<u>DISCLAIMER</u>

UNITED STATES NUCLEAR REGULATORY COMMISSION'S

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

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

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

Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, October 22, 2009

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

1   UNITED STATES OF AMERICA

2   NUCLEAR REGULATORY COMMISSION

3   + + + + +

4   ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

5   (ACRS)

6   + + + + +

7   SUBCOMMITTEE ON ESBWR

8   + + + + +

9   OPEN SESSION

10   + + + + +

11   THURSDAY

12   OCTOBER 22, 2009

13   + + + + +

14   ROCKVILLE, MARYLAND

15   + + + + +

16   The Subcommittee convened at the Nuclear

17 Regulatory Commission, Two White Flint North, Room

18 T2B3, 11545 Rockville Pike, at 8:30 a.m., Dr. Michael

19 Corradini, Chairman, presiding.

20

21 SUBCOMMITTEE MEMBERS PRESENT:

22   MICHAEL CORRADINI, Chairman

23   WILLIAM J. SHACK, Member

24   JOHN W. STETKAR, Member

25

CONSULTANTS TO THE SUBCOMMITTEE:

    THOMAS S. KRESS

    GRAHAM B. WALLIS

NRC STAFF PRESENT:

CHRISTOPHER BROWN, Cognizant Staff Engineer

    KATHY D. WEAVER, Cognizant Staff Engineer

    AMY CUBBAGE

    IAN JUNG

    DENNIS GALVIN

    HULBERT LI

    LAURA DUDES

ALSO PRESENT:

    HERBERT BUTLER

    RICK WACHOWIAK

    IRA POPPEL

TABLE OF CONTENTS

1

2

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

4   (11:20 a.m.)

5   CHAIR CORRADINI: Why don't we get

6   started? So, we're in our third day of our ESBWR

7   subcommittee for the ACRS. My name is Mike Corradini,

8   Chair of the subcommittee.

9   Today, we have a new group, or a modified

10 group of subcommittee members in attendance.

11 Professor Abdel-Khalik will be here eventually. I

12 think Dr. Armijo and Dr. Banerjee may not be here, but

13 we have a new member Dr. -- or Mr. Stetkar. Excuse

14 me. Don't want to give you that vaunted title. As

15 well as our consultants, Tom Kress, Graham Wallis and

16 Bill Shack.

17   The purposes of the meeting again is to

18 review resolution of reactor systems, mechanicals

19 systems and I&C systems, and cybersecurity issues for

20 the ESBWR design certification. I will skip over a

21 lot of the preliminaries since we've been discussing

22 this throughout the week. We have with us today GEH

23 Nuclear Energy, as well as the staff, and our main

24 focus today will be on instrumentation and control

25 systems.

1 Let me remind everybody the rules of

2 participation in today's meeting. They've been

3 announced as part of the notice of the meeting in the

4 Federal Register on September 28th. A transcript of

5 the meeting is being kept and will be made available

6 as stated in the Federal Register notice.

7 It is requested that speakers first

8 identify themselves and speak with sufficient clarity

9 and volume so that we can readily be heard. And also,

10 I wanted to make sure everybody puts their cell phones

11 on silent mode.

12 We have not received any requests from the

13 members of the public to make comments, okay? But we

14 do have a bridge line open. We are going to have two

15 parts to the meeting. Before our break, we're going

16 to have discussions on I&C that will be open, and we

17 have an open bridge line. Then after the break, we

18 will go into closed session because some issues that

19 are going to be discussed are protected information,

20 designed as part of the proprietary work of GEH

21 pursuant to 5 USC, or security related information.

22 I'll ask the staff if they have any other

23 comments before I turn it over to GEH.

24 MS. CUBBAGE: Sure. I'll just give a

25 brief background of the topics and why we're here.

1 The first topic is a follow up from the subcommittee

2 meeting we had almost a year ago now, December last

3 year.

4 There was some specific items of concerns

5 that were addressed by the subcommittee. I'll note

6 that Charles Brown was one of the ones that had some

7 significant comments, and I'll note that he's not here

8 today. So, I hope that this information gets back to

9 him because we're not going to be able to go through

10 this level of detail at the full committee.

11 Also, we have an additional topic of

12 cybersecurity. That's a topic report that the

13 committee has not heard about before. So, those are

14 the two topics today, and I'll introduce -- did you

15 want to go ahead to GE now?

16 CHAIR CORRADINI: So, just go ahead to GE.

17 Is Rick going to lead us off, or Ira? Who is --

18 MR. BUTLER: I'll lead off.

19 CHAIR CORRADINI: Herbert will be first.

20 MR. BUTLER: It's Skip Butler. Herbert is

21 my full name. I'll be the lead presenter on the ESBWR

22 Engineer Manager for I&C. On my right is Ira Poppel.

23 He's principal engineer and lead designer for I&C on

24 the ESBWR, and to his right is Lloyd Heckle, who is

25 our software QA manager, and who has been instrumental

1 in developing some of the things that we'll present

2 here today.

3 Also, you'll hear later from Matt Bohne,

4 who is our cybersecurity lead. He'll join us at the

5 front at that time. Okay, if we could go to the next

6 slide, Rick?

7 Just to step through the high level

8 topics, we'll talk about the changes from Rev 5 to Rev

9 6. They have been substantial. When we met on

10 December 3rd, there was a lot of work in progress, but

11 unfortunately for the ACRS committee at that time, you

12 weren't privy to it because it wasn't part of Rev 5.

13 But there has been a significant amount of work done

14 over the last nine months. That's to say the 4th

15 quarter of `08 through June, when we submitted the

16 preliminary copy of DCD Rev 6.

17 We got some feedback from that meeting,

18 from the ACRS, and we'll touch on that. We broke the

19 pitch into three main parts: regulatory compliance,

20 the software systems and software design process, the

21 I&C design principles, which really focus on IEEE

22 standard 603 compliance, which really stands the test

23 of time, even in the digital age. Then we'll close

24 for some questions.

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

1 just like to highlight the topics on the right. The

2 RAIs are obviously the staff's request for additional

3 information. The ECAs are engineering changes from

4 GE. The cars are the corrective actions; the LDRs are

5 minor licensing deficiency reports or tracking items.

6 CONSULTANT WALLIS: Let me interrupt with

7 a question. I mean principles is a long way from

8 final product. How do you know when the final product

9 is good enough? You can have determinacy to infinity,

10 or a tiny bit of it. How do you know when it's enough

11 with I&C?

12 MR. BUTLER: We will present that in one

13 of the slides, and there's actually a backup

14 calculation that demonstrates that.

15 CONSULTANT WALLIS: So, you're going to

16 get to that?

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

18 CONSULTANT WALLIS: Principle seems an

19 awful long way. It's like saying you've got the

20 general design criteria, and now you've got the

21 answer.

22 MR. BUTLER: I think we have a bit more

23 than that, and we hope to convince you of that. Okay,

24 just to highlight on this, I would say there's been a

25 substantial amount of work first suggested to us in

1 RAIs from the staff, but also we took those RAIs, and

2 ensured through our appendix B program that the

3 conforming changes that were necessary through the

4 LTRs and through the entirety of the document all

5 chapters were addressed, and that's why the GE driven

6 component is there.

7 So, the guidance back from the ACRS

8 committee on the 3rd of December can really be

9 summarized into two main points. One was a concern

10 about the design and development process for digital

11 I&C for the ESBWR, and the ACRS committee asked for

12 RAIs to help highlight and expand upon that.

13 Actually, the majority of those RAIs the

14 staff had already issued to us. They just weren't

15 ready for submittal, and so they weren't presented on

16 the 3rd of December. The second point has to do with

17 level of detail. Again, there were a number of RAIs

18 culminating in our last RAI, which is RAI 7-1.139,

19 which really spoke to additional level of detail, and

20 we'll present that as well.

21 Okay, just to add some perspective around

22 the recommendation for enhanced design process, and

23 the DACs to support it, there was about an 80 percent

24 increase in DACs from Rev 5 to Rev 6 for I&C, and if

25 you just look at the perspective here, whether you

1 look at the DCD page count, or the chapter count, the

2 number of DACs for I&C are 663, okay? So, I'd like to

3 present that in a little bit more explanation. So,

4 hold on.

5 So, the first part of that is that if you

6 look at a digital implementation, a significant part

7 of that is the applicant software that is going to be

8 the first of a kind for any new plant to be licensed

9 in this country. So, if you follow the IEEE standards

10 for a system and software development process, GEH

11 thinks that you have to have a number of specific

12 design, audit and hold points. Those are all very

13 well articulated in our LTRs for the software

14 development plan, the software QA plan and

15 cybersecurity plan.

16 And so, really a significant number of

17 these DACs are specific to ensuring that all

18 applications on all the software platforms adhere to

19 the IEEE standards, starting with 603, and follow a

20 structured approach with traceability.

21 The rest of them are based upon ensuring

22 that functions to be performed on each one of those

23 platforms for the safety function are met and

24 testable. That's where the DACs and ITAACs come from,

25 and they're really based on that, as well as the

1 diversity that we have in our overall system, which

2 we'll hit later.

3   Okay, to speak -- one example to provide

4 additional design detail, the last RAI that we

5 received on this topic, and there were several, is RAI

6 7.1-139, and specifically the staff asked us to

7 provide additional architectural detail and design in

8 block diagram format to ensure that there was a real

9 design for each one of these safety functions within

10 each platform.

11   And so, we've done that by adding eight

12 new figures, revising nine figures, and obviously,

13 there's a significant amount of table and text that

14 goes with those revisions to the DCD.

15   MEMBER STETKAR: Are you going to go

16 through some of those figures later, because --

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

18   MEMBER STETKAR: Okay. Let me ask a

19 fundamental question then because we did raise the

20 issue about two years ago of why GEH does not include

21 in the DCD functional logic diagrams that show the

22 actual -- I'm not talking about details now, middle-

23 level information, signal inputs, coincident logic,

24 including interlocks, manual signals, automatic for

25 each -- for all of the protection and safeguards

1 functions. We've been asking for that now for two

2 years, and we still don't have it.

3 MR. BUTLER: I would note, and this is

4 perhaps not tactful, that all of the other vendors are

5 including those in their DCDs so that we can indeed

6 look at an integrated instrumentation and controlled

7 system design, and determine what signals are the

8 input signals, how those signals are processed in real

9 logic, how they're combined with both manual inputs

10 and interlocks, time delays, and look at the output

11 signals.

12 That's very, very important for a design

13 overview to see how the integrated design will really

14 work for pinch points. We've learned an awful lot in

15 30 years of experience that adhering to very focused

16 specific design criteria for individual functions does

17 not necessarily provide an integrated design that

18 indeed is a -- I don't know what the correct word to

19 use is. Perhaps prudent design is the best word.

20 And yet, we still don't see those logic

21 diagrams that -- that the -- the eight diagrams that

22 you've mentioned are not that type of diagram.

23 They're a much simpler, higher-level non-specific type

24 of information.

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

1 year ago with respect to the information regarding the

2 integrated design at that level of detail. And again,

3 I'm not -- don't get me wrong. I'm not trying to

4 emphasize detail of -- of chip sets or lines of code,

5 or anything there. I'm back up at somewhere between

6 the information that exists now in the DCD, and -- and

7 basically the equivalent of the information that is

8 traditionally provided in a Final Safety Analysis

9 Report.

10 MEMBER STETKAR: So, there must've been an

11 active decision made about why those types of diagrams

12 were not included in the DCD, and I'm rather

13 frustrated about that.

14 MR. BUTLER: Okay, so we have shared in an

15 informal way the preliminary logic diagrams with the

16 staff. They've been given an opportunity to walk

17 through those. What we were asked to do in the RAIs

18 was to provide additional detail at the level of the

19 block diagrams. We've done that.

20 What we've committed to do with the

21 extensive number of DACs is to provide the information

22 related to the detail design, the logic diagrams, the

23 SDSs. All of that material that you may be seeing

24 with the other vendor submittals will be available to

25 staff review through the DAC process. So, we're not

1 trying to not provide that information. We're

2 providing that information at a later date using the

3 DAC process, and the LTR's that we've committed to are

4 extremely vigorous with hold points that allow for

5 these review packages to be developed for staff audit.

6 MS. CUBBAGE: I just wanted to clarify. I

7 think you said they were provided informally. They

8 were provided on the docket, which is not part of the

9 DCD.

10 CHAIR CORRADINI: Okay, say that again,

11 Amy. I'm sorry.

12 MS. CUBBAGE: The logic diagrams were

13 submitted on the docket, and provided to the ACRS.

14 MEMBER STETKAR: Okay, two questions.

15 Yes, indeed, we -- we got those, and I have them. I

16 looked at them two years ago. But it was my

17 understanding that they were not necessarily directly

18 related to the ESBWR; that they might be somewhat

19 preliminary and generic in nature, at least the set

20 that I saw.

21 MS. CUBBAGE: Well, they're related to the

22 ESBWR, but they are not -- they don't have finality.

23 MEMBER STETKAR: Right. Well, I guess the

24 concern that I have is that if the design is not final

25 at that level, what design are we certifying? If the

1 design is not final because these diagrams are

2 preliminary, and for whatever reason are not included

3 in the formal design control document, what exact

4 design are we certifying? I mean the -- because

5 they're not final, and won't be final until apparently

6 few -- prior to fuel load, at least on North Anna.

7 MS. CUBBAGE: I think it'd probably be

8 best if we let GE continue, and you can ask that of

9 the staff when we present.

10 MEMBER STETKAR: Okay.

11 MS. CUBBAGE: But I guess the bottom line

12 is that's currently not a level of detail that we are

13 reviewing for certification.

14 MEMBER STETKAR: Okay.

15 MR. BUTLER: Okay, next slide. Okay, what

16 we wanted to show here was the rigor with which in

17 tier 2 chapter 7, we've identified the regulatory

18 requirements for each one of the platforms. So, in

19 this chart, upper left, you'll see that there is a

20 series of columns, each one of those columns

21 represents one of the systems rolling up to one of our

22 diverse platforms. We have three diverse safety

23 platforms for our D3, and on the left are all the

24 regulatory requirements specific to a digital INC,

25 software-driven system.

1   The middle chart on the left takes that

2   one step further, where we've taken all of the

3   critical 603 criteria, and we've also associated them

4   very explicitly with each one of the systems that roll

5   up to the platforms. Then within each section of the

6   chapter, there are summary regulatory conforming

7   statements having to do with things outside of digital

8   INC and software instrumentation and so forth.

9   So, that creates the entire packet for

10 chapter 7 of the Regulatory Compliance. We've done

11 that in a structured way so that we can have a cross-

12 reference and traceability mapping to the Tier 1

13 commitments. The Tier 1 commitments basically have

14 two components. One is the system-driven or NPL

15 driven aspects of each one of the systems and

16 functions for the safety system, and then the Tier 1

17 DAC and ITAACs. There's a complete traceability

18 matrix for all of that.

19   MEMBER STETKAR: Again, I haven't been

20 reading through your slides quickly enough. So, slow

21 me down.

22   MR. BUTLER: That's okay. The first part

23 you can take advantage of once in a while.

24   MEMBER STETKAR: Okay, I'll do that. Was

25 there a change between Rev 5 and Rev 6? You mentioned

1 now that you have three -- you call them independent

2 diverse platforms. In Rev 5 there were -- in my

3 thinking, I'm not a digital INC design guy. There

4 were three platforms. How -- have you made changes

5 between 5 and 6 to the definition of those platforms,

6 if I can use that term?

7 MR. BUTLER: No, no. The only thing that

8 we've done --

9 MEMBER STETKAR: Because there's not an

10 ICP that used to be the ATWS Standby Liquid Control

11 System.

12 MR. BUTLER: Right. So, in the first

13 slide I tried to show that there were a number of

14 LDRs, licensing deficiency reports, that were raised

15 internally to identify a lack of clarity and

16 consistency with which we described the architecture

17 in the system. So, really, from Rev 4 through Rev 6,

18 the architecture has not changed.

19 MEMBER STETKAR: The architecture is

20 basically the same, okay. That's what I thought. I

21 just wanted to make sure that there was more of a

22 descriptive process than kind of what you're --

23 MR. BUTLER: Right. And so, with that as

24 the backdrop, what we did do with respect to an ECA

25 was to add one additional implementation of ICP, which

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

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

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

MEMBER STETKAR: Okay.

CHAIR CORRADINI: Will you be here in November?

MEMBER STETKAR: Yes.

CHAIR CORRADINI: Good. Let's move on.

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

1   Okay, so we need to have a software and

2   systems development process. Ours is IEEE compliant.

3   We've worked on this for a number of years to ensure

4   that we have one that will stand the test of time in

5   an implementation for the entirety of the DCIS. What

6   this chart tends to show is in the first waterfall

7   model, our software management plan, which really

8   serves as the overall framework or skeleton for the

9   development of the I&C systems in hardware and

10   software.

11   To the bottom left -- excuse me, to the

12   upper right is our software quality assurance program

13   manual, and the fact that these DACs and ITAACs are

14   just a sampling of the design and hold points where an

15   independent review will occur, either a peer review or

16   verification review, to substantiate that the design

17   is ready to proceed.

18   Then   in   the   bottom   left   is   the

19   cybersecurity program plan. You'll hear more about

20   that in our closed session.

21   The important thing here is that these

22   three documents work together so that all of the

23   entrance and exit criteria to a review step are

24   integrated with one another; they're traceable, and

25   they're documented with reports and bases documents in

1   our documentation control system.

