transient.
8 In other words the problem with this is
9 it's nonpredictable and nondeterministic. And the
10 Common Q platform topical report recognizes that, if
11 you go back in the deterministic description of it, it
12 talks about you have to keep the burden on this
13 interrupt driven process below I think they said 70
14 percent -- that seemed kind of high -- but below 70
15 percent, and only make sure you didn't have overruns,
16 in which case I couldn't find out what happens if you
17 have an overrun, whether it stops and recycles and
18 starts all over again.
19 MR. BROWN: It goes to a default trip
20 state.
21 MEMBER BROWN: Okay, so it was not clear
22 how I really had a system that is both predictable and
23 repeatable from input out through the observation and
24 trip functions to all three of the microprocessors.
25 MR. BROWN: Okay, let me try to clear it

1 up a little bit because the topical report talked
2 about the capabilities of the entire machine in a
3 number -- which is used in a number of applications.
4 You would not necessarily use all those capabilities
5 to do a function like the -- let's take the DTF
6 function for example. And the typical way the
7 protection processor works is it reads all of its data
8 input at the beginning of execution, it executes, and
9 at the end of execution transmits its outputs. So --
10 MEMBER BROWN: Want to say that again?
11 MR. BROWN: Okay, the typical way the
12 controller functions --
13 MEMBER BROWN: In the Common Q platform.
14 MR. BROWN: -- in the Common Q platform,
15 the program starts and reads its data first, and this
16 is the dataset for that calculation -- it completes
17 the calculation, the program set of modules and then
18 it outputs its information. When it inputs its
19 information it reads data from IL cards if they are
20 local. Data is already at the IL cards converted, and
21 reads the data back. It may also read data from the
22 support system if it's a support system function, but
23 if it's a DTF it will not.
24 It will take in all of its analog sensor
25 data during the beginning and then will calculate each

1 one of the protection functions. At the end of that
2 it will provide an output to the HSLs. Now all of the
3 interrupt with communications are in the second
4 processor, so the only thing we are getting in the
5 first processor is the real time tick, and agree, the
6 loading is kept at 70 percent, because loading could
7 vary by different data, there is always that
8 possibility. So that guarantees that you will always
9 get cyclic information.
10 When you go to the communication section
11 and you transmit that first piece of data, that is
12 cyclic because it is tied to the cyclic nature of the
13 execution of the program that is tied to the clock
14 interrupt. That will always be a cyclic transmit, and
15 it's received from a cyclic task. So if you look at a
16 processor, it has two potential serial inputs, and one
17 potential serial output. And these are independent,
18 all three are independent. So there is a receive
19 buffer for Serial Link 1, there is a receive buffer
20 for Serial Link 2, and then there is a transmit
21 buffer. So when Serial Link 1transmits, fills its
22 buffer, Serial Link 2 transmits, fills its buffer,
23 then the application task can be dumping into the
24 buffer three. What happens when the first message is
25 done, that interrupt keeps that first serial message

1 processor from reading it once it is stored into a
2 part of RAM, second serial message the same thing, put
3 into dual-ported RAM. So those don't interrupt each
4 other.
5 And then finally the transmission task.
6 The way you assure that these interrupts can be
7 properly serviced is that the amount of time available
8 to the service the interrupts is very long with
9 respect to the amount of time that either the program
10 periodicity or the communication time. So there is a
11 majority of dead time in they communications
12 processor. It's mostly waiting for activity, and it
13 can perform all three basic tasks it has Receive Link
14 1, Receive Link 1, and transmit output without ever
15 having a situation where it could be overloaded.
16 Since those are all cyclical tasks, it is driven to
17 become deterministic because it is keyed to
18 deterministic tasks that either starts the
19 transmission, read by deterministic task that executes
20 the data, and then the transmission to the next tier
21 down, which would be the two-out-of-four voter, is
22 periodic, and predictable.
23 MEMBER BROWN: In the Common Q report,
24 topical report, I think I understood everything you
25 said, it also made the comment that for each

1 application you need to do a timing analysis in order
2 to confirm that you are really not deterministic -- I
3 understand what you are saying, what you are doing,
4 you are forcing yourself not to overload the internal
5 communications structure, so that you don't get into
6 circumstances where you are not getting just a lot of
7 wait time; I mean that is fundamentally the scheme of
8 what you are doing. I don't want to argue about that
9 right now.
10 But the --- I didn't see that requirement
11 it's part of the design requirements, so like a timing
12 analysis and the acceptance test for the ITAAC, the
13 sole thing for determinism says a report will be
14 issued that says it's deterministic. It doesn't say
15 how they are going to do it. It doesn't replicate
16 what the Common Q platform says you need to do in
17 order to ensure that in order to meet this quote
18 metric that they have in there.
19 MR. BROWN: But there is an ITAAC that
20 says the platform has to be demonstrated to be
21 deterministic, and that would be the test.
22 MEMBER BROWN: You are talking about a
23 time response test?
24 MR. BROWN: Yes.
25 MEMBER BROWN: Well, I built a system

1 out of interrupts, okay, and you end up having to do a
2 lot of tests statistically to get -- if it's deployed
3 -- to get a good feel. So when you want to do a time-
4 response test, you are not going to get the same
5 number every time in these systems.
6 MR. BROWN: Oh, absolutely, there is a
7 band of acceptable values.
8 MEMBER BROWN: And so you also run a
9 number of tests in order to make sure you come into
10 the bandwidth, come into the band. But that is why
11 you don't want to end up at the end -- I'm talking
12 about the design process now and then the test, there
13 was no timing analysis shown, and I can probably
14 accept this, I think, I'm going to have to think about
15 what you told and look back at the report again. But
16 without some type of looking at the application what
17 you all have got in a number of modules and what you
18 demonstrate, and the assumptions, and there is no
19 requirement for that to be done, other than -- the
20 only thing that would be required to be done is in the
21 full operational test that you do a time response
22 test, and that was the only place I saw a test. But
23 that in itself is not conclusive, depending on how
24 it's run.
25 MR. BROWN: If you read the topical test,

1 there is a requirement for us to do --

2 MEMBER BROWN: In the topical report?

3 MR. BROWN: Yes, there is a requirement

4 for us to do that complete timing analysis and provide

5 it.

6 MEMBER BROWN: The topical report doesn't

7 require you, it just says it needs to be done. It

8 says it will be done, but are you all subsuming that

9 under the guise of your design that you all then have

10 to do that that.

11 MR. BROWN: Yes.

12 MEMBER BROWN: Even though it is not

13 called out as an acceptance criteria in the ITAAC for

14 the qualification part of this system.

15 MR. BROWN: We will do that as a basis

16 for establishing the ITAAC deterministic tests. I

17 mean that is the logical solution. We will do that

18 timing analysis to satisfy ourself the system meets

19 its performance requirements. It is required for us

20 to submit that --

21 MEMBER BROWN: And within the time

22 response needed by --

23 MR. BROWN: Most demanding accident?

24 MEMBER BROWN: -- most demanding

25 accident, okay. I'll cut that off right here. Thank

1 you.

2 CHAIR ABDEL-KHALIK: You have one last

3 slide, I guess, your conclusion slide. Please

4 proceed.

5 MR. MURRAY: In the conclusions we feel

6 that the FSAR provides a complete set of licensing

7 basis and the requirements for the I&C systems, as

8 well as the 3&4 departures provide the design

9 advancements to eliminate obsolete equipment to

10 utilize current technology control systems. And that

11 was our last slide.

12 CHAIR ABDEL-KHALIK: Thank you very much.

13 At this time we can switch to the staff's

14 presentation.

15 MR. HEAD: Mr. Chairman, if I could, I

16 would to propose that we had some questions earlier,

17 and if we have time after the staff finished we would

18 --

19 CHAIR ABDEL-KHALIK: We will get to them.

20 Thank you.

21 MR. WUNDER: Mr. Chairman, Mr. Holahan is

22 being called, he's on his way down, and we thought

23 that this would be a good time for him to deliver his

24 remarks. Could we possibly just take a four or five

25 minute recess until he gets down here?

1 CHAIR ABDEL-KHALIK: Well, we can answer
2 --
3 MR. HEAD: No, no, people next door are
4 finalizing our responses. So I will just tell you we
5 had planned on getting back to you on some of those
6 today.
7 CHAIR ABDEL-KHALIK: But later?
8 MR. HEAD: Yes.
9 MR. WUNDER: I'm just told that he will
10 be here in about five minutes.
11 CHAIR ABDEL-KHALIK: Okay, we will take a
12 five minute break.
13 (Whereupon, at 1:49 p.m., the proceeding
14 in the above-entitled matter went off the record and
15 resumed at 1:54 p.m.)
16 REMARKS BY THE DEPUTY DIRECTOR OF THE OFFICE OF NEW
17 REACTORS
18 CHAIR ABDEL-KHALIK: Okay, we are back in
19 session.
20 Mr. Holahan, would you like to make a
21 statement?
22 MR. HOLAHAN: Thank you. My name is Gary
23 Holahan. I'm the deputy office director with the
24 office of new reactors, and Mike Johnson, our office
25 director, is also interested with the committee, and I

1 think that his calendar just gotten a little tied up
2 because we were prepared for this morning.
3 I want to make three points which I hope
4 will be helpful to the committee in getting through
5 not only this one but the digital I&C issues for each
6 of the other design certifications as well.
7 First is, the staff does recognize that
8 digital I&C is a very important issue. In some ways
9 maybe it's the most important issue for the new
10 reactor designs. Digital systems can enhance safety
11 and reliability, but they bring with them new and
12 different issues and concerns, and we need to deal
13 with those. We take these issues very seriously, we
14 take the ACRS' concerns of these issues very
15 seriously. We won't always agree on all the details
16 and it's going to take a fair amount of dialog, but we
17 take the ACRS issues seriously. We intend to address
18 them, we have a very good I think working relationship
19 with the committee, and certainly with the committee
20 staff.
21 We meet with committee staff every single
22 week. They are invited to our staff meetings on
23 Monday mornings, and I think it's produced a very good
24 working relationship.
25 The second issue I want to put is, there's

1 been a lot of discussion as to how and what the
2 decision-making process is, and what I want to
3 emphasize is that the review and approval of digital
4 I&C systems, like other safety systems in the new
5 reactor designs, is really a licensing activity, and
6 needs to take place, needs to be done, needs to be
7 done well, as part of the design certification and COL
8 process. Not as part of the field inspections. We
9 will do field inspections, we will do inspections of
10 digital I&C issues, we will involve our technical
11 digital I&C experts, but that is not a substitute for
12 making the licensing and safety decisions as part of
13 the design certs and the combined license process.
14 That's not just a legal issue. Clearly as
15 part of Part 52 calls for a safety decision to be made
16 as part of the design cert and COS. But we also have
17 experience with trying to inspect safety and quality
18 into systems in the field, and it doesn't work? It
19 doesn't work well. This has been one of the
20 characteristics of fire protection issues for decades.
21 Inspection needs to be clear in its role, inspection
22 activities need to be based on a clear licensing basis
23 to ensure that what is assured through the inspection
24 activities is based on a good technical evaluation
25 done as part of the licensing process.

1 And I know there has been a lot of
2 discussion about the role of inspection in these
3 activities, but I would encourage the committee to
4 focus on the design cert system a the most logical
5 place to make safety findings on digital I&C and other
6 systems. Combined licenses, where necessary, where
7 issues don't get fully closed at the design cert
8 stage, and not to try to use the inspection process as
9 a second level of review.
10 I think we with the committee's advice
11 need to come to a position on a good enough licensing
12 basis to make the final safety determinations in the
13 licensing process itself.
14 The third point I'd like to emphasize is
15 the staff, the ACRS, and the Commission has struggled
16 with digital I&C as a difficult topic for more than a
17 decade. We have been through this topic in each
18 design cert in the 1990s. It is continuing, and I
19 suspect for a long time it will continue to be a
20 challenging issue.
21 We think that the staff of the Commission,
22 and at least the ACRS in the past, and I know that one
23 of the values of having a new committee is that you
24 can raise issues that may have been missed before, and
25 I think those are good things to address.

1 In the past the staff, the Commission, and
2 the ACRS came to what we think is a practical approach
3 for assuring the safety of plants with -- based on
4 digital technology. And that is really with two major
5 aspects to the review. One is assuring that the
6 design itself is a good design, that it's based on up
7 to date and state of the art standards, that it is
8 done through a well planned and structured process,
9 that it's tested to the extent that systems can be
10 tested, and it's checked for things like independence
11 and communication between channels and between various
12 parts of the system, all of these things are normally
13 done.
14 But we also recognize, and maybe this is
15 an inherent characteristic of digital systems, that it
16 is really hard to come to a conclusion that the system
17 is without flaw. The systems are complex, the
18 software is getting more complicated I think all the
19 time, and recognizing how difficult it is to make a
20 determination that a digital-based system is
21 inherently reliable, the Commission took a position,
22 and I think it was a very practical position to say,
23 we need to push the systems to the state of the art
24 that they should be as good as we know how to make
25 them; they should not have any identifiable design

1 flaws, and I think that our interactions with the
2 committee and with the applicant are very good ways to
3 identify areas of concern; but ultimately none of
4 these systems will be good enough that it doesn't need
5 some kind of diverse -- either diversity within the
6 system or a backup system.
7 And that decision that especially because
8 of concerns over common cause failures of software
9 that we cannot now and maybe we could never get to the
10 point of saying that these digital safety systems
11 don't need a backup. A backup that is diverse,
12 independent, and in itself reliable.
13 We chose this as a practical way of
14 dealing with all the residual concerns that we have
15 with digital systems. So we don't want a system that
16 we know has weaknesses, it's overly complex or it has
17 communications, we are not comfortable with it, fair
18 enough, and we are going to deal with those.
19 But we think, and I would encourage the
20 committee to think, about the value that the backup
21 system brings to the overall decision-making process.
22 The residual concerns, you can't quite get to the
23 point of saying there are no flaws in some of the
24 code, thousands of lines of code. I'm not sure how we
25 would ever get to make such a determination.

1 Diversity, either inside or as a backup to the
2 protection system, goes a long way in giving the staff
3 comfort that the unknown unknowns in digital systems
4 are reasonably well covered.
5 It's an area that we focus our review, and
6 we recognize that some of the designs that are under
7 review -- and I don't want to speak to the ESBWR, our
8 experts are here to do that this afternoon, but we are
9 concerned about communication interactions within the
10 protection system. We are certainly concerned about
11 interactions, communications, between the protection
12 system and its independent and diverse background, so
13 I think what you will see on the part of our review,
14 we are addressing residual concerns by convincing
15 ourselves that the backup capability his solid, its
16 independent and diverse on the protection system, and
17 this combination of reviewing it, reviewing the system
18 to be high quality plus a reasonable backup is the
19 balanced approach to digital I&C.
20 Those are basically the messages I wanted
21 to leave you with. Our staff is here to cover the
22 details this afternoon. We interacted with your
23 committee and your staff on these issues. If you need
24 more management attention or you are not getting what
25 you need to resolve any of these issues, we are

1 available to address such concerns, and let me leave
2 it with that.
3 CHAIR ABDEL-KHALIK: Thank you very much.
4 We will proceed with the presentations.
5 STPCOLAR FSAR - CHAPTER 7 - STAFF PRESENTATION
6 MR. MUNIZ: Good afternoon, my name is
7 Adrian Muniz, and the staff is going to be presenting
8 the finding on the SER with open items for Chapter 7,
9 instrumentation and controls. Here with me is Dinesh
10 Taneja, the lead reviewer for the review of the
11 Chapter 7, and he will be in charge of the technical
12 discussion.
13 Some of the topics that we are going to be
14 discussing are the Tier 1 departure, the Tier 1 3.41
15 that addresses obsolete data communication technology,
16 and digital I&C platform selection. We will also be
17 discussing the digital I&C platforms and the Tier 2*
18 departure, and get changes or put the design
19 compliance with foreign regulations codes and
20 standards.
21 We will also be discussing the DAC/ITAAC
22 process for implementing the digital I&C design
23 details. And also as part of our review we reviewed
24 in Chapter 7 the Setpoint Methodology Technical Report
25 that was omitted by the applicant, to resolve the

1 bracketed items in the technical specifications.
2 Members of ACRS identify some items of
3 interest, and we prepared some slides to discuss those
4 topics. We are prepared to discuss them in detail.
5 However in the interests of time we propose that we
6 treat those slides as backup slides and if you have
7 specific questions we will refer to those in
8 addressing your questions.
9 CHAIR ABDEL-KHALIK: Much of this
10 material was covered by the applicant, but if
11 necessary we will revisit the issue as appropriate.
12 Thank you.
13 MR. MUNIZ: And just an update, in the
14 SER we identify four open items, all of them are being
15 closed and are being tracked right now confirmatory
16 items. Also since the SER was written one new open
17 item was identified in the area of the instrument
18 setpoint methodology, and we will provide details as
19 to what that open item is.
20 So with that I will turn it over to
21 Dinesh.
22 MR. TANEJA: Good afternoon. I am Dinesh
23 Taneja. I'm in the Office of New Reactors,
24 engineering division, and I'm the lead reviewer of
25 this South Texas COL application. I've been at this

