Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
ESBWR Col Application Subcommittee

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Wednesday, December 3, 2008

Work Order No.: NRC-2567 Pages 1-217

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON ESBWR COL APPLICATION

+ + + + +

WEDNESDAY, DECEMBER 3, 2008

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 1:00 p.m., Michael Corradini, Chairman, presiding.

COMMITTEE MEMBERS:

MICHAEL CORRADINI, Chairman

SAID ABDEL-KHALIK, Member

GEORGE E. APOSTOLAKIS, Member

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR., Member

WILLIAM J. SHACK, Member

CONSULTANTS TO THE ACRS

THOMAS S. KRESS

GRAHAM B. WALLIS

ACRS STAFF PRESENT:

HAROLD VANDERMOLEN, Designated Federal Official

NRC STAFF PRESENT:

CHRISTINA ANTONSEA, ACRS

JOE ASHCRAFT, NRO/DE/ICE2

ROYCE BEACON, NRO/DE/ICE1

KIMBERLY CORP, NRO/DE/ICE2

JEFFREY CRUZ, NRO/DNRL/NGEI

EUGENE EAGLE, NRO/DE/ICE2

DENNIS GALVIN, NRO/DNRL/NGEA

IAN JUNG, NRO/DE/ICE2

HULBERT LI/NRO/DE/ICE2

LEROY MARDIN, NRR/DE/ICE2

KENNETH MOTT, NRO/DE/ICE1

SAN RHOW, NRR/DE/ICE2

DINESH TANEJA, NRO

PETER YARSKY, NRR/DSS/SNPB

ALSO PRESENT:

ROBERT ATKINSON, Dominion

FLOYD BROWN, Entergy

SKIP BUTLER, GEH

PATRICIA CAMPBELL, GEH

WAYNE DONNE, Dominion

ROSALYN EFF, GEH

PAREEZ GOLUB, GEH

STEVE KIMURA, GEH

RICK KINGSTON, GEH

RICH MILLER, GEH

IRA POPPEL, GEH

RICH WACHOWIAK, GEH

DAVID WAKAYAMA, GEH

TABLE OF CONTENTS

AGENDA ITEM PAGE

Opening Remarks and Objectives

By Chairman Michael Corradini 5

GEH Presentation of DCD Chapter 7,

Instrumentation and Controls 7

NRC Presentation of SER Chapter

with Open Items 175

Adjournment

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

(1:01 p.m.)

CHAIRMAN CORRADINI: This is a meeting of the Advisory Committee on Reactive Safeguards and the Subcommittee on the ESBWR. My name is Mike Corradini, Chairman of the Subcommittee. Our Subcommittee members in attendance at the moment are Said Abdel-Khalik, Dennis Bley, John Stetkar, Phil Shack, and Charles Brown was here just a second ago. Our consultants are Dr. Tom Kress and Professor Graham Wallis.

The purpose of this meeting is to discuss Chapter 7 of the SER with open items associated with the ESBWR design certification. The Subcommittee will hear presentations by and hold discussions with the representatives of the NRC staff and the ESBWR applicant, General Electric Hitachi Nuclear Energy, regarding these matters. The Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed position and actions as appropriate for deliberation by the full committee. Harold Vandermolen is the designated federal official at this meeting. Where is Harold hiding? Okay, over there.

All right. The rules for participation in today's meeting have been announced as part of the

notice of this meeting previously published in the Federal Register on November 18th, 2008. Portions of this meeting may be closed to protect information that is proprietary GEH Nuclear Energy and its contractors, pursuant to 5 USC 552(b)(c)(4).

A transcript of the meeting is being kept and will be made available, as stated in the Federal Register notice. It is requested that speakers first identify themselves and speak with sufficient clarity and volume so we can readily be heard. In this small room, don't speak too loudly or you could blow us out. We have not received any requests from members of the public to make oral statements or written comments.

Just last comment, if we all remember, we were going to have this meeting or this part of the Subcommittee meeting combined with Chapter 14, but due to issues relative to approvals they've been split. But we'll probably have questions for GEH and the staff and probably leading back to questions we had or issues relative to Chapter 14 relative to ITAAC and DAC.

So we'll proceed with the meeting, and I'll call upon Mr. Richard Miller of GEH Nuclear Energy to begin. Mr. Miller?

MR. MILLER: Okay, thank you. Just give

me a second.

CHAIRMAN CORRADINI: No problem.

MR. MILLER: I'm Richard Miller, GE Hitachi, ESBWR, INC Engineering Manager. I'll be starting off the discussion or presentation, followed by Ira Poppel, our DCIS Lead Engineer for GE Hitachi; and then Steve Kimura discussing DAC, GE Hitachi Lead Requirements Engineer.

To start off, I'm just going to give you a short introduction on the ESBWR. And just to get everybody acclimated about the overall DCIS, which Ira is going to give us a DCIS overview in a few seconds, I just wanted to acquaint you with the subject. DCIS is distributed control and information systems. We have both a safety-related area and a non-safety-related area.

Safety related we refer to as being Q-DCIS, and you'll see that acronym a lot in our DCD; and N-DCIS stands for non-safety related. We have different platforms that we have identified here, and you probably have seen that within our DCD, and also here on our non-safety side. This is our diverse protection plan for diversity, and Ira will be getting into that later.

MR. WALLIS: Can I ask you right off?

MR. MILLER: Yes.

MR. WALLIS: Diversity and redundancy and that sort of thing, what's the measure of how good it is? I mean, it sounds good, but is there some kind of measure of how good this is and whether you need to be more diverse or you could be less diverse?

MR. MILLER: I guess that's a question for Rick on the TRA for reliability or Ira.

MR. POPPEL: If you treat diversity and redundancy separately, the diversity is defined as we do the Chapter 15 transients and accidents assuming a common cause failure of the traditional safety systems, and then we compare the results against the 10 CFR 100. And if we do not pass, we must mitigate it. And so then it becomes a diverse protection system function added to its functional list. So that's how we know when we have enough diversity, okay? So every common cause failure that would harm the public is mitigated by the diverse protection systems --

MR. WALLIS: So it's based on some regulation rather than some probability of success?

MR. POPPEL: Yes.

MR. WALLIS: It's not directly tied to the PRA in some way?

MR. POPPEL: Now you should answer that.

MR. WACHOWIAK: So in terms of how this would relate back to the reliability of these systems, we start out, as Ira said, looking at it from a meet the regulation sort of aspect. Then what we do after that is done, we'll go back and we'll do a check using the PRA to see if, one, given what we know, we've missed something, that there might be some other vulnerabilities that are out there; and that's done through the various focused PRAs that we got in the application. We also look at is there something where it might be considered too much additional systems for diversity because, once again, as everyone knows, when we introduce a new control system, we introduce more failure modes. So we look at that as a back-end check to make sure that by just adding diversity we haven't gone and included failure modes that are detrimental to the plant. And I think in one of the previous meetings we discussed that we did find one of those, and we addressed the diversity issue differently than adding a control system and was in the isolation valves for the isolation.

MR. WALLIS: But there's no measure of success for that? There's no quantitative measure of success? Because there would be in a PRA. You'd have

a number, a bottom line.

MR. WACHOWIAK: Right. And when we did this, we used core damage frequency, large release frequency, and conditional containment failure --

MR. WALLIS: So your measure of success --

MR. WACHOWIAK: -- probability as the measure of success.

MR. WALLIS: -- is reflected in the PRA then?

MR. WACHOWIAK: Yes, it is.

MR. WALLIS: Okay. Will we see any of that today?

MR. WACHOWIAK: That was not the purpose of today's presentation.

MR. WALLIS: No, I know.

MR. MILLER: Yes, that chapter has already been presented.

CHAIRMAN CORRADINI: What's your name, please?

MR. WACHOWIAK: Rick Wachowiak.

MR. MILLER: I can give you the spelling of that later. Okay. I'm going to turn, basically, the session over to Ira Poppel to give you a DCIS overview. I'd like to hold the Q&A until the latter part, but if you feel that you have a question --

CHAIRMAN CORRADINI: We'll try our best.

MR. MILLER: I know you'd like to get into that, and we'll accept that. So at this point in time, I'll present the meeting over to Ira Poppel.

MR. POPPEL: My name is Ira Poppel. I work in DCIS for ESBWR and, more recently, from the Lungmen DCIS. That's my background and a few years before that in GE.

In general, the way this will hopefully go is I will talk to the slides and you guys can look at the words. And one of the things about the slides is they're busy, but it's a large DCIS system. And you'll see several representations of the same DCIS system. These are not options. We're just trying to emphasize different things.

This is an overview of the DCIS. In the lower left, you can see the Q-DCIS system divided into the four divisions. In general, we have remote multiplexing units in the field which acquire an output data, and we have controllers in divisional separated fire-zoned areas in the control building, so they're --

MEMBER BROWN: What's the field?

MR. POPPEL: I'm sorry. The reactor building in the case of Q-DCIS and everything else in

the case of N-DCIS.

MEMBER BROWN: So other than the reactor building --

MR. POPPEL: Well, we have non-safety systems in the reactor building, too. But the only place that safety systems exist is in the control building and the reactor building.

MR. WALLIS: Are these collections, these liners, are they all independent or are they multiplexed through the same --

MR. POPPEL: We'll talk about that in detail. This is a functional diagram, but all our communication from the field to the control room area, the safety or non-safety, is dual- redundant and, in some cases, triply-redundant fiber.

MR. MILLER: Yes, Rich Miller here. You have four divisions, and the divisions are separated, yes, for the safety systems.

MR. WALLIS: These divisions has a common fiber?