2   Okay, so for the procedure design and the

3   design principles, really we wanted to focus on five

4   main themes: simplicity, independence, redundancy,

5   determinacy or deterministic behavior, and diversity.

6   CHAIR CORRADINI: This looks like

7   something I have at the university. I like this

8   foundation.

9   MR. BUTLER: We try and have one.

10   CHAIR CORRADINI: Thank you.

11   MR. BUTLER: Otherwise, we wander.

12   CONSULTANT WALLIS: It's so high-level.

13   This looks like a preliminary lecture, though.

14   CHAIR CORRADINI: Well, this is -- I

15   understand this. Keep on going.

16   MR. BUTLER: Okay, so -- all right, so the

17   next -- okay, so it's sometimes useful to define our

18   system based upon what we do, and what we don't do.

19   So, I just want to make it very clear to the staff,

20   and to the ACRS committee that is reviewing many

21   designs, both in the retro-fit fleet, and new units.

22   What we don't do: we do not mix signals of

23   safety and non-safety in a prioritization module

24   concept. That is not what we do for the ESBWR. We

25   keep each one of our safety functions, subsystems and

1 platforms independent, separate, isolated and diverse

2 to achieve all the safety functions including diverse

3 actuation.

4   Okay, so let's take a look at RPS, Reactor

5 Protection. This is a derivative block diagram from

6 7.2-11a, which is in the back up, and what we try to

7 convey here very clearly is everything is broken down

8 into simple blocks for sense, command and actuate.

9 Each one of these functions is clearly defined in the

10 system design descriptions, and the logic diagrams,

11 and in the implementation and hardware that we have

12 that is targeted. Mike?

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

14   MR. BUTLER: Okay.

15   CHAIR CORRADINI: I'm trying to look for

16 things as you're talking. I'm sorry. Excuse me.

17   MR. BUTLER: Okay. So, what we're trying

18 to convey here is that is that an implementation of a

19 power plant's DCIS is a very complex endeavor, and

20 will be a very complex delivery, but you need to break

21 it down into simple parts.

22   So, we have a lot of simple parts, but

23 each one of the simple parts basically follows this

24 approach: there is a solution to be achieved. There

25 is a platform, a diverse platform, picked to implement

1 it on. It is broken down into system functions and

2 components, and each one of them is clearly

3 identifiable, and where appropriate has an audit and

4 hold point in the three LTR's, and a sample thereof is

5 in DAC or ITAAC.

6   Okay, go to the next chart. Okay,

7 independence: this is a bit of an eye-chart, but

8 you'll see at the bottom below the big, dark line, the

9 safety system and the four divisions. So, each one of

10 the shades of green represent a clear and distinctly

11 separate implementation per division for the three

12 diverse platforms.

13   So, we'll see this chart again when we

14 talk about diversity, but it's important to note that

15 the only communication that is allowed to occur

16 between RTIF, NMS, as well as in that layer and

17 between SSLC/ESF and the four divisions of that layer

18 is the two-out-of-four voting, which we've had in the

19 analog days as well. That is the only thing that

20 communicates between those four divisions. Nothing in

21 the safety system communicates with DPS, which is in

22 the shaded blue.

23   Okay, so the next chart. Okay, in the

24 area of redundancy, first of all, all of the safety

25 DCIS meets the redundancy principles in IEEE-603 for

1 censors, controllers and actuators. In particular,

2 for SSLC/ESF, that has -- within each division, it is

3 self triply redundant, and that's to ensure that we do

4 not have an inadvertent actuation because that system

5 has the capability of firing the squibs, which of

6 course we want to happen when it needs to happen. You

7 absolutely don't want it to happen when it shouldn't

8 happen.

9   Similarly, all safety DCS design is single

10 failure proof, and this is -- okay, and this is to

11 ensure that there is no unintended, inadvertent

12 actuation throughout -- throughout the system. Okay,

13 in short, the DCIS does not act as a credible

14 initiator to an inadvertent event.

15   Okay, all of it is redundantly powered,

16 primary power, as well as power in the cabinet or the

17 chasse. So, that's to ensure that there is absolutely

18 no reason that safety power doesn't reach the

19 controllers or the IO packs, or anything else. Also,

20 on the non-safety side, we are also redundant. Either

21 dual redundant, or triply redundant.

22   Okay, determinacy or deterministic

23 systems: This was an interesting topic for discussion

24 on the 3rd of December. We do make a commitment to

25 deterministic behavior for the digital I&C, both the

1 | controllers as well as the networks.

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

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

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

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

1 would like to convey very clearly is that for the

2 safety system controllers, as well as for DPS, the

3 communication is buffered or isolated from the

4 controller in its program loop so that the program

5 loop in the controller will always proceed through

6 it's algorithmic process in the stated period of time,

7 independent of whether or not data comes in or not.

8 Of course, the application layer code will

9 look for is the data present, and is the data what I

10 expect? But presence or not of data on the memory

11 busses that the controller can read is not in any way

12 going to adversely affect the programming loop of the

13 controllers used in the safety system or DPS.

14 CONSULTANT WALLIS: Do I misunderstand

15 that is you're asking something to control, the

16 position of a control rod, you can tell it -- you have

17 an input, and then you have to measure where the

18 control rod actually is, and have some feedback that

19 goes back to --

20 MR. BUTLER: Correct.

21 CONSULTANT WALLIS: So, it's not -- it

22 needs the data in order to control properly, doesn't

23 it, to know that it is controlling properly?

24 MR. BUTLER: It does, right.

25 CONSULTANT WALLIS: I get the impression

1   it's also the forward stuff here. You have to have

2   this feedback --

3   MR. BUTLER: Well, we actually have an

4   animation, but we're not allowed to share that with

5   you. But what I would say is that --

6   CHAIR CORRADINI: That helps, thanks. Go

7   ahead,

8   MR. BUTLER: The point that we're trying

9   to convey here is that the data that is required for

10   the application program to run the logic to perform

11   the safety function is made available. Ira, the

12   little pointer? Is made available outside the

13   controller on these shared memory locations.   The

14   shared memory location is an implementation to ensure

15   that the data that is required will appear in the

16   memory register that will be read by the controller,

17   but in a controlled way so that this is isolated so

18   that there's no way for data coming in from this data

19   feed for the data acquisition can interrupt the

20   programming or the memory used to run the program.

21   The controller is isolated from that

22   portion of the world that it needs to interface with.

23   CONSULTANT WALLIS: But whether it works

24   or not cannot be independent of the mechanics of the

25   thing it's controlling, can it?

1   MR. BUTLER: Again --

2   CONSULTANT WALLIS: I don't see how I&C

3 can ever be designed by itself, because it's

4 controlling something which itself has response

5 characteristics.

6   MR. POPPEL: There are -- there are two

7 answers -- directions your answer can go. The first

8 thing is these are safety systems, and as indicated,

9 VPS. Okay, they're doing things like saying, we need

10 to make sure that when the reactor level gets here,

11 the reactor scrams. Okay, that's the control loop.

12 They -- the visions acquire their own data at a

13 specific time in the --

14   CONSULTANT WALLIS: It tells a lot about

15 the thing which is measuring the level, then this can

16 affect the whole system, can it not?

17   MR. POPPEL: For that division.

18   CONSULTANT WALLIS: Yes. So, you have to

19 know something about things that can happen to the way

20 in which you measure the level, and when you design

21 the controller, don't you?

22   MR. POPPEL: Yes.

23   CONSULTANT WALLIS: Or, is it completely

24 independent?

25   MR. POPPEL: No. We have data quality

1 checks, okay? But for example, we can't fix or deal

2 with a broken transducer.

3 CONSULTANT WALLIS: No.

4 MR. POPPEL: If the transducer is

5 erroneously indicating level, okay, then we say,

6 there's our divisional failure. We've got three other

7 divisions where -- and in our case, we could have two

8 other divisions that are -- assume correctly

9 indicating level, and that two-out-of-four voting

10 logic in all divisions will result in the right thing.

11 The point is the acquisition of level in -

12 - within the division is the control loop. The data

13 coming in horizontally, the two-out-of-four data from

14 the other divisions trip data is asynchronous.

15 Division 1 can't control or ask, or deal with when Div

16 2 sends it in. It's just that Div 1 looks, and it's

17 memory location 3, and sees that there's two trip data

18 without any indication of how it got there, when it

19 got there, or why it got there, okay? And so, that's

20 this.

21 The thing you mentioned about control rod

22 positioning isn't a safety system in the ESBWR, and

23 you are correct that obviously if you're positioning a

24 control rod, you need to have feedback where it is.

25 That reverts to Skip's previous comment in that the

1 reactor can -- the rod control and information system,

2 RCIS, is its own system.

3 In other words, it needs to know where

4 control rod position is. It measures control rod

5 position redundantly. It pulls it. So, RCIS is

6 saying, I'm responsible for knowing where it is. And

7 by the way, I'm not getting that data from some other

8 system over the network. It's my system.

9 Okay, now I happen to send that data to

10 other networks so other people can see rod position,

11 but I don't care whether other people see rod

12 position. I can control rods whatever happens to the

13 data once it leaves me.

14 And so, yes, we do have that, but that's

15 non-safety. It's not quite the same thing as this,

16 but we don't mix control over the network. Another

17 way of saying that is our non-safety networks can go

18 down, and all the controllers will control

19 autonomously. Completely they could go down.

20 They won't go down because they're

21 redundant. They've got all kinds of good stuff that

22 Skip mentioned, but nevertheless, we are not dependent

23 on them for anything but operator input, alarms and

24 stuff like that. Plant stability and control is

25 assured without the networks.

1   CHAIR CORRADINI: Okay, go ahead.

2   MR. BUTLER: Okay, determinacy in the

3   communications.   So, we have a lot of communication

4   data   links.   We   call   them   networks   or   network

5   segments.   We wanted to show some examples, and to

6   discuss briefly how they are deterministic.

7   So, in RTIF, there are intradivisional

8   communications.   We're showing those in blue, and we

9   have interdivisional for the two-out-of-four voting.

10   And we have a safety network, which is communicating

11   to the non-safety, and that's in green.   The green and

12   blue are implementations in Scramnet, which is a brand

13   name   for   Reflective   Shared   Memory,   which   is   a

14   mechanism whereby you design and configure the network

15   and   its   nodes   so   that   it's   deterministic   what   the

16   network it, and when you configure and deploy the

17   network, it becomes totally hardware based.   There's

18   not   a   software   overhead   that   runs,   and   the

19   communication happens by having each node broadcast to

20   the appropriate nodes that it needs to place data in.

21   That   process   happens   on   the   order   of

22   nanoseconds, tens of nanoseconds depending on the size

23   -- no it's microseconds. Sorry, yes. Sorry.

24   MR.   POPPEL: Next   year   will   be

25   nanoseconds.

1 MR. BUTLER: Yes, next year will be

2 nanoseconds.

3 CHAIR CORRADINI: No, I'd just rather have

4 a design that any time -- go ahead.

5 MR. BUTLER: Okay, so microseconds. So,

6 for the purposes of the cycle time required, or

7 response time for the reactor protection system, which

8 for a BWR is in tens of milliseconds, this system is

9 deterministic once deployed and configured. It is

10 hardware based, and it's an order of magnitude, or two

11 or more faster than is required by the reactor

12 protection plant process response times.

13 Okay, that's how we share the data between

14 the divisions, and how we share the data from the RTIF

15 platform to the non-safety broadcast elements in

16 green. Okay, so that's one example of a network

17 implementation that is totally dedicated to this

18 technology platform.

19 In the next slide, we'll show the diverse

20 communication network protocol for the SSLC/ESF. If

21 you go to the next slide, which is 2 of 2. So, again,

22 we have to have a way for the is SSLC/ESF to perform

23 the two-out-of-four voting. We are using Ethernet to

24 do that, and the way in which we assure that this

25 protocol and media is deterministic is to control what

1   is going to be put on the network.

2   So, the message and its content size and

3   the transmit rate that is required in order to achieve

4   the response time for the functions that's being

5   implemented.   So, here we have an Ethernet network.

6   It's 100 megabits or more, depending on when we

7   implement the first one.   And it only is running an

8   infinitesimal amount of data so that for all practical

9   purposes, collisions or the probability of a collision

10   is infinitesimal.   So, this will always deliver the

11   message between the divisions.

12   MEMBER SHACK: This does nothing but

13   deliver the result of the voting?

14   MR. BUTLER: It does nothing but carry

15   bypass status, trip status and message authentication

16   and quality.   So, it only carries three things.   This

17   network, once set up, is between the four divisions of

18   SSLC.   Nothing else will be allowed to be on this

19   network, and it is configured and locked down at the

20   time the system is deployed and tested.

21   It does not communicate with any other

22   network in the safety systems, or a shared non-safety

23   network anywhere.

24   MR. POPPEL: Another way of saying that it

25   doesn't communicate is there isn't any other

1 components of any other network on this network. The

2 only thing on it is Div 1, Div 2, Div 3 and Div 4.

3 That's why we're very sure that it's not going to be

4 communicating with anything else.

5 MR. BUTLER: Okay, so the next one. So,

6 diversity: we feel very strongly that diversity is a

7 critical aspect of safe and reliable digital nuclear

8 power plant. This chart, which is presented both in

9 Chapter 7, Tier 2, as well as in the D3 LTR is our

10 concept for diversity.

11 You'll see on the safety side there are

12 three clearly diverse platforms, RTIF NMS, SSLC/ESF,

13 and the independent control platform. And on the

14 right are the non-safety platforms. The most

15 important one is the DPS in terms of providing for the

16 overall safety functionality of the plant.

17 So, if you go to the next slide, what

18 we've tried to do here is bring this into a derivative

19 graph of Figure 7.1-1. So, here, we're presenting the

20 horizontal layers to clearly communicate that the

21 ICP's in dark green, they are microprocessor and

22 operator -- operating system-free implementations and

23 programmable logic.

24 They are diverse from the RTIF NMS

25 platform, which itself is diverse from the SSLC/ESF

1 platform; each one of them being modular in their own

2 right, in a different technology stack in hardware and

3 software, each one of them not communicating between

4 the layers. And of course diverse protection system.

5 Okay, next chart. Any questions?

6 CHAIR CORRADINI: John?

7 MR. BUTLER: We have backups of many

8 functional diagrams. I think in terms of -- while

9 John is thinking, I'll fill the non-awkward silence

10 space, and say that I think in terms of the key

11 questions that we saw with the staff from the ACRS

12 meeting on the 3rd of December, particularly the

13 comments provided to us by Charlie Brown, we've tried

14 very hard to address them in quite a few RAIs, and

15 self initiated corrections to Tier 1 and the LTRs, and

16 to serve -- have that serve as the basis for the Tier

17 1 DAC and ITAACs, which particularly on the DAC side

18 should assure that the design is safe and fit for use.

19 CONSULTANT WALLIS: So, there's no measure

20 of success at the end? I mean in all design processes

21 I'm familiar with, you have your potential for design,

22 and you set out some specifications and all that

23 stuff. Usually, they have some numbers with them.

24 When you get to the end, you say, did my design meet

25 my objectives? And I've got some measurement I

1   compare it with, specifications, and probabilities of

2   success, and failure and all that stuff, and I know

3   the thing will work according to the way I want it to

4   work.

5   At this time, I don't have any measure of

6   whether it will work according to the way I want it to

7   work. That's the problem I have with the I&C, and I'm

8   just an outside looking in from another field. Is it

9   ever going to happen that you're going to have this

10   sort of --

11   MR. BUTLER: Yes.

12   CONSULTANT WALLIS: -- measure of how well

13   you're doing at the end of it?

14   MR. BUTLER: Yes, and the -- the

15   formulation of those detailed documents are done as

16   part of preparing for each one of the baseline record

17   review events that are part of the life cycle steps

18   that we go through. All of that is identified in the

19   SMPM principally, but complemented by the SQAP, and

20   then the cybersecurity --

21   CONSULTANT WALLIS: I don't know what

22   those mean.

23   MR. BUTLER: Okay, those are the licensing

24   topical reports that describe in detail what the

25   development process is, and for each one of the six

1 primary system and software development lifecycle

2 states, there are clearly described minimum entrance

3 criteria and exit criteria with the requirement that

4 the design basis is thoroughly documented, and that

5 summary audit packages are presented for licensing and

6 staff review.

7 MR. WACHOWIAK: And so, let me -- let me

8 take that one step further, going into what's in our

9 Tier 1 document. Skip mentioned earlier that there

10 are many, many times now in Tier 1 associated with

11 this, and it's just exactly what you're talking about

12 there. There's the step to take the currently

13 reviewed document, like the software management

14 program plan, one of those. It says you need to do

15 something for this platform.

16 We do the something, and that's one of our

17 line items in Tier 1 that gets checked as part of the

18 DAC closure. Then you take that, and you do something

19 else with it. In some cases, it's a -- it's the

20 factory acceptance test. I'll jump down to some of

21 the other steps.

22 Factory acceptance test: that's in Tier 1.

23 We get the factory acceptance test done, and that

24 piece is done as part of the ITAAC closure. Overall,

25 it flows down through the entire I&C platforms. Each

1 one of them has all of the different checkpoints, and

2 in the end, it rolls into the human factors

3 evaluation, verification and validation of the entire

4 thing, which then covers exactly what you're saying

5 you'd have, but it's done in steps that are now, we

6 think, excruciatingly detailed, laid out in Tier 1 so

7 that everybody knows where all the checkpoints are,

8 and what needs to be looked at to be sure that you can

9 proceed onto the next stop.