1 task for the last about two years now, and I've had a
2 good supporting cast of characters in our branch, that
3 have supported review of this application. And I
4 personally have been with the Agency now over three
5 years; spent one year in Office of Research and the
6 rest of the time in the Office of New Reactors. And
7 prior to that since 1981 I have been involved in the
8 nuclear field in various capacities, I& C engineering,
9 startups, operations, electrical engineering,
10 supervision. So there is considerable experience that
11 came into reviewing this application.
12 And Jack Zhao that helped me in this
13 review has significant experience with digital
14 technologies, and PLCs and DCS equipments, and that
15 was a great asset in trying to review these
16 applications.
17 Primarily, the change that drew this
18 application was the obsolescence of this communication
19 system that is in the certified design. So this is an
20 example of an idea. If that technology wasn't
21 obsolete, it could have been implemented as is.
22 Because of the change, the way the applicant chose to
23 address that is, they couldn't use their technology,
24 so what they did was, the used the platforms that have
25 data and communication capabilities. So they removed

1 the data communication by addressing it by each
2 individual platform with inherent capability built
3 into it. And the original design was based on shared
4 sensor, it was a multiplex system, and it was based on
5 the FDDI technology which was discussed this morning.
6 MEMBER BROWN: My two questions are done,
7 so you can based on other people's interest.
8 CHAIR ABDEL-KHALIK: When the time comes
9 we'll get to it.
10 Please proceed.
11 MEMBER BROWN: Just wanted to let you
12 know that.
13 MR. TANEJA: The one thing that is to
14 notice is that the Tier 1 sections on neutron
15 monitoring system, the reactor protection system and
16 core cooling systems, the functional requirements that
17 are required in those sections, so there is no impact
18 to those sections because of this departure. So the
19 conclusion that we came to that the functionality of
20 the I&C is still the same, it's just how that function
21 is accomplished is being done a little differently.
22 But what it does is exactly the same thing.
23 MEMBER STETKAR: I'm a little curious,
24 Tanesh, because they've changed a few things. They've
25 made active decisions -- when you say functionality,

1 yes, in the broad sense that if I get low level and
2 high drywell pressure I am supposed to do something.
3 But how they have implemented those functions, and
4 I'll ask you the questions that I asked the applicant
5 this morning. They've changed how they implement for
6 example alternate rod insertion. They have changed
7 coincidence logic to two out of two coincidences from
8 separate SLFs within a division to one out of one in
9 many cases.
10 I'm curious how you conclude that there
11 are basically no changes.
12 MR. TANEJA: No, no, the functionality as
13 described in these systems, core cooling system,
14 right, is essentially saying that the system, needs to
15 respond to these events a certain way, right, that
16 these pumps need to start if you have a low level
17 condition in the reactor vessel, right. System
18 performance requirements are identical. The reactor
19 needs to trip if you have high drywell pressure or low
20 level, right? Those requirements at that level did
21 not change.
22 MEMBER STETKAR: It's a very high level.
23 MR. TANEJA: Exactly.
24 MEMBER STETKAR: It's a very high level.
25 MR. TANEJA: Right, now how you

1 accomplish that -- now your question on two out of
2 two, right, this was one of our review concerns. We
3 had a number of our eyes on that topic, and
4 essentially from the regulatory compliance side of it,
5 right, we have basically regulations which states that
6 you have redundant systems that are independent and
7 safety systems so you really address an issue of
8 single random failure. Redundant I&C systems. So if
9 you look at it, there are three trains in safety
10 systems, three pumps, three trains, three RHR pumps
11 and three, you know. So you need one out of three to
12 do the safety function, correct. So you have
13 basically four divisions of I&C which take four
14 different readings, and they come up to a decision to
15 start one of the pumps. So I can essentially have a
16 single failure that can take out a whole division, but
17 I still have the other division that is going to
18 perform the function, right?
19 MEMBER STETKAR: Two out of two versus
20 one out of two?
21 MR. TANEJA: I believe the whole decision
22 of the design is to improve reliability of the system
23 from the point of view that the two out of two logic
24 will prevent any inadvertent actuations.
25 MEMBER STETKAR: Now let me stop you

1 right there.

2 MR. TANEJA: Okay.

3 MEMBER STETKAR: That's what you believe

4 personally. I believe that I can't understand why

5 they made the specific decisions for some signals and

6 some decisions for other signals; that's what I

7 believe. And I believe that preventing a rare

8 spurious actuation in many cases may be worse than

9 reducing the reliability of something under conditions

10 when it's required to act. That is what I believe.

11 Now that is my belief. We are not regulating the

12 nuclear power industry based on your belief or my

13 belief. We are regulating the nuclear power industry

14 based on a determination of adequate safety.

15 MR. TANEJA: Right.

16 MEMBER STETKAR: And if I see someone

17 making a change to a design, I want to understand why

18 they made that change, and I want to understand that

19 indeed the reasons for that change and the way it was

20 implemented are indeed at least safety neutral or

21 safety improvement, not reliability improvement in

22 terms of availability of the plant to produce electric

23 power, not nuisance neutral in terms of nuisance to

24 operators for spurious signals, I want to make sure

25 that indeed they improved or at least did not reduce

1 safety.

2 MR. TANEJA: The philosophy of the design

3 is maintained. The reactor protection system is a

4 fail-safe system.

5 MEMBER STETKAR: I'm not talking about

6 reactor protection. I'm talking about emergency core

7 cooling actuation.

8 MR. TANEJA: And that system is a fail-

9 as-is system, right?

10 MEMBER STETKAR: That is a fail-as-is,

11 and energized to actuate system.

12 MR. TANEJA: Correct. So when you have a

13 two out of two, a redundancy within a division, right,

14 that is really installed to prevent inadvertent

15 actuations.

16 MEMBER STETKAR: That's right.

17 MR. TANEJA: Right. Now a lot of

18 concern, and I have the same concern, that would

19 rather have an actuation than not have an actuation,

20 because that is a safe state, correct. The way this

21 logic is designed is if you have a failure of one of

22 those SLFs, then it goes to one-of-one logic. It does

23 not sit there on two-out-of-two logic, that one gets

24 thrown out.

25 MEMBER STETKAR: That's not what I saw in

1 the logic, and I'd like to have the applicant confirm
2 that, because I felt that I needed a positive output
3 from both of those to actually actuate the device.
4 MR. TANEJA: Self-diagnostic, if you take
5 one out, then you are at one out of one.
6 MEMBER STETKAR: If it's in bypass under
7 some of those logics that's true, and in most of them
8 I believe if one of the SLF fails -- but let's let the
9 people who designed the system answer that.
10 MR. TANEJA: But that was the concept of
11 the certified design which was carried over.
12 MR. MURRAY: Would you like us to answer
13 that question?
14 MEMBER STETKAR: Yes, I would actually.
15 CHAIR ABDEL-KHALIK: Yes, please.
16 MR. BROWN: Okay, my name is Ed Brown,
17 I'm from Westinghouse. For the two out of two
18 designs, there is -- there are two types of bypasses.
19 One is an automatic output bypass which when a failure
20 is detected online from one of the SLF processing
21 logic channels, the logic is changed to one out of
22 one. There also is a manual capability to perform
23 that SLF bypass also. So most of the failures are
24 detectible by online diagnostics, so when that failure
25 is detected, there is an automatic bypass of a failed

1 select processor channel, that changes the logic from
2 two out of two to one out of two -- one out of one,
3 I'm sorry.
4 MR. TANEJA: And that was the last
5 certified design which was carried over.
6 MEMBER STETKAR: That is certainly not
7 apparent in any of the schematic diagrams that are
8 available in the FSAR, because those schematic
9 diagrams seem to indicate serial connections of the
10 output devices from the individual SLFs, which is not
11 -- is not quite consistent from what I just heard.
12 MR. BROWN: I believe in Section 7 it is
13 described in words. And it is also described in the
14 ITAAC as things that will be testable.
15 MEMBER STETKAR: Okay, let me cut to the
16 chase here. In the SER I see words that are parroted
17 back, the same words that are parroted back from the
18 FSAR. They are very high level words. I see
19 references to figures, in Chapter 16, the same figures
20 that are referred to this morning. I do not know how
21 any of the equipment indeed is aligned to any of those
22 logics, nor which are deferred to one out of one, or
23 which starts with one out of one. And I come to a
24 final conclusion that says, the staff found the
25 applicant's response to RAI 07-9 acceptable. For a

1 detailed technical evaluation of this ESF design
2 concept and its regulatory compliance refer to Section
3 7.3 of this SER. I read it, it doesn't say much.
4 Verification of the implementation of these ESF design
5 concepts described above will be performed via Tier 1
6 Section 3.4 DAC ITAAC inspections.
7 I just thought that we heard that we are
8 making licensing decisions based on safety at this
9 stage, not into ITAAC DAC inspections. An inspector
10 can indeed confirm that something is wired up on a
11 two-out-of-two logic or a one-out-of-one logic; that's
12 what I would expect them to do. I would expect the
13 staff at this stage to be answering questions about,
14 why did you change this from a one out of one -- or
15 I'm sorry, a two out of two to a one out of one. I
16 didn't see any of those questions. I read the RAI.
17 MR. TANEJA: That was a question that we
18 asked. Jack, there was a specific RAI on that
19 question, correct.
20 MR. ZHAO: This is Jack Zhao, New Reactor
21 Office. I know there was one.
22 MEMBER STETKAR: Did you get an answer to
23 that in terms of a list and the reasons why they
24 changed each one?
25 MR. ZHAO: I didn't hear that. What I

1 hear is that the response I've seen -- I have been
2 away from this project for six months, but I cannot
3 remember exactly.
4 MEMBER STETKAR: I'd be interested to see
5 that detail.
6 MR. TANEJA: What I recall in the
7 response to that RAI was, what was said this morning
8 that the ECCS components and the containment isolation
9 components would be using redundant buses, okay. The
10 functions that are not -- you know the consequences of
11 that function actuation is not critical, those would
12 use single buses. That was one of the responses. And
13 the other thing I recall that it made a reference to
14 some table in Chapter 16 for a list of components.
15 MEMBER STETKAR: I couldn't find that
16 table, so if it exists I'd really be thrilled to see
17 that table. It doesn't refer to a table; it refers to
18 five figures.
19 MR. TANEJA: Well, I think we had asked
20 that question, which components would be part of the
21 two, and which components would be, you know, on a
22 single bus.
23 MEMBER STETKAR: I'd love to see that,
24 because for the life of me I can't understand why a
25 two-out-of-two logic is required for low pressure

1 injection, for example.

2 CHAIR ABDEL-KHALIK: Would the applicant

3 --

4 MEMBER STETKAR: I asked them this

5 morning. That is one of the things that is on the

6 table.

7 MR. MURRAY: Right, that is one of the

8 follow up questions.

9 MEMBER STETKAR: What I'm trying to do is

10 to find out how deeply the staff has probed into these

11 changes in a design at this stage of the licensing

12 process, because they are changes to a design.

13 MR. TANEJA: Yes, those are -- that is

14 one of the departure issues, and basically the way we

15 understood that change was that that actually was

16 simplifying the design and taking some complexity out

17 of it rather than making it more complex. See, two

18 out of two logic makes things complicated; it's not a

19 simple thing. See, if you already have four

20 divisions, okay, one out of four to actuate two out of

21 four is what the existing plant -- if we looked at the

22 SRP guidance which is our regulation there is no

23 regulation that states that we must have a two-out-of-

24 two within a division. We do not require that.

25 MEMBER STETKAR: Correct.

1 MR. TANEJA: If you look at 603 there is
2 no requirement for that. It is - -basically addresses
3 the issue of inadvertent actuations to prevent -- it's
4 basically an aide to make a better operation of a
5 plant, not really to make it safer. Safe would be to
6 start the pump regardless of whether you need it or
7 not.
8 MEMBER STETKAR: Not necessarily.
9 MR. TANEJA: Not necessarily, right, but
10 the way the regulations, fail safe means, you know if
11 a condition occurs, my safe condition is to go into
12 that safety mode. So we actually do not have any
13 specific regulation that requires that you must have a
14 redundant feature within a division, so we cannot
15 really say that they don't meet a certain regulatory
16 requirement if they don't do it. I couldn't find one,
17 unless you know of something. I'd love to hear that.
18 MEMBER STETKAR: I'm not talking about a
19 regulatory requirement; I'm talking about
20 understanding a change in a design and the impact of
21 that change on fundamental plant safety. Have I
22 improved plant safety by making that change to the
23 design? Have I maintained the same level of safety as
24 the original certified design? Or perhaps because of
25 an inadvertent oversight have I reduced the level of

1 safety? Based on that change? I'm only talking about
2 the change. I'm not talking about philosophical --
3 MR. TANEJA: Let's say two out of two for
4 containment isolation functions, that's critical, all
5 right. Now if I'm just taking -- I don't want the
6 list of components. All containment isolation
7 functions. They are very well defined. I can't
8 inspect -- I know which ones have containment
9 isolation values. When I go to inspect them, or an
10 inspector goes to inspect, containment isolation is a
11 very well defined component. It's not like you know
12 that we have to sit there and decipher, is there a
13 containment isolation or not, right?
14 ECCS components, clear cut, we know what
15 ECCS components are. They are part of the ECCS
16 system. From my experience with BWR, E-21s, E-41s,
17 HPCI, RCIC, ECCS. Clear cut. You know, from the
18 power sources to my inventory of suction, where I'm
19 taking the suction from, and where I'm pumping to, and
20 what drywell you need to line up that system, that
21 makes up the ECCS system.
22 So for us when we looked at it, you know,
23 yes, we wanted to have a list, but we didn't see a
24 whole lot of value in having an inventory of
25 components clearly identified. I thought those

1 systems were adequate for that purpose.

2 CHAIR ABDEL-KHALIK: The applicant will

3 follow up with that information, so please proceed

4 with your presentation. Thank you.

5 MR. TANEJA: Sure.

6 MEMBER STETKAR: Dinesh, I'm sorry, I was

7 searching for a reference here. You have to be

8 careful, because I am going to try to keep people

9 precise. And what I was searching for is the

10 reference I finally found. In the FSAR in Section

11 B.3.3.1.4 of the technical specifications, they make

12 reference to a non-two-out-of-two coincidence,

13 something that has been changed to a one-out-of-one,

14 specifically for containment isolation. That is all

15 it's called out is containment isolation. So in this

16 area where you are talking about two of two for

17 containment isolation, that is one area where they

18 made a change. I just wanted to get that on the

19 record. Thanks.

20 MR. TANEJA: Okay, on this slide this is

21 from the DCD. This figure comes out of the DCD, which

22 really shows the function of the obsolete data

23 communication multiplexing system. And as you can see

24 from this figure that communication is shared by RPS

25 and ECCS. If you lose that communication, basically

1 you render the whole division inoperable. And this
2 change, going to the next figure, which also shows the
3 figure out of DO-1, it shows the block diagram of the
4 SSLC logic and where you can see that the social
5 multiplexing system is used both for the inputs, which
6 are shared by the ESFs and the RPS modules, and the
7 outputs that go out of the CM use to RM use, you know,
8 is done on the EMS system. . Now that portion of it on
9 the outputs is strictly for the ESFs, because I think
10 the RPS even on the existing, the old certified
11 design, was hardwired. But these common weakness on
12 the design that we certified was on the EMS side, and
13 that was a weakness. And that's why there was a lot
14 of attention given in the design certification on the
15 EMS system, because it was very critical to the
16 functionality of the complete division.
17 So the applicant on their design when they
18 were addressing this obsolescence they basically
19 elected to divide up the SSLC system into three very
20 distinct platforms. They separated out the ELCS, NMS
21 and RTIS, and I think we heard a lot of that
22 discussion this morning on that one, and I believe we
23 had a good presentation on their communication
24 capability, which is inherent to each of the platform,
25 it's all built into. So this is what really replaced

1 the obsolete data communication capability of the
2 SSLC.
3 And this is a simplified block diagram
4 that shows the new design which essentially shows that
5 all the -- for the RPS, the RTIS function, you -- all
6 your inputs are hardwired. There is no -- there is no
7 communication used there. Everything is hardwired
8 into the DTS. They do not share any of the inputs
9 with the ELCS or the ESF systems, so the ESF systems
10 are basically using the -- that is a Common Q platform
11 so it's using the communication capabilities to get
12 the remote data into the DCFs.
13 And the Note 5, which basically says that
14 each function may be accomplished by the multiple
15 processor to minimize any hardware or software
16 complexity or operational impact. And I think that
17 one is basically on the loading of the processors.
18 And like it was mentioned this morning, the Common Q
19 SER has these plant specific action items. If you are
20 to use a Common Q platform for a given plant the
21 licensee must address those specific action items in
22 order to use that platform. And one of the action
23 items as described this morning was the form of timing
24 analysis for that application to demonstrate that the
25 timing would be within the bounds of the Chapter 15

1 analyses. All the event analysis. So that becomes a
2 requirement for the design if that platform is to be
3 used in this application, then that would become a
4 requirement, and our -- and our lifecycle development
5 phase, in the requirement phase we expect to see all
6 those requirements identified even at that phase.
7 Not until this thing is built, we want to
8 see those things right there. That that requirement
9 is identified, and it's being designed to those
10 requirements. That is our expectation.
11 MEMBER BROWN: When is that going to be
12 done?
13 MR. TANEJA: Well, that is part of the
14 post-COL activity because the applicant has chosen to
15 go that route, and based on our Part 52 license, they
16 have the option to either do it as part of the COL
17 application, or do it after they get the COL.
18 MEMBER BROWN: Who is going to review
19 that report?
20 MR. TANEJA: Who is going to review that
21 report?
22 MEMBER BROWN: Yes, who is going to do
23 the final -- if they are required to do it, who is
24 going to execute the review to see if it was done
25 satisfactorily?