MR. POPPEL: It depends on which system. The ECCS systems are radial triply-redundant fiber from the control room area to the reactor building. The NUMAC, the reactor trip system and the neutron monitoring system are ring systems.

MR. MILLER: And that's per division.

MR. POPPEL: Per division. Up front, we should make sure everybody understands these divisions are isolated in the IEEE 603 sense; they're isolated in the Reg Guide 175 sense; and they're isolated in the cyber security sense, okay? Other than doing two out of four logic, the divisions do not communicate with each other. We never have safety talk to -- excuse me. We never have non-safety give controls to safety. We never have Div X give controls to Div Y. In other words, it's entirely within the division.

MEMBER STETKAR: You say never. That's a big word. What about things like RWC USDC containment isolation valves or FAPCS containment isolation valves, which theoretically, I would assume, is controlled from N-DCIS for their normal functions.

MR. POPPEL: Safety functions are controlled --

MEMBER STETKAR: Not the safety functions. If you want to align FAPCS, for example, for cooling or you want to shut down cooling, you need to open some isolation valves that maybe containment isolation valves that are controlled from Q-DCIS for their isolation function.

MR. POPPEL: Yes.

MEMBER STETKAR: Does N-DCIS also talk to those valves?

MR. POPPEL: No.

MEMBER STETKAR: Not at all?

MR. POPPEL: You control them by Q-DCIS per division VDUs and then you operate the non-safety pumps from the non-safety sides.

MEMBER STETKAR: Okay. Thank you.

MEMBER BROWN: Before you go on, the RMUs you put in, they're in the reactor building?

MR. POPPEL: Yes.

MEMBER BROWN: Now, that is a radiation area, isn't it?

MR. POPPEL: There's nothing in the containment, okay?

MEMBER BROWN: I'm sorry. It's not clear from reading the section where these are.

MR. POPPEL: They are in an environment suitable for their design in terms of radiation and temperature and --

MEMBER BROWN: Okay. So radiation is like a normal background --

MR. POPPEL: Yes.

MEMBER BROWN: -- main control room type radiation environment?

MR. POPPEL: A little higher.

MEMBER BROWN: Normal operation --

MR. POPPEL: Yes, absolutely.

MEMBER BROWN: Okay. But under accident considerations?

MR. POPPEL: They are designed for that.

MEMBER BROWN: And so that calculation has been made, and there is a radiation ghost, you know, the ghost reg, whatever, is considered in the design of the components, particularly the solid space components, etcetera, that go in there? The electronic --

MR. POPPEL: Yes, yes. The other way of saying that is they're not located in areas that do have excessive environment temperature, radiation, humidity, etcetera. The end result is --

MEMBER BROWN: Okay. So they're in the reactor building and not inside the containment building?

MR. POPPEL: Yes.

MEMBER BROWN: Okay.

MR. WACHOWIAK: Ira? This is Rick Wachowiak. I want to make --

MR. POPPEL: You can stand close to here.

MR. WACHOWIAK: I just want to make sure

that when you say valve and when Ira says valve you're talking about the same valve because I don't think you are. When you said it controls the isolation valve, do you mean the valve that isolates the flow through the pipe?

MR. POPPEL: Yes, that's the --

MR. WACHOWIAK: That valve is an air-operated valve. It has multiple solenoids. Safety-related solenoids are controlled by the Q-DCIS, and the non-safety-related solenoids on that valve are controlled by N-DCIS so that the valve, the big valve, can be controlled by N-DCIS non-safety. However, the control system, which is what Ira is talking about here, the control systems are completely separate, and they never talk to each other. That's separate solenoids. So just to be clear, you can have the big valve talked to by both, but the control systems, the individual solenoids and things like that, are separate from safety and non-safety.

MEMBER BROWN: I don't recall seeing that in the figures, in the chapters.

MR. WACHOWIAK: There's a --

MEMBER BROWN: There's just some solenoids there, but the source of whatever is not very --

MR. POPPEL: We actually have a picture on

this, which maybe will help clarify the issue when we get to it, okay?

MR. MILLER: There's about 46 slides here. We usually have about 410 so . . .

MR. WALLIS: But most of them are clearer than this one?

MR. MILLER: Yes.

MR. POPPEL: Yes. But this is the entire DCIS of the plant. So this is the safety stuff. These are the safety displays. Everything is within a division. There are, I'll just call them, broadly, gateways now to connect them to the non-safeties. And the data flow, with few exceptions which have been documented, two exceptions which have been documented, is bound to up from safety to non-safety. And, again, we don't have any non-safety control talking to safety.

The non-safety stuff is this area, and it is functionally the same in terms of we have multiplexing equipment in the field. In this case, the field is the turbine building, the pump houses, water pump house, electric building, etcetera. So they're all over the place, depending on where data is acquired and where data has to be output.

They have dual and triply-redundant

controllers, so we can talk about the reliability associated with that. And we have some strange controllers that do things like control rod blocking and stuff like that, things you're familiar with like rod work minimizers, and things you're less familiar with like automatic thermal limit monitors. But they have their own segments.

You'll hear me use the word segments, and you'll see that there are five of them. So you should not think in terms of what happens when the network goes down. There are five dual-redundant networks in this plant, and they are independent.

So we haven't talked yet about plant investment protection, but it's an A system and a B system here. And if the A DCIS doesn't work, it doesn't affect the operability of the B. So in the normal course of events, these things are connected together through network-managed switches such that the operator is transparent. In other words, any non-safety display can perform any non-safety function, but if one segment goes down there will be displays left which can operate the remaining things.

So the network degrades very gracefully, but when you ask things like about data storms for the network or failures in the network, there is no "the"

network. There's many, many networks, and there's other reliability things we'll talk about, too.

MR. WALLIS: The word "foreign" on this diagram, what does that mean?

MR. POPPEL: Oh, foreign means that we understand that there will be package control systems like, say, the condensate demineralizers purchased by others and not native GE DCIS. And everything that comes in from the outside world goes through a gateway that will have firewall functionality. In other words, we know there's something out there in the field that's not ours, but we do have to control it and accept data from it. And so even though it's in a well-protected area of the plant, we still don't let it attach directly to our networks.

MEMBER BROWN: So you stated that the safety systems were all ring systems -- let me finish -- and the ECS systems were radial systems, but there's no indication in the chapter as to how that ring, what that means, how it's set up, as opposed to the radial. If I look at the diagram and just pick the safety area, they all go straight up. They look radial to the amateur that's sitting here looking at it. So I'm not sure I know what you mean because it's not discussed.

MR. POPPEL: We have another diagram which indicates, which touches on that. But, again, we just wanted to give you an overview first.

MEMBER BROWN: I just want to know what a ring was. The only ring I see on here is at the top of that other figure that you've got the hole connected where you seem to have the five networks in a ring bus but only two connections between all of them, which with dual paths and five busses but they all utilize the same dual redundant wiring going between all five of them.

MR. POPPEL: Okay. Let us get further into it, and then, hopefully, this will become clearer.

CHAIRMAN CORRADINI: Let's move on for the moment, but he's got a question you're going to have to answer eventually. So go ahead.

MR. POPPEL: And we can. It's just the question of time. I mean, we can actually answer that right here, right now; but I'd like to get the overview done first.

MR. MILLER: Yes, we're at a high level right now.

MEMBER BROWN: That's fine.

MR. MILLER: We'll work down through the

details.

MEMBER BROWN: I'll try to restrain myself.

MR. MILLER: Okay.

MR. POPPEL: Okay. This is exactly the same drawing, except it's emphasizing something different. Here is Q-DCIS, and in this time you can see we've written in functions, so reactor trip, isolation condenser, etcetera. And you can see the same five network segments. You can see that they have their own displays in the control room so they can work independent of the other segments, although normally they don't have to. You can see what functions, so here's PIP A and PIP B, so you can see that FAPCS-A is controlled here and with its multiplexers and FAPCS-B is controlled here, and those are each dual redundant networks. So the DCIS is single failure and A and B are separate from one another.

That is also true of the balance of plant control, which is the biggest and which has, essentially, what you traditionally think of as balance of plan. And then we have the Y display panel. We have some other things I'll talk about, and we have the plant firewall and we have the outside

world. This is a thing to try and help you understand where systems are controlled, which the first diagram didn't tell you.

MEMBER BROWN: Is this somewhere else in the DCD? Is this the first time we've seen it? This wasn't --

MR. POPPEL: I can't remember --

MEMBER BROWN: It's irrelevant. Go ahead. I'm sorry. You answered the question --

MR. POPPEL: Okay. This is boilerplate. We believe we meet the requirements for current and existing plans, and the DCIS supports that our past plan concept of 72 hours. All of the safety systems, be it reactor trip or ECCS, is organized in four divisions utilizing two out of four logic and the four divisions, the only communication between themselves is message authentication, plus trip status, plus bypass status.

MEMBER BROWN: Could you repeat that again? The only --

MR. POPPEL: The only communication we allow between the divisions is message authentication information, which is quite extensive to be able to tell it's good and not a corrupt message. And the only data that goes there is there has been a

parameter trip, level, pressure, etcetera, and the divisions' bypass status. And with that information, each of the other divisions is able to make a determination that there has been a two out of four per parameter un-bypassed trip.

MR. WALLIS: Now, why four and why two? Is this some sort of engineering judgment or is there some logic behind it?