10 CHAIR CORRADINI: So, I guess the one

11 thing that you said, since again I'm not very good at

12 this, this was not in Tier 1 previously?

13 MR. WACHOWIAK: In Tier 1 previously, we

14 had the high level -- we had high level statements

15 that said, for all the platforms, you do this kind of

16 thing. And it -- it -- the concern was it was not

17 explicit enough that you could go and say, what

18 document do I have to have in my hand to say that we

19 did this thing for all the platforms?

20 It is now very explicit in Tier 1 which

21 information you have to have to say that that

22 particular element is closed, and you've gotten

23 through that step in the lifecycle process, and could

24 move onto the next step.

25 CHAIR CORRADINI: John, did you have a

1 question?

2 MEMBER STETKAR: I do, but I don't know

3 quite how to formulate it, and it's not so much a

4 question. It -- I'll defer to Charlie Brown on the

5 independence and communications. I think he may still

6 have some questions about the interdivisional

7 communications, but that's -- that's his issue, and

8 I'm not going to speak for him in this forum. And

9 he's not here, so he had an opportunity.

10 My concern still remains at the area that

11 I mentioned at the outset, and that is that looking at

12 the instrumentation and control system design, I see a

13 lot of very typical high-level information regarding

14 design principles and -- and functional requirements

15 and things like that, as would apply to any fairly

16 complex system.

17 I now see more detailed information where

18 commitments to confirm that those details are in fact

19 actually implemented according to all of the design

20 criteria, and all of the requirements. It's the

21 equivalent of saying that, I'm going to drive from New

22 York to Los Angeles, and then obey every single

23 vehicular rule in every single locality that I pass

24 through.

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

1 New York to Los Angeles. At the detail, I'm going to

2 verify that I -- that I obey every single rule; that I

3 stop at every single stop sign, and that indeed

4 there's a check that I do that.

5 The problems is that I don't know if I'm

6 going across the United States. I don't know if I'm

7 going through Mexico. I don't know if I'm going

8 through Canada because I don't have that intermediate

9 set of information to tell me how the integrated

10 design will be implemented.

11 I don't actually have that travel route,

12 or I can't find it. And that's -- that's not a

13 question. It's still that same basic concern that --

14 that when being asked, at least at the level I tend to

15 think of a design when being asked to certify a

16 design, I'm missing that fundamental intermediate

17 information.

18 CONSULTANT WALLIS: My -- my problems is I

19 don't know what's my probability of actually getting

20 there. That's what I'd like to --

21 MEMBER STETKAR: Probability is a

22 different issue. We need the route to lay out the

23 probability.

24 CONSULTANT WALLIS: What can go wrong

25 along the way as I take the route?

1   CHAIR CORRADINI: Can we just go back --

2   let me just go back to your comments. So -- so, now I

3   understand the comments. So, the question to them

4   versus the staff is?

5   MEMBER STETKAR: No, it's -- I don't have

6   a question. That's -- I prefaced by saying I don't

7   really have a question. It's a feeling of uneasiness,

8   and it's probably more a question to the staff in

9   terms of what level of assurance does the staff have,

10 and we probably should get the staff up here, and ask

11 them. What level of assurance does the staff have

12 that they have sufficient information at that level?

13 Because I don't have it.

14   I do, as a matter of fact, have copies of

15 those preliminary logic diagrams. I would be pretty

16 happy if they were in the DCD, but apparently GEH

17 doesn't think that's appropriate.

18   CHAIR CORRADINI: So, let me just turn the

19 question so I understand it, John -- or your comment.

20   So, the point is that between the high level, the

21 overall level, and the details, there are examples of

22 the intermediate. But to use your analogy, they may

23 take Route 94, but then again, that's not set in

24 stone. They may decide to take Interstate 70.

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

1 it.

2 MS. CUBBAGE: And I think that the DAC

3 approach is when you take a route that gets you to a

4 safe end product. We don't ascribe that we need to

5 know whether it's this route or that route.

6 MEMBER STETKAR: I think my concern, Amy,

7 and maybe it's better if you come up, but it's for

8 both. It's that 25 years ago, early `80s, we saw

9 several examples where people followed every single

10 detail, deterministic design criterion, and still had

11 a design that followed all of the rules.

12 They stopped at every stop sign, but that

13 particular design had -- had vulnerable pinch points

14 in it, or perhaps from an integrated operational --

15 when I say operational perspective, I don't mean

16 operate the plant, produce megawatts. I mean

17 functional operation of the system.

18 There were things that were overlooked

19 until somebody stepped back and took an integrated

20 look at that design, and said, okay, the decision has

21 been made to actually use this particular route. And

22 indeed, that route is an acceptable route.

23 MS. CUBBAGE: And that information will be

24 available before they install equipment; that

25 information will be available to the staff as part of

1 the ITAAC closure process.

2 MEMBER STETKAR: Except it's my

3 understanding, and this is part of the concern about

4 DAC closure, the discussion we've been having, that if

5 I'm convinced that information will be available, the

6 question is when will it be available, and what will

7 be done with it by whom when it becomes available?

8 Because in particular for the ESBWR, it is not

9 available at the COL stage.

10 MS. CUBBAGE: That's right.

11 MEMBER STETKAR: It will only be available

12 some time prior to fuel loading. Therefore, there

13 will be no --

14 MS. CUBBAGE: Well, step back. It's not -

15 - it's not going to be all of the stuff is dumped on

16 us a month before fuel load.

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

18 schedule.

19 MS. CUBBAGE: This is going to be made

20 available to us well in advance, and with the whole

21 points, they're going to get -- they're going to

22 engage the staff in the inspection process before they

23 go and install the equipment.

24 CHAIR CORRADINI: But the -- if I might

25 just interject? I -- we're a bit off topic, but

1 you've actually gone the other branch, which I think

2 staff is aware of and we're aware of, which is this is

3 now more generic to all the certifications --

4   MS. CUBBAGE: Yes.

5   CHAIR CORRADINI: -- and how that

6 inspection or -- I'm afraid I'll use the wrong word,

7 but how that looking will be done.

8   MEMBER STETKAR: That's absolutely true,

9 Mike. It is -- it is not ESBWR specific. The only

10 difference with ESBWR, and I hate to say this again,

11 is that the ESBWR is the only DCD that I've seen --

12   MS. CUBBAGE: Big objection to that. I

13 don't think that's necessarily true that all of the

14 DCDs have a complete --

15   MEMBER STETKAR: I'm saying the last two

16 years.

17   MS. CUBBAGE: Well, are they using the DAC

18 approach?

19   MEMBER STETKAR: They claim they're trying

20 not to, but that's their own decision.

21   MS. CUBBAGE: That's their choice. If

22 we're using a DAC approach, we've concluded that we

23 don't need that information.

24   CHAIR CORRADINI: Was there something else

25 that -- Ian, did you want to say something?

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

2 switch --

3   CHAIR CORRADINI: Well, just for a minute,

4 organizational standpoints. So, you don't have any

5 questions of the folks up here at this moment?

6   MEMBER STETKAR: I don't at this moment.

7   MR. WACHOWIAK: I think to get back to

8 your comment on that you said you didn't see it, it --

9 it depends on where you're looking to find what the

10 I&C system is supposed to do, okay? So, if you look

11 in the analysis sections, it will tell you what the

12 SSLC/ESF system is supposed to do. You won't

13 necessarily find those step-by-step things what it's

14 supposed to do in chapter 7 with the I&C. You find

15 that in the sections that describe the analysis that

16 we did for the plant.

17   So, in part, that was why the transmittal

18 of the simplified logic diagrams, if you will, took

19 place. The staff said, we see this in these other

20 sections. How do we know that in your design process,

21 you're actually putting that into the design? We

22 showed them the intermediate step, said, okay, we see

23 that what you said it's going to do is being put into

24 your process, as our process that they're certifying

25 describes.

1   So, that -- that's how that gets together.

2 The problem in putting the simplified logics into the

3 DCD while we're using the DAC process is that you --

4 you or someone else can not only infer from those

5 logic diagrams what the system is supposed to do, but

6 you can also make judgments of what it is not going to

7 do.

8   We run the risk of misleading you because

9 not all of the things are there. You might decide

10 that it's not going to do something, where in fact it

11 may do that.

12   So, in your analogy, what do you do when

13 you get to the big pothole that you can't drive over?

14 We wouldn't have that in there, but you have to --

15 you have to deal with that when, through -- when

16 you're doing the final logic diagram, and we might

17 have to put something in that you would think is not

18 there by looking at the simplified volumes.

19   MEMBER STETKAR: That's fine. I'm glad

20 you made that -- that distinction. I guess my concern

21 is that I would like the opportunity to at least ask

22 you the question at this point in the review process

23 whether or not you've thought about the fact that

24 there might be a pothole. Because under these

25 conditions, if there is a pothole, it seems like it

1 could be a problem. It's taking this travel analogy a

2 little bit overboard, but it's --

3   MR. BUTLER: We know that there will be

4 potholes, and we feel very comfortable with the fact

5 that the structured process that we define, and that

6 we've committed to will allow us to discover those

7 potholes, and document our solution to them as DAC.

8   MR. WACHOWIAK: So, for one example of a

9 pothole that is known now, which I think Skip covered

10 in his presentation: the issue of data storms. Right?

11 That is a pothole that we know about with digital I&C

12 systems. We've designed our architecture such that

13 the communication and the -- and the way that the

14 application program processed the communication does

15 not -- is not amenable to data storms, being

16 interrupted by data storms.

17   So, we saw that one now. We know how to -

18 - how to implement that, and we give a requirement for

19 the system that says, that operating system has to

20 continue to perform its application function over and

21 over and over again independent of whether there's

22 data there or not.

23   So, we can see the potholes that we can

24 see now, but the ones we don't see, our process is

25 what handles dealing with them.

1   MEMBER STETKAR: Let me back you up to a

2   bigger one, and pushed it off to November a bit, but

3   it -- it's -- it relates to my concern about the

4   information for the digital I&C design. Not so much

5   digital, the I&C design. And that is the new function

6   for isolating CRD under certain conditions, and then

7   bypassing the isolation of CRD under other conditions.

8   This seems to be something where someone has

9   identified an issue, and the plant design has been

10   changed because new valves have been installed, both

11   isolation valves and new bypass valves. So, there's

12   been physical hardware changes, and of course the I&C

13   has been changed appropriately to implement those

14   necessary functions.

15   It's difficult. I understand the signals

16   that are being used. I can read the words. I don't

17   see the logic diagram that I'd like to see. Several

18   of the same signals are being used for both isolation

19   and bypass, low GDCS --

20   MR. POPPEL: You mean same parameters, not

21   same signals.

22   MEMBER STETKAR: That's the information

23   that I'm looking for. But I could see --

24   MR. POPPEL: We said that the ICP bypass

25   is implemented on the independent control platform.

1   It's very clear the independent control platforms are

2   in fact independent, have their own censors, and are

3   not using common hardware, software with SSLC/ESF.

4   That is clearly stated in the DCD.

5   It is impossible for anybody to believe

6   that we're using the same transmitter in both systems.

7   It's very clear that --

8   MEMBER STETKAR: When you say it's

9   impossible, it isn't impossible.

10   MR. BUTLER: The words that we tried to

11   write were an attempt to clearly communicate, along

12   with our commitment to IEEE Standard 603 that we have

13   independent censors with independent signal path for

14   IO to the controllers for everything. Everything is

15   kept separate down to the instrument.

16   MEMBER STETKAR: It's just really hard

17   for me. It's difficult to see that just by reading

18   the words in all of the places in the document. It's

19   -- it would be nice to see --

20   MR. POPPEL: But I mean if for example we

21   had a picture, and it showed a common transmitter

22   feeding the ICP and SSLC/ESF, you could rightly say,

23   how come you said over here they were separate, and

24   over here you do the same one? And you say, boy, did

25   we get screwed up. You caught us. But we didn't feel

1   we actually had to draw a picture of that, because we

2   said here they weren't going to be the same. We're

3   very clear about it.

4   MEMBER STETKAR: Okay, I guess I'll have

5   to go back and search to make sure that is --

6   MR. POPPEL: But that is one of the valid

7   potholes that you would -- you would say. If we're

8   going to have this thing that does all these, one of

9   the things you have to consider is independence of the

10   signal because the signal is what could've gotten you

11   there in the first place.

12   So, when we went through our portion of

13   the design for this, and decided what platform to put

14   this on, we adjusted to that pothole by saying, it has

15   to go on one of our independent platforms that does

16   not use the same signals, just for the specific reason

17   that you've pointed out there.

18   So, I think where we are now is a question

19   of how do you find this information, rather than it

20   not being there?

21   MEMBER STETKAR: That is exactly right.

22   That's exactly right.

23   CHAIR CORRADINI: Okay, so a lot of what

24   you're asking I think we really need the staff's

25   discussion. So, do you have -- does this committee

1 have anymore of the folks from GEH before we ask the

2 staff to come up? No? Ian, you were going to say

3 something. Are you going to wait until -- do you want

4 to wait until --

5 MR. JUNG: Wait until the introduction to

6 ask people.

7 CHAIR CORRADINI: All right, so why don't

8 we start the switching around? Thank you very much.

9 I appreciate it. Don't go far. Familiar faces are

10 coming up.

11 MR. JUNG: Thank you, Chairman. As my

12 staff gets set up and gets ready, I think the key

13 message I want to send to ACRS is Mr. Brown and John

14 and subcommittee provides us with smart advice. We

15 heard your -- we heard your issues, and we responded,

16 and we worked with the GEH.

17 We spent a significant amount of time.

18 Level of detail has been -- there's some subjectivity

19 as I discussed in earlier meetings, and staff

20 struggled the last couple of years regarding level of

21 detail that we felt that we needed. And when the

22 ESBWR certification came in, there was an expectation

23 of design detail. It wasn't quite there, but given

24 Part 52 framework of the design acceptance criterion

25 ITAAC, staff had to make some decisions on some of

1   these elements.

2   But I think we've gotten to a point where

3   we have to make some decisions, and I know -- I know

4   it's not John's comments. I see some points, but when

5   we talked to GEH, we had some points given their

6   design stage. And we got a significant amount of

7   information. We consider the earlier simplified logic

8   diagrams submitted to the staff twice in Revision 3 or

9   earlier, and Revision 5 stage.

10   We looked at both stages to see how

11   they're progressing. We looked at the issues in terms

12   of it's still something that used to be in the DCD or

13   not? And we clearly made a decision it's not. We

14   felt it's going to change as the design gets

15   implemented as it goes.

16   CHAIR CORRADINI: So, just one

17   clarification for John to make sure. You said there

18   were two submittals from your version, Rev 3 and Rev

19   5. Have you seen both, John?

20   MEMBER STETKAR: No.

21   MS. CUBBAGE: After the meeting in

22   December --

23   MEMBER STETKAR: I've seen Rev 5.

24   MS. CUBBAGE: That would've been some time

25   about nine months ago.

1   MEMBER STETKAR: About a year ago. So,

2 it's probably time.

3   CHAIR CORRADINI: I'm sorry. I didn't

4 mean to interrupt you. Go ahead.

5   MR. JUNG: Yes, thank you. I think that

6 overall, ACRS' comments resulted in enhancing the DCD,

7 and it provided additional confidence to the staff

8 based on the results. I think the overall Safety

9 Evaluation Report improved, and I'd just to thank you

10 for that. I think the staff is ready to provide you

11 with the side of the story regarding these issues.

12   MS. CUBBAGE: I'd just like to follow up

13 with one comment related to what Ian was saying. It's

14 that we can't lose sight of the fact that the DCD

15 becomes the FSAR, and there has been a lot of work in

16 previous years on working one what level of detail is

17 appropriate for an FSAR, and we take a look at some

18 other FSARs, and that's part of our consideration.

19 So, let the staff go ahead.

20   CHAIR CORRADINI: So, may I just -- just

21 as a kind of point of organizing the discussion, there

22 will be certain things that we will start bleeding

23 back into the generic issue of -- of if one goes down

24 the path of staying with DACs, and the staff is

25 reviewing that relative to attributes and some design

1 details, as examples or maybe even some specificity,

2 how does one -- if it doesn't end up being design --

3 the design set at the DCD stage, how does one go

4 through the verification and validation beyond that?

5 That's a generic thing that if we go that

6 route, you guys may know something. We can discuss

7 it, but that's another committee, another group that

8 is essentially going to look at it for all the various

9 certifications, versus clarifications here that the

10 committee needs to feel more comfortable with what's

11 going on.

12 So, we'll go back and forth, but I guess

13 for my mind, I just want to make sure that I get it

14 clear because I don't want to necessarily leave it in

15 GEH's or the applicant's corner relative to the

16 generic issues. So, is it --

17 MR. GALVIN: Hulbert is going to speak to

18 that. I mean each design chooses a different set of

19 DAC for their level of design. So, it's not just a

20 generic issue in the sense of, you decided to give us

21 this level of design, and they've given us this level

22 of DAC. All the other design centers have done

23 something different. So, I mean it's --

24 CHAIR CORRADINI: Right, but it's --

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

1 course the whole verification process is --

2 CHAIR CORRADINI: That's what I'm talking

3 about. It's not so much that the details are

4 different. I'm aware of that. It's more a matter of

5 given there are certain things that are left to ITAAC,

6 to DAC and ITAAC verification, that process, we can

7 talk about it, but it's over here. We're not going --

8 we're not going to worry about it today.