1 MR. TANEJA: Well, it is part of the DAC
2 ITAAC activity, right. It's in the 3.1, there's a DAC
3 that requires those work to be done. Implementation
4 of the software/hardware development is a DAC item.
5 And that requirement is -- it's on a targeted ITAAC
6 list so the staff is going to inspect it.
7 MEMBER ARMIJO: But not review it? I
8 have a big problem with this inspect/review. Is there
9 going to be an equivalent of a design review, a
10 licensing review at that stage or not? The answer I
11 get is, yes, we are going to inspect it, but I don't
12 know if that means the same thing.
13 MS. DUDES: No, the answer to that
14 question for the Part 52 process is that the safety
15 decisions have been made in licensing, and that it
16 will be an inspection targeted inspection, but it will
17 be an inspection to verify compliance with the
18 licensing basis. Sorry, this is Laura Dudes.
19 MEMBER ARMIJO: Yes, I understand.
20 MEMBER BROWN: So let me amplify what
21 Laura just said. So the ESR for the Common Q platform
22 becomes an integral part of the licensing basis?
23 MR. TANEJA: Well, the SER for the --
24 MEMBER BROWN: The action item from the
25 SER becomes a -- it's effectively an inspection item.

1 MR. TANEJA: Right.

2 MEMBER BROWN: If I'm wrong, you just

3 said that, and in order to verify that it was done

4 correctly, somebody has to review it.

5 MR. TANEJA: Correct.

6 MEMBER BROWN: Who is going to do that

7 review? Is it -- you say staff.

8 MR. TANEJA: Well it is part of the -- it

9 is part of the DAC inspection process, because this

10 work is now implemented. It's implementation of that

11 platform. It's an implementation.

12 MEMBER BROWN: Okay, let me ask the

13 question another way. You get the report.

14 MR. TANEJA: Right.

15 MEMBER BROWN: There's two ways. As an

16 inspector, I say, hey, I got a report. They tell me

17 the number is 69. Check. Okay, I'll put the thing

18 aside. This is like taking a micrometer and measuring

19 the diameter of a pipe. It doesn't work for this.

20 How do you know they did the timing analysis

21 correctly?

22 MR. TANEJA: Let's not say that it's that

23 simple of an inspection.

24 MEMBER BROWN: Come on, I'm trying to

25 give the thought process.

1 MR. TANEJA: Thought process --

2 MEMBER BROWN: This is not the same in

3 terms of complexity or difficulty of what I would call

4 standard site inspection.

5 MR. TANEJA: That is the reason, that is

6 the very reason, over these questions, is why there is

7 that pilot program that is being implemented at this

8 stage to figure out exactly what needs to be done in

9 those inspections.

10 MS. DUDES: Excuse me, this is Laura

11 Dudes again. Again, we understand that an I&C

12 inspection may be a little bit more complicated, and

13 in fact we do have staff and inspectors who can

14 actually go beyond the measuring of a pipe, and we --

15 we as NRO and our counterparts in the Inspection

16 Program Branch understand that there is the complexity

17 of that type of inspection, and for those

18 implementation activities within the Common Q SE,

19 which are specific -- I mean we made our safety

20 determination on the platform, and wrote the safety

21 evaluation based on the Common Q platform with

22 specific items for which we will verify implementation

23 of that via another regulatory activity beyond

24 licensing, which is inspection, develop inspections

25 that will cover satisfactorily verifying that the

1 licensing basis established in the safety evaluation
2 report is in fact what is being implemented in the
3 plant.
4 CHAIR ABDEL-KHALIK: We have heard your
5 message. We have heard Mr. Holahan's message. And I
6 think the committee will address this issue from a
7 generic philosophical approach, and the committee will
8 make its opinions known to the commission and to the
9 staff. Thank you. So this is not the place to
10 debate this issue now. So please proceed.
11 MR. TANEJA: All right, next slide. I
12 think we have seen this one already. This was
13 actually a better picture. This came out of the
14 application; these guys had a nice color picture of
15 it. So basically that is a layout of the
16 architecture. Now next slide, these are the specific
17 items of interest coming out of this departure. We
18 basically started our review of the application at the
19 stage of acceptance review. And during the acceptance
20 review, you know, we had a number of meetings with the
21 applicant, and we came out with a number of changes to
22 the application at the acceptance review process. And
23 the review of the application actually was deferred to
24 Rev. 2 by the time we actually started to review the
25 application, because there was significant additional

1 information hat got added from initial to middle to
2 the Rev. 2 stages. And since then we have written a
3 number of RAIs, and gone through a number of meetings
4 to get to where we are today to make the conclusion
5 that we are here with the Phase 2 phase of the SER
6 review.
7 I think the response to RS 07-6, we talked
8 about that, that added a new supplemental section,
9 7.1S to the COLA. 7.9S is another supplemental
10 section that was added to the DCD FSAR to elaborate on
11 the communication capabilities, both the safety and
12 the nonsafety side. The PDN was discussed in there,
13 and how the system is different and independent from
14 the safety communication networks.
15 And that is really described in 7.9S, and
16 the RAI 07-9 is where the clarification on the ELCS
17 function was provided. That was the RAI where we were
18 talking about this two out of two versus one out of
19 two, and I think that is the RAI where we got into
20 that discussion to try to figure it out a bit. Next
21 page.
22 The Common Q platform like we've talked
23 about it is already qualified and reviewed by the NRC,
24 and the same platform is being used in the AP1000
25 designs and their safety applications. The associated

1 design for the STP 3 & 4, it conforms to the ISG-04,
2 and it also conforms to all the current regulatory
3 guidance standards on data, in today's date. The
4 certification was based on for example IEEE 279. And
5 then it was certified. One of the biggest changes
6 that was made was that any new I&C platform that is
7 being added will conform to the IEEE 603 requirements.
8 We used the current version of the SRP
9 Chapter 7 to do these evaluations, of the application.
10 And basically the design that we saw for the SSLC in
11 the application, it offered significant enhancements
12 for what was certified for the ABWR.
13 So in conclusion to this section, the
14 South Texas I&C design that was in the COLA, and
15 including some of the RAI responses which still is a
16 confirmatory item, it adequately addressed all the
17 applicable licensing basis, and is in compliance with
18 the applicable regulation, regulatory guides and
19 standards.
20 The SLC design I&C platforms including
21 inherent data communications capability are in
22 compliance with current regulations, regulatory
23 guides, and standards. Specifically IEEE 603 and its
24 companion standard 7-4.3.2, 2003 version.
25 All open items have been resolved that

1 were related to this departure, and all the proposed
2 COLA changes are being tracked right now as a
3 confirmatory item.
4 The Tier 2* Departure, essentially this
5 departure is where they address compliance to the
6 current regulatory guides for the INC design. And
7 based on this departure, the safety related I&C
8 systems on all three of the platforms now conform to
9 603-1991 and the current versions of the applicable
10 reg guides, and the NUREG-0800, the SRP and the Branch
11 Technical Positions.
12 So those really are the things that give
13 us confidence that the design is going to be at this
14 level, and these are all the requirements.
15 And in response to one of our RAIs, the
16 applicant provided supplemental tables, 1.9S-1, and
17 1.9S-1A, these two tables were added which identify
18 the IEEE standards and the related regulatory guides
19 that are specific to developing software. And these
20 reg guides came into place after the design was
21 certified, so these were added to the COL application.
22 So in conclusion I have to say that the
23 design now complies with the current regulation,
24 regulatory guides and standards, and all open items
25 have been resolved, and we are basically tracking

1 these are confirmatory items.

2 And for the interest, I guess I added

3 these two tables to our backup slides, just to --

4 these were part of the RAI response. They are not in

5 the application; for your interest. Basically it

6 points to all the very recent regulatory guides, for

7 example, 1.168 through 1.173, all these reg guides are

8 very specific to the development of these software and

9 hardware systems. And their companion IEEE standards

10 are on 1.9S-1D.

11 Configuration management software test

12 documentation, software requirement specification,

13 software unit testing, V&V. So that is really what is

14 our BTP 7-14, which these folks are complying to for

15 developing these platforms. So that really is the

16 guidance that is most up to date right now that we are

17 following for getting these designs built to a good

18 quality standard.

19 MEMBER BROWN: I want to make one

20 observation. You state the Common Q platform was

21 approved and has been evaluated for use and found

22 suitable for use. The difficulty is when you put them

23 into a specific application they can be applied in a

24 manner which is not satisfactory. So the fact that

25 the platform is functionally okay, but you can execute

1 it such that it doesn't give you the end result. So
2 you are going to review, at least I will, any of these
3 applications to see that the application of that
4 platform -- if you notice in my comments I didn't
5 argue about the platform so much as how it was
6 utilized in the specific system. And how it's
7 characteristics were used to try to ensure that you
8 got the satisfactory performance, that was the point.
9 So my point being is that using that is an
10 argument for why everything is okay is like telling me
11 why a Motorola 68000 is okay because we've used it
12 before. It doesn't matter if it is not used -- I
13 just wanted to make sure you understood that, because
14 I've heard that comment before that this has already
15 been approved. It makes it sound like why are you
16 asking. Because the way it's done. You don't have to
17 say any more.
18 MR. TANEJA: Yes, I agree with you.
19 MEMBER BROWN: Because we need to on with
20 it. But I just wanted to make sure you understood
21 that point.
22 MR. TANEJA: It's the same. It's very
23 relevant thinking, so I agree with you on that one,
24 but it needs to be applied very judiciously for its
25 safety application.

1 MEMBER BROWN: Appreciate that.

2 MR. TANEJA: I believe.

3 CHAIR ABDEL-KHALIK: I believe the
4 comments made on slides #17 - #19 have been made
5 several times today, and I would recommend that we
6 move on to slide #20;.

7 MR. TANEJA: The setpoint methodology
8 document is actually one of those DAC ITAAC item that
9 was originally the intent of the applicant was to
10 actually treat that as a full COL activity. And under
11 a separate activity that was trying to address the
12 bracketed items for the tech spec, the applicant
13 elected to use the option where they were going to go
14 with the setpoint control program. And part of the
15 setpoint control program was to promote the setpoint
16 determination methodology.

17 So we received that document and we
18 reviewed it as part of Chapter 7, and our evaluation
19 of that as SCP's setpoint methodology is captured in
20 Chapter 7.1-4 I think it is.

21 And we've completed our review -- next
22 slide -- the basic couple of items of interest is that
23 this report was prepared by Westinghouse for this ABWR
24 application, and that methodology is very very similar
25 to what we have received for AP1000 which was already

1 reviewed and approved by the staff, the AP1000
2 methodology. And we had primarily one significant RAI
3 on this one, which was adequately responded to, and
4 the rev one of the methodology was issued
5 incorporating all the response to that RAI, and then
6 we were reviewing the Rev 1 item, and there was one
7 minor reference that we found that basically
8 references to a topical report on stability analysis
9 for the OPRM setpoints, and that topical report is
10 intended to be part of the fuel amendment which is
11 like a beyond COL activity. So right now we have
12 identified that, and we have initiated an RAI on that
13 one, and we are tracking that one as an open item at
14 this stage.
15 CHAIR ABDEL-KHALIK: What do you expect
16 the answer to be? Is it related to GE7 fuel, or is it
17 to whatever fuel they are going to have after that
18 amendment?
19 MR. TANEJA: Have you guys figured out
20 anything? Right now we felt that that was not -- the
21 COL application right now assumes IBR, right. So when
22 you see this application referring to that, can we
23 take that? The question is, you know, how can you
24 reference something that does not exist, or does not
25 exist in this application? And that was our question.

1 So I only heard that resolution.

2 MR. MURRAY: The question was which fuel

3 is it based on.

4 MR. QUINN: Yes, Bob Quinn, Westinghouse

5 Licensing, been involved in nuclear power and nuclear

6 fuel for about 30 years now. Our strategy at this

7 point going forward is we are going to remove the

8 reference to the topical report from the setpoint

9 methodology report, and we will be bringing in an

10 actual calculated value for OPRM, based on the

11 stability option 3 from the BWR owners group, and we

12 will be applying the uncertainty analysis as

13 documented in the current technical report, and we

14 will actually be providing that, that sample value, in

15 the report. So for GE7 fuel we are going to stick

16 with the approved approach, which is approved in the

17 DCD FSER for the BWR stability option three approach

18 to OPRM, calculating the setpoints.

19 MEMBER ARMIJO: And what happens when you

20 put the real fuel in the SVEA, whatever it is? Are

21 you going to redo that analysis?

22 MR. QUINN: Yes, we --

23 MEMBER ARMIJO: Will the staff review

24 that again?

25 MR. QUINN: The setpoint -- I'm sorry,

1 the stability topical report is going to be submitted
2 next month as part of a number of topicals related to
3 the fuel amendment which we'll, be doing after COL, so
4 we'll be redoing the calculation for the stability
5 setpoints, as part of that, and we will be using that
6 topical, which we hope to have approved at that time,
7 as the basis for doing it.
8 CHAIR ABDEL-KHALIK: Let's move on.
9 MR. TANEJA: So essentially because of
10 this one open item we are unable to finalize our
11 conclusions on the setpoint methodology.
12 Now these next few slides are on the items
13 that the members were interested in finding out more
14 on, and if you like I will go through them.
15 CHAIR ABDEL-KHALIK: I will defer to
16 Charlie at this point. You heard -- or have you
17 received sufficient information from the applicant
18 regarding your questions?
19 MEMBER BROWN: We didn't spend a whole
20 lot of time on this, but I didn't have any questions
21 on this. The diverse systems I think we probably
22 agree, I think they were diverse. And they were
23 redundant.
24 CHAIR ABDEL-KHALIK: How about the issue
25 of determinism?

1 MEMBER BROWN: They were analog. My
2 memory is failing at this point. They were hardwired
3 analog, if I remember. They were not FPGAs even were
4 they? Okay, my memory is failing me; thank you.
5 MEMBER ARMIJO: I think you have a typo
6 on your slide #23. I don't think I've ever seen the
7 certified US ABWR at this time. You have a certified
8 ABWR design. I'm just wondering what do you mean by
9 that?
10 MR. TANEJA: I have seen it both ways in
11 Appendix A.
12 MEMBER ARMIJO: Is it in the DCD?
13 MR. TANEJA: Yes, it's in Part 52,
14 Appendix A.
15 MEMBER ARMIJO: It seems that the U.S.
16 has dropped out so many times, that sounded like a
17 mix-up with some other certified design.
18 CHAIR ABDEL-KHALIK: That's fine. Are
19 there any questions for the staff at this point?
20 MEMBER BROWN: One question on diversity
21 applications. It's not on the specifics, but for the
22 analysis used in this project for the diverse systems,
23 is their response based on the same conservative
24 casualty analysis or accident analysis that your
25 primary systems are based on?