MR. POPPEL: The reason we have, the RPS systems has always been four some things, and it was a one out of two twice in the traditional relay designs. They did not distinguish parameters. A trip in one division from level would scram you if you had a trip on pressure in another one. So ours is per parameter. We've kept the four. In the ECCS systems, we went to four because we wanted to be an n-2 plant, and that, in fact, is the second bullet. The tech specs allow us to have a division out of service, and we will occasionally for testing batteries, and accept a single random failure in another division and still be able to operate all the ECCS.

MR. WALLIS: So that's why you have four?

MR. POPPEL: Yes. And that way you satisfy the single-failure criteria. There's two divisions left to decide to do something. This is

going to get into the power and the actuators and hopefully explain a little bit better how we can do some of the things that we're doing. First of all, you should know that per division we have two inverters, two batteries, two power feeds, two power supplies on every DCIS component.

MEMBER STETKAR: In several places -- I might as well ask it now since you have a picture up here. There are several places in the DCD where you reiterate the fact that you have fully redundant power supplies for each division of Q-DCIS, each capable of supplying 72 hours of power. That's not quite true, is it? Because if you lose a battery, you only have 36 hours. I know the inverters may be capable of supplying --

MR. POPPEL: No, that's correct. We're not --

MEMBER STETKAR: But both batteries are not connected to both inverters.

MR. POPPEL: That's correct.

MEMBER STETKAR: So without operator action, you only have 36 hours; is that correct?

MR. POPPEL: In one division --

MEMBER STETKAR: In one division.

MR. POPPEL: -- which can be out of

service indefinitely.

MEMBER STETKAR: But in the DCD, you say you have 72 hours --

MR. POPPEL: Well, we've gone through the phrasing with that several times. Together, the division runs for 72 hours. If we take one battery out of service, even though the division remains completely functional and everything is running but it's only good for 36 hours, we declare the division out of service. But it's a very funny out of service because it's still working --

MEMBER STETKAR: That's an administrative unavailability --

MR. MILLER: We do not take credit for it in our analysis.

MEMBER STETKAR: Not operationally you don't take it out of service. That's what you're --

MR. POPPEL: That's correct. It still works. So in other words, the scram system will still scram you because, in general, you need to scram well before 36 hours. But what's trying to be shown from this is that this design is in each of the division. We can single-fail anything, and the division keeps running: an inverter, a battery, a battery charger, a power supply, etcetera. And so, therefore, when we do

a battery test, we can take that completely out of service. The power is still fed in here from the AC source to the inverter, so we don't even shut down the power on that side. But that battery is out of service, and the division is good for 36 hours, and it's declared out of service.

MEMBER STETKAR: But with AC power it's good forever.

MR. POPPEL: Yes. And that AC source is either from, on all four divisions, is either from either of the preferred or alternate power feed. The preferred and alternate, the normal and alternate preferred power feeds, or the on-site diesels can supply the AC for those inverters, either of the on-site diesels.

MEMBER BROWN: So the only thing you lose if the battery has gone out is you lose that 72-hour within that division?

MR. POPPEL: Which is kind of a moot point, for the scrams at least because you'll certainly scram well before that. The whole plant is designed -- well, let me go to this thing. I want to make another point. Here is one of our explosive squib valves, and you can see it has four igniters on it, okay? So you could say this is either a

depressurization valve or a GDCS valve or whatever, but there's one valve. But the valve is not attached to a division like an active plant. It's not like a motor. It's not like a pump. It's a mechanical valve which can be fired from any one of four inputs. So in other words, division X being out of service says, you know, means this same valve can still be fired from division Y or Z and, in this other case, the diverse protection system. But the point is is that taking that entire division out of service doesn't remove that valve. In fact, taking two divisions out of service doesn't remove that valve.

Now, of course, we have analyses that say what if the valve fails mechanically? But from the DCIS viewpoint is the whole ECCS keeps working even with two divisions completely gone.

MR. WALLIS: Now, when you say four actuators, this is four of what? This isn't four --

MR. POPPEL: It's actually an igniter in a --

MR. WALLIS: But it's one explosive --

MR. POPPEL: Actually, two, but yes.

MR. WALLIS: It's only one piece that actually breaks and opens the valve?

MR. POPPEL: Yes.

MR. WALLIS: So it sort of cascades down from four to two to one?

MR. POPPEL: Yes. And we agree with what you just said. The valve can fail mechanically, and we have analyses that assumes what if a DPV fails and what if a GDCS valve fails? But from the point of view of DCIS, we can lose two divisions and still operate the entire ECCS spectrum. Oh, and this whole scheme is designed, of course, to support the 72-hour operator hands-off so that as long as two safety divisions have batteries and loss of off-site power and a design basis accident, this thing works for the 72 hours without operator input.

MEMBER BROWN: Did you skip a couple of pages?

MR. POPPEL: Well, I wanted to talk on the -- no, I did want to talk from the pictures.

MEMBER BROWN: Are you going to go back?

MR. POPPEL: If we have time, we'll certainly go back, unless you have a specific question?

MEMBER BROWN: Yes, I want you to address the deterministic of the plant state --

MR. POPPEL: Okay.

MEMBER BROWN: You don't have to do it

now. Finish the overview.

MR. POPPEL: No, no, no, that's actually an important thing, and I should have said that up-front. In our view, deterministic means things are not driven by events, they're driven by time. So the ECCS systems and the reactor trip systems look to see if there's a level trip every X milliseconds; it doesn't matter what else is going on. So it doesn't matter if you're in a transient, it doesn't matter if you've got another trip, they're going to look to see if level is exceeding or below its trip value every, in the Lungman case, the number is 25 milliseconds. We hope to do a little better with the next generation NUMAC.

MEMBER BROWN: Just a point of information, Lungmen is what?

MR. POPPEL: Twenty-five milliseconds.

MEMBER BROWN: No, no, no, but it's an ABWR?

MR. POPPEL: Yes.

MEMBER BROWN: So am I looking at, essentially, the DCIS for an ABWR put in an ESBWR?

MR. POPPEL: The NUMAC product line, as you know, is a retrofit on existing plants. It's a front-fit in Lungmen, but it's a general purpose

programmable box highly evolved towards being a trip system or neutron-monitoring system. And so, yes, we hope to take advantage of that technology and upgrade it to the next generation. And so these systems exist. We have no technical doubt that we can build a neutron-monitoring system with a NUMAC product because we have. That's not the ESBWR. The ABWR is different numbers of LPRMs. The ABWR has tips instead of --

CHAIRMAN CORRADINI: That's fine. The reason I asked the question is when it's appropriate, as you go through here, when something is uniquely an ESBWR type of needed instrumentation or control, I'd like to know it because then I'd want to understand how the design differs or at least functionally how you're thinking about it.

MR. POPPEL: Okay. That's fair.

CHAIRMAN CORRADINI: It looks the same, but I just want to make sure.

MEMBER BROWN: I'm not finished yet.

CHAIRMAN CORRADINI: I interrupted Charlie.

MEMBER BROWN: Because I'm not quite, I had a slightly different definition. Whether it complies with yours or not, I'm not quite sure. But

the RMUs take all the, in each division they have certain sensors assigned to each division, I won't use the nuclear system and just use pressure, whatever those factors are. And so the RMU sucks in all that data, processes it, and I'm not going to talk about the multiplexing yet, but the idea is each training, each division, I'm trying to phrase this right because I'm screwing it up because I'm not used to seeing it in this form, each division should go through in the RMU, and the problem here is multiple microprocessors as you go through within a specific 25 milliseconds is what you said. It should take every piece of data, convert every piece of data, A to D, in other words the signal condition of A to D, whatever you want to do on filtering that, it gets picked up and sent to the data trip unit or whatever you call it, DTU. I guess that's where the algorithms and stuff are handled for doing something, I guess. There's no definition.

So there's two microprocessors in a row. And then you feed out to what's called the trip logic unit where you develop your, well, I guess the trip, the signal rises above a level and it trips something in the trip logic unit. I'm not quite sure what those look like. The point being is that every 25

milliseconds in that division, including both microprocessors, including processing of all the sensors and the trip logic unit saying, "I tripped," it all happens in 25 milliseconds. That's deterministic. If it's not, then it's not deterministic. That's my definition.

MR. POPPEL: Yes, it is deterministic, but I did not mean to mislead you.

MEMBER BROWN: Well, I didn't say you did.

MR. POPPEL: It looks, in Lungmen's case, again, ours will be better. In Lungmen's case, it looks every 25 milliseconds. But your overall concern is addressed by the reactor trip system overall requirement that says from the time a measured process exceeds its set point might be a better way to phrase it, until the scram solenoids drop out it's 60 milliseconds, period. So in other words, yes, those time slices are divvied up to the microprocessors in there, but rest assured there is an overall requirement --

MEMBER BROWN: No, that's an overall time response. I understand that, okay? I think I understand it in you all's case. I mean, obviously, when a sensor pressure goes above or below whatever the right metric is, some value, the RMU processes

that and sends it off to the DTU, which generates the trip signal which then trips the trip logic unit and then processes something out through the next thing you call an, I don't know, OIU or something like that, it feeds out then to your scram low drivers or what have you. And when those scram low drivers be energized or I guess de-energized in the reactor stuff, that has got to meet your overall time response. But you have to have a fast enough process deterministically within each of the processes where every parameter gets monitored, evaluated, and passed through, and you have, at least in systems I used to deal with, you had to assume that a trip occurred for a signal if parameter, you know, didn't quite reach its value or it be deemed as a trip. So it went through one processing cycle, and it doesn't pick it up until the next, so you've got a couple. I mean, that contributes to your overall time response, along with all the other stuff in the series.