9 MS. CUBBAGE: Right. I think what Dennis

10 is trying to emphasize is that it's a give and take

11 between Tier 1 and Tier 2 and the DAC. If they'd give

12 more detail here, you'd get less detail in the DAC.

13 CHAIR CORRADINI: Sure, okay.

14 MS. CUBBAGE: It's a different approach.

15 CHAIR CORRADINI: Great. Thank you. So,

16 go ahead, Dennis. Do you want to --

17 MR. GALVIN: Well, the staff here will

18 brief you on the follow up to the December 2008.

19 Hulbert is going to go through some of the issues you

20 raised, and the staff overall review, and the follow

21 up to your issues. Hulbert?

22 MR. LI: My name is Hulbert Li. I'm the

23 lead reviewer for ESBWR I&C systems. The purpose of

24 today's meeting is to brief the subcommittee on the

25 issues brought up last December, and also we'll

1 address some of the staff's perspective with four

2 pillar and plus one design principal, bring up Mr.

3 Charlie Brown. Also, we request the advice of the

4 subcommittee on the I&C systems.

5 The committee members, Dennis and myself

6 and Leroy Hardin, will address the cybersecurity area,

7 and we also have Joe Ashcroft on the committee. This

8 is in-line with today's subjects, and last December

9 SCS meeting, and we used the transcript to relay the

10 message to GEH, and also follow up with additional

11 requests for additional information/questions.

12 GEH responded to our questions, and also

13 updated the DCD Revision 6 and also implement

14 additional detail information. The first question the

15 subcommittee pointed out is the cross reference

16 between Tier 1 and Tier 2. It's not clearly related

17 in this Revision 4, Revision 5 DCDs.

18 So, GEH made improvements in Revision 6,

19 and they provided cross-reference, and the obvious one

20 is the table 7.1-2 and 14.3-1a, and the 7.1-2 gave the

21 reference for all these IEEE Standard requirements,

22 how to detail -- detail address in the Tier 2

23 sections. So, it's very helpful information for staff

24 because we will be able to find out precisely, but the

25 ESBWR design implemented those IEEE-603 requirements.

1   The 14.3-1a gave cross reference to

2   Chapter 15 analysis requirement. This Tier 1 section

3   how to verify that there was -- there was analysis

4   requirements. So, staff found these cross-references

5   very useful. These are just two examples. There are

6   many other references in Revision 6.

7   The second comment from SER is there's no

8   -- the documentation is not complete, and at that

9   time, we still had questions for GEH to request for

10 consistency between the DCD sessions. So, in Revision

11 6, GEH provided detailed consistent checks for all

12 these sessions, and this example I'm putting up is

13 Tier 1, Section 2.2.15. It addressed the

14 applicability matches for the IEEE-603 requirements.

15   They identified all the requirements in

16 603, and also cross referenced to every safety system,

17 how they implement those IEEE-603 requirements.

18   The second session is Tier 1, Section 3.2,

19 and the software development. They provided detail,

20 instructions how to verify each platform goes through

21 every lifecycle to the final product, to demonstrate

22 how they achieve those lifecycle design process. So,

23 staff reviewed those in detail, and found those

24 acceptable.

25   The third question is additional

1 information on the architecture of the I&C system, and

2 appropriate ITAAC and DAC should be added. As in the

3 presentation earlier, there was detail of the ITAAC

4 diagrams provided in the DCD, and those are in the

5 block diagram form in Section 7.1, 7.2, 7.3 and 7.4.

6 This block diagram form is compatible to the other

7 design certification application.

8 I was also the lead reviewer for AP1000.

9 I think those block diagram types of drawings are

10 compatible in the AP1000.

11 MEMBER STETKAR: Excuse me, very

12 compatible with a very high level set in the AP1000.

13 MR. LI: Right.

14 MEMBER STETKAR: But those are -- those

15 are very high-level principles. It says, we have four

16 signals from some censors coming into something that

17 does some processing, and it sends a signal out to

18 some individual division. That's -- I can draw those

19 diagrams.

20 MR. LI: Yes, I think --

21 MEMBER STETKAR: The AP1000 also has the

22 functional logic diagrams.

23 MR. LI: It's docketed information. It's

24 not part of the design certification.

25 MEMBER STETKAR: I understand that.

1   MS. CUBBAGE: I don't think that's the

2 same information as docket --

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

4 address that.

5   CHAIR CORRADINI: Okay, all right.

6   MEMBER STETKAR: No, no, no. It's in the

7 DCD on the AP1000.

8   MR. LI: It's the drawings --

9   MEMBER STETKAR: The drawings that I'm

10 looking for are in the DCD. They're in the design --

11 I wouldn't have this discussion if they weren't. They

12 are. They also have the high-level diagrams. The

13 ones that you're --

14   CHAIR CORRADINI: Okay, so you're going to

15 address this? Hulbert, you're going to address this?

16   MR. LI: I'll address this issue. We go

17 through twice: first in the DCD Revision 3 stage. We

18 requested -- basically, we tried to compare with the

19 DCD description whether those diagrams reflect the DCD

20 description. And then, Revision 5 of DCD, they make

21 lots of changes in the DCD. So, we request again for

22 those diagrams.

23   Those diagrams are a little bit lacking

24 because they constantly working on the DCD itself

25 first. And then after that, finalize of the third

1 stage, then they update the drawing. So, the drawing

2 reflects the DCD itself. So, for our minds, DCD is

3 the appropriate design certification document.

4 Drawing is just supplement to make more clear to read,

5 but not necessarily represent everything discussing

6 the DCD.

7   MS. CUBBAGE: This is comparable to the

8 systems reviews where PNIDs, etcetera, are available

9 for audit, and are not part of the certification.

10   MR. LI: But we anticipate there are more

11 refinement for those diagrams when the design is

12 getting more mature in the final stage.   And so, we

13 plan to have an audit of those final logic diagrams in

14 our high-tech resolutions stage, rather than put a

15 design certification.   The problem is putting the

16 design certification -- if they change something, and

17 forget changes something, then making contract, this

18 conflict statement.

19   That happened in the -- in our early

20 review.   We consistently had a problem because some

21 other -- Chapter 7 discusses something in I&C, not

22 necessarily consistent with what Chapter 7 says.

23   So, we bring up these to the -- and they

24 tried to consolidate all the I&C related information

25 into Chapter 7. So, Chapter 7 became very -- so, any

1 change, they just go to one place to make change.

2 Don't have to -- you know, they may miss somewhere.

3 Another concern is the design

4 certification is for a long time, maybe 15 years, even

5 longer, and the technology may change. The logic

6 diagram I reviewed 30 years ago with operating plan.

7 It's quite different from current language.

8 MEMBER STETKAR: I'm sorry, Hulbert. The

9 logic diagrams that I looked at 30 years for operating

10 plants look an awful lot like the logic diagrams that

11 I see for new designs coming in. I'm not saying we're

12 going to use an oxcart or a horse, or a Maserati or a

13 jetpack to get across the United States. That's

14 technology.

15 The fundamental best route across the

16 United States has not changed, and the depiction of

17 that logic, how we take input signals, what input

18 signals we use, whether they're pressures,

19 temperatures, levels, flows and what combinations of

20 those particular input signals I decide to use to

21 implement a particular function, such as injection or

22 isolation, that's fundamental safety system design.

23 That is not based on rapidly changing technology

24 because next year we might have even yet a faster

25 processor.

1   If you're saying they're changing the

2   fundamental logic because of chip speeds, that's a

3   real problem.

4   MR. LI: They way they present on the

5   diagram has changed. It's not the same. It used to

6   be draftsman drafted, and now they computerized

7   everything. It's a software-driven drawing. This

8   current -- that background does not necessarily need

9   adjustment to anything. It's a computer-based

10 drawing.

11   So, the symbols of how these are is not

12 quite the same as how they were in the past.

13   MEMBER STETKAR: It's true the symbols

14 look different. I'm concerned about -- I'm not

15 concerned about whether I have a comma, or a period or

16 a semicolon. I'm not concerned whether I have a

17 computer that drew a triangle instead of a

18 parallelogram or something. I'm concerned about how

19 the basic fundamental safety system actuation logic is

20 implemented, and that doesn't change -- that shouldn't

21 change whether I have a CAD program drawing the

22 drawings, or whether I have a draftsman sitting in a

23 room with a pencil drawing the drawings. It's the

24 same drawing. It's the same logic.

25   MR. LI: This is the detail discussed in

1 how they foresee their design. Logic diagram is the

2 tool for the designer to implement the requirements.

3 MEMBER STETKAR: It is, but the problem that

4 we've seen in the past is that people who look at each

5 function individually, and many people do, specify

6 criteria for that function within -- within the

7 boundary conditions that they use for that particular

8 function, and that is done function by function by

9 function.

10 At some point, there is an integration

11 process where all of those functions are integrated

12 into the logic. Someone decides that indeed some

13 input signals may be shared among functions. Some

14 input signals -- some functions may indeed require

15 separate input signals.

16 There may be particular interlocks or time

17 delays that are inserted, and until you see -- until

18 you're able to see the whole system in front of you, I

19 guarantee you that reading words about individual

20 signals and individual functions you will not see the

21 problem.

22 MS. CUBBAGE: I think --

23 MEMBER STETKAR: I don't know --

24 MS. CUBBAGE: I don't think anyone is

25 disagreeing with you that that has to be done. It's a

1 matter of timing.

2   MEMBER STETKAR: It is. It is.

3   MS. CUBBAGE: So, the question is do we

4 feel comfortable --

5   MEMBER STETKAR: That is the question,

6 yes.

7   MS. CUBBAGE: Do we have a comfort level

8 with the level of detail that's been provided, plus

9 the verification process that will happen through the

10 ITAAC inspections to have confidence that GE will in

11 fact implement this design as advertised in the DCD?

12 And we've gone to an excruciating amount of detail

13 looking at their topical reports that document the

14 design process that they're going to follow to make

15 sure that these outputs are going to be appropriate,

16 and we have hold points to make sure that we have an

17 opportunity to inspect this information before they

18 install it in a plan.

19   That is kind of the fundamental place

20 where we're at.

21   MR. WACHOWIAK: This is Rick Wachowiak

22 from GEH. Is it on? Wrong trajectory. Rick

23 Wachowiak from GEH. And so, since we're licensing --

24 we're certifying the process right now, as Amy said,

25 there was a test in there. They read the words for,

1 for example, how the ECCS system is supposed to

2 actuate, signals and things like that. They look at

3 our process that says it will be translated into logic

4 diagrams.

5 They asked us for the interim logic

6 diagram. They reviewed that logic diagram, and yes,

7 indeed it did do what the DCD said, and it didn't have

8 these issues that you're talking about. And so, they

9 -- what they're saying is this process is sufficient

10 to produce an output, a result, that we can all live

11 with as long as we check it at these interim points.

12 So, that -- that process there was tested,

13 and it -- and we believe that with the DAC that we're

14 proposing, that the process that we're certifying is

15 appropriate with the Tier 1 information that we have

16 in our documents.

17 MS. CUBBAGE: And I will also take it to

18 the parallel situation with the rest of the plant.

19 They may have a system that may say there's going to

20 be a valve. Well, they don't have to specify today

21 that it's going to be what kind of valve, etcetera,

22 etcetera. But we've gone out; we've done audits are

23 part of the design certification. We've looked at

24 their design specifications. We've looked at the

25 drawings they have for the specific components, but

1 that level of detail doesn't become part of the

2 certification.

3   MEMBER STETKAR: Sure.

4   CHAIR CORRADINI: Go ahead.

5   MEMBER STETKAR: Are you done at that

6 point? Should we go forward?

7   CHAIR CORRADINI: Let's go forward because

8 I think we're okay on time. Go ahead, Hulbert.

9   MR. LI: Thanks. The staff conclusion

10 basically summarized the requested information from

11 GEH a picture of I&C and other levels of detail

12 question based on SER's recommendation and meeting

13 transcript.

14   The DCD's Revision 6 provides information

15 described in Chapter 7 one through four. DCD Revision

16 6 ITAAC verify the 603 requirements for every safety

17 related assistance. And also, they give the lifecycle

18 implementation verification ability. It's easy to

19 verify each life cycle.

20   So, staff concluded substantiate I&C

21 design information DCD including DAC and ITAAC

22 conforms to the regulatory requirement under Part 52,

23 and provides reasonable assurance of safety. The

24 implementation of DAC and ITAAC will be inspected by

25 the staff to ensure the appropriate design

1 implementation and as-built design will be verified.

2 MR. GALVIN: If I could just clarify the

3 third bullet. You won't see all 603 requirements in

4 Tier 1. You know, something like QA and what's the

5 other one? Equipment qualification are covered by

6 other -- other sections of the Tier 1. So you won't

7 see a one-to-one correlation of every --

8 MEMBER STETKAR: In the tier for I&C.

9 MR. LI: It will be a different. Next few

10 slides we give a fresh perspective for the four pillar

11 and platform design principles. And the redundancy,

12 because they follow 603 requirements, and they are

13 safety related I&C system are physically and

14 electrically separate in four divisions, located in

15 four corners, also the fire protection requirement.

16 And the ITAAC commits to FMEA to confirm

17 the safety related I&C system satisfied single failure

18 criterion. And non-safety system network segments are

19 either triple redundant, or double redundant for most

20 occasions. The staff found the I&C design redundancy

21 design principle.

22 Independent: staff reviewed the

23 independent design principle based on the DCD design

24 information and the DAC/ITAAC verification process.

25 From the earlier presentation, the intradivisional

1 data like trip and bypass is same for the two-out-of-

2 four voting logic. So, they are -- it's very limited

3 intradivisional communication.

4 The reactor trip and these independent

5 control platforms is point-to-point data link, and

6 then the SSLC/ESF platform uses the Communication

7 Interface Module, and those are to be verified in the

8 ITAAC stage.

9 So, staff carefully reviewed the DCD

10 information, which included statement of communication

11 independence; found that I&C design made that

12 communication independent principles.

13 Dependency: DCDs state that Q-DCIS

14 internal and external protocol are deterministic. In

15 GEH's definition, determinism means a specific

16 function always be accomplished within that required

17 time period or space of time. And this character,

18 deterministic character will be inspected during the

19 ITAAC resolution process because each platform defines

20 a specific function to be performed at certain times,

21 and those are part of the V&V, verification and

22 validation process.

23 So, during the ITAAC closure stage, we

24 will review those baseline reports to verify they do

25 have those determinants building into their systems.

1   Defense and depth in diversity: The

2 license topical report provided these three analyses

3 for the Standard Review Plan's BTP 7-19 guidelines.

4 The specific method is the NUREG-6303. It's the

5 chapter 16 analysis scenario to analyze defense and

6 diversity ability in the ESBWR I&C system.

7   The diverse protection system design

8 document in Tier 2, Section 7.8, and associate ITAAC

9 is documented in Tier 1, Section 2.2.14. Staff has

10 reviewed these three designs and finds them

11 acceptable, and we addressed them in our SER.

12   Simplicity: Basically, the ESBWR designs

13 follow IEEE-603 design requirements. So, it's -- in

14 earlier presentation, they showed the sense, command

15 and actuate approach. This design made the

16 independent isolation separation requirements.

17 Intradivisional communication is very limited. So,

18 staff concluded this design followed the simplicity

19 principles. This concludes my presentation. Any

20 questions?

21   CHAIR CORRADINI: John, or any members?

22   MR. JUNG: John, if I may, I want to speak

23 to some of your thinking earlier regarding adding --

24 potentially adding things to the logic diagram.

25   You mentioned that it's really hard to

1 fully grasp integrated -- look up the I&C systems. I

2 think we have to look at it from the other way, and as

3 part of our staff review process, we went back to

4 earlier operating reactor FSARs from the `70s to some

5 of the late `80s.  Some of them in the `80s became

6 quite expensive, and agency went backwards a little

7 bit.

8 Agency realized that it's very hard to

9 maintain licensing basis, and any time certain changes

10 are made in a FSAR, they have to come in for licensing

11 reviews and things. So, some of the late `80s, `90s,

12 the agency began to allow some of the detailed

13 information off of FSARs. For example, PNIDs and

14 things in many cases are not part of the FSARs in

15 current operating reactor.

16 Looking at the ESBWR FSAR and the DCD,

17 right now Tier 2 is about 500 pages now.

18 MS. CUBBAGE: Chapter 7.

19 MR. JUNG: Chapter 7. And Chapter 7 also

20 is part of the supporting function for supporting

21 system, and in a way I&C system force the design basis

22 safety functions in Chapter 15.

23 So, Chapter 15, Chapter 6, it's -- when

24 you got to those chapters, when you talk about certain

25 sections, it talks about I&C, and then I&C says, refer

1 to Chapter 7.

2   In Tier 1, Tier 1 contains not just the

3 commitment, but overall in Part 52 design

4 certification itself is a sort of design commitment by

5 itself because the Atomic Energy Act says, 185B says,

6 this is a design that will be constructed down the

7 road. But in Tier 1, it still has a high level

8 description, functional arrangements, interlocked

9 bypasses and testing requirements, and then it goes

10 into ITAAC.

11   That's probably for I&C areas; it's

12 probably 200 to 300 pages. So, when the ACRS think

13 about adding more into the DCD, it's -- I know you

14 have the benefit of having more confidence and

15 clarity, but if you think about it carefully in the

16 sense that does it -- this area eventually might get

17 into thousands and thousands of pages if some of the

18 design details are implemented, and all the FSARs are

19 implemented.