1 MR. TANEJA: What we found on that one is
2 that these -- on slide #26 is the summary of the
3 assumptions made for making that diversity analysis.
4 They used the worse case postulated common mode
5 failure of the safety system, concurrent with each of
6 the design basis event. That's in Chapter 15. The
7 analysis, they used a realistic modeling values as
8 opposed to the licensing, the worse case values.
9 MEMBER BROWN: Okay, that is what I
10 missed.
11 MR. TANEJA: These were the three key
12 things that I picked up when I was going through that.
13 Essentially they have to not remove shutdown system
14 has capability to -- which is independent of --
15 MEMBER BROWN: Yes, that is manual.
16 MR. TANEJA: All manual, right?
17 MEMBER BROWN: Yes.
18 MR. TANEJA: So that has full capability
19 of bringing the plant to full shutdown. So
20 essentially I think one of the conditions was that you
21 cannot go there for at least an hour, so you have to
22 be in the control room doing everything within an
23 hour. So that was one of the -- and I think the
24 digital failure that was assumed in this analysis was
25 the multiplexing system because that took down the

1 whole division. That was the worst failure that was
2 assumed.
3 MEMBER BROWN: I'm done with that, thank
4 you.
5 CHAIR ABDEL-KHALIK: All right.
6 MR. TANEJA: And I think, John, your
7 question was whether the change of the platform had
8 any impact to this diversity implementation.
9 Basically the platform and its architecture. And I
10 think this figure that 7C, one figure in the
11 application, this figure, in the shaded areas, that
12 the worst features that are added, so you can see that
13 they really bypass everything that is digital that go
14 straight to the components.
15 MEMBER STETKAR: That helped a lot.
16 MR. TANEJA: Yes.
17 MEMBER BROWN: I was satisfied with that
18 one when I saw it, no problem.
19 CHAIR ABDEL-KHALIK: Are there any other
20 questions for the staff?
21 Okay, thank you very much.
22 Let me just try to catch up on the action
23 items. There is an action item related to the
24 documentation for each ESF component, as to how the
25 SLF coincidence logic is implemented, its actuation.

1 This is one of the issues raised by John. And we --
2 MR. HEAD: And that was from this
3 morning.
4 CHAIR ABDEL-KHALIK: Right. We
5 essentially have it for the ADS, but for nothing else.
6 MR. HEAD: That is one of the ones we are
7 supposed to be talking about here in just a minute.
8 CHAIR ABDEL-KHALIK: There was a need for
9 follow up on departure 7.2.2, departure 7.2.6, and
10 7.3.9.
11 MR. HEAD: 7.2.6, the zero pressure?
12 CHAIR ABDEL-KHALIK: Yes.
13 MR. HEAD: And 7.2.9 was the --
14 CHAIR ABDEL-KHALIK: 7.3.9, 7.3.9 was the
15 shutdown cooling.
16 MR. HEAD: All right, okay.
17 CHAIR ABDEL-KHALIK: Do you have
18 responses for any of these or any of the other follow
19 up items that we identified prior to that with regard
20 to Chapter 14?
21 MR. HEAD: I believe we are poised to
22 give you an answer on those four, but begging your
23 indulgence, I'd like to take a break and just make
24 sure I know where we are, and then we'd come back and
25 answer.

1 CHAIR ABDEL-KHALIK: Okay, we will take a
2 10 minute break. We will reconvene at 10 after 3:00.
3 (Whereupon, at 2:57 p.m., the proceeding
4 in the above-entitled matter went off the record and
5 resumed at 3:09 p.m.)
6 CHAIR ABDEL-KHALIK: We are back in
7 session.
8 At this time STP would like to provide
9 answers to some of the questions that were raised
10 earlier today.
11 MR. HEAD: Exactly, I am going to turn
12 over the first one to Craig Swanner, if you will
13 identify which one we are talking about specifically.
14 MR. SWANNER: Do we want to do the
15 Chapter 14 one first?
16 MR. HEAD: Yes, go ahead.
17 MR. SWANNER: There was a question when
18 we were going through Chapter 14 regarding I&C and it
19 was on whether preoperational testing -- or there was
20 any preoperating testing of ELCS, because one of the
21 committee members asked, looked through the chapter
22 and couldn't find any mention of the acronym ELCS.
23 The answer to the question is, ELCS is part of the
24 overall SSLC system, and preoperational testing of
25 SSLC is described in Chapter 14.2.12.1.11 of the

1 application, and in there it has a parts referring to
2 ESF, and the requirements ESF go to ELCS. So the
3 acronym doesn't appear in the chapter, but it is
4 covered.
5 MEMBER BROWN: So RPS is also part of the
6 --
7 MR. SWANNER: That's correct.
8 MEMBER BROWN: -- safety -- and it has
9 its own separate section. So there is a little
10 dichotomy there in terms of I guess ELCS is not as
11 important as the RPS, tongue in cheek? The RPS was
12 very -- I won't say very detailed, but it's got a
13 listing, whereas the SSLC when it's a little bit more
14 --
15 MR. SWANNER: Generic.
16 MEMBER BROWN: -- generic.
17 MR. SWANNER: That's correct.
18 MEMBER BROWN: So it's a little hard to
19 connect the dots between one needs -- can be generic
20 and the other can't. I got the answer. I'm not so
21 sure I like it.
22 MR. SWANNER: That is the answer.
23 MEMBER BROWN: Okay.
24 MEMBER STETKAR: Is that the only answer
25 regarding Chapter 14? Because it really didn't answer

1 the question that I asked.

2 MR. SWANNER: Can you repeat the

3 question, please?

4 MEMBER STETKAR: My question was, is

5 there a preoperational test of whatever acronym you

6 want to use, ELCS, SLLC, let's focus on ELCS, that

7 tests the function from what I call end to end, in

8 other words if I had a sensor out in the plant that is

9 supposed to sense reactor vessel level and eventually

10 starts a high pressure core flooder that indeed a

11 functional test is performed where I insert a low

12 level signal which I can do at the sensor itself,

13 verify that indeed the combinatorics -- the full

14 combinatorics is processed through the digital I&C

15 system and that indeed the pump starts. In a single

16 test, not a piecemeal three level overlapping test

17 which is indicated in Chapter 14.

18 MR. SWANNER: If there is -- as part of

19 the tech spec, there is a surveillance for each of the

20 ESF functions that is a full comprehensive function

21 test, end to end, specified tech spec, Able 3.3.1.4-1.

22 and that is to be performed on a refueling outage

23 basis.

24 CHAIR ABDEL-KHALIK: Could you repeat

25 that number, please?

1 MEMBER STETKAR: I was asking for a preop
2 test though, because I would really like to understand
3 before I start up this plant that it is going to work
4 on day one, not find out that two years later that
5 maybe it had a problem.
6 MR. SWANNER: We can take that and figure
7 it out.
8 MEMBER BROWN: That was the question.
9 MR. HEAD: Where was the more
10 comprehensive testing? That was in the tech specs?
11 MR. SWANNER: That was in the tech specs.
12 MEMBER BROWN: But that's a surveillance
13 issue.
14 MR. HEAD: We would know that we are in
15 that condition before we start the plant up. I
16 understand your question. Before that we are going to
17 know that answer.
18 MEMBER STETKAR: In pre-op would be a
19 good time to find out if there was a bug.
20 MEMBER BROWN: Same applies to the
21 protection system.
22 CHAIR ABDEL-KHALIK: So is this issue
23 going to be followed on?
24 MR. HEAD: Yes.
25 MEMBER BROWN: So for the RTIS as well,

1 or RPS, whatever.

2 MR. HEAD: The basically logic control,

3 safety logic control system.

4 MR. MAUCK: My name is Jerry Mauck.

5 During one of the ITAAC's has that the system has to

6 be shown to be functional, as part of the ITAAC

7 closure once the system is in, and also as part of the

8 site acceptance testing you do an end to end test on

9 it then.

10 MEMBER STETKAR: I just didn't see it

11 specified in that way that you are saying it orally

12 right now. Because in writing, the acceptance

13 criteria specifies, it's where that ITAAC sits, it

14 specifies under acceptance criteria -- in the FSAR now

15 --

16 CHAIR ABDEL-KHALIK: Is the answer as

17 simple as providing us this ITAAC, a reference to that

18 ITAAC, then that would be adequate. If not, we are

19 going to --

20 MEMBER STETKAR: Sure. It specifies a full

21 end-to-end test.

22 CHAIR ABDEL-KHALIK: Right. Okay, thank

23 you. Please proceed.

24 MR. SWANNER: Sure. And then the first

25 question that you had on Chapter 7, moving on to --

1 CHAIR ABDEL-KHALIK: There is a question
2 about the steam line velocity.
3 MR. HEAD: That will be Chapter 3.
4 CHAIR ABDEL-KHALIK: Okay, that's fine.
5 MR. SWANNER: Moving on to the four
6 questions that you had for Chapter 7, the first one as
7 I understood it, please correct me if I'm misstating
8 the question, but it's where in the application are
9 there are required ESF actuation logic redundancy
10 specified?
11 MEMBER STETKAR: I am not sure whether
12 you stated the question correctly. That's not what I
13 asked, but let's see what you answered.
14 MEMBER BROWN: Just tell him your
15 question.
16 MEMBER STETKAR: What I'm interested in
17 is seeing where in the FSAR I can find the information
18 that we were discussing earlier with respect to
19 coincidence logic within a single division, for
20 actuation of ESF equipment. So if that is what you
21 are -- because I know I can find different divisions
22 for equipment.
23 MR. SWANNER: That is what I am trying to
24 answer.
25 There have been several RAIs on this issue

1 as you are well aware. The first one was our response
2 to 07.03-1, which you may have in front of you. The
3 other one was a response to 07-9, and both of those -
4 - one of the RAIs describes the list of tech spec
5 functions for ESF, and describes which one is -- has
6 required redundancy in the division, and which one
7 goes to one-out-of-one voting, and then in 07-9, it
8 describes the I guess criteria for how we selected the
9 redundancy for each of the functions. That
10 information resides, and I think you located the place
11 in the FSAR, it is again in the tech spec bases, it's
12 in the description for 3.3.1.4, and then as well it's
13 shown in the figures B.3.3.1.4.-1, through 5. And
14 it's only shown as a system level, like for example,
15 3.3.1.4-4 shows the ADS logic; 3.3.1.4.-3 shows the
16 HPCF C logic. 3.3.1.3-2 shows the remaining ECCS
17 logic, things like low pressure flutter, RCIC and HPCF
18 and then the 3.3.1.1 -- or 3.3.1.4-1 shows the
19 remaining systems that are actuated by ESF.
20 MEMBER STETKAR: And that is literally
21 the way to interpret those figures, such that every
22 piece of equipment which is associated with low
23 pressure flooding divisions B and C, for example,
24 apply the logic that is shown in 3.3.1.4-2.
25 MR. SWANNER: That is correct.

1 MEMBER STETKAR: Would apply to that.
2 Okay. That probably -- that's the way to interpret
3 that, then that would satisfy what I'm interested in,
4 because someone could indeed go confirm that indeed
5 that equipment was actuated that way. Behind all of
6 this is actually a deeper question regarding why the
7 redundant design -- as I understand it, the redundant
8 -- I won't call it redundant -- the two out of two
9 coincident logic has been removed from the certified
10 design for whatever the set of equipment that is
11 controlled under B.3.3.1.4-1 which is containment
12 isolation and a number of what you call ESF support
13 functions, which I have to go look at, which there are
14 some cooling water systems in there, ventilation,
15 things like that. So there is apparently a rationale
16 behind that.
17 MR. SWANNER: There is, and that is
18 described in the responses to 7.3-1 and 07-9.
19 CHAIR ABDEL-KHALIK: Okay.
20 MEMBER STETKAR: Okay.
21 CHAIR ABDEL-KHALIK: Proceed.
22 MR. SWANNER: The next one is I believe
23 on standard departure 7.2-2, and that would be on
24 backup SCRAM.
25 MR. CHAPPELL: My name is Coley Chappell

1 with STP 3 and 4 setpoint licensing, and I had the
2 pleasure to address ACRS on a number of earlier
3 occasions, and I'm glad to be here again today. I
4 will handle a couple of questions. The first is, on
5 the departure 7.2-2 it's a standard departure, this
6 cleared up a description in Tier 2 that shows that the
7 backup relays are energized. The backup relays, in
8 order to energize a SCRAM, they are energized in a
9 logic that is two out of two, so two channels
10 coincident, that would then energize a relay, and they
11 are redundant channels. So therefore no single
12 failure can prevent or cause an actuation of the
13 backup SCRAM function.
14 The description that is provided on the
15 figure shows on the left hand side for a normal SCRAM
16 that the relays are open. On the right hand side it
17 shows the relays closed. And it's a power
18 distribution system, but that shows what a trip
19 condition is on the relays. That is based on the DCD
20 information as shown on that data.
21 MEMBER STETKAR: You are going to have to
22 walk me through that again. I'm sorry, I hate to be
23 really dense about it, but you are going to have to
24 walk me through it again.
25 MR. CHAPPELL: The description is correct

1 in that it describes an energized to actuate backup
2 SCRAM function.
3 MEMBER STETKAR: Energize to actuate
4 backup SCRAM function?
5 MR. CHAPPELL: That is correct.
6 MEMBER STETKAR: Okay.
7 MR. CHAPPELL: So the logic is that two
8 out of two, coincident channel, will energize the
9 relay, will energize the solenoid, close the relay.
10 MEMBER STETKAR: Close the relay.
11 MR. CHAPPELL: And then will energize the
12 solenoid valves that will then vent the SCRAM air
13 header.
14 MEMBER STETKAR: Got you.
15 MR. CHAPPELL: There are redundant
16 channels, so if one channel has a failure in it, the
17 redundant channel will actuate those valves.
18 MEMBER STETKAR: Okay, I understand that.
19 I am still not clear -- I am looking at a figure 7.2.8
20 in the FSAR that shows the relay contacts in a -- I'm
21 an electrical engineer so look at normally closed
22 contacts as the thing when the coil is deenergized.
23 And it shows a bunch of normally closed contacts as
24 energizing the SCRAM solenoid valve, which is, and I
25 will quote from the design DCD, this is from the

1 design DCD Section 7.2.1.1.4.1, normally closed relay
2 contacts are arranged in a SCRAM logic circuitry
3 between the air header dump valve solenoids and the
4 air header dump valve solenoid 125 volt DC power
5 source such that when in a trip state, parenthesis,
6 coiled deenergized, the relays will cause energization
7 of the air header dump valve solenoids, air header
8 dump initiation.
9 So that says in the original design it was
10 as it is shown as an electrical engineer, I would
11 understand this figure such that when you deenergize
12 the relays you would energize the solenoid and dump
13 the air, and from what I understood you to say is that
14 it has now been changed to energizing those coils to
15 energize. So that is a change in the way that those
16 interface relays work.
17 A point to the staff now, staff's SER
18 concludes that indeed this is acceptable because --
19 let me see -- I can't find the quotation. They
20 essentially did that all they did was clear up and
21 make the way the system operates consistent with the
22 way it's shown on the drawing. That is not true. It
23 was changed.
24 MR. CHAPPELL: I may comment on that and
25 simply say that in the way that the description is

1 written, the way it's described on a normal SCRAM, the
2 way it is described for a backups SCRAM.
3 MEMBER STETKAR: I'm not arguing about
4 the normal SCRAM. I'm going to keep focus over here
5 on the backup SCRAM.
6 MR. CHAPPELL: I also, sort of used to
7 looking at the prints in a certain way. This print is
8 confusing to me in the sense that I have to compare
9 both left-hand and right-hand sides because it is
10 described as a power distribution. It's showing on
11 the power, on the left-hand side the normal SCRAM,
12 those contacts are normally closed.
13 MEMBER STETKAR: That's right, the relays
14 are normally energized. I'm an electrical engineer.
15 I understand how those A contacts work.
16 MR. CHAPPELL: Right, and so what it's
17 shown is, on that print it's shown in trip condition.
18 MEMBER STETKAR: Yes.
19 MR. CHAPPELL: And on the right-hand side
20 those contacts are shown closed, which would not be a
21 trip condition under a description -- well, if the
22 description in the DCD were correct is what I would
23 say. And the description in the DCD compared to the
24 design that is provided in the COL with the departure
25 7.3.9. 3.

1 MEMBER STETKAR: Let me see if I -- I am
2 probably being too dense here. In the original DCD
3 design, was it necessary to energize a SCRAM, a backup
4 SCRAM air header dump valve solenoid to dump the air?
5 Did I need to actually apply voltage across the
6 solenoid coil for the dump valve, for the solenoid
7 valve, in the original design, yes or no?
8 MR. CHAPPELL: I can't answer that
9 question, and the reason I can't answer that question
10 is because I looked at this one issue, this one
11 paragraph, but not at the extended condition.
12 MEMBER STETKAR: Okay, because if I read
13 the words and I look at the drawing, again, this is
14 from the DCD, it says -- I hate reading this stuff --
15 when in a tripped state -- they are talking about -- I
16 don't want to quote the whole thing again -- when in a
17 tripped state coil deenergized the relays will cause
18 energization of the air header dump via solenoids.
19 That is a pretty clear statement that seems consistent
20 with the drawing that I'm staring at.
21 So it seems like the original design was
22 an energize to dump the back SCRAM air header --
23 energize the solenoid valve.
24 MR. CHAPPELL: Right.
25 MEMBER STETKAR: And what I've heard you

1 say that that is still the case, I still need to
2 energize those solenoids to dump the backup --
3 MR. CHAPPELL: You still energize --
4 MEMBER STETKAR: Energize the solenoids.
5 MR. CHAPPELL: It's still energize to
6 actuate.
7 MEMBER STETKAR: Right, so now the
8 question is, how do those relays in between work?
9 Because in the original design I used to remove power
10 from the relay coil to get the output contacts to
11 close to apply power to the solenoid. And what I
12 heard you say -- and I might be wrong -- but from what
13 I heard you say I now need to apply power to the relay
14 coil to close the output contacts from that relay to
15 apply power to the solenoid. Is that correct?
16 MR. CHAPPELL: It does apply power -- it
17 does require power application to the relay to cause
18 the contact to close is my understanding.
19 MEMBER STETKAR: So you've changed the
20 way those relays operate from the design, from the
21 certified design?
22 MR. CHAPPELL: That is my understanding.
23 MEMBER STETKAR: Okay.
24 CHAIR ABDEL-KHALIK: Is the documentation
25 adequate?