There's no explanation. The reason I'm asking this and pulling the strings because there's just no detail on how, what you all's concept and what that means. And the idea that every parameter in every division, whether it's a reactor safety one or engineered safeguards division, should be processed

within some measured time. In other words, it doesn't selectively do some in one sample cycle or one program cycle and then do some others in another one or what have you. There's just no, there's no specific details. That's what I need to try to be comfortable. So you don't have to, we can go on, but I just want to make sure --

MR. POPPEL: Well, we do do what your concern is, but if your observation is that detail isn't in the DCD, you're right. But in terms of we do do what you say. Everything has a required time in which it has to actuate and to meet the overall --

MEMBER BROWN: Well, I need to understand that it's, in fact, deterministic and how you -- you make the statement, so I don't have any problems with the statement. How you get there is important in order to make sure we agree with how this is proceeding. I'm not doubting you. It's just we need to see it or I need to see it. Whether anybody else does is irrelevant, I guess. Maybe it's not irrelevant.

MR. WACHOWIAK: And it's different between the one platform and the other, the way it's achieved.

MEMBER BROWN: You mean between NUMAC and --

MR. WACHOWIAK: NUMAC and TRICON.

MEMBER BROWN: -- TRICON?

MR. WACHOWIAK: The specifics of how that's achieved is different. This is Rick Wachowiak. I just wanted to point out that both systems do, in fact, perform deterministically, as your describing it, but they accomplish the same feat in a slightly different manner. So what you're saying is you don't see the details of how it does that in the --

MEMBER BROWN: Well, I mean, for instance, what if you all made an explicit within your DCD that you have no external interrupts coming in to any of the divisions that would stop that cycle, but you didn't talk about internal interrupts that are generated internally. There's no mention of those at all as to whether there are any or not and what they do and whether they are non-recoverable or can go into la-la land or can slow down the process or what have you. There's just no discussion of it. And, again, that is a factor. Interrupt-driven systems are very, very difficult to be predictable. The fact is you could call them impossible to be predictable because they can just stop. And a watchdog timer, resetting those is not defined as being deterministic. I mean, it may bring it back in service, it may send out an

alarm telling you you've got a thing out of service, but it's not suitable for a deterministic-type process.

MR. POPPEL: For the reactor trip systems and neutron-monitoring system, if it stops, it scrams.

MEMBER BROWN: No, I caught that. I understand that point.

MR. POPPEL: So in other words, all the watchdog timer has to say is the process isn't running, just like if you lose communication from the field. I don't know what reactor water level is. The assumption is it's tripped, okay? And so all the way through that system, the self-diagnostics' critical faults is when -- I shouldn't say that. Critical faults within a division will trip the division. If you have two divisions tripped, you will scram. So they're not used for warnings, they're not used for alarms, although, in fact, they do that. They are used to scram the plant if the systems are not performing per their requirements.

MEMBER BROWN: Okay. But the side point on that is that watchdog timers can be applied in a multiple of ways. They're not all the same. For instance, if you have program sample times or cycle times of 25 or 50 milliseconds and that's what you run

through, your overall time response is 60, your watchdog timer might not operate for 75 seconds. They don't necessarily ride right on top of your agreed upon sample time. They can. You run the risk of having it send alarms all the time because it's telling things, but you will have variability within those program cycles. They're just not absolutely precise.

So where the watchdog timer is, you may think that it's, you know, yes, when it literally goes outside the band, it sends a trip. That's good, the plan. But if you vary outside the band where your time response may be exceeded it may not necessarily do, it may not do that in time. So your train is not really available in that time, and you don't know it. So it's an undetected processing thing.

You don't need to answer that. I'm just saying that's more of the concerns of looking at this thing and where is that detail.

CHAIRMAN CORRADINI: If I can just jump in, I think what Charlie is saying is that the lack of detail gets him nervous, so he's trying to extract the details. So we should go on, but I think you're going to see us coming back to that in various places so we can get comfortable as to what's going on.

MR. MILLER: Rich Miller here. Some of that detail probably was provided in the LTRs on the NUMAC and --

MEMBER BROWN: What's an LTR?

MR. MILLER: -- which we took out. Licensing topical report.

MEMBER BROWN: Okay. I have never --

MR. MILLER: And we took them, we removed them from the certification, baseline --

MEMBER STETKAR: I don't think it was. I read the LTRs. Not the level that Charlie is asking about. LTRs are pretty high level.

CHAIRMAN CORRADINI: Move on.

MR. POPPEL: Okay. This has to do with -- one of the concerns, major concerns also seem to be however you wanted to phrase it: cyber security divisional independence, IEEE 603. This is, again, the same DCIS --

MEMBER BROWN: While you had that other picture -- I'm sorry, Mike. There it is. When I look at this picture and I remember what's in the, there's a figure 7.2-1 in your DCD, although much more compressed, I don't see any network operation within this train for performing its function.

MR. POPPEL: Not this picture, but we have

it on the picture coming.

MEMBER BROWN: Well, no, for performing its protection or safety function, sensing through the RMU to the trip logic unit, I mean the DTUs to the trip logic unit out to the lower drivers, etcetera, I did not, I was trying to discern that again from Chapter 2. It's not clear that there is no network involvement in all of that. It should be a straight-through hardwired microprocessor --

MR. POPPEL: Let us show you the next picture --

MEMBER BROWN: Maybe that's not the case then.

MR. POPPEL: No, no, it is the case, but this isn't the picture to show the data flow. This is power, and this is to demonstrate how a single mechanical actuator can handle multiple divisions.

MEMBER BROWN: Okay.

MR. POPPEL: That's what the purpose of this picture is.

MEMBER BROWN: All right.

MR. POPPEL: Nothing else. Okay. Same drawing as before. The safety systems are on the left side here, non-safety, and the outside world. The intent of this picture is to indicate to you that we

have considered the communication paths between all of our boxes. And I don't want to say firewall; that means a different thing to different people. But we have considered the needs of the communication path and the fact that information on it is guarded in some way or isolated. This has to do with data isolation, as well as the physical and fiberoptic isolation that you would automatically assume.

But the idea is is that, in general, the formal firewall is here where the brick is, and this is the outside world. And then there is varying degrees of difficulty getting back through the system such that, for example, well, we probably won't have time to go through it except to say that, for example, a network managed switch is not just a typical ethernet switch you have at home. The network managed switch is capable of asking the question that says, "Who just plugged into me? You're not on my list. You're not allowed to communicate."

MEMBER BROWN: But that's from outside the firewall.

MR. POPPEL: From any place. In other words, if the switch is sitting there in the plant and it has a spare port, which it won't, and somebody plugs a laptop into it and says, "I'm going to take

over the plant," no. The switch is going to say, "I don't recognize you. I don't recognize your nodal address. I'm not going to let you communicate," not to mention it will make all kinds of appropriate alarms. And that has nothing to do with the controllers. The controllers are separate, just trying to get into the plant network, okay?

So the only thing that's allowed to be on the network are those things that we define to be allowed on the network that has specific nodal addresses, etcetera, and none of the outside world knows any of those nodal addresses incidentally. It can't be spoofed backwards through a shared memory. And that concept goes in the major network segments.

And then, of course, on the safety side, we certainly don't want to call them firewalls, but we might want to call them data isolators. But they're basically things which say that I'm allowed to communicate in this direction but not in the other direction, okay?

So the point is it's not just one firewall. The cyber security and the independence and the Reg Guide 175 is baked into the design such that, although we expect changes in future regulations in this area, we do not expect that our configuration

will much change as a result of that. This is a very robust system which we could describe in a lot more detail than I just said, but I just don't want you to think that there's one box called a firewall, just like on your PC at home, and if it fails everybody gets in. That's not the way it works.

MEMBER BROWN: That still didn't answer the question I asked last time.

MR. POPPEL: About?

MEMBER BROWN: The stuff within the division.

MR. POPPEL: We haven't got there yet.

MEMBER BROWN: Okay, that's fine. I just wanted to make sure you didn't we --

MR. POPPEL: I understand. I just wanted to make sure everybody understood that there wasn't just one firewall.

MR. MILLER: We've gone almost 50 minutes, so we've got to move on.

MR. POPPEL: All right.

MEMBER STETKAR: Ira, a real quick question. This one is easy. Q-DCIS cabinets, forget the RMUs, Q-DCIS cabinets, are they only located in the control building?

MR. POPPEL: Yes.

MEMBER STETKAR: There aren't any out there --

MR. POPPEL: That's correct.

MEMBER STETKAR: Thanks.

MR. POPPEL: All right. Reactor trip and NMS is a NUMAC-based product. This is just to give you an idea of how many ways the reactor can be shut down, not the data flowing down. It's failsafe and n-2, which we discussed. You can scram and isolate this reactor software-free, basically by directly interrupting the current to the solenoids. That's reasonably traditional.

We have a new system called DPS which can scram the reactor. And whoever asked, that is something the ABWR does not have. It is an ESBWR unique system so far, and it has the ability to scram the reactor and do some ECCS functions and isolation functions as defined by that common cause failure rule we discussed before. We have a back-up scram that's safety-related, and we have --

MEMBER BROWN: The DPS, is that non, is that --

MR. POPPEL: It's non-safety.

MEMBER BROWN: No, I understand that, but does it use the network or is it completely

independent of software?

MR. POPPEL: No, it's not independent of software. It is a strictly redundant control system by itself. One thing we have to discuss is the diversity. The FMCRDs in this plan and the ABWR have the ability to motor the rods in, which existing plants do not have. So there is such a thing, if you will, as a non-safety motor scram which says you've got a hydraulic scram command, run the rods in even though there shouldn't be any rods there. They should be well above it, but that happens independently. And then, of course, there's the traditional ATWS/SLC systems that can shut the reactor down with boron.