20   So, something to think about is already

21 it's very complex to understand that, and then down

22 the road, none of us are here, and inspectors are

23 looking at it, and trying to see how -- they're trying

24 to inspect the plant. It's going to be even harder

25 for them to inspect and find out the significant

1 elements of the design they need to look into, and

2 more than likely the licensee themselves are going to

3 have a difficult time.

4 So, the reason I'm mentioning this is that

5 some of the FSARs, if you go back to some of the very

6 early FSARs, it's only this thin. The ECCS system

7 does this. Very high-level statement description that

8 eventually got into a lot more details.

9 But I think the question is in terms of

10 additional information, and I've been asking to

11 Hulbert and my staff, do you guys have sufficient

12 information to make a reasonable-assurance finding

13 based on the DCD description, and the description in

14 Tier 1? If they follow within Appendix B type of QA

15 requirements, are they going to get to the outcome,

16 which is a safe and sound design?

17 And their answer has been yes pretty much

18 since last year, and additional detail came in. Yes,

19 it's good. So, I just want to have ACRS consider that

20 there's some point that the design details maybe

21 warrant getting into a realm that it may actually have

22 impact on our review. Sometimes, when we look for

23 additional details, actually we started getting

24 additional RAIs.

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

1 decisions, and given the ITAAC availability for

2 verification inspection by the staff, and they're

3 working on the process to ensure beyond the licensing

4 stage, the agency still has enforcement and oversight

5 responsibility. We're going to work through that.

6 So, I believe -- I think the staff are

7 very comfortable with that decision that they're

8 making. So, I just want to share the information with

9 the staff.

10 MEMBER STETKAR: I appreciate that, and I

11 also appreciate the desire and need to keep the DCD

12 for the FSAR a tractable document, and it's well on

13 its way to violating that criterion already. But I

14 think that what I'm asking for, at least in my

15 opinion, is not more detail. It's intermediate

16 information because indeed in the DCD right now, there

17 is excruciating detail for commitments to follow

18 criteria, and those are -- those are well defined.

19 Those are auditable by inspectors

20 certainly, so inspectors can know how to do their job.

21 You've left very well the inspector confusion or

22 judgment. You tried to do a very good job to try to

23 pull that out of the inspection process.

24 The thing that I'm struggling with is that

25 you don't really rely on inspectors to think about the

1 fundamental implementation of safety functions. Their

2 job as inspectors is to make sure that the licensee

3 said they were going to build it in this particular

4 way, and in fact it was built in that way, and there's

5 traceable documentation to show that indeed that

6 process was followed, but at a fairly small level of

7 detail, and it's an audit function. It's not a design

8 review function.

9   MS. CUBBAGE: Let me just clarify. When

10 DAC are involved, it's not going to be a random

11 inspector that doesn't know I&C out in the field.

12 This is going to be a very detailed process.

13   MEMBER STETKAR: That gets out into the

14 other part of the DAC issue I think that Mike brought

15 up earlier that I don't particularly want to bring up

16 because it's not just the ESBWR.

17   CHAIR CORRADINI: If I might just

18 interject? I'll let you guys converse some more. I

19 think Amy's -- what I'm hearing is Amy's answer is

20 you're uncomfortable -- your lack of comfort -- you

21 should be -- you should be comforted by the fact that

22 the inspection will do it in a disciplined,

23 consistent, organized fashion that won't be class-

24 specific nor region specific. It'll be coordinated.

25 That's what I thought you -- I guess my only -- my

1 only -- if I get to the staff, I think where John is

2 coming from is, at least what I'm hearing him say is

3 that if you took the 500 pages and you replaced them

4 with 200 pages of detail, you might be better off all

5 the way around.

6 MEMBER STETKAR: Well, no. I'm sensitive

7 to the fact that because it is DAC/ITAAC, and because

8 the inspectors who are -- still I come back to the

9 point that the only thing that I've heard the

10 inspectors will be performing is a design

11 implementation audit function, not a design review.

12 Inspectors will not be producing a safety evaluation

13 report of the I&C design. That -- there will be no

14 safety evaluation report of the I&C design, other than

15 what we are discussing today.

16 MS. CUBBAGE: But I believe the committee

17 has heard some recent discussions that I haven't been

18 part to about the ITAAC and DAC closure process, and

19 there is a possibility that there could be topical

20 reports in for review that would then be later relied

21 upon to resolve DAC, but that's --

22 MEMBER STETKAR: If I were more

23 comfortable about that processing, I wouldn't be so

24 uncomfortable right here today. And that's a reason

25 for my discomfort.

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

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

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

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

22   CHAIR CORRADINI: Back to Dennis.

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

1   MEMBER STETKAR: Okay, that's a bit

2 surprising that something that complex that -- that

3 it's implemented perfectly, and there weren't any

4 questions when you looked at those diagrams because

5 the diagrams are pretty involved.

6   Also, did you -- did you ever get a

7 functional logic diagram of the leak detection and

8 isolation system? I couldn't find out, which is a

9 pretty pervasive system that closes valves and opens

10 things.

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

12 1711.

13   CHAIR CORRADINI: I'm sorry?

14   MR. LI: Typical isolation in the type

15 John was asking --

16   MEMBER STETKAR: No, I meant in these --

17 in these -- the drawings that are on the docket that

18 I've seen; that was one of the functions that I didn't

19 stumble across.

20   MS. CUBBAGE: GE, do you recall if -- if

21 your simplified logic package included any leakage

22 detection?

23   MEMBER STETKAR: LDIS.

24   MS. CUBBAGE: LDIS.

25   MEMBER STETKAR: I couldn't find it, but

1 again, the only thing I have is what I pulled -- I

2 think what you sent to our staff.

3 MR. BUTLER: Off the top of my head, I

4 don't think we can -- Skip Butler. Off the top of my

5 head, I can't recall.

6 MEMBER STETKAR: The thing that I'm trying

7 to do here is get a sense of what level of examination

8 was done by the staff relative to those drawings, and

9 if -- if there were any questions that evolved out of

10 them, and if there was any sense of completeness of

11 those drawings, or whether they're just simple for

12 information only?

13 You said they're filed on part of the

14 docket, but they're not -- they're not part of the

15 DCD. So, therefore, they're treated somewhat

16 differently.

17 MR. LI: Yes, we just added basis. We do

18 not go through every one to verify. I think we

19 concentrate on these DCD warnings.

20 MEMBER STETKAR: Understand.

21 MS. CUBBAGE: And that's similar to the

22 process. Again, I'll come back to the mechanical

23 systems side. We don't go out and look at every

24 drawing that GE produces. We sample.

25 MEMBER STETKAR: But in the DCD, I think

1 for most of the mechanical systems there are at least

2 simplified PNIDs that indeed show all of the valves,

3 things like pumps and pipes and valves. I didn't have

4 too much difficulty understanding how the mechanical

5 systems worked from simply the information that was in

6 the DCD.

7   MS. CUBBAGE: We do have PNIDs that we

8 also looked at.

9   MEMBER STETKAR: They go beyond.

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

11   MEMBER STETKAR: They go beyond those, but

12 the information in the DCD is --

13   CHAIR CORRADINI: John, I don't know if

14 you have another question.

15   MEMBER STETKAR: No, I don't.

16   CHAIR CORRADINI: Okay, I at least want to

17 summarize the give and take here as I understand it,

18 since I'm not as adept at this. So, what I'm hearing

19 at least from you, John, is that -- that what Rick's

20 point was about the using the -- I'll call them the

21 intermediate diagrams as a point for auditing actually

22 is a good step, at least in looking at if the design

23 criteria were being followed.

24   MEMBER STETKAR: Yes.

25   CHAIR CORRADINI: Okay, and there's more

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

2 MEMBER STETKAR: The thing -- the thing

3 that bothers me is that there does not seem to be any

4 active use of those. In other words, I'm hearing that

5 the staff used those drawings as a way to verify the

6 words, which is good. I mean that's sort of step one.

7 The second part of the step is a critical

8 examination of that logic to see whether there are any

9 -- I don't know what the right term is, the

10 politically correct term. Areas where there might be

11 division -- I don't want to use the word deficiency

12 because the problems is that you can follow all of the

13 design criteria and implement those criteria, and put

14 -- potholes is a good word.

15 You can even look at those criteria in

16 perhaps six different ways. Perhaps four of those

17 ways may be clearly deficient. It might not -- it

18 might not be clear which is the better way to

19 implement the design. Now, you say, well, it's not

20 the proper --

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

22 what's --

23 MEMBER STETKAR: That's right. And

24 recognize it is not the staff's design, and it is

25 certainly not the ACRS' function to design --

1   CHAIR CORRADINI: However much we try to?

2   MEMBER STETKAR: No.

3   CHAIR CORRADINI: Okay.

4   MEMBER STETKAR: It is, however, I think,

5   a function to look at the design and ask questions,

6   critical questions, to say, why did you do it? Why

7   would you implement it this way? And there might be a

8   perfectly good answer.

9   MS. CUBBAGE: At the end of the day, we're

10   not going to have -- we don't have a function of

11   looking at everything the applicant does. We rely on

12   process. We rely on Appendix B. We've looked at

13   their process. We've seen some of their outputs, and

14   that's where we make our conclusions.

15   MR. JUNG: John, from -- BTP-19 describes a

16   lifecycle. Even though intention was for software, it

17   also includes hardware outputs. You might've seen

18   BTP-9 lifecycle table. For GEH, ESBWR design over

19   perspective, there are some there in the requirements.

20   Depending on which discipline you look at, some are

21   planning requirements. You can look at the simplified

22   logic diagram being one of the outputs. It's in the

23   design stage of lifecycle.

24   So, the staff relies on -- the reason that

25   whole lifecycle, structured detailed lifecycle came

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

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

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

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

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

1 have a role of oversight, inspection and enforcement

2 that we believe Part 52 framework clearly lays out and

3 differentiates licensing functions and the inspection

4 functions through ITAAC and DAC.

5 So, we relied on those -- both licensing

6 framework, and the structured process that is going to

7 come along, and we feel comfortable at this point.

8 The degree of oversight that we put on, if those

9 concerns are significant concerns, then we could put

10 additional resources to inspect those areas. Yet, I

11 believe that the structure they put up in a 603 -- the

12 Tier 1 and 603 requirements that amounts to more than

13 600 DAC items, plus several hundred more ITAAC items,

14 I believe the agency has put up significant

15 restrictions, and oversight that if those are

16 implemented and verified through inspection, I think

17 we'd feel comfortable.

18 John, you are looking for -- my belief is

19 you're asking for something. Yes, more -- additional

20 confidence, and you're looking for something missing.

21 I'm not sure. There might be, but you're almost

22 getting to the situation where we're looking at almost

23 a perfect review that given the resources we have, we

24 may not be able to achieve it at this point.

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

1 asking for a perfect review. It's my opinion. I

2 think my fundamental concern is that indeed we are in

3 a situation now where we are relying on a process at

4 this stage in the design review.

5 We are, as an agency, relying on adherence

6 to a process to give us confidence that the final

7 design indeed will -- will meet the ultimate

8 objective. Certainly, you must have a process.

9 Certainly, someone must adhere to a process for that

10 to be achieved. That's a necessary function.

11 Is it a sufficient function? I don't

12 know. That's the issue. The -- the discomfort that I

13 have is that we seem to be relying on a process, and

14 then immediately auditing compliance with very, very

15 specific, very, very fine structure criteria. And

16 we're developing a perspective that says, well, as

17 long as things are specified very broadly at a high

18 level, as long as we have a defined process and as

19 long as we audit a few specific details, then by

20 definition the designs shall be acceptable.

21 We've removed that thought process from

22 looking at somewhere in between, and say, does the

23 design act as it will be implemented? And I don't

24 mean implemented in detail by chip sets or lines of

25 code again. As it will be implemented in the

1 fundamental logic, is there anything there? Have we

2 critically looked at that part of the process to ask

3 ourselves does anything in that intermediate level of

4 the information strike our attention to say, we should

5 at least question it, or perhaps something might be

6 changed?

7 And now is the time to change it when it's

8 all on paper. It's not the time to change it when

9 things are actually being constructed.

10 CHAIR CORRADINI: If I might -- I didn't

11 mean to stop you, but on the other hand, I think we've

12 gone back and forth now, and we understand the

13 position. Just to paraphrase to end it, if it's all

14 right --

15 MEMBER STETKAR: That's fine.

16 CHAIR CORRADINI: -- is that what I'm

17 hearing from Ian is that they have looked at this

18 intermediate area between high level and detail, and

19 have tested it, and they feel comfortable. You have -

20 - you still have a bit of discomfort because in the

21 testing, you would expect to see -- I don't know what.

22 I can't get into details, but you're looking for

23 more.

24 So, I think -- I don't know if we can get

25 much more out of this at this point. Yes, Graham?

1   CONSULTANT WALLIS: I think I'm going to

2   support what John Stetkar is saying. But by looking

3   back at what we're been doing on these other two

4   dates, and the process we've gone through there over a

5   period of years, and we're looking at all hydraulic,

6   mechanical-type issues, in this process, we've learned

7   several times that the devil is in the details.

8   We look at cartoons of a high level, which

9   you've seen many times in DCD and on slides here, and

10 sometimes they mislead because they give the wrong

11 impression. They don't show the details. They don't

12 show that this pipe, which is connected this way,

13 actually has some bends and some things in it. They

14 don't show the details of how these valves operate and

15 so on, and it has taken us, as you know, Mr. Chairman,

16 some time. We're going back maybe two years. We're

17 asking questions to resolve some of these issues.

18   Without understanding those details, we

19 wouldn't know if the design would work. We wouldn't

20 have the assurance that the design would work. And I

21 don't see how an inspector can ever do that at that

22 sort of level that we've been examining these other

23 systems.

24   There's no way an inspector is going to

25 look at a piping system for some ECCS, and say, that's

1 going to work, but it has to work. He can check the

2 details specified at some lower level detail, but you

3 can't look at the whole thing and say, I know it's

4 going to work. That's not his job.

5 So, I have that sort of concern. I think

6 it's a bit like what John's concern is. This was a

7 long process, and it doesn't seem to be -- there

8 doesn't seem to be a chance to do it here with this

9 issue. Maybe I&C is different.

10 And then I see that when we do get the

11 details, sometimes the design is going to be specific,

12 much more specific. And then it may be the real punch

13 point. I mean everything else has been decided. This

14 is all DACs and ITAACs, and you've got to get the

15 plant running. All of a sudden, you've got the

16 specific design, which inspectors can't review.

17 There's going to be a real crunch for the staff. What

18 are we going to do?

19 Well, in the case of previous issues that

20 we have in these other matters, we brought in

21 consultants, and we wouldn't be able to look at the

22 steam dryer response without bringing in an expert

23 when we ought to look at core stability without

24 bringing in an expert.

25 Are you going to be hiring some experts at

1 the last minute to look at the specific I&C design,

2 and advise on whether it is a good design or not?

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

4 that.

5   MS. DUDES: Well, may I? I apologize. I

6 did come in late. I'm Laura Dudes, Deputy Director,

7 Division of Engineering. I just wanted to -- I know

8 we've had some generic conversations regarding DAC,

9 the inspection associated with I&C. The senior

10 management of NRO is very much engaged in what that

11 inspection process will look like in terms of this is

12 not an inspector going out and looking at a chip, or a

13 function, or following a procedure.

14   This will be a dedicated design inspection

15 team. It's an engineering design verification with

16 headquarters experts, perhaps contractors, and it is

17 not actually going to be done at the last minute, but

18 is actively being planned right now in terms of how we

19 plant a pilot, or first engineering design

20 verification inspection, focusing on I&C.

21   So, we will actually be able to get some

22 lessons learned within the next year or two on how

23 this is going to work, but I hate to leave the

24 committee with an impression that we think that the

25 DAC inspections are going to be done by field

1   inspectors with not the right amount of skills and

2   education and design experience to verify some of that

3   implementation.

4   MEMBER STETKAR: Let me -- I've got ten

5   minutes.

6   CHAIR CORRADINI: Well, I was hoping that

7   we were at the end of our discussion, unless you have

8   something more to -- if we're going to go back and

9   forth on philosophy, I'm going to take some

10   prerogative here, and say --

11   MEMBER STETKAR: We are, but I have

12   examples where indeed plants were built -- these are

13   plants that are currently operating. They were built.

14   They satisfied all of the design criteria. They were

15   inspected, and indeed problems were found later, only

16   when people backed up to the level that I'm talking

17   about. Because people never looked at them at that

18   level in those days.

19   Problems were found. Not problems that

20   violated any safety criteria. Not problems that

21   violated any single failure design criteria.

22   Problems, however, if you had two failures, it would

23   fail everything because nobody ever looked at that.

24   Nobody was ever required.

25   MS. CUBBAGE: Can you be more specific

1 about what is it --

2 MEMBER STETKAR: A particular power plant

3 had three diesel generators --

4 MS. CUBBAGE: No, no. Not the -- no, no.

5 I'm not asking about the specifics of the issue. I'm

6 asking about the specifics of this intermediate layer

7 that you feel is missing. Is it the simplified logic?

8 MEMBER STETKAR: Yes. That's exactly it.

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

10 MEMBER STETKAR: When we looked --

11 MS. CUBBAGE: -- you're implying that no

12 one is ever going to produce or look at those, and --

13 and they are going to be produced. They're one of the

14 outputs, and the staff is going to have the

15 opportunity through the DAC inspection process, with

16 the appropriate expertise, to look at those before

17 equipment is installed.