1 MEMBER STETKAR: Yes, well, it's -- I am
2 not sure that an electrical engineer will look at the
3 drawing and understand the way it works, which is why
4 I raised the question initially. It's not clear to me
5 that the staff had a full understanding that that part
6 of the design had been changed.
7 Now is it an important change in the
8 design? I'm not going to the issue of value judgment.
9 But it is a change in the design, and it fundamentally
10 changed a failure mode, a deenergize to actuate the
11 safe condition for those relays, to an energize to
12 actuate the safe condition of those relays. So it's
13 not something that is simply clearing up the potential
14 misinterpretation of a drawing; it seems to be an
15 actual change to the design. I don't know why the
16 change was made, but it seems to be a change unless I
17 am misinterpreting something.
18 MR. CHAPPELL: Fundamentally the normal
19 SCRAM function is a deenergize to actuate, so a loss
20 of power --
21 MEMBER STETKAR: I'm not arguing about
22 the normal SCRAM function.
23 MR. MURRAY: Have we made an actual
24 change, is the --
25 MEMBER STETKAR: I am only talking about

1 the backup SCRAM function. As best as I can tell
2 there has been absolutely no change in the normal
3 SCRAM function, and I understand the verbal
4 description of that, and I can look at the electrical
5 drawing, and I can see how that works.
6 Look at Figure 7.28 and how the system now
7 works, and see whether or not those contacts make
8 sense.
9 CHAIR ABDEL-KHALIK: STP will clarify
10 this.
11 MR. HEAD: And we will have an
12 interaction with the staff on whether there needs to
13 be additional clarification, an update of some sort.
14 CHAIR ABDEL-KHALIK: Okay, thank you.
15 MR. MAUCK: Let me add one point to that.
16 The name is Jerry Mauck. I'm with STP I&C. That ARI
17 SCRAM system is there only to meet the ATWS rule 10
18 CFR 50.62, which is never deenergize to actuate; it's
19 always energize it to actuate. So it meets the ATWS
20 rule.
21 MEMBER STETKAR: It does, and the final
22 end device, the solenoid, has always been -- they
23 solenoid valve to dump the air header pressure has
24 always as best as I can tell been an energize to
25 actuate. It's just how I get that thing energized

1 seems to have changed.

2 MR. TONACCI: Excuse me, this is Mark

3 Tonacci, why don't we take an IOU on this one?

4 CHAIR ABDEL-KHALIK: Thank you.

5 MR. SWANNER: And I apologize a little

6 bit for backtracking to the first one where we talked

7 about the ITAAC and the ITAAC that were mentioned, the

8 two ITAAC that are relevant in that case is Table 3.4-

9 1, ITAAC No. 2 -- excuse me, Table 3.4 ITAAC 2, and in

10 the case of reactor protection it's Table 2.2.7, ITAAC

11 No. 2, and if you go and follow the systems, for

12 example ESF and neutron monitoring you will find

13 similar comprehensive tests, end-to-end tests, in

14 ITAAC in each of them.

15 MEMBER STETKAR: Thanks, that's -- that

16 will at least point us toward a reference.

17 MR. HEAD: But they don't say end to end,

18 they say --

19 MEMBER STETKAR: They don't. They say

20 comprehensive.

21 MR. SWANNER: Yes.

22 MEMBER BROWN: You said 2.2.7?

23 MR. SWANNER: 2.2.7 is for RPS, and 3.4

24 is for general SSLC. It's somewhat repetitive, I

25 agree.

1 MEMBER BROWN: I went through 3.4, let me
2 tell you, it was number what?
3 MR. SWANNER: Tests will be performed --
4 MEMBER BROWN: Didn't change in the SR?
5 MR. SWANNER: Yes, tests will be
6 performed on as-installed SSLC, using simulated input
7 signals. System outputs will be monitored to
8 determine operability of function -- of safety-related
9 functions.
10 MEMBER STETKAR: But again that is pretty
11 general.
12 MEMBER BROWN: That's high level, that is
13 so general it could be anything. Somebody could --
14 (Simultaneous speaking.)
15 MR. SWANNER: 2.2.7.
16 MEMBER BROWN: I had that one. Item
17 which?
18 MR. SWANNER: Item two.
19 MEMBER BROWN: I don't have that layout.
20 MR. SWANNER: I can read that one as
21 well,
22 MEMBER BROWN: Get those iPods moving,
23 right?
24 MR. SWANNER: Tests will be conducted
25 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

1 you go back and look at Table 7.2-1, there are some
2 strikeout beside this value range, and that strikeout
3 is a solid line, and then the next value is 15 KPAG,
4 but if you look close at the 15 KPAG, there is
5 actually a negative sign beside it. So it's negative
6 KPAG to 30 KPAG --
7 MEMBER STETKAR: Hokey smokes. That is
8 "hokey smokes" for the recorder. Thank you.
9 CHAIR ABDEL-KHALIK: Okay, thank you.
10 MEMBER STETKAR: So thank you.
11 MR. SWANNER: And the last one was on
12 7.3-9, and that is on shutdown cooling, and I will
13 turn that over to Coley.
14 MR. CHAPPELL: So I'll continue
15 discussion on the follow-up items on Standard
16 Departure 7.3-9. First of all I want to clarify the
17 description of the design. The suction isolation
18 valves inboard and outboard isolation valves on RHR
19 shutdown cooling receive isolation signals from Level
20 3 drywell pressure, high drywell pressure, and lead
21 detection. There is another suction isolation valve
22 that is interlocked, closed, with an ECCS initiation
23 signal. The purpose of this isolation valve is to
24 align the RHR system in a low pressure flutter mode
25 upon initiation of ESF. That initiation can be from

1 Level 1, or it can be from high drywell pressure. But
2 the signal actually comes from the ESF initiation, so
3 it's not a direct Level 1 initiation signal that is
4 confirmatory or anything for a shutdown cooling
5 isolation valve, and it's a different set of valves.
6 The actual containment isolation valves are isolated
7 by a Level 3; that has not changed. So the intent of
8 the departure was to clarify this description. I
9 think we will maybe take a look at that and make sure
10 that we have done so.
11 MEMBER STETKAR: I was writing notes.
12 Just run it by me quickly again.
13 MR. CHAPPELL: Okay, effectively there
14 are three valves.
15 MEMBER STETKAR: Yep.
16 MR. CHAPPELL: There are two inboard --
17 there's an inboard and outboard isolation valves.
18 MEMBER STETKAR: Right.
19 MR. CHAPPELL: That receive a Level 3
20 isolation signal among others. There is a third
21 shutdown cooling suction valve whose purpose is to
22 align the RHR system to low pressure flutter mode. It
23 does that upon an ECCS initiation signal of which are
24 included Level 1 and hydraulic pressure. So the
25 design has not changed.

1 MEMBER STETKAR: Has not changed, I was
2 trying to clarify which valves are actuated by which
3 station.
4 MR. CHAPPELL: Which of the valves are
5 repositioned. All of the valves are normally closed.
6 MEMBER STETKAR: Yes, okay, thank you.
7 CHAIR ABDEL-KHALIK: So I guess the
8 question that was raised in much simpler terms, do we
9 get a low pressure safety injection if the Level 3
10 signal failed?
11 MR. CHAPPELL: If -- well, those valves
12 are normally closed, and the overriding condition --
13 the reason those valves are closed is in order to
14 ensure that you don't drain the vessel, and the
15 overriding function is to inject. So there is no
16 interlock back from those valves that would present an
17 injection if those -- if those valves were closed, but
18 that signal failed, those valves would still be
19 closed, and the suppression of the suction valves
20 would still be --
21 MEMBER STETKAR: I was thinking -- I try
22 to think about safety across all operating modes, so I
23 was thinking in low pressure cooling conditions, if
24 you had a loss of coolant, indeed, when you were lined
25 up for shutdown cooling, and those valves would be

1 opened, I don't know when your protection -- do you
2 keep your protection system enabled during --
3 MR. CHAPPELL: In all modes you are
4 required to maintain the minimum number of operable
5 systems. So if you have -- if all the valves are open
6 that would be inoperable for the low pressure flooder,
7 because the suppression pool cooling suction is
8 interlocked closed.
9 MEMBER STETKAR: If those valves are
10 open. On the other hand if they get a signal to close
11 from a Level 3 and they close, you should be able to
12 initiate an injection?
13 MR. CHAPPELL: There are a number of
14 factors, but that seems logical.
15 MEMBER STETKAR: Okay. I think the
16 fundamental point is, I don't think they have changed
17 the design here. I think it's partly my
18 misinterpretation of the wording and not being able to
19 fight through the logic diagrams, quite honestly.
20 From what I heard you say it hasn't really changed.
21 MR. CHAPPELL: Correct.
22 MEMBER STETKAR: Thanks.
23 CHAIR ABDEL-KHALIK: Is there anything
24 else that we need to follow up on, or that completes
25 the list of items?

1 MR. HEAD: That completes our feedback
2 for the day.
3 CHAIR ABDEL-KHALIK: And I guess there
4 are follow-up to the follow-up items that you will
5 come back to us and to the staff?
6 MR. HEAD: Yes.
7 MEMBER STETKAR: And by the way, as
8 critical as I am, thanks a lot. I know you guys did a
9 lot of quick searching, so I really appreciate that.
10 CHAIR ABDEL-KHALIK: Thank you very much.
11 MR. HEAD: We appreciate the opportunity
12 to provide the feedback today.
13 CHAIR ABDEL-KHALIK: Thanks.
14 PUBLIC COMMENT
15 CHAIR ABDEL-KHALIK: At this time on our
16 schedule we are to provide an opportunity for public
17 comments, and therefore I've asked our staff enable
18 this phone line for any member of the public who has
19 joined us in this meeting to make any statements or
20 comments.
21 Is the phone line open? Are there any
22 members of the public who wish to make a comment?
23 (No response.)
24 Let's just verify that the phone line is
25 open before we terminate this process.

1 MR. HACKETT: The line is open.

2 CHAIR ABDEL-KHALIK: Is there any member

3 of the public who wishes to make a comment?

4 (No response.)

5 The answer is none, so let's proceed to

6 the next item on the agenda, which is the closure,

7 subcommittee discussion ands closing remarks.

8 SUBCOMMITTEE DISCUSSION AND CLOSING REMARKS

9 CHAIR ABDEL-KHALIK: I would like to just

10 go around the table and see if the people have any

11 additional comments or questions or closing remarks.

12 Charley.

13 MEMBER BROWN: I think mine got answered

14 at this point other than the one open item still on

15 the site and security, whenever we see that, so I'll

16 hold that one in abeyance. I've still got to think

17 about the deterministic discussion that we had; that

18 was a good discussion, but I need to go integrate some

19 of that.

20 CHAIR ABDEL-KHALIK: Thank you. John.

21 MEMBER STETKAR: My only comment is a

22 fairly general comment, and that is because of the

23 importance of instrumentation and control, I'll stay

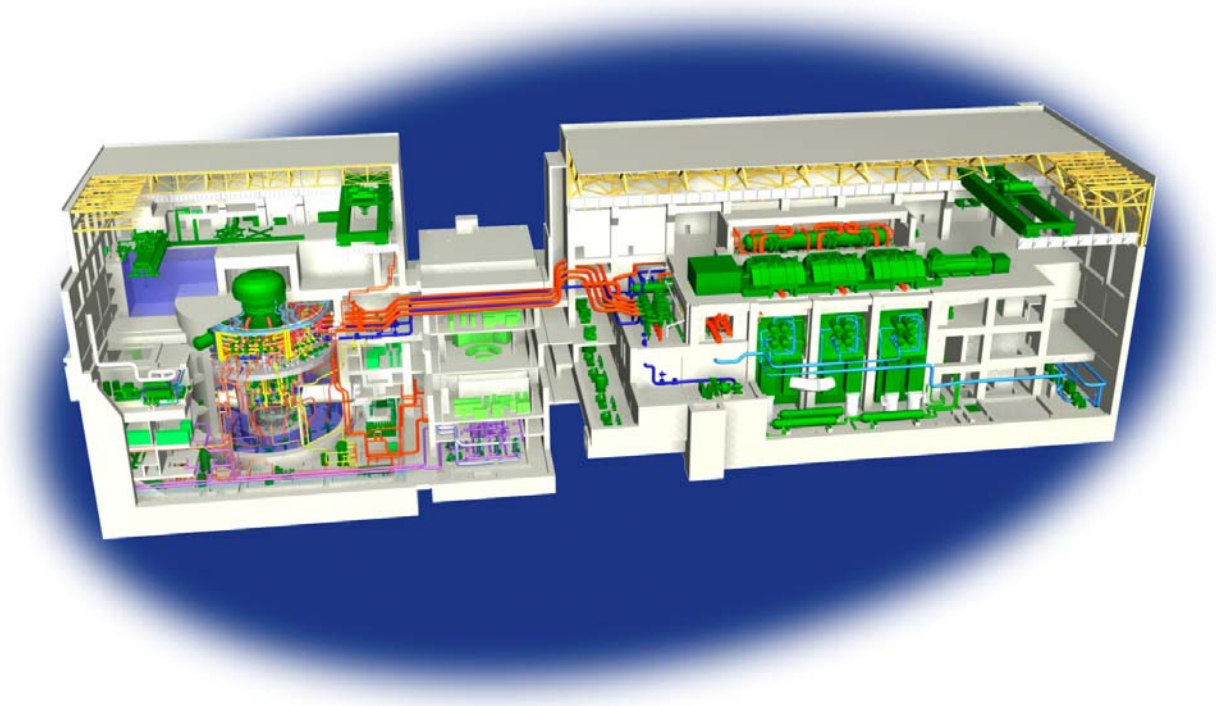
24 away from the digital aspect of that, I think it's

25 very important that the documentation in the FSAR at

1 the COL stage contains consistent and enough detailed
2 information such that when those ITAAC inspections are
3 performed, the inspectors indeed have sufficient
4 information so that they can confirm that the design
5 is actually implemented according to at least the
6 functional logic. So that's my only -- the reason I
7 was asking several of these questions was to try to
8 examine that level of detail, and to try to highlight
9 areas where it may not be quite as clear in the FSAR,
10 thinking from the perspective of somebody who is going
11 to go out and actually try to verify that the design
12 is installed in the way that it is supposed to be.
13 That -- I've gotten some assurance that that
14 information is available. I'm not quite there yet on
15 some of the other stuff.
16 CHAIR ABDEL-KHALIK: Okay, Sam?
17 MEMBER ARMIJO: No comment.
18 CHAIR ABDEL-KHALIK: Bill?
19 MEMBER SHACK: For a nonprofessional, I
20 just want to say I thought it was a very helpful
21 discussion today.
22 MEMBER RYAN: No additional comments,
23 but thanks for everybody's participation.
24 CHAIR ABDEL-KHALIK: Mario.
25 MEMBER BONACA: I share John's views on a

1 number of items, and you know I wonder if there is
2 more there of the same type, which is not necessarily
3 a misrepresentation but an inconsistency between what
4 is in the text of the FSAR and the plant as built. So
5 I'm sure that with time we will get a better
6 understanding, but in general I learned quite a bit
7 today.
8 CHAIR ABDEL-KHALIK: Okay, thank you.
9 Well, let me express the committee's appreciation to
10 STP and the staff for a really informative
11 presentation today. Thank you very much.
12 Meeting is adjourned.
13 (Whereupon, at 3:47 p.m., the proceeding
14 in the above-entitled matter was adjourned.)
15
16
17
18
19
20
21
22
23
24

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

14.1 Preliminary Safety Analysis Report Information (N/A)

14.1S Applicable Regulations and Regulatory Guides

14.2 Initial Test Program (ITP) Test Descriptions

14.2S Initial Test Program Supplemental

14.3 Tier 1 Selection Criteria and Processes

14.3S Selection criteria for site-specific systems, emergency planning and security ITAAC