MEMBER STETKAR: Are you going to talk about ATWS/SLC at all? I was just trying to page ahead, and I didn't see it.

MR. POPPEL: In a very indirect way with diversity, okay?

MEMBER STETKAR: Okay. I'll wait until you get there.

MR. POPPEL: The only intent of this drawing for the ECCS systems is to, you've seen all of these before, but I just wanted to point out that the valves needed to do stuff are explosive valves or solenoid-operated valves. There aren't any motor-

operated valves in the ECCS systems that have to operate for the systems to run, okay? So in other words, they all fall in that category of a single valve with multiple divisions on it, be it done by solenoid, air-operated solenoids or explosives. So every one of those valves that you see there can be operated by multiple divisions.

MR. WALLIS: This is a cartoon, and it does not show the real layout of the plant?

MR. POPPEL: That's correct. It's just a functional -- we wanted to leave you with the feeling that the n-2 thing, again, and the fact that all of our stuff does not require divisional motors. These are the ECCS systems, and these are the other things that the SSLC/ESF box controls. Our ECCS functions are automatic. They can be manually initiated. We are using the TRICON, which, per division, is a triply redundant control system.

One of the ways that the TRICON is different than the NUMAC stuff is the fact that our ECCS is extremely slow. And, in fact, we have large time delays built into it. So whereas the reactor trip functions are defined in tens of milliseconds from bad things to the scram, this stuff is defined as multiple tens of seconds from the bad things to when

they have to actuate as analyzed by, you know, the Chapter 15 folks.

CHAIRMAN CORRADINI: So can I just repeat what you said? When you said extremely slow, you mean it has a long time constant for action?

MR. POPPEL: It has built in time delays that are in the logic.

CHAIRMAN CORRADINI: Okay, thank you.

MR. POPPEL: Yes. So in other words --

MR. POPPEL: So whether the TRICON operates in milliseconds or tens of milliseconds or hundreds of milliseconds is irrelevant if you have a 150-second time delay built into the logic.

CHAIRMAN CORRADINI: Thank you.

MR. POPPEL: But the NUMAC has lots of self-diagnostics, and it is, within each division, triply redundant, meaning the controller can fail and it will still operate and be alarmed. One of the reasons I stress that is we pointed out to you that any division can operate one of those valves because of that two out of four stuff. So you can point out, well, then what happens in terms of an inadvertent actuation if any division can do it and the division fails? Within the division, we have many points so there won't be single failures. So in other words,

for one of those squibs to fire, we need three things in the division to close contacts. So in other words, if you will, we made it very easy for any division to fire the squib and we've made it hard for any one division to fire the squib. So you need multiple failures within a division to get in an inadvertent actuation of a squib or a solenoid valve.

CHAIRMAN CORRADINI: Can you say that again, please? Just can you repeat just so I understand?

MR. POPPEL: So here is a valve, say the pressurization valve or the isolation --

MEMBER BROWN: And one solenoid. Pick one solenoid and tell him because that will --

MR. POPPEL: Okay. A single solenoid or a single squib igniter has three switches in a series to it within that division and it has a triply redundant controller controlling the three divisions. So each one of those switches --

MEMBER BROWN: The three switches?

MR. POPPEL: Three switches --

MEMBER BROWN: There's a controller for each switch?

MR. POPPEL: No. Each switch does a two out of three vote from the controller.

MEMBER BROWN: From each of the three controllers?

MR. POPPEL: Yes. Well, the three controllers tell the switches each switch what to do, and the three switches say has there been a two out of three command telling me to close? So if a single switch goes berserk, nothing happens. If a single controller berserk, nothing happens. So very difficult to fire within a division, but any one division can fire.

MEMBER STETKAR: I read the topical report. I get interested in spurious signals, too. When I read the topical report, I'm interested in, I don't care about all of the input stuff because, in my experience, the output stuff is what gives you problems. So I'm interested in the output interface, the RMU that actually sends the signal to fire the squib. In the topical report, I thought that I read that there was a clever organization of RMUs where you have one cabinet for, pick a division, on one floor of I guess this is the reactor building and another cabinet with the other two of the three series of the triple redundant on a different floor, in a physically separate cabinet. Is that the real design for the ESBWR, or is that just a --

MR. POPPEL: Yes. No, no, that's --

MEMBER STETKAR: Okay, fine, thanks. Continue. That's important in terms of -- that's more important than anything else that you said for a spurious operation.

MEMBER BROWN: But the RMUs are input. They take sensor input.

MR. POPPEL: They are also --

MEMBER BROWN: That's not in the, that wasn't in the DCD either, so I didn't see that.

MR. WALLIS: When I was reading this stuff on the actuation, things have to happen in order for it to work. It doesn't go off inadvertently. Doesn't this somehow reduce the probability of it going off when you want it to go off?

MR. POPPEL: Absolutely --

MR. WALLIS: A trade-off of some sort.

MR. POPPEL: Yes.

MR. WALLIS: That's right, but, I mean, this can go on forever. You can have lots of things in series and more and more multiple -- there must be some mathematics that says how you optimize it.

MR. POPPEL: If we wanted to make sure that the squib would always blow, we would have one switch. That would also mean if there was an

inadvertent failure, a single failure would cause a LOCA. So, therefore, clearly, we need more than single failure.

MR. WALLIS: There must be some math that tells you when you're good enough?

MR. POPPEL: And the math has been graciously done by Rick Wachowiak who has actually not only calculated things like what happens if we have a DBA and the stuff works but what are the chances of an inadvertent actuation causing that.

MR. WALLIS: So that rationale is somewhere available? Because the words don't really tell me what the rationale is.

MR. KRESS: Less involved. One is you want to reduce the probability of the thing not working. That's one probability. If an inadvertent works, that's another issue. I mean, it has to do with cost benefit, so you must have two sensitive criteria.

MR. WACHOWIAK: That's correct. It is a cost benefit or an optimization problem, and there are probably an infinite number of solutions. So the process that we followed was we would start with a two out of four system with the triple modular units. I think they were, those choices were made, one, because

two out of four met our requirements and it was similar to what we had done in scram systems before, so it's like a heuristic sort of choice. We make that choice, and then the triple modular system for controlling each of those divisions was made basically because we were looking into those systems for ABWRs at Lungmen and with the other vendors so that, once again, it was a choice that was made independent of doing any numbers.

Then, as we said before, we went through and we would model that system that way and determine do we have any high probability vulnerabilities for failure to actuate, given that system that we chose based on our judgment; and, at the other side, are there any thing for spurious actuations that we cause as problems. On the first iteration through, no problems with reliability doing that, but we --

MR. KRESS: What number did you use for that? Minus 7 CDF?

MR. WACHOWIAK: We have to split this into two segments, again, because some of this is difficult. For the individual logic controllers, we have data from logic controllers that are out there. If a logic processor fails, we have mean time between failures for various manufacturers, and those are

listed in the PRA. We use that. What we don't have, as everyone knows, we don't have a good handle on what's the common cause software failures for these, so we had to come up with something for the common cause software failure. Luckily, that piece of it doesn't fall into this optimization because if you have common cause failures then what you're doing within these divisions is irrelevant anyway. So good thing we can take the common cause failures off the table. Those are the things we know the least about in terms of numerics, but we do know about component types of failures, so logic processors, some number of mean time, hours mean time between failure, we convert that.

So in the first pass through, we didn't see any issue with reliable actuation of equipment. We did see, there are some scenarios, higher inadvertent actuations than we thought we should tolerate. So we went and we added the second RMU, so you have to do two independent switches to actuate the system.

MR. WALLIS: So when you do all this, you've designed this thing and then you do some evaluation. You must have a bottom line which says the probability of it not working when you want it to

is X, so the probability of it working when you don't want it to is Y, and there's some criteria which says X and Y have to be less than something. But you don't give us any of those numbers.

MR. WACHOWIAK: You're right. We didn't put those criteria --

MR. WALLIS: So I have no idea how good it is.

MR. WACHOWIAK: And the values that we looked at for an inadvertent actuation of a DPV, which is, essentially, a LOCA, what we said is that probability of inadvertent actuation of that valve should be less than the random probability of a pipe break of that same sort of size, so random probability of a large LOCA is what we compared for the DPVs. What we compared for some of the other things that have less impact, we would allow. What we compared for some of the other things that have less impact we would allow. So in terms of a single opening of an SRV, we used it as a fraction of a spurious opening of a mechanical SRV. So we compared it to the underlying consequence of what the spurious actuation was going to do. So an analogous --

MR. WALLIS: And all this is true when all the equipment is new? The thing that concerns me

about this is the same thing that concerns me about sort of big computer systems and so on. We know that there are problems with growing and stuff that happen. I don't know how you keep track of all that stuff.

MR. MILLER: Those are the diagnostics.

MR. POPPEL: Yes, that's what it will end up with. We hadn't planned to talk a lot about self diagnostics in this meeting, but suffice it to say is that if the processors behave incorrectly we believe we will know about it.

MR. WALLIS: So you're continually sending signals around saying, you know, is it working right and is there some --

MR. POPPEL: Yes. For example, the TRICON switches are periodically closed and monitored to see that they're closed and not cause anything in the final system to do anything. So if I said it was 100 percent, you wouldn't believe me, but I believe TRICON uses the words like three or four 9s percent of the system is covered by the diagnostics per component. And so, for example, we feel very comfortable of saying, when we say what if the controller fails, well, first, there's three controllers. What does failure mean? If they stop, for example, the switches

that are being controlled by the controller are expecting communication. If they don't get communication, they will individually alarm, saying, "I'm not being talked to like I'm supposed to," but they're also programmable to say, depending if you want fail safe or fail as-is, that, "If I haven't heard, don't do anything."