18 MEMBER STETKAR: The question is will the

19 people who've looked at that do the type of

20 confirmatory audit that you talked about before, that

21 says, someone designed it that says A and B and C

22 should do this. And yes, indeed A and B and C do

23 those things. So, they said that we would design it

24 this way. They implemented the design that way, and

25 our inspectors confirmed that the design was

1   implemented that way.

2   I'm looking for something that says, A and

3   B and C, because of the way that the intermediate

4   level logic, which it's my understanding inspectors

5   will not be inspecting.

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

7   fundamental disconnect.

8   MEMBER STETKAR: The way that was

9   implemented --

10   MS. CUBBAGE: There's a fundamental

11   disconnect in your understanding of the DAC process.

12   MEMBER STETKAR: Because we haven't heard

13   -- this committee has not heard --

14   CHAIR CORRADINI: No, we haven't. But now

15   I'm going to -- we're back into a process, which I --

16   this is the second part of the discomfort, which I

17   think is not just this subcommittee. The whole -- all

18   the members have expressed it relative to the ITAAC

19   process.

20   So, I guess I'd say I think we understand

21   it. I'd like to go into break for going in the closed

22   session, but I think the specifics have -- I think

23   privately you can give the examples of your concern,

24   which leads you to the need to make sure we're clear

25   on this. But I don't know if we're going to get much

more out of this doing this again. One more round of

the discussion isn't going to get us there.

Okay, so at this point, I'm going to thank

the staff, thank the members. Take a break until ten

of.

(Whereupon, the above-entitled matter went

off the record at 10:33 a.m.)

GEH Nuclear Energy

ACRS Committee Meeting
22 October 2009

ESBWR
Design Certification
Chapter 7 I&C
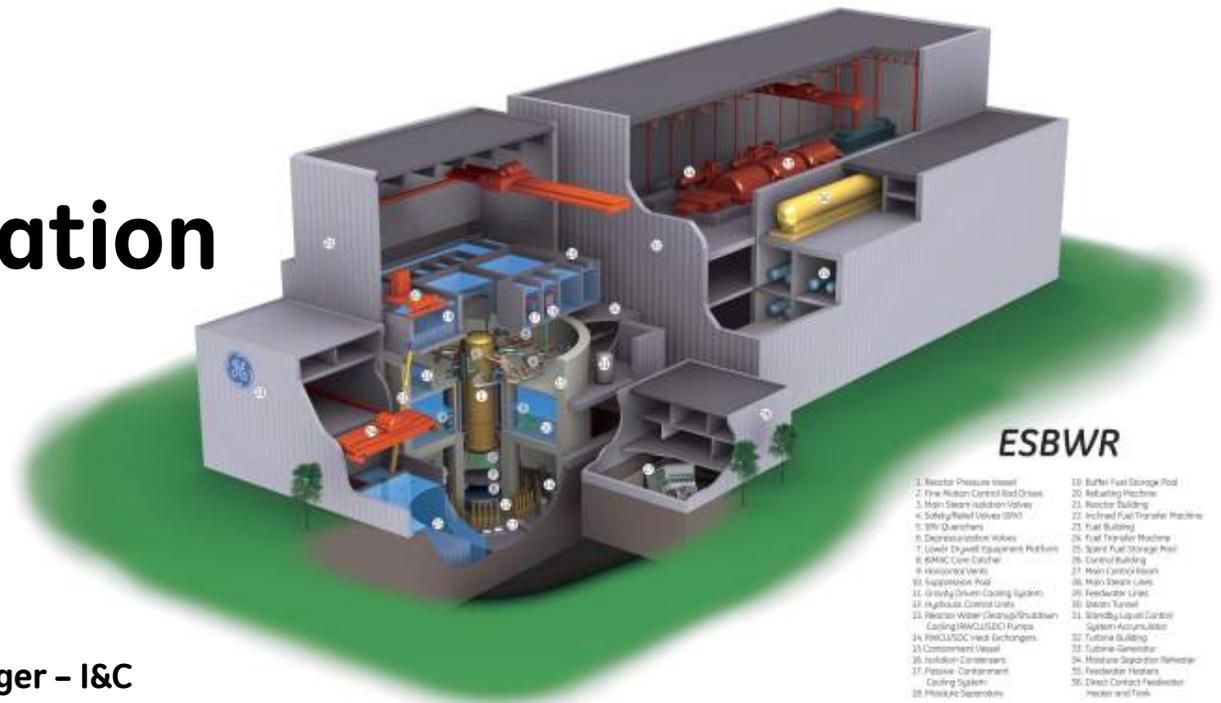
ESBWR

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

GE | HITACHI

Rev. 4 dated 2009-10-20

ESBWR I&C Design Certification Topics

- **Changes to Chapter 7 I&C in Rev 6**
- **ACRS Guidance on I&C based on Rev 5**
  - Design Process and DACs
  - Level of DCIS Design Detail
- **Regulatory Compliance – The Approach**
- **Software Design Process – The LTR Trinity**
  SMPM, SQAPM and CySPP
- **I&C Design Principles – The Overview**
  - Simplicity
  - Independence
  - Redundancy
  - Determinancy
  - Diversity (D3)
- **Questions?**

Changes to Chapter 7 I&C in Rev 6

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

Substantial INCREASE in PROCESS and DESIGN DETAIL

GE | HITACHI

ACRS Guidance on I&C based on Rev 5

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

From: William J. Shack; Chairman

To: Mr. Borchardt; Exec. Director Operations

CONCLUSIONS AND RECOMMENDATIONS:

1. The applicant has an acceptable process for developing the Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) for the Initial Plant Test Program as described in Section 14.2 of Chapter 14.

2. **The Design Acceptance Criteria (DAC) for the Distributed Control and Instrumentation System are incomplete. The staff has issued requests for additional information (RAIs) that address the DAC needed to ensure adequacy of the design process.**

3. **The Tier 2 Design Certification Document (DCD) should include additional information on the architecture of the instrumentation and control (I&C) system, and appropriate ITAAC and DAC should be added to the Tier 1 DCD.**

4. We will review the resolution of open items in SER Chapters 7 and 14 during future meetings.

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

Recommendation – Enhance Design Process and DACs

Tier 2	Ch. 7	Other	Total	Ch.7 % Tot
Chapter count:	1	19	20	5.3%
Page count :	485	~7,515	~8,000	6.1%

Tier 1	Ch. 7	Other	Total	Ch.7 % Tot
DAC count :	663	25	688	96%
ITAAC count :	801	586	1,387	58%
DAC+ITAAC count :	1,464	611	2,075	71%

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

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

NRC Request:

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

GEH Response:

17 New or Revised Figures provided w/ descriptive text...

New [Qty 8] – (See Backup for copies):
- Figure 7.2-11a, RTIF Functional Block Diagram
- Figure 7.2-11b, RTIF Functional Block Diagram - OLU Detail
- Figure 7.2-12, NMS Functional Block Diagram
- Figure 7.3-6, SSLC/ESF Division 1 Layout
- Figure 7.3-7, SSLC/ESF Functional Block Diagram
- Figure 7.3-8, SSLC/ESF Interdivisional Communication Detail
- Figure 7.3-9, SSLC/ESF Safety-Related VDU Communication Detail
- Figure 7.3-10, SSLC/ESF Nonsafety-Related Communication Detail

Revised [Qty 9]:
- Figure 7.1-1, Simplified Network/Functional Diagram of DCIS
- Figure 7.2-2, RPS Interfaces and Boundaries Diagram.
- Figure 7.3-1a, SRV Initiation Logics
- Figure 7.3-1b, GDCS and DPV Initiation Logics
- Figure 7.3-2, GDCS Equalizing Valve Initiation Logics
- Figure 7.3-3, LD&IS System Design Configuration
- Figure 7.3-4, SSLC/ESF Functional Block Diagram
- Figure 7.3-5, SSLC/ESF System Interface Diagram
- Figure 7.4-3, Isolation Condenser System Initiation and Actuation

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

Regulatory Compliance – The Approach

Tier 2

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

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

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

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

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

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

Tier 1

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

Cross Reference and Traceability Matrix

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

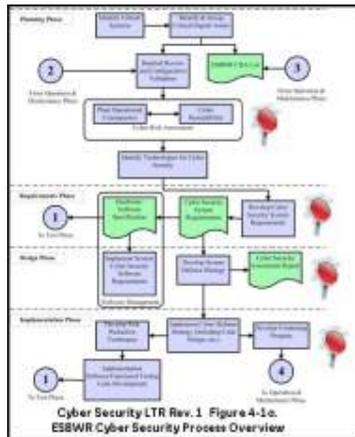**~2,280 Regulatory Conformance Statements**   **1,464 DAC and ITAAC Commitments**

Regulation... Foundation for Quality, Safety and Reliable I&C System DESIGN and Software PROCESS
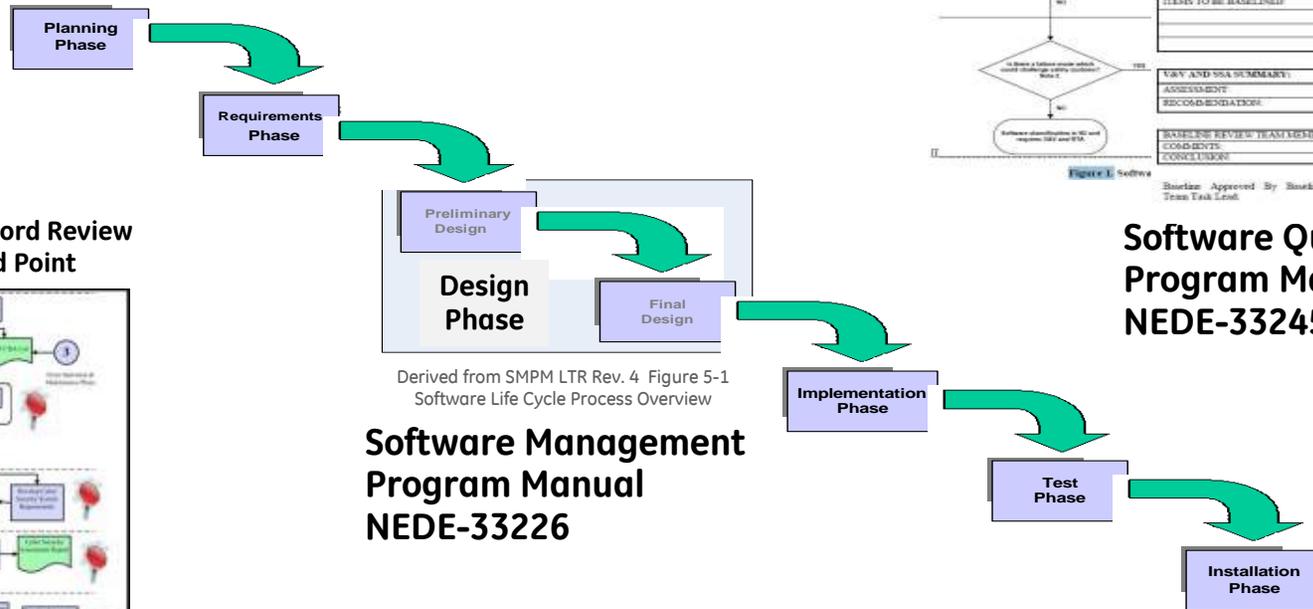
Software Design Process – The LTR Trinity
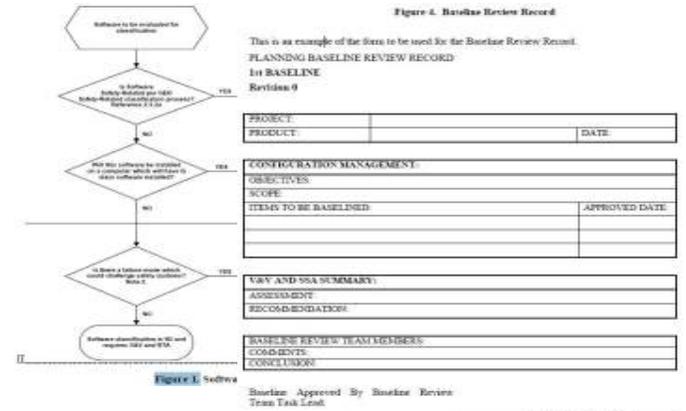
**KEY:**

Baseline Record Review Audit or Hold Point

Cyber-Security Program Plan NEDE-33295

Planning Phase

Requirements Phase

Preliminary Design

Design Phase

Final Design

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

Software Management Program Manual NEDE-33226

Implementation Phase

Test Phase

Installation Phase

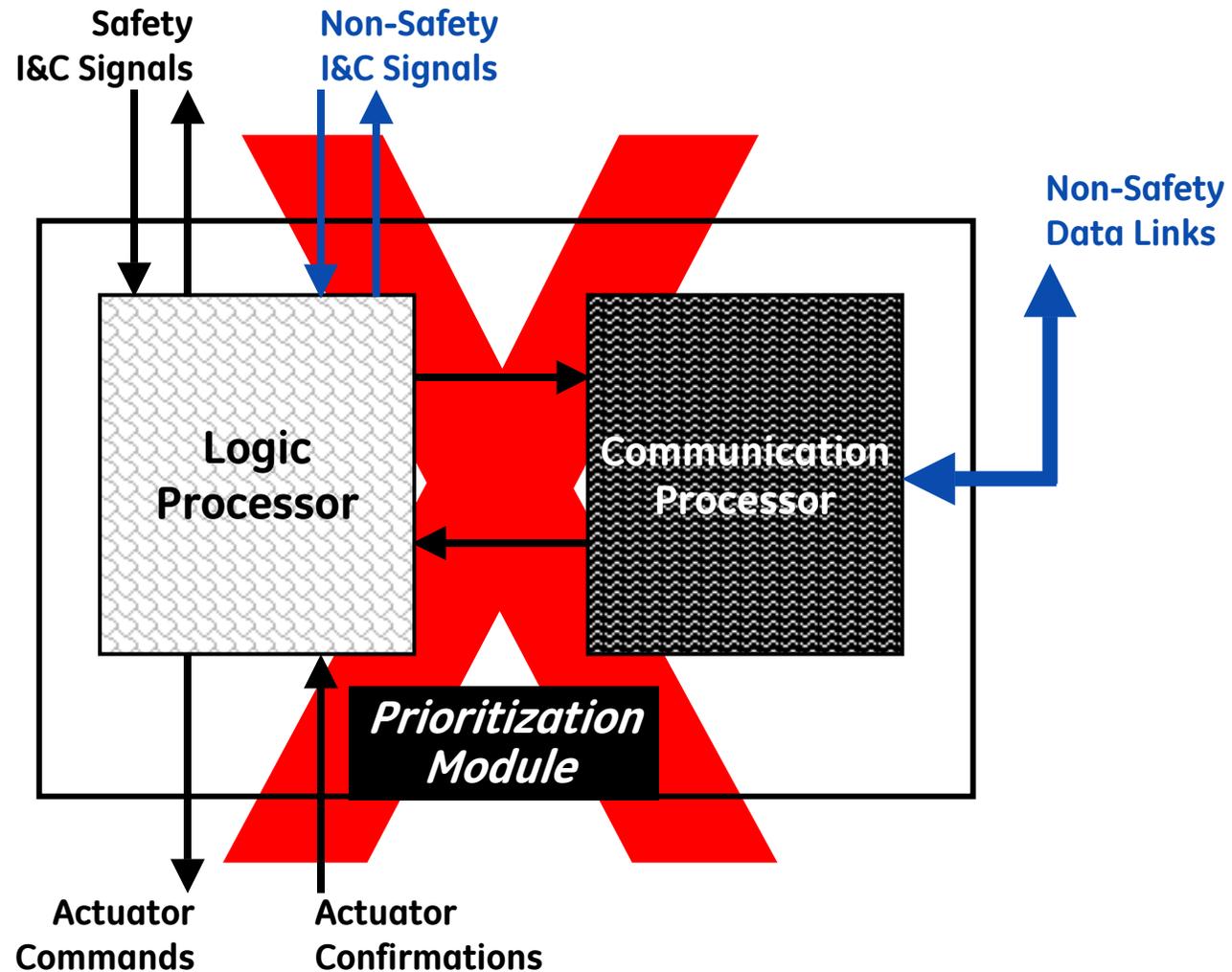**Software Quality Assurance Program Manual NEDE-33245**