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

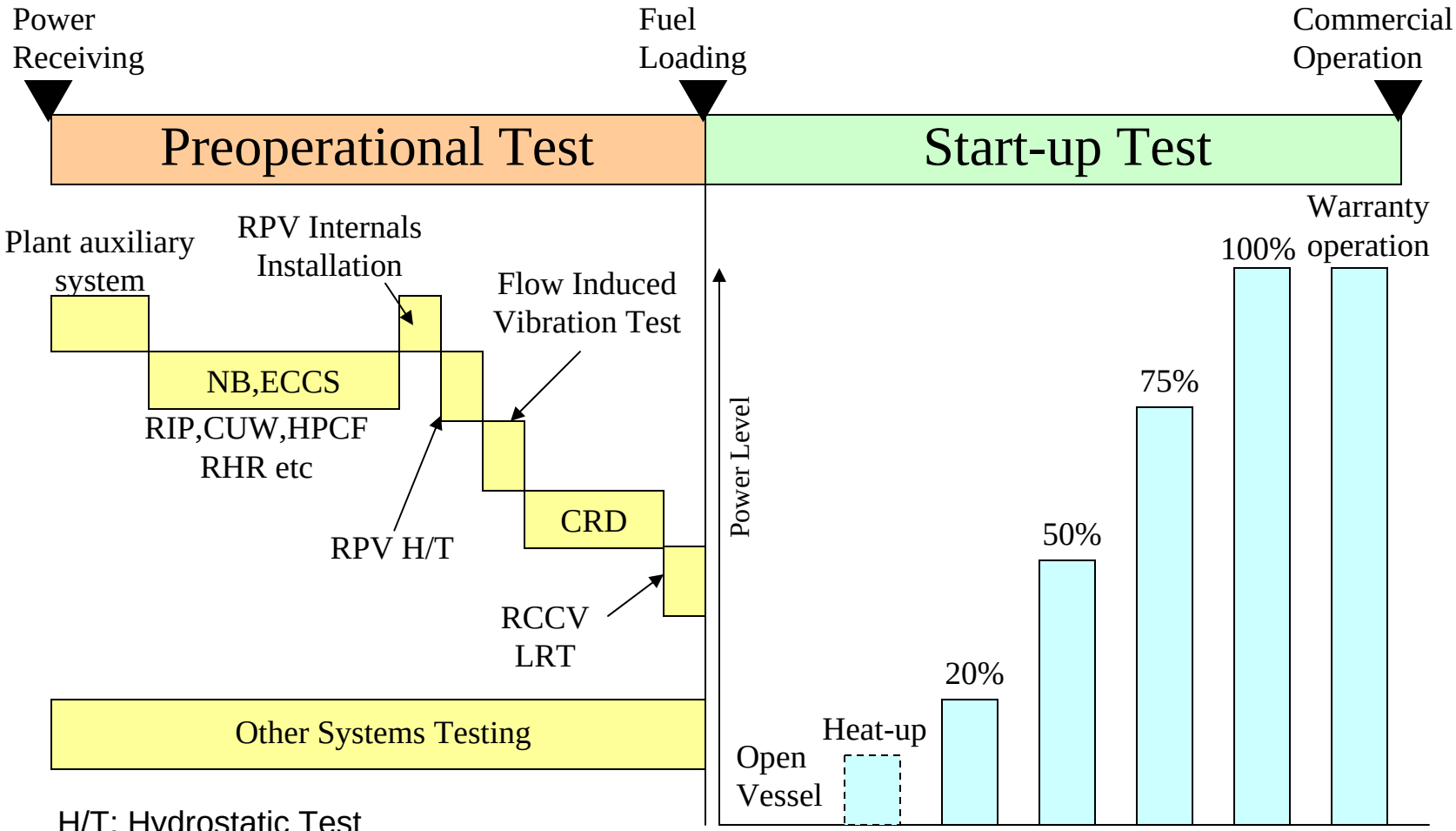
- STP Startup Manager provides technical direction of plant startup activities.
- STP operations staff under the leadership of the Operations Shift Supervisor responsible for the operation of the plant.
- Startup test performance and data collection done by members of the Startup Test Group as directed 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

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 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

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

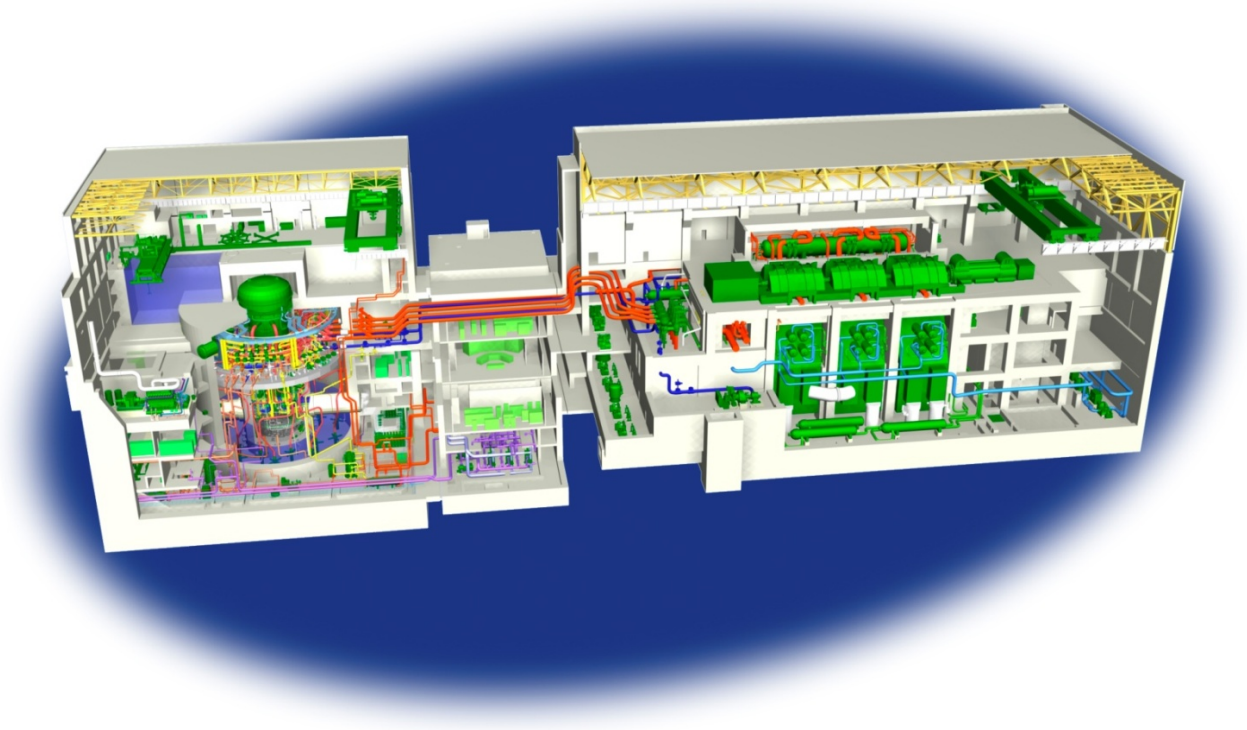
14.3S ITAAC

- 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

7.1 Introduction

7.1S Instrumentation and Control Platforms

7.2 Reactor Protection (Trip) System (RPS)

7.3 Engineered Safety Feature Systems

7.4 Systems Required for Safe Shutdown

7.5 Information Systems Important to Safety

7.6 All Other Instrumentation Systems Required for Safety

7.6S Interlock Systems Important to Safety

Contents of Chapter 7 (cont'd)

7.7 Control Systems Not Required for Safety

7.8 COL License Information

7.8S Diverse Instrumentation and Control Systems

7.9S Data Communication Systems

7A Design Response to Appendix B, ABWR LRB I&C

7B Implementation Requirements for Hardware/Software Development

7C Defense Against Common-Mode Failure in Safety-Related, Software- Based I&C Systems

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

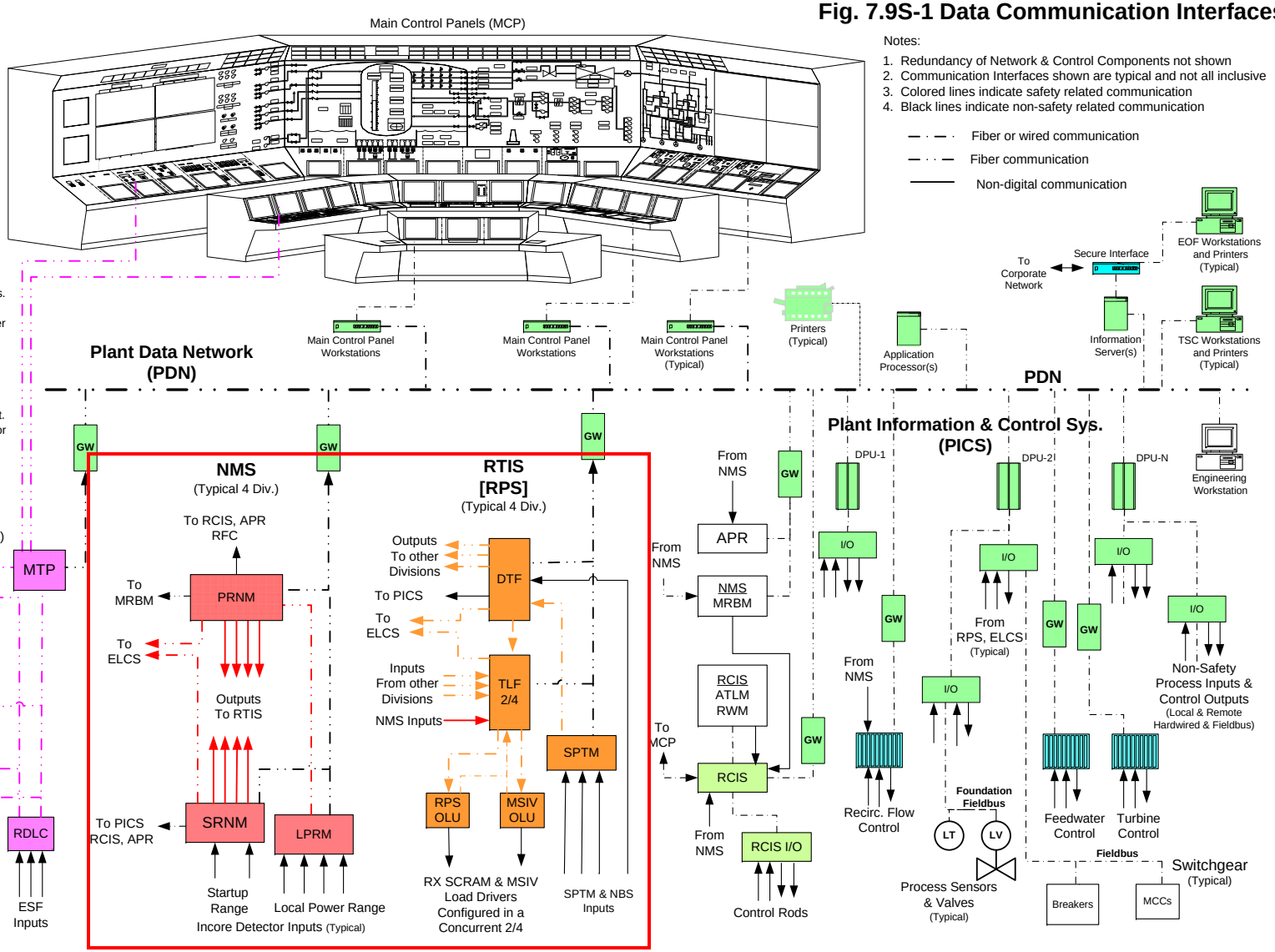
- ABWR DCD SSLC implements RPS and ESF using a common essential multiplexer system (data highway)

- 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

Notes:
1. Redundancy of Network & Control Components not shown
2. Communication Interfaces shown are typical and not all inclusive
3. Colored lines indicate safety related communication
4. Black lines indicate non-safety related communication

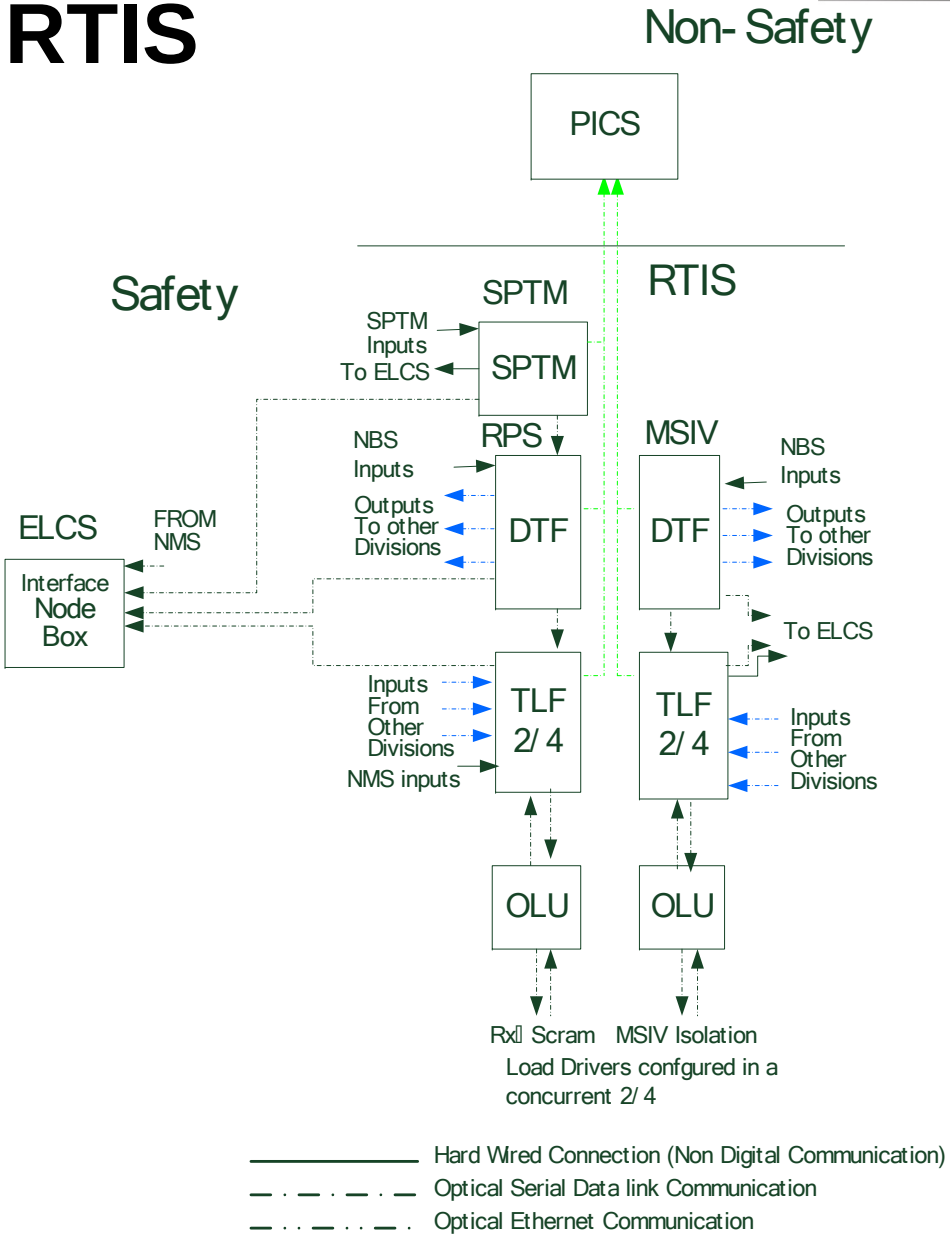


Features of communication design (FPGA)