So in other words, it's not just one box that you can say system fail. There's intelligence all through the components of the system, and those components are under a self-diagnostic regime. And the self-diagnostic regime is part and parcel of the safety-related software and part and parcel of the safety-related software management plan.

MR. WALLIS: Does it recognize spurious signals, too?

MR. POPPEL: Well, for example, a switch, a spurious signal might be, say, one of the three controllers said to fire. The switch will alarm and say, "I've been told by one but not by two." So that's a system alarm. All unusual things like that are built into the self diagnostics of the system. I can't say that it's perfect, but it is extremely well covered, and it is possible to say there aren't any single failures. You can't point to one box and say

that component or that thing fails and this bad result will happen. You need multiple failures in the ECCS to cause inadvertent actuations, and you need multiple failures to not have actuations when you want them. But essentially our multiple failures are two divisions of fail for whatever reason, so we're an n-2 plant. We don't care why they failed, they just failed and they're not going to tell that squib to fire, but the other two are. But on the other side of it, they're not going to have a single failure that individually tells us where to fire by accident.

This picture is the, again, it shows our NUMAC products, RPS and RTF, being able to be displayed by the divisional display. It shows the switches, it's actually more complicated than this, but do the two out of four voting. It shows the main TRICON chassis, and it shows the multiple eight or nine chassis in the field in the reactor building that acquire an output data, in other words measure level and output squibs.

MEMBER BROWN: It's called an RXM here, as opposed to an RMU?

MR. POPPEL: RXM is the triconics term for it.

MEMBER BROWN: Oh, where's the sensors?

MR. POPPEL: The sensors go into here, into the field RMUs, and the actuators come out of those.

MR. MILLER: The sensors are on racks that are on --

MEMBER BROWN: Okay. Let me start again. There's a thing called a TRICON RXM or expansion chassis. Does that have the RMUs and the TRICON platform in it?

MR. POPPEL: Yes. This expansion chassis is in a cabinet called an RMU. The RMU, that chassis is there, along with a whole bunch of terminal boards to which they wire the field transmitters and attach the field actuators and the squibs and solenoids.

MEMBER BROWN: So that's an RMU?

MR. POPPEL: Yes.

MR. MILLER: They're within the RMU cabinet.

MR. POPPEL: Yes. That's the electronics of the RMU. There's other things in the RMUs. I don't mean to make it sound complicated. There's things like power supplies and --

MEMBER BROWN: Yes, yes, that's fine.

MR. MILLER: That's hard wired into the RMU from the instrument --

MEMBER BROWN: I just didn't hear the RMU cabinet based on all the rest of the discussion throughout the entire Chapter 7. That's all. It was more of a functional, as opposed to cabinet, like the RTIS were referred to as cabinets. Are they cabinets?

MR. POPPEL: Yes.

MEMBER BROWN: Or are they something else?

MR. POPPEL: As a matter of fact, RMU cabinets, RMU panels, RMUs are meant to be something in which there's electronics and terminal boards to which field input and output signals are attached.

MEMBER BROWN: M says multiplexer. That's a functional thing to me, as opposed to a box. That's very confusing, but that's --

MR. POPPEL: Well, the multiplexing comes about by that one wire in the triconic system is, in fact, three fibers.

MEMBER BROWN: That's the same in the RPS system?

MR. POPPEL: Yes, I want to --

MEMBER BROWN: Let me ask that question a different way. The RMU sucks in all, gets all the data. The sensors feed it, all of them. You've got five sensors, and they all feed that one RMU in the one division. I just picked five for -- then the RMU

then grabs that data via one program cycle or something like that, and then it transmits the data to the DTM. Is that done serially?

MR. POPPEL: That is done with a dual redundant fiber scram net ring.

MEMBER BROWN: So that's where you get the little internal network then?

MR. POPPEL: Yes, although because the word network is so imprecise, for example --

MEMBER BROWN: I didn't want to use that term.

MR. POPPEL: I know but --

MEMBER BROWN: It's a data transmission, like a wire.

MR. POPPEL: Yes, and so is this.

MEMBER BROWN: That's fine.

MR. POPPEL: It's just that, as Rich said, they're done differently. It happens that the TRICON system is a radial design.

MEMBER BROWN: I'm back to RPS. The real point of it, is that multiplex data? It's not like all the data is put into a set of buffers if it goes through and calculates it and the next BTM grabs it in the next program cycle and pulls this stuff out and does its calculations with it. It's almost like it

feeds it and it collects, feeds and collects, feeds and collects, and you've got to -- that's another point of this data process as you go from microprocessor to microprocessor. In terms of how you do that, it may be within your deterministics. It's done so fast; that's fine. But there's a necessity, at least in my mind, to understand how that's going to see that it is, in fact, a deterministic process.

I have one other non -- you don't need to answer that because you probably can't. I'll forget it next week, quite frankly; that's how old I am. I can barely remember to put my pants on in the morning, much less --

CHAIRMAN CORRADINI: You're on tape now. Come on.

MEMBER BROWN: Oh, I'm sorry, I'm sorry. The point being is that on the logic units, the two out of four voters, is that a --

MR. MILLER: Just to clear things, we're not in the DCD certifying TRICON or NUMAC at this time. We were asked to take them out of the DCD, so we are going to use these products, but it's not part of the certification at this time.

MEMBER BROWN: It doesn't need that for this.

MR. MILLER: Actually, I think it does need that because if we go and we take two different vendors for a triple modular redundant system, one of them might do it the way you said where it puts it all into a buffer and sends that, and a different one would do it it gets the parameter, sends it, gets the parameter sends it. So by not committing, by not certifying TRICON, we're also not certifying the method by which we're transferring information --

MEMBER BROWN: Yes, and that's troublesome from the standpoint of knowing what you're certifying because you can also do the two out of four voting logic. Is that software voting? Is it where you trip and have a solid-state switch where you then, you know, solid state switch where you have four solid state switches that are in some arrangement like you do relays and they perform the two out of four voting? Or is it where you set four flags or three flags or two flags, and now it says, "Okay, I'm up?" It's a whole different method and has a whole different layer of vulnerabilities with which you have to deal.

MR. POPPEL: And you are, I'm actually tortured because I want to answer the question specifically. But more broadly, we understand what you just said. We have software management plans

which go from the requirements that will say things like, you know, parameter to dropping out the scram solenoid and traceable paths all the way through multiple tests, so even though, as Rich says, we might not be able to say or might not want to say, because we're pretty sure what we'll use, but we might not want to say exactly what's going on. We have a process in place to say that, in the end, what we wanted to go on will result in it. It's an auditable process, it's a safety process. Hopefully, it's an improved software management plan process, and it goes to the entire life cycle of the software from initial specification, verification, validation, and testing. And so in the end, no matter how it's done, it's going to drop out the solenoids in 60 milliseconds.

MEMBER BROWN: I understand that. But still, from the standpoint of certifying it, we're asked to certify it with this big box of uncertainty as to how, not the technology that's used but how it's going to be done.

MR. WACHOWIAK: And I think that's going to be covered in the DAC.

MEMBER BROWN: I read the guide, and the guide says I'm going to do a block FMEA of some diagrams. That's the design acceptance criteria.

There is no more definition. It can be whatever, and we'll have no idea what that is. They are not vague. They are cloud diagrams, effectively.

CHAIRMAN CORRADINI: Let's move on. I think --

MEMBER BROWN: I'm just giving you that thought process. It's not in the DCD. It's not in Chapter 7. But that, while its methodology sounds satisfactory, there's nothing that defines what needs to be reviewed. How good are the blocks? The blocks in Chapter 7 are very high level.

MR. MILLER: But the blocks have to meet regulations, right?

MEMBER BROWN: I have no idea what they have to do. The few reg guides I looked at don't tell you how to draw that says you have to design a system that meets these overarching criteria. So I'm trying to restrain myself and not do --

CHAIRMAN CORRADINI: That's okay. We'll restrain you in case you get out of control.

MEMBER BROWN: Oh, good. I'm not out of control yet.

MR. POPPEL: Okay. I'll pass on this. We discussed this. I wanted to talk a little bit about displays, and I wanted to make several points

associated with the main controller. All of these displays, there's very few switches in the main control room. The switches are either fail-safe type switches or fiber type switches or they're VDUs. The VDUs are connected to the DCIS room, the two non-safety DCIS rooms or the four safety DCIS rooms, only via fiber and with a robust communication protocol. And those rooms are in an different environment and a different fire zone than the main controller. So in other words, the loss of the main control room does not cause anything to happen to the automatic logic or the manual logic capability that's in those DCIS rooms. And, of course, the loss of any one DCIS room is the same as the loss of a division. I'm sorry, yes? Well, and I also wanted to make sure that the Q-DCIS were indifferent fire boundaries and the two non-safety DCIS rooms, and all of them are in a different fire boundary than the remote shutdown panel. So the traditional scenario for inadvertent actuations are something is in the main control room causing all kinds of bad things to happen. However the main control room is lost, via smoke or fire, whatever actuation, we lose none of the automatic or manual capability of the safety or non-safety systems, and the remote shutdown panels are individually capable of

operating div one, div two, or the plant investment protection systems or the balance of plant systems, depending on what tower is available associated with the accident in question. So the remote shutdown panel should be thought of as little control rooms because they have the same displays, safety and non-safety, that the operator has at the main control room with the same human factors that the operator would see in the main control room.