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

I&C Design Principles – The Overview

Safety & Reliability

Independence | Redundancy | Determinancy | Diversity (D3)
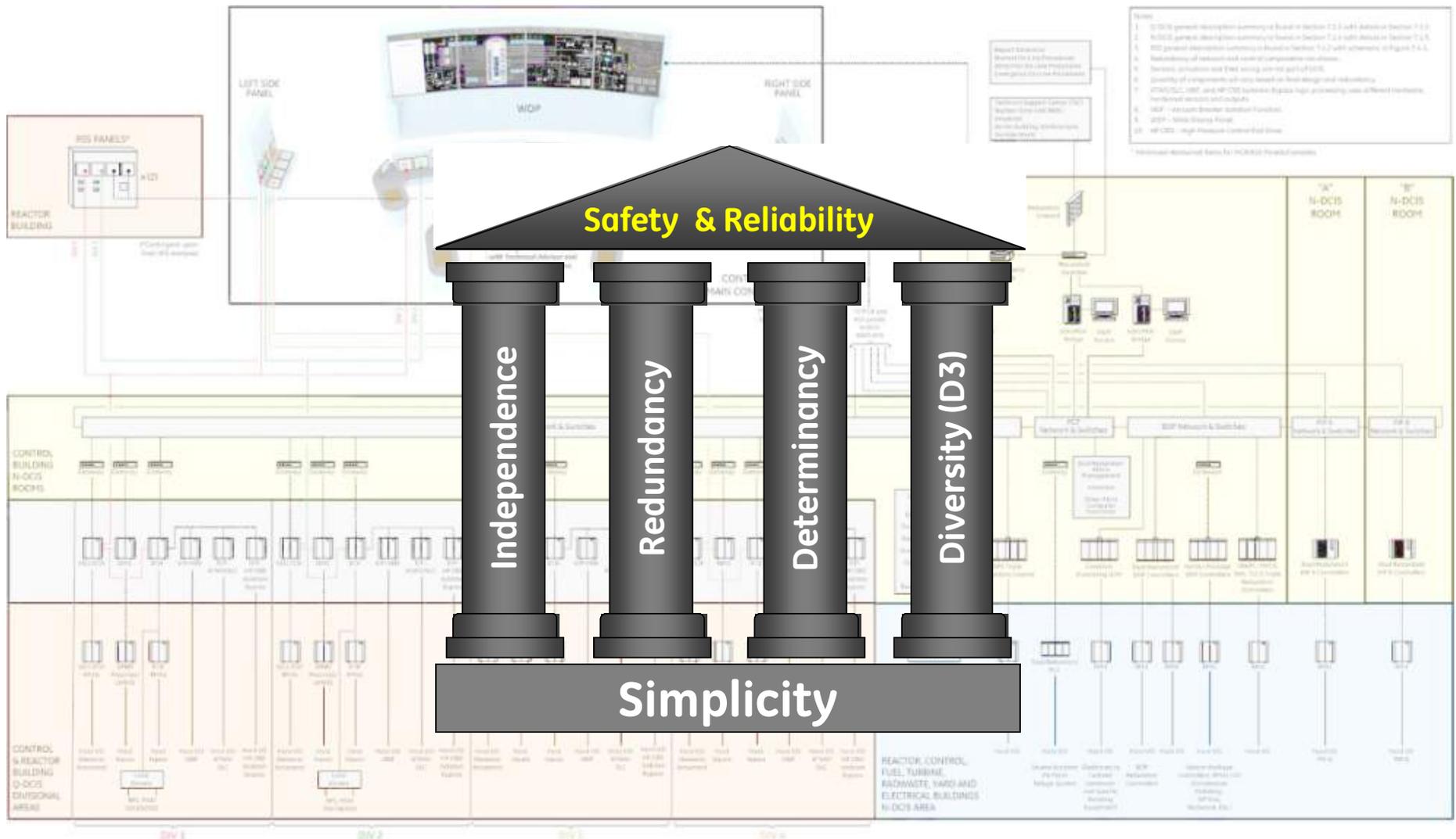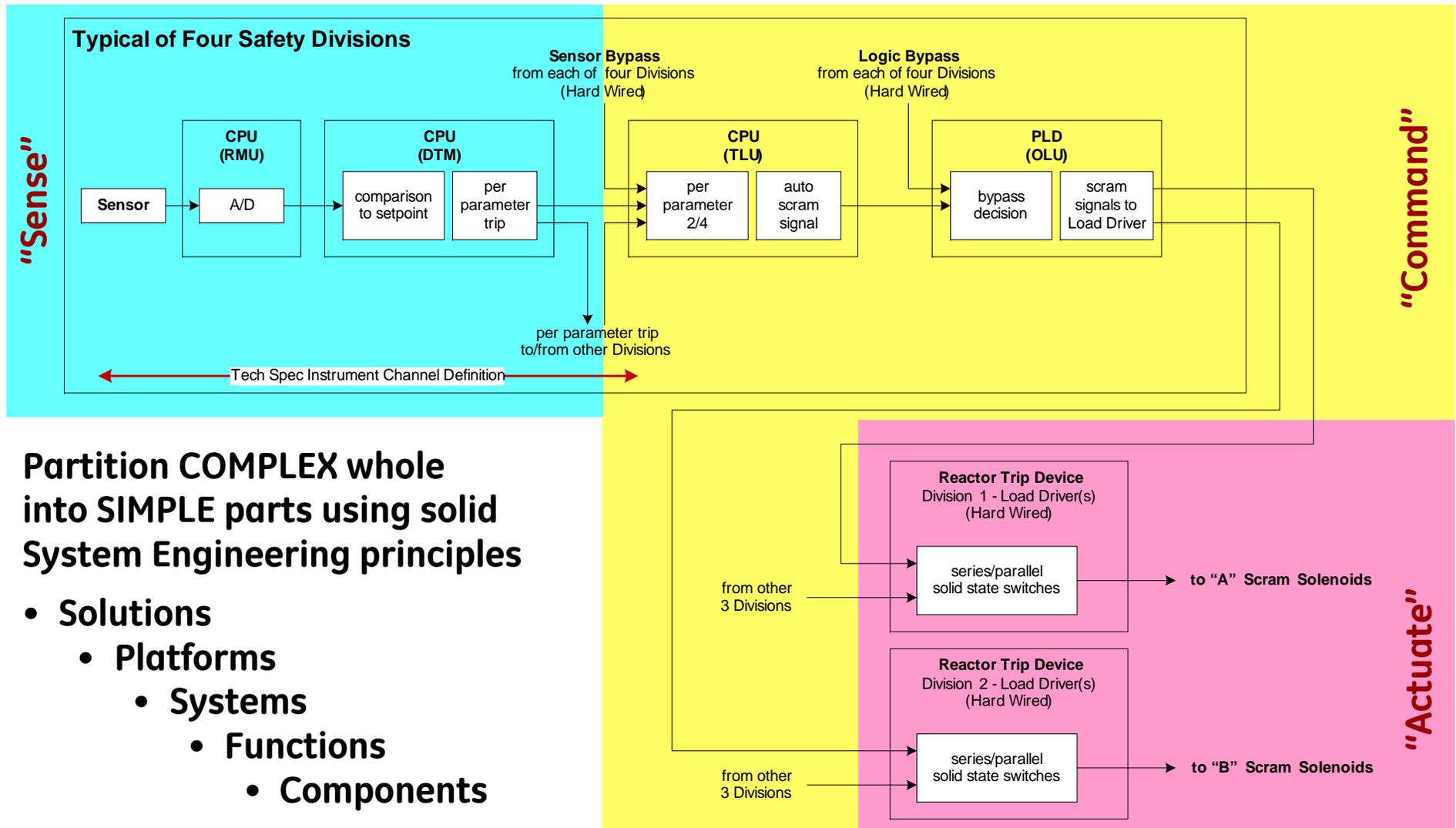
Simplicity

Based on IEEE Std 603

Design Principle – Simplicity

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

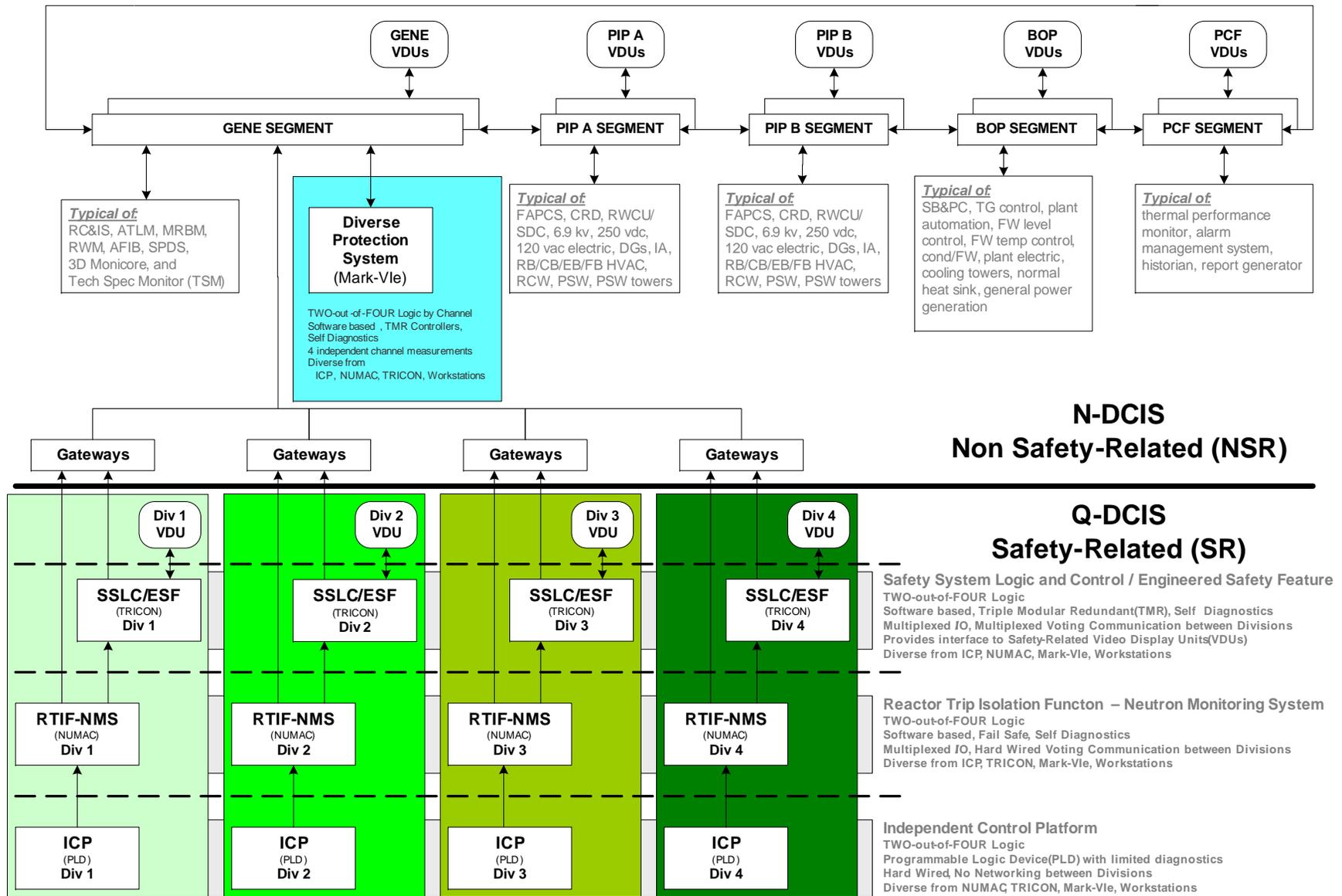**ESBWR DCIS is SIMPLE... Does NOT use "Prioritization Module"**

Design Principle – Simplicity...   RPS Example

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

SIMPLE... Functions are Separate, Isolated and INDEPENDENT

Design Principle – Independence... DCIS Platforms

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

Strict IEEE Std 603 Compliance... Channel and Divisional INDEPENDENCE

GE | HITACHI

Design Principle – Redundancy

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

- Sensors, Controllers and Actuators

SSLC/ESF DCIS:

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

All Safety DCIS design is Single Failure Proof for:

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

All DCIS is REDUNDANTLY powered (primary and cabinet)

- Safety DCIS is REDUNDANT with its Division

Non Safety DCIS may use REDUNDANT:

- Sensors, Controllers and Actuators

As required for plant availability including single failure proofing

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

ESBWR DCIS meets or exceeds requirements for REDUNDANCY

Definition of... Determinancy

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

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

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

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

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

Design Principle – Determinancy... Controllers

RTIF-NMS, SSLC/ESF and DPS controllers use similar operating principles but different HW/SW specific implementations of the programming loop concept
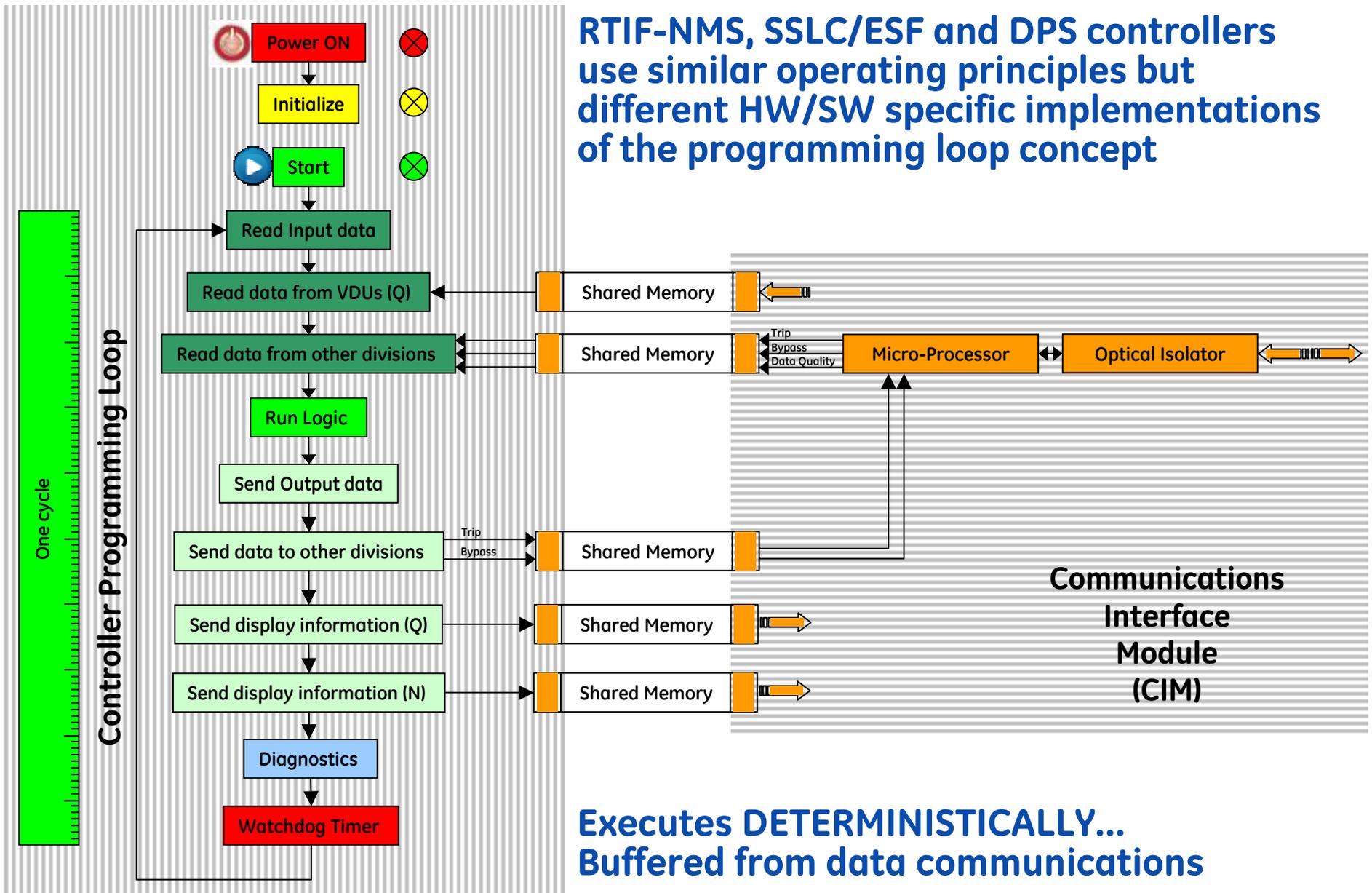
Executes DETERMINISTICALLY...
Buffered from data communications