- 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



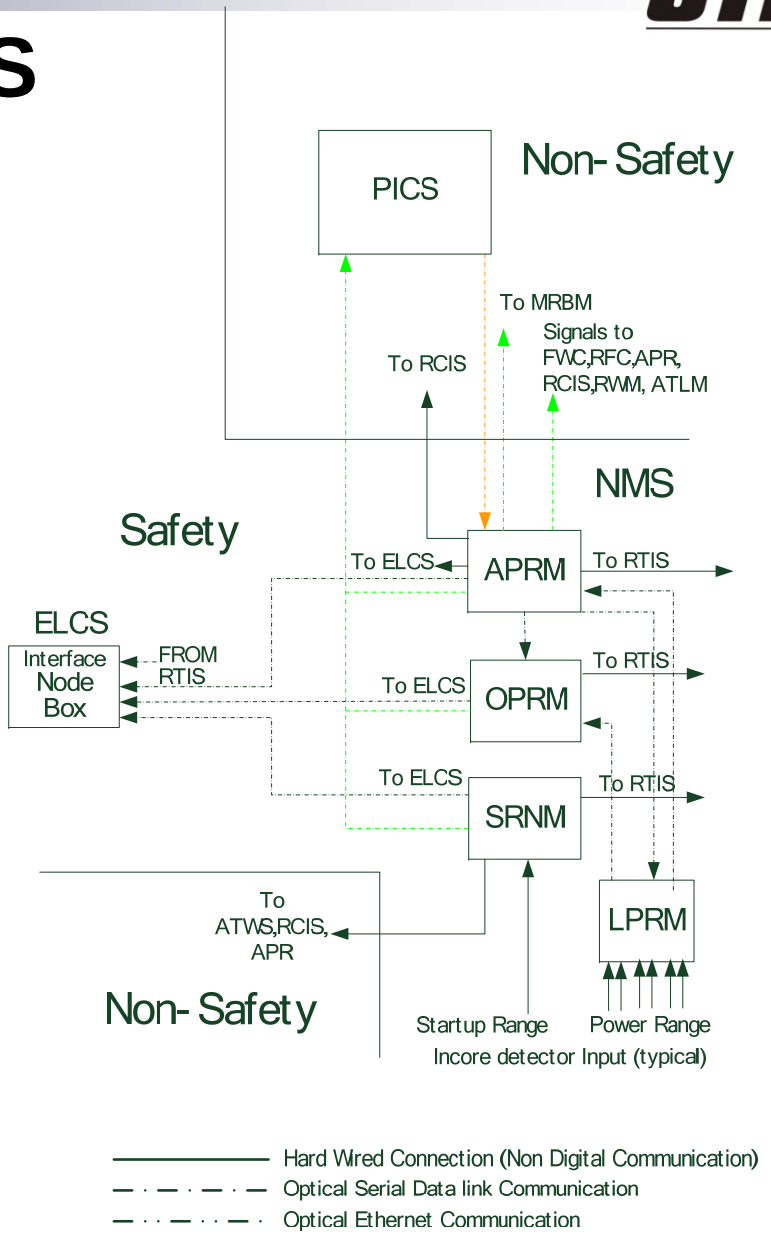
Communication in NMS

- 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)



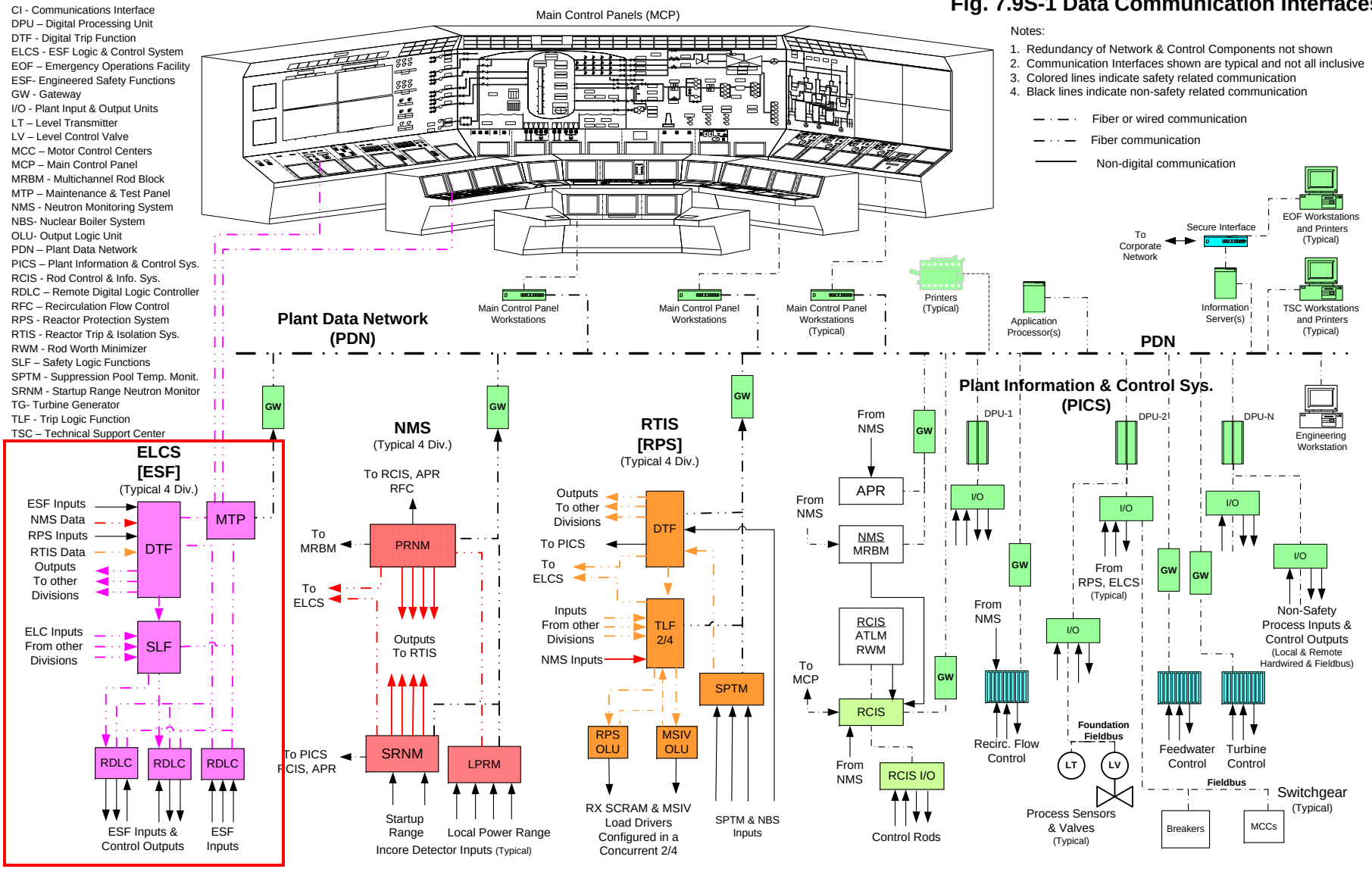
Non-Safety to Safety Calibration Communication in NMS

- 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

Notes:
1. Redundancy of Network & Control Components not shown
2. Communication Interfaces shown are typical and not all inclusive
3. Colored lines indicate safety related communication
4. Black lines indicate non-safety related communication



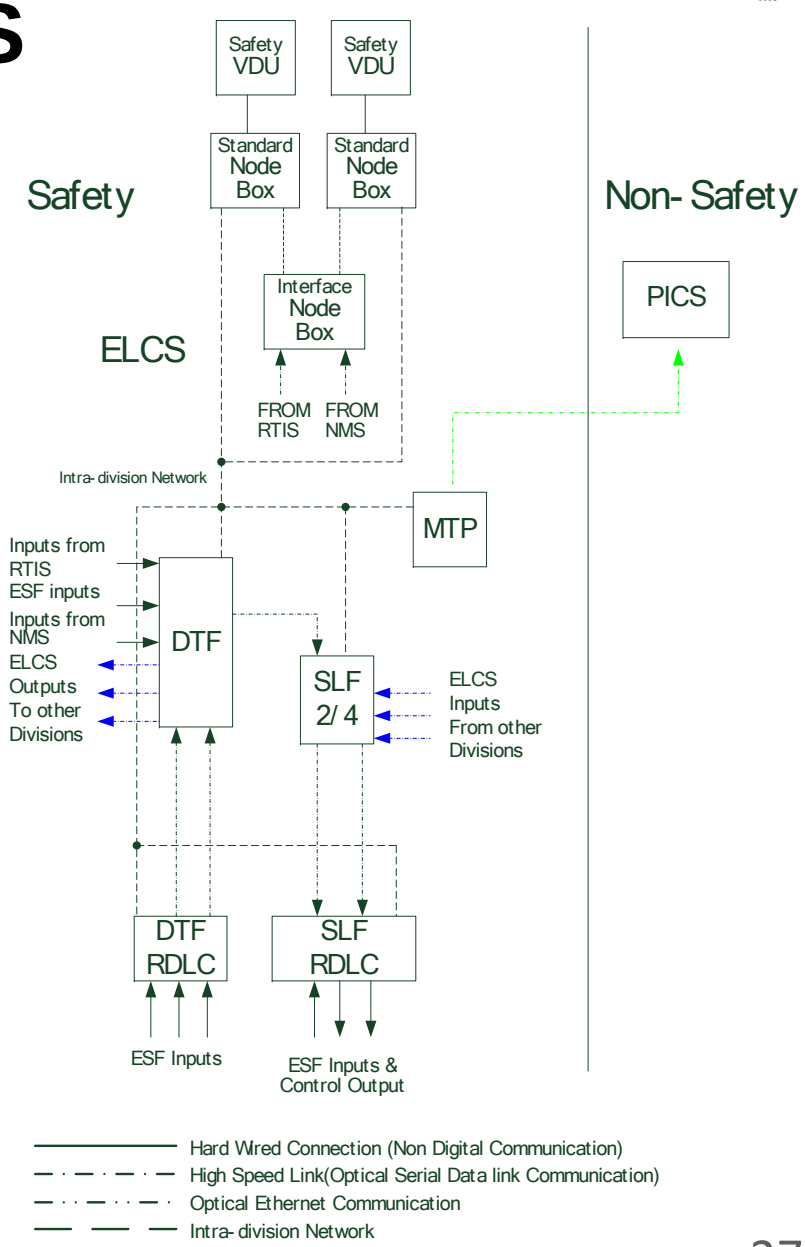
Features of Communication Design (ELCS)

- 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

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

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

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

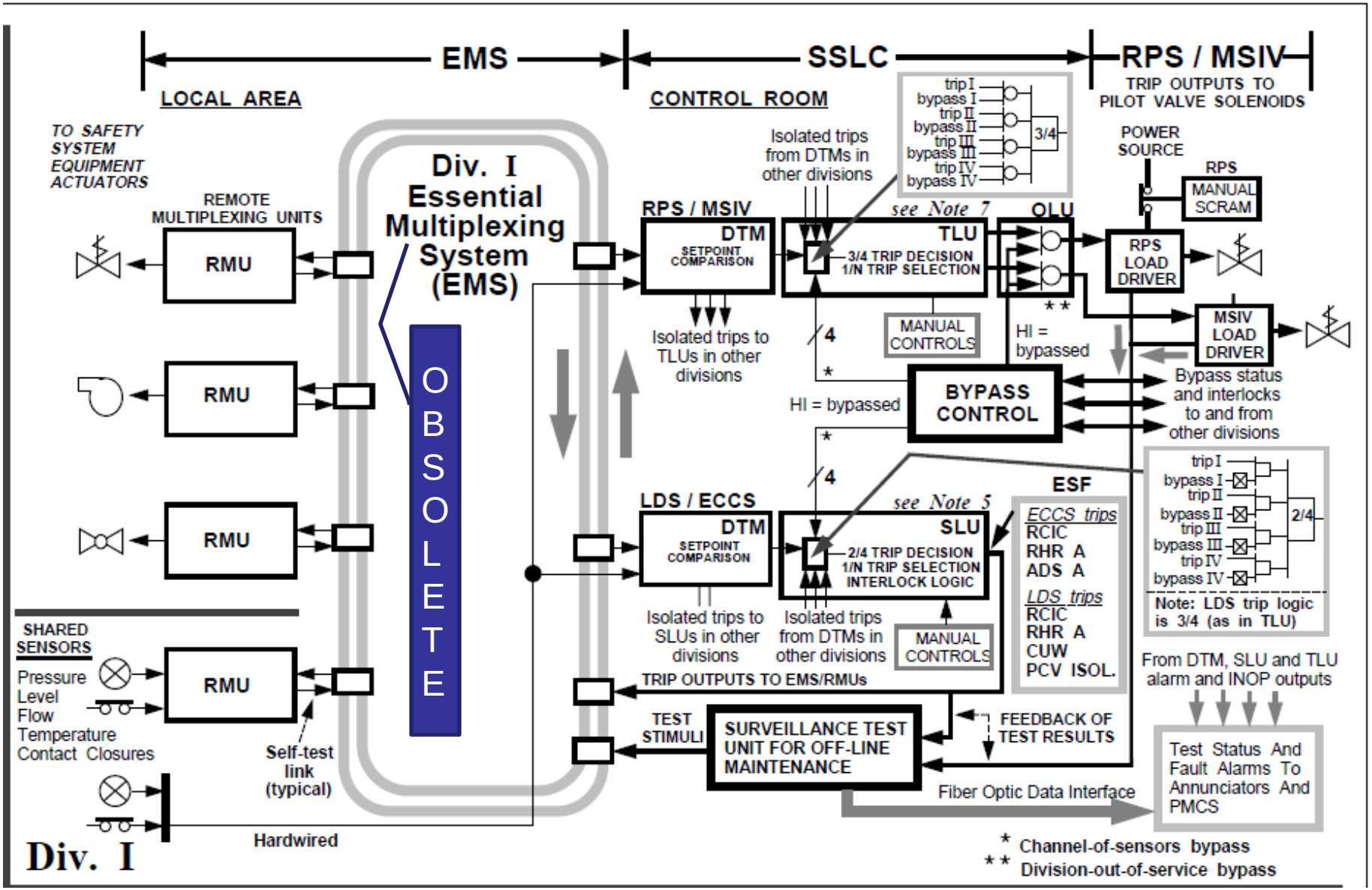
ACRS Items of Interest	•Diversity and Defense-in-Depth •Independence of Data Communication Functions •Deterministic Features of Data Communication Functions •Simplicity of I&C Design
Open Items	All of 4 open items in the SER with OI (Phase 2) have been closed and are being tracked as confirmatory items. One new open item identified after SER issuance.

Tier 1 Departure T1 3.4-1

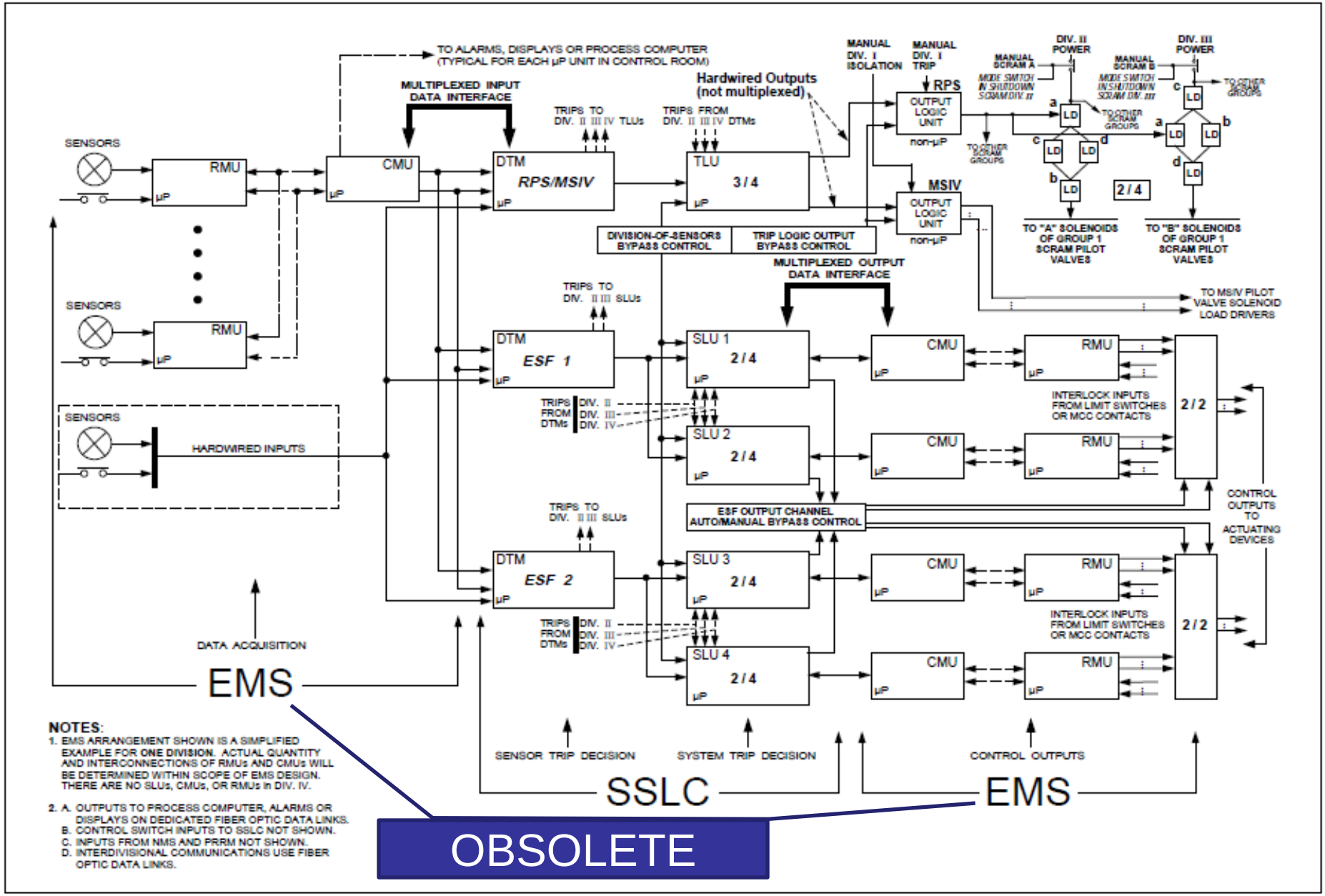
- Brief description
  - I&C design for STP 3 & 4 incorporates by reference the certified ABWR DCD with one significant . This departure primarily resolves issues associated with obsolete data communication technology used in the certified ABWR Safety System Logic and Control (SSLC) design. Tier 1 departure 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