MEMBER STETKAR: Now we're interrupting. You're going to talk about the remote shutdown, if we get to it. And if we don't, I'll interrupt you. Let me pull back to the main control room because I understand everything that you said if I think in terms of a designer thinking about the way the system should respond to design basis accidents. I don't understand what you said where fire and smoke does not cause inadvertent actuation. I'd like you to explain a little bit why I cannot have a fire in the main control room that affects, for example, the safety VDU that fires the squib valves for, you know, DPDs, for example. Why can that not happen?

MR. POPPEL: The safety VDU does not fire the squib valve. The safety VDU gives a command which has a sequence numbers, addresses, cyclic redundancy

checks, etcetera. The authentication wrapped around the message that says I've pushed a button that says fire is much, much bigger than the one or zero which says fire itself. And it goes to the --

MEMBER STETKAR: Let me interrupt you, please.

MR. POPPEL: -- and then you have to do it twice. So the chances of a fire melting the VDU causing that communication, that very specific communication to happen in that very specific time interval, while I can't say it's zero, it's next to incredible.

MEMBER STETKAR: How does an operator, if an operator wants to -- and let me not use DPVs because I know they're interlocked with the reactor pressure. Let me initiate ICS, which is not interlocked with reactor pressure. How does the operator initiate ICS? Does he simply touch the screen and say open condensate return valve?

MR. POPPEL: There's a whole human factors group that deals with those things, but we have an overriding rule that says no actuation is done with a single action. That gets rid of the coffee, you know, spills and the elbows on the --

MEMBER STETKAR: I understand that. But

on the --

MR. POPPEL: So what will happen is, in most probability, the way we did it at Lungmen is you touch the valve and a pop-up comes up, and it says what do you want to do with this valve?

MEMBER STETKAR: But it's on that VDU.

MR. POPPEL: That VDU.

MEMBER STETKAR: Okay. So why can a fire not open that valve if the fire affects that VDU?

MR. POPPEL: Well, when you say it's on that VDU, what's on that VDU is, if I touch the screen, I'm sending that authenticated message out of the control room by fiber. And the message must be just so as received by the TRICON to say this is a legitimate command to open the valve. And then he has to do it again. So in other words, armed fire or a select, you know, action. So in other words, for the VDU to actually, the operator or the VDU to actually cause that to happen you have to have two very, very precise messages in a precise time interval to get to the TRICON and be received by it for it to be considered authentic. So a VDU under smoke or fire assault is not going to do that.

MEMBER STETKAR: Is not going to do that?

MR. POPPEL: Is not going to do that.

MEMBER STETKAR: It's impossible?

MR. POPPEL: I would have said it's statistically impossible, but a 64-bed --

MEMBER STETKAR: Okay. The reason I raise this is that this says "does not cause." The DCD says "does not cause." And in fact, when the staff comes in, the SER says a fire in the control room does not cause a whole bunch of things, except for maybe a turbine trip. And the words "does not cause" are very, very precise, specific words. That means it's impossible, cannot happen. You said that it could happen under certain combinations of multiple, I don't want to call them hot shorts because we're not talking about hot shorts but spurious signals.

My only point here, and we don't have the time to discuss this, is that, from a design perspective, we, when we think about the design, need to think about all of the possible things that could go wrong with that design in all possible locations. And saying that something cannot happen is a very, very strong statement. Saying that it's not very likely for the following reasons is much different, but in all of the written words that I've seen it says it cannot happen, and that's a very, very strong statement. That is a, it's a beyond robust design.

It's a design that is really different. So that's why I ask the question because of the statements of fires in the main control room cannot cause spurious actuation of things. We can discuss this for a long time, but I wanted to understand. I understand now your concept of the dual armed fire within a certain, you know, confirmed within a certain period of time. I've seen a lot of systems like that.

MR. POPPEL: But maybe not the message authentication.

MEMBER STETKAR: Yes, Siemans has one.

MR. POPPEL: Well, okay. I mean --

MEMBER STETKAR: Continue.

MR. POPPEL: Okay. I'll leave it with Rich to deal with impossible versus highly unlikely.

CHAIRMAN CORRADINI: On that note, let's keep on going.

MR. POPPEL: Okay. This is the diversity slide that Rich first put up, and a few points so you walk away understanding what we've done --

MR. MILLER: Excuse me a minute. You notice on the screen the hatch marks, because we changed it to PDF, are a little different than your handout. Just to note that. The handout is correct, although the handout printed a little different than

our normal PowerPoint.

MR. POPPEL: The reactor trip in ECCS, these are two different systems. By systems, I mean in this case hardware, software, platform. They do not have a common operating system. They do not have common hardware. So ECCS is separate from reactor trip.

Somebody asked are we going to discuss ATWS/SLC and the vacuum breaker isolation valve, that's a third separate safety-related platform. It's not really a hardware/software system. It's a non-multiplex ASIC type design that doesn't use an operating system, but it is completely separate from these. The only common thing in this whole row is they're all powered by divisional power.

MEMBER ABDEL-KHALIK: How about instability detection?

MR. POPPEL: Instability detection is in NMS in the reactor trip system, if you will, the neutron monitoring system. So all of those are separate, and they're all different than the non-safety. So safety separate from each other and safety separate from non-safety. In this particular case, we have the triply redundant DPS system here, and we wanted to make a point clear that it is a separate

hardware/software platform from the safety system. So the triply redundant DPS is there to mitigate against common-cause failure of the safety systems, and those are the safety systems that we're talking about the common cause failure of.

So to do that, the DPS has some scram functions, some isolation functions, and some ECCS functions. Those are the functions that are needed to accomplish the 10 CFR 100 limits, should that stuff fail.

In addition, in this same row, because it's also important, you may have heard the word BiMAC, you may have heard the word system, you may have heard the word severe accident system. This is the system that says everything else has failed, the core has melted through the vessel, and, therefore, none of the other stuff worked because if it did work the core never even got it covered. But if it didn't work and then what this system will do is dump the gravity pool of water pools into the vessel bottom, and it does that with its own separate power and, I don't want to use DCIS, it's basically a PLC, but it's a pretty simple-minded design, okay? And so it will run if everything else fails.

And then the last row, this is safety

again, versus non-safety, and so these systems are non-safety and, in general, all our control systems are Mark VIe's done as either a triple redundant or dual redundant.

MEMBER BROWN: By control system, you mean like a feed water controller?

MR. POPPEL: Yes, exactly.

MEMBER BROWN: So when you talk about triple redundant, presumably one controller is controlling at any one time, or are they fighting each other?

MR. POPPEL: No, no.

MEMBER BROWN: There's no architecture description for that in here; that's why I ask.

MR. POPPEL: Okay. When the rest of the world decided that they wanted highly-reliable control systems, one of the ways to go about it was the nuclear way, which was to have independent systems and multiple systems. Most of the commercial folks did not like that. They just wanted one box, which had an extremely high reliability. So the three controllers in the triple redundant control systems talk to each other all the time, constantly, through their cycles of acquiring data, etcetera, etcetera, and they talk to output switches that do two out of three voting.

In the case of the turbine, we actually have three servos on each of the valves.

MEMBER BROWN: So they're all synchronously operating effectively?

MR. POPPEL: On the --

MEMBER BROWN: It sounds like the shuttle control systems for --

MR. POPPEL: Yes. Within a triply redundant control system, they are synchronized, but they are not in any way synchronized with each other, other triply redundant control systems, or with safety or --

MEMBER BROWN: You've got three controllers controlling a bell, those three controllers, if you're going to be doing this, sound like they need to be synchronized with each other. In other words, they're processing all the information --

MR. POPPEL: In reality, what happens is the last thing on the way, the two out of three voter on the analog output or the discrete output is what determines whether that thing happens. So in other words, if two messages don't arrive there at the same time, it doesn't do anything. So in that sense, they have to be synchronized.

But the point I'm trying to get across

with this is that the triply redundant control systems and the dual redundant control systems that exist have been applied. In Lungmen's case, for example, we have a steam bypass and pressure controller and a reactor level control system that is, in fact, made up of a Mark VI. It will not be identical because we have different types of actuators, different this and that. But there is no question that they can be built, they exist, and we have, for the Lungmen case not yet because it depends on the actual components inside the box, but we have analyses from Lungmen which indicate mean time between failures of these overall non-safety systems beyond a thousand years, okay?

MEMBER BROWN: That's analysis?

MR. POPPEL: That's an analysis. You know, and it's hard --

MEMBER BROWN: Do you really believe that?

MR. POPPEL: Well, what we're trying to do -- in fact, I do. But I'll say it in this way. The reason that the thousand years isn't as important as greater than a hundred years because what we're trying to do in Chapter 15 is say this is not an anticipated operational event the failure of this control system, it's an accident. And we can easily justify the 100 years.

As an anecdotal point, the TRICON folks will tell you, and this time I will use the word never, they have never failed to close a contact when they were supposed to. They have never failed to, it never inadvertently closed a contact. That doesn't mean they've never failed. The whole design of the triply redundant control system is to have all kinds of failures and survival and get them analyzed in time so that you can fix it before the next failure. But that's 7,000 TRICON systems and I forget how many TRICON years of operation. So I can say, at least so far, never.

The Mark VIs, VIe's haven't been around as long as the TRICONs have. However, because they control the main turbine, etcetera, etcetera, in commercial industries, there's a large incentive to make them very reliable systems. And the only reason I'm saying this is that's what our non-safety systems are composed of is we don't have single failures in the DCIS for non-safety or what you might call balance of plant control. We believe that means the plant is much less likely to initiate transients as opposed to having systems deal with them. And that goes with the transmitters that feed them, the power that feeds them, and the actuators that they supply.

MEMBER STETKAR: Let me ask you a couple of questions, and this is a better slide to kind of focus those questions. First, a quick one. You mentioned, and I paged ahead and you're not going to talk about it, but the Q-DCIS deluge, the BiMAC deluge, and in Chapter 7 is the first time I came across the independent batteries and things like that. What's the design life on those batteries if I have no AC power, if I have no chargers?

MR. POPPEL: The correct answer is I don't know, but I recall a conversation with John Stryhal, and they're going to make them, I believe, the same 72 hours that the other, the safety battery is.

MEMBER STETKAR: But that hasn't officially been specified yet or you just --

MR. POPPEL: I just don't know.

MEMBER STETKAR: Okay, fine.

MR. MILLER: You said design life or you mean --

MEMBER STETKAR: How long will they operate without the battery charger.

MR. MILLER: We can table that item and --

MEMBER STETKAR: Yes, I'd appreciate that only because those things might be required at some later time.

MR. MILLER: I think it's 72 hours, but we'll confirm.

MEMBER STETKAR: Okay, thanks. Because I hadn't seen those --

MR. WACHOWIAK: I think it's longer than 72 hours.

MEMBER STETKAR: I hadn't seen those anywhere else, but I didn't go back and double check. That was the simple one. The more complicated one is ATWS/SLC, and I'm not, what I'm trying to do is to understand how the different parts of the plant fit together. As I understand it, your independent control platform, the third block from the left under Q-DCIS is your ATWS/SLC platform. And I know that that's a diverse means of actuating SLC, or is that the only means of actuating SLC?

MR. POPPEL: No, DPS can --

MEMBER STETKAR: DPS can do it, too. Do the signals from that ATWS/SLC platform go through DPS to the squib valves?

MR. POPPEL: No. For everything DPS does, for want of a better word, it does it in parallel with the safety system. So it's not a series path to get to the recovered action.

MEMBER STETKAR: Okay, got that. One

function I noticed that was described was isolation of the SLC injection line, so you don't inject nitrogen. There's a low level on the accumulator isolation signal that isolates the SLC injection lines. Where is that signal developed?

MR. POPPEL: Okay. Imagine a cabinet in the Q-DCIS room, one per division, and it's called the RTIF cabinet. And in this bay, they have, if you will, the reactor protection system. So there you will see the DTM chassis, the DLU chassis, etcetera, and you can look at that. And in another bay that will have the ATWS chassis, okay? So this is all safety, it's all powered by safety, but the ATWS/SLC and the VPIF are done, even though they look like a NUMAC chassis, they're not a NUMAC chassis. It's like an ASIC type system, you know, where just --

MEMBER STETKAR: Just say that it's developed in that --

MR. POPPEL: Yes, it is.

MEMBER STETKAR: Okay. So the isolation is developed in that ATWS/SLC?

MR. POPPEL: Yes.

MEMBER STETKAR: Now, here's a question that I don't know the answer to, and it might be a thermal hydraulic. If I have an ATWS condition, and I

have a couple of signals. One signal is to actuate SLC, and another signal is to run back or stop, in this case, feed water from that. Will I get to a level one signal on that feed water?

MR. POPPEL: Yes.

MEMBER STETKAR: Okay. Thank you. Hence, my question now. Under the SSLC ESF function, there is a SLC, a standby liquid control, actuation signal from SSLC ESF; is that correct? Because that's on low level, it fires it because you take credit for the water going in. How does now the situation that I have a real ATWS, I have a level-one signal, SSLC ESF says inject SLC that has a confirmatory open signal for those isolation valves. I now get to a low level in the tank. The low level comes in through this other platform that says close the isolation valves while level is still low. Who wins?

MR. POPPEL: I didn't -- if you tell those valves, the injection valves to fire --

MEMBER STETKAR: Not the squib valves, the isolation valves. The isolation valves --

MR. POPPEL: Once you told them to fire, they're going to dump, and then the only logic left is the level logic.

MEMBER STETKAR: But the level, you're

saying that the level logic in this other platform overrides the SSLC low level in the vessel logic to open the isolation valves? Is that what you're saying?

MR. POPPEL: I'm probably not understanding the question well.

MEMBER STETKAR: Okay. I have to use a graphic here. This is the reactor vessel, and if I have lower than level one in the reactor vessel, I have a LOCA signal. And the LOCA signal actuates standby liquid control and not only fires a squib but gives a confirmatory open signal, from what I could read, to the isolation valves. In case, for some reason, the isolation valve was closed, it sends a signal to open that isolation valve. That's what I read.

MR. WACHOWIAK: The piece that you're missing is that if we have an ATWS signal it also generates an ADS inhibit, which is preventing the second sequence from doing what you're saying it's going to do.

MEMBER STETKAR: The second sequence?

MR. WACHOWIAK: Yes, the level-one actuation in the ECCS system is inhibited by the ATWS.

MEMBER STETKAR: Well, but you said just

running back feed water will give you level one.

MR. WACHOWIAK: It will. But if you have a confirmed ATWS signal, it generates an ADS inhibitor, which eliminates that level-one trip from doing anything.

MEMBER STETKAR: But that inhibits the DPVs and the GDCS squib valves --

MR. WACHOWIAK: And I would expect it also to --

MEMBER STETKAR: I didn't expect anything, so I just read what I read.

MR. WACHOWIAK: Right. So you didn't see where it also prevented the standby liquid control and ECCS injection in addition to the DPVs actuate SRVs, DPVs, and GDCS valves.

MEMBER STETKAR: I saw where that inhibited those things so I don't blow down the vessel and I don't inject GDCS.

MR. WACHOWIAK: We'll have to check on --

MR. MILLER: Yes, we'll table that item and look at the DCD --

MEMBER STETKAR: It's not in the DCD.

CHAIRMAN CORRADINI: We need one person to speak at a time.

MR. MILLER: Rich Miller. We'll table

that item and then look into it and make sure the proper words are in the DCD.

MEMBER STETKAR: Thank you.

CHAIRMAN CORRADINI: So this is more of a time check. We're at a break point. Is this a time we can break and come back after 15 minutes of --

MR. MILLER: I would say so. We've got a few more slides on diversity, but we can pick up at that point.

CHAIRMAN CORRADINI: All right. So let's take a break for 15 minutes, until ten of.

(Whereupon, the foregoing matter went off the record at 2:42 p.m. and went back on the record at 2:59 p.m.)

CHAIRMAN CORRADINI: We are back in session. We're energized. We're triply redundant. Let's do it.

MR. MILLER: Rich Miller to get back on the diversity. We've got this slide up here, and we've got a few more slides here for this on diversity.

MR. POPPEL: Okay. This is, again, another representations of the same DCIS and has a little bit more but different kinds of information on it that I wanted to emphasize. You may see the same

five segments that by now you should be used to drawn there as arrows. But a little hard to tell in terms of some of the things we wanted to say about determinism and network security.

MEMBER BROWN: There's six segments up there. Where's the --

MR. POPPEL: One, two, three, four --

MEMBER BROWN: What's the one up at the top?

MR. POPPEL: That's a, if you will, not the control network. That's called a plant data highway and has things that are relatively innocuous on it, like printers.

MEMBER BROWN: Oh, okay. All right.

MR. POPPEL: It's not what you would call a control network, although it still has -- and, incidentally, that's the network that the outside world connects to. The outside world doesn't get to directly connect to the control network and the connection is through one of those managed switches. However, in this particular area, this is a safety system. This is the SSLC ESF, and see this little arrow here, and we have the same kind of little arrow here on the non-safety side. What this is meant to say to you is we are not doing close-loop control over

the network. In other words, this box has a job to do: measure this level, multiply it by three, and output that contact. The level it needs, the algorithm it needs, and the contact it's controlling is all within that closed loop. It's not coming from another division. It's not coming from non-safety. So it's a stand-alone little thing that has nothing to do with, for example, the two out of four thing for the voting or for the displays that are being run by the system. Similarly, on the non-safety side, okay? So this is deterministic because, I'll be cautious with that word, but, say, because the program is meant to be that way. This is deterministic because the Mark VI controller is controlling its own data acquisition, okay? It's not asking the network to give it data. It's saying, "Hey, remote multiplexer connected to me, I want to find out about this level, and I'm asking you now."

MR. WALLIS: It's not deterministic as stand alone?

MR. POPPEL: Okay. Stand alone. But it asks for that level every ten times a second, whatever set up the program. So in other words, the level is not coming from another controller over a switch and back into it.

MR. WALLIS: But it measures the level.

MR. POPPEL: It measures the level --

MR. WALLIS: And supplies both, doesn't it?

MR. POPPEL: The point I wanted to make was, for example, the reactor level controller, it actually has four level transmitters, but that's not so much the point. It has RMUs in multiple locations in the reactor building to acquire level.

MR. WALLIS: So there's something in the vessel which actually measures the --

MR. POPPEL: Oh, yes, that's the standard differential pressure --

MR. WALLIS: That gives some signals to anything that needs it.

MR. POPPEL: Wrong way to phrase it. For control purposes, be it safety control or reactor level control, that transmitter is connected to an RMU for that system to be used by that system in order to do whatever control it needs. It can make available to anything else, "Hey, you want to know what reactor level is? I'll tell you." But those things that we make it available to aren't controlling reactor level or not controlling the safety system.

MEMBER STETKAR: I think he's asking, I

think he was asking a different direction question. Was the question that if ECCS needs to know reactor level