15 / 20

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

Safety-to-Safety Communications

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

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

Safety-to- Non Safety

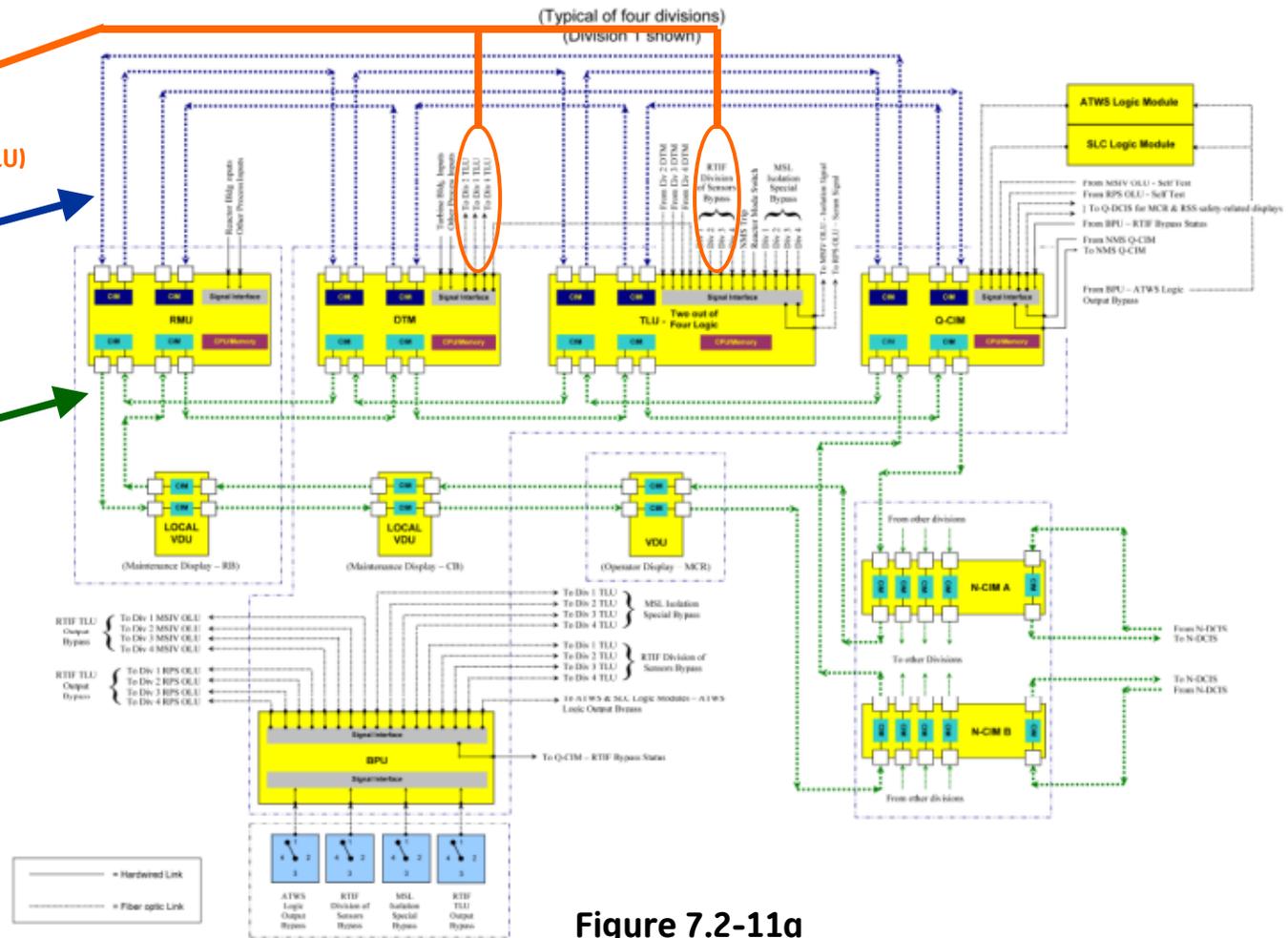**All CIM devices are Safety-Related Equipment**

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

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

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

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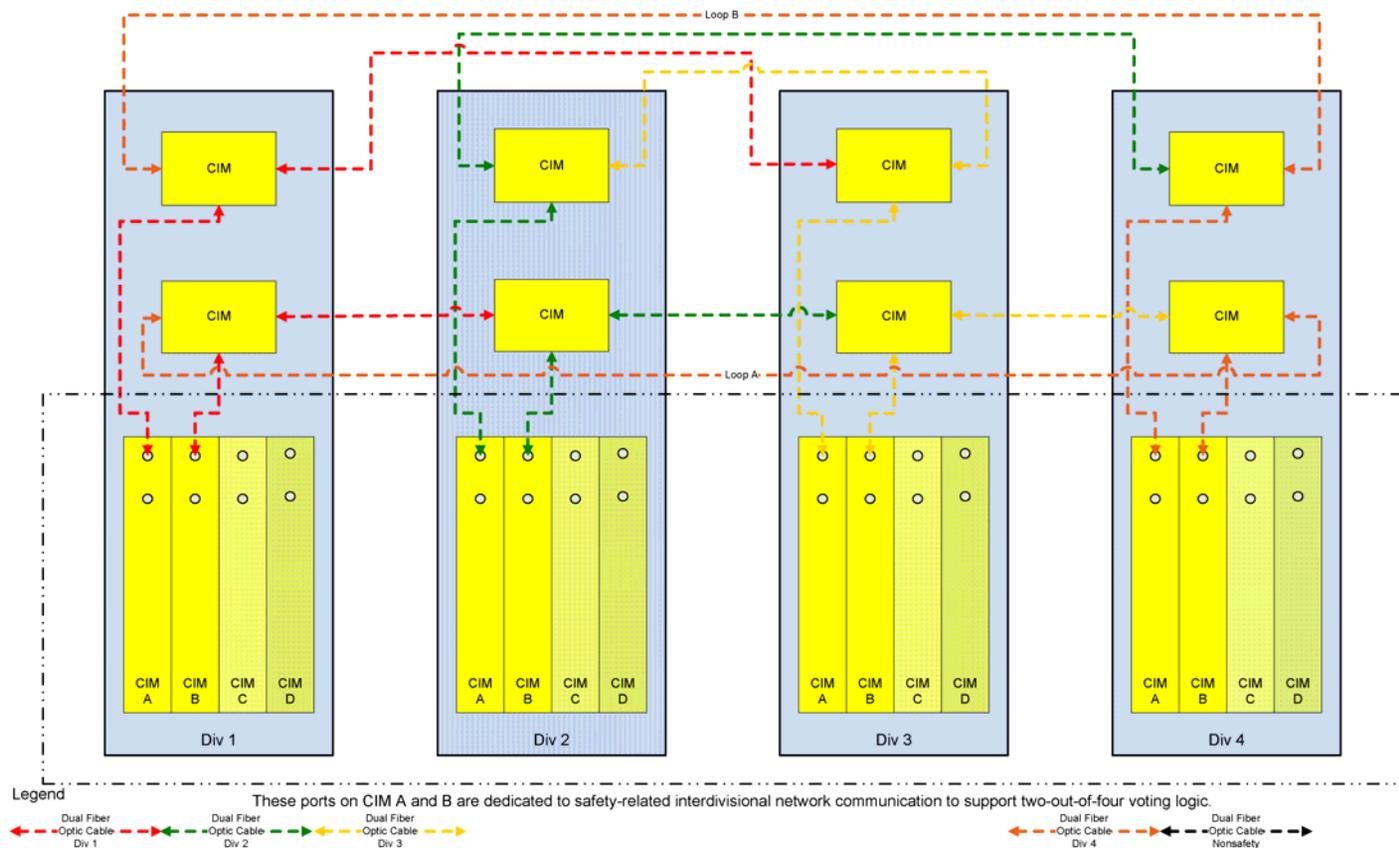**Extremely lightly loaded 100 Mbits/Sec Ethernet**
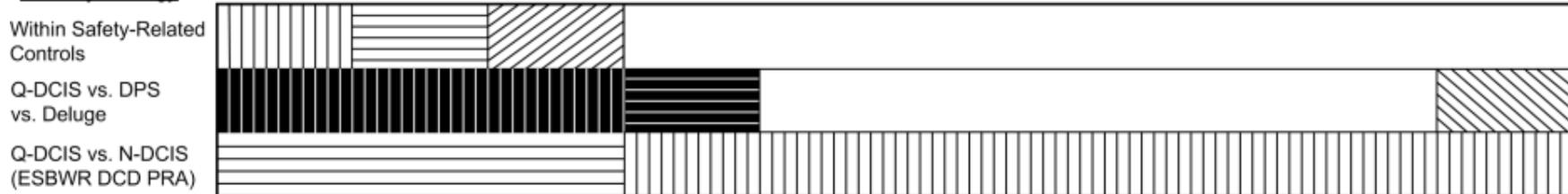

Figure 7.3-8
SSLC/ESF Inter-Divisional Communication Detail

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

Design Principle – Diversity... The DCIS Platform Concept

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

Diversity Strategy

Within Safety-Related Controls
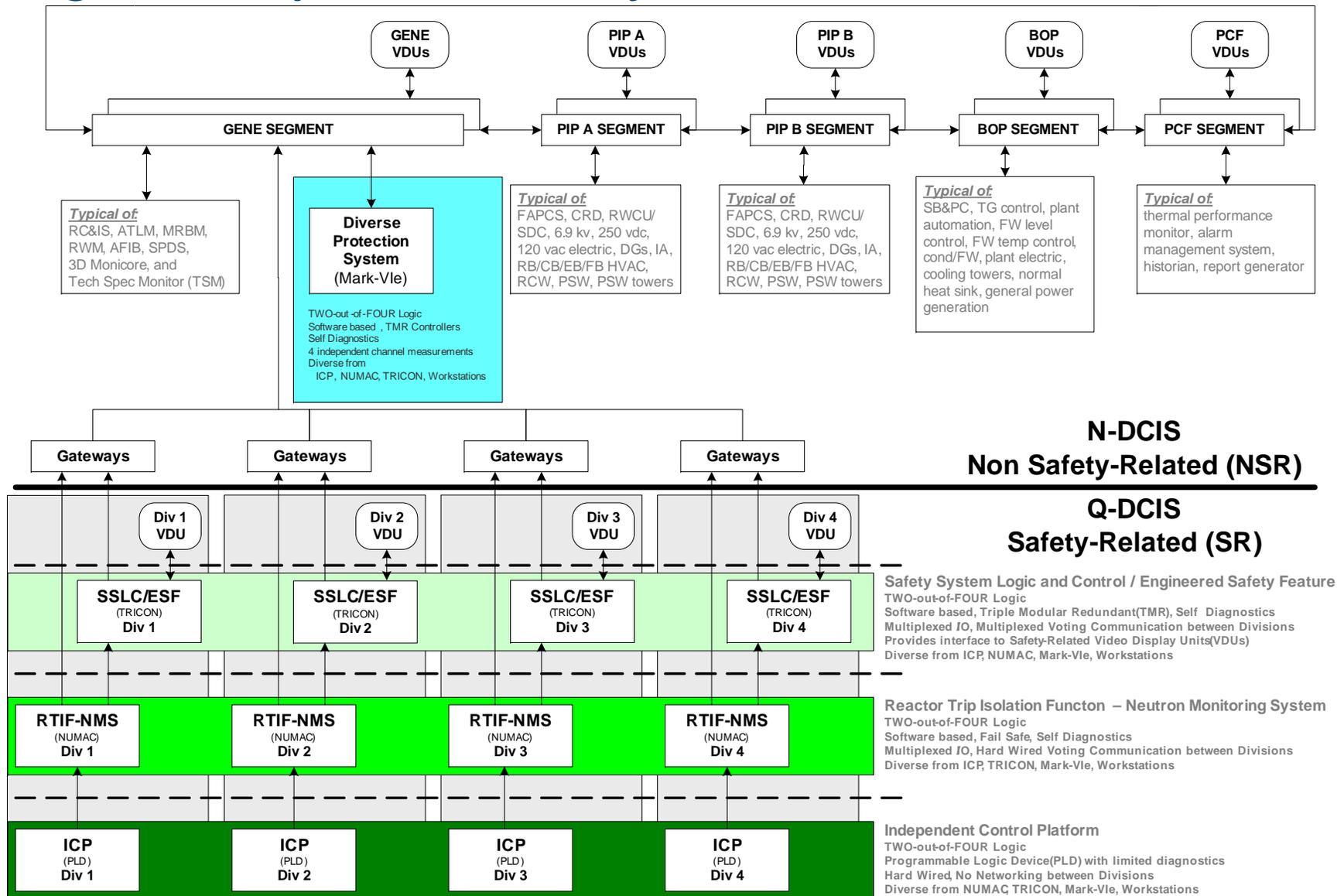
Q-DCIS vs. DPS vs. Deluge

Q-DCIS vs. N-DCIS (ESBWR DCD PRA)

NOTE: Crosshatching denotes different platforms or networks.

DCD Rev 6 Figure 7.1-4 and D3 LTR Figure 1.1
ESBWR Hardware/Software (Architecture) Diversity Diagram

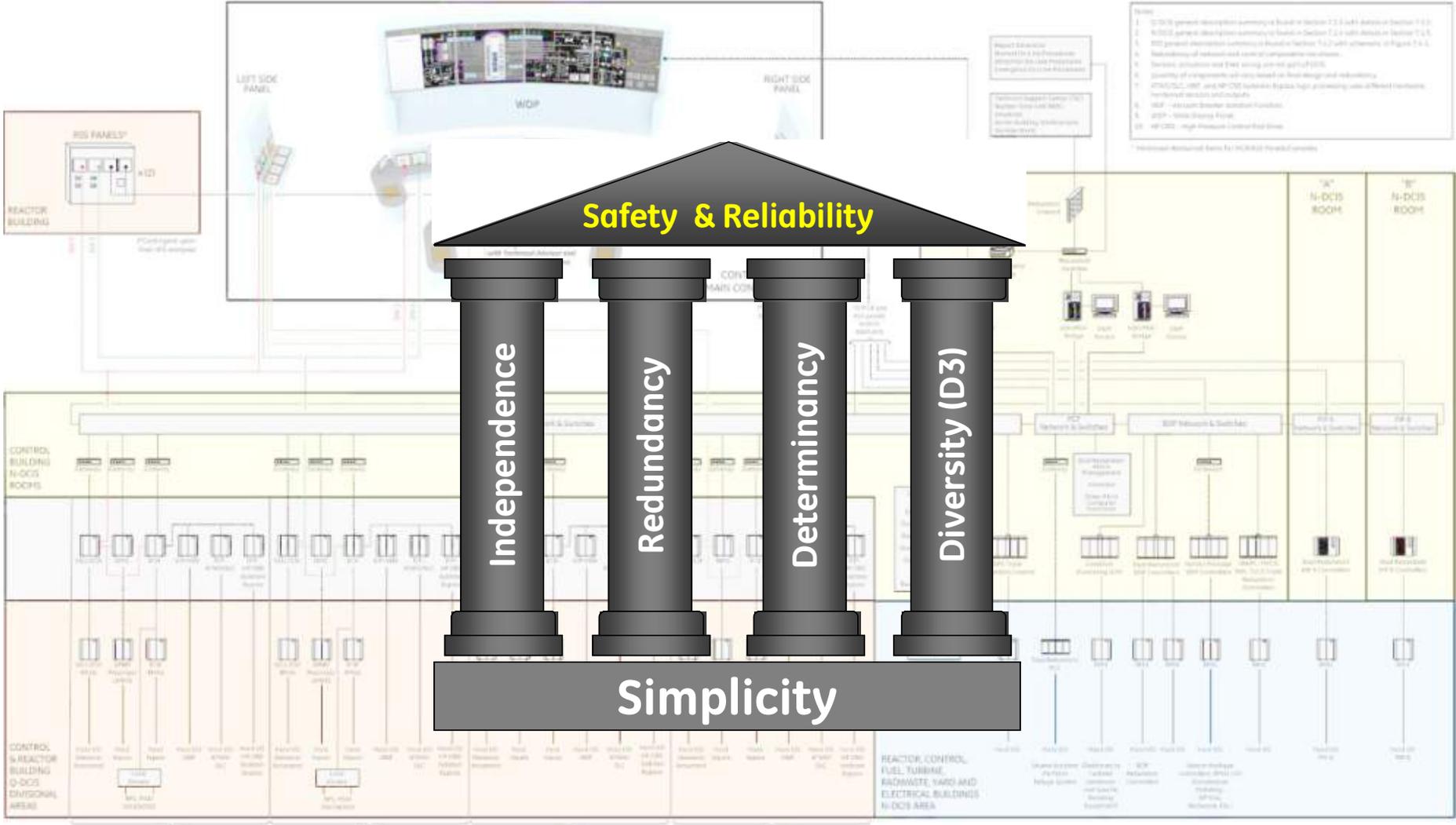# Design Principle – Diversity... The 4 DCIS Platforms

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

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

Questions?

Safety & Reliability

Independence | Redundancy | Determinancy | Diversity (D3)

Simplicity

Regulatory Compliance + Software Process + Design Principles

Presentation to the ACRS Subcommittee

ESBWR Design Certification Review

Chapter 7, "Instrumentation and Controls"

October 22, 2009

Purpose

- Brief the Subcommittee on the staff's resolutions from earlier ACRS Chapter 7 interactions from December 2008

- Provide staff's perspective on the four pillars plus one design principles

- Request advice from the subcommittee

Chapter 7 Review Team

- Project Manager
  - Dennis Galvin

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

Timeline

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

Resolution of Specific ACRS Comments

1. Cross-reference between Tier 1 and Tier 2

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

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

Resolution of Specific ACRS Comments

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

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

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

Resolution of Specific ACRS Comments

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

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

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

Resolution of Specific ACRS Comments

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

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

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

Staff Conclusion

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

Redundancy

- All safety-related platforms are organized into four physically and electrically isolated divisions

- FMEA will be used to confirm that the safety-related I&C systems satisfy single failure criterion

- Nonsafety-related network segments are triple/double redundant

- The staff finds the ESBWR I&C design meets redundancy design principle

Independence

- The staff's review of independence design principle is based on DCD design information and the DAC/ITAAC verification process

* The only inter-divisional data (trip or bypass) is sent for the "2-out-of-4" voting

- The RTIF-NMS and ICP platforms use "point-to-point" data link. The SSLC/ESF platform uses communication interface modules (CIM)

- The staff's careful review of the DCD information which include statements of communication independence finds that the ESBWR I&C design meets the communication independence principle

Determinism

- DCD states that Q-DCIS internal and external protocols are deterministic

- Determinism means a specific function always be accomplished within the required time period specified

- The deterministic character will be inspected during ITAAC resolution process

10/22/2009

12

Defense-in-Depth and Diversity (D3)

- The license topical report provided D3 analysis following SRP BTP 7-19 guidance

- The diverse protection system design is documented in DCD Tier 2, Section 7.8, and the associated ITAAC is documented in DCD Tier 1, Section 2.2.14.

- The staff has reviewed the ESBWR D3 design and finds acceptable

Simplicity

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

10/22/2009

14

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Committee Questions

Discussion/Committee Questions