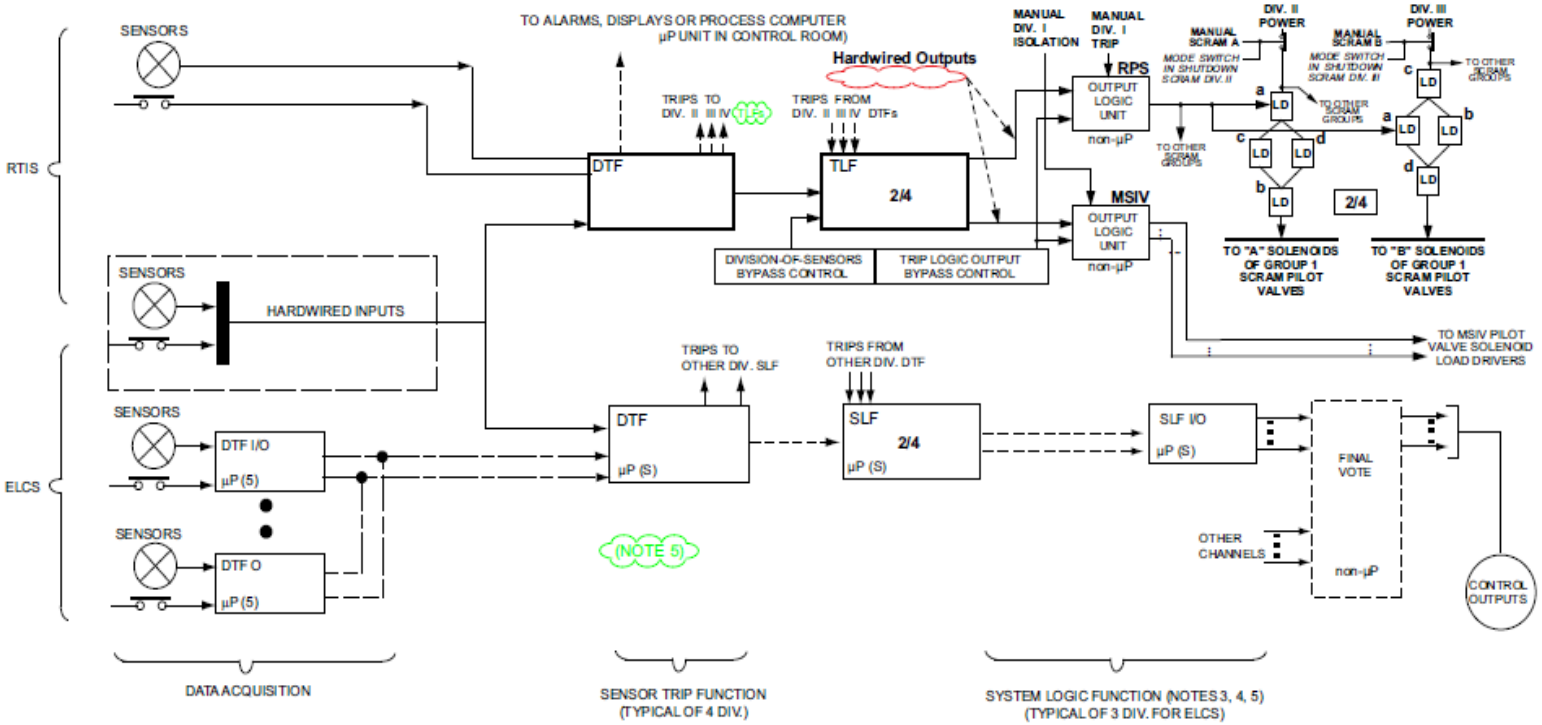
ABWR DCD Figure 3.4b SSLC Block Diagram

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

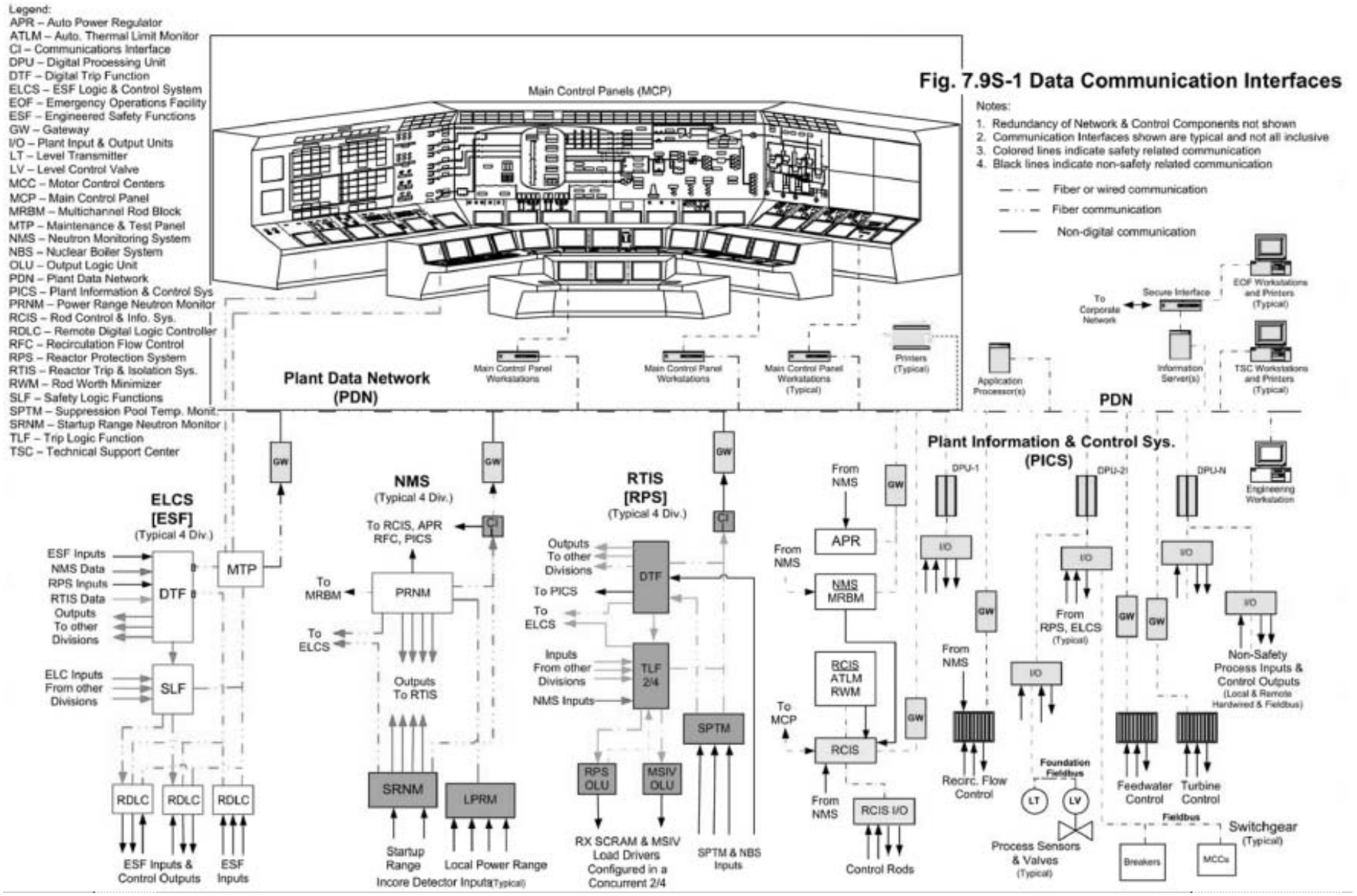
2. A. NOT ALL CONTROL SWITCH INPUTS SHOWN.
   B. INPUTS FROM NMS AND PRM NOT SHOWN.
   C. INTERDIVISIONAL COMMUNICATIONS USE FIBER OPTIC DATA LINKS.

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

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

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.

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.

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.

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 separate (**post COL**) activity, 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)

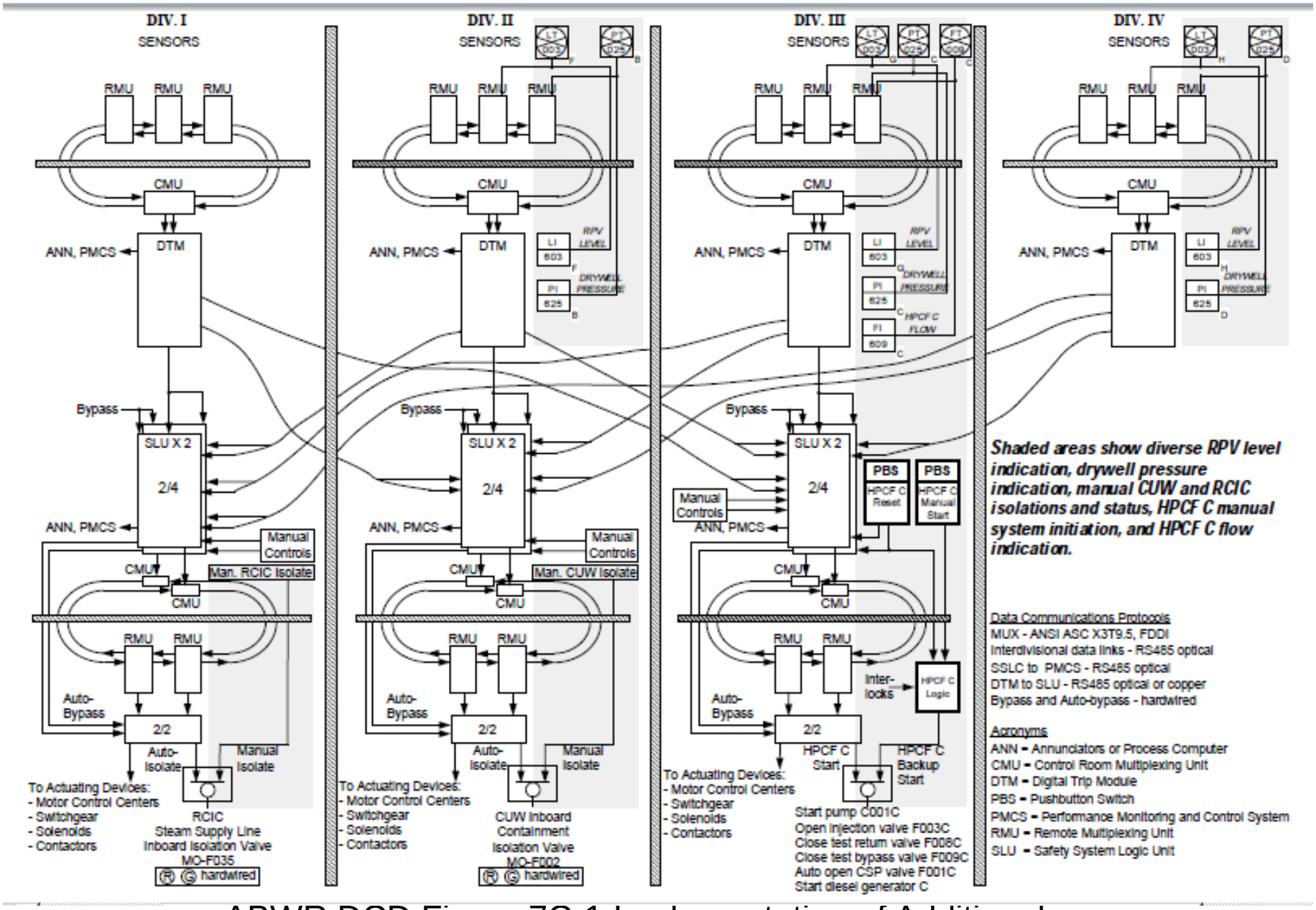
- Specific items of interest
  - This technical report is prepared by Westinghouse for STP 3 & 4 to document the instrument uncertainty calculations for the RPS and ESF functions for the ABWR plant.
  - This STP 3 & 4 ABWR setpoint methodology is similar to the AP1000 setpoint methodology topical report.
  - 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)

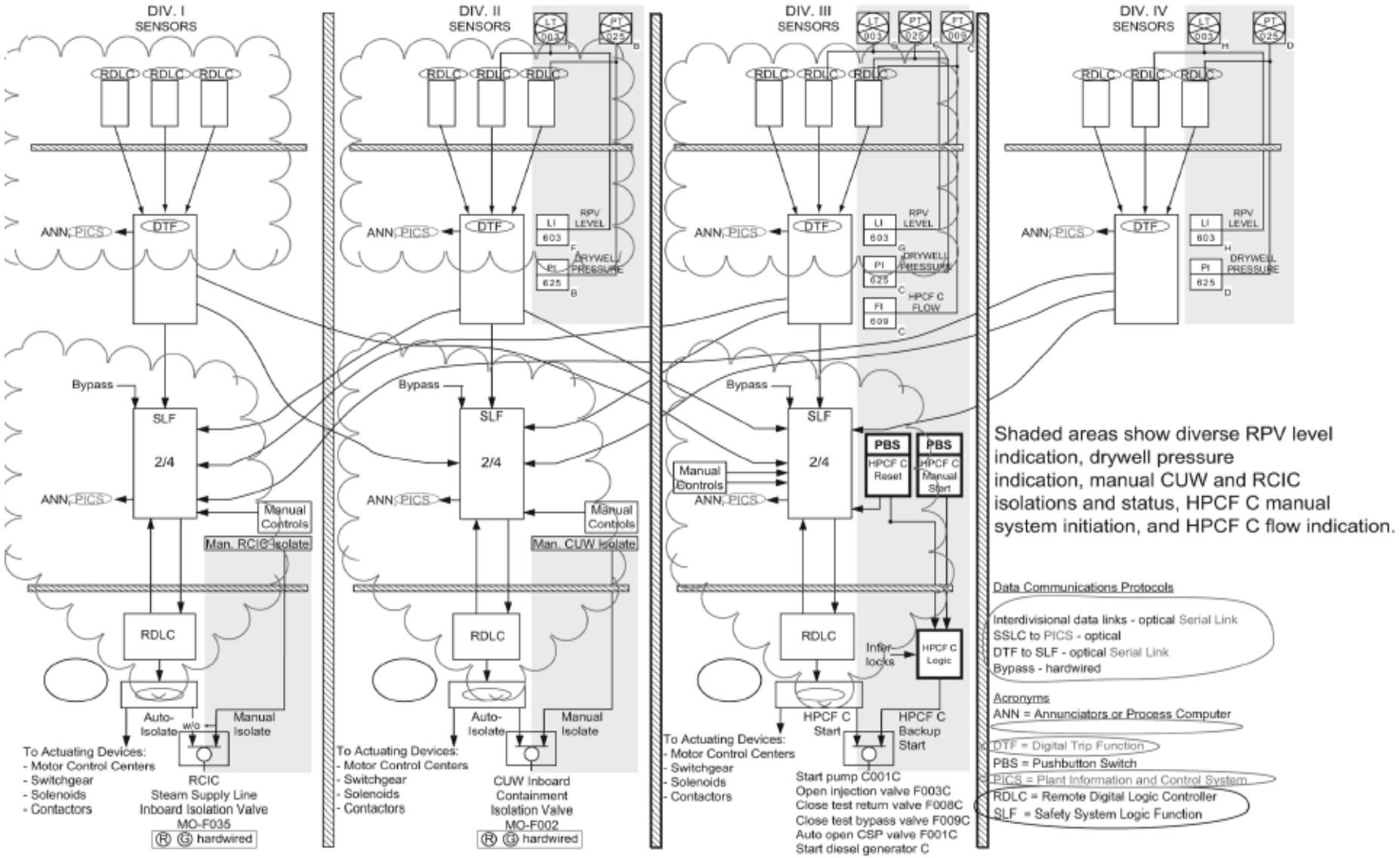
- Conclusion
  - As a result of one open item identified above, the staff is unable to finalize its conclusions relating to “Instrument Setpoint Methodology” in accordance with the NRC requirements.

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.

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.

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 operate deterministically 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.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Simplicity of I&C Design (continued)

- Specific items of interest
  - Examples of simple safety system I&C design features:
    - Each SSLC division is independently controlled from a set of dedicated safety FPD (flat panel displays) in the main control room.
    - Only one-way communication is allowed from SR to NSR components.
    - Microprocessors are used for making “simple” logic decisions.
    - Software is developed as a structured set of simple modules.
    - Each module performs a prescribed task that can be independently verified and tested.
- Conclusion
  - STP 3 & 4 digital I&C design follows the philosophy of simple design employed in the certified ABWR design.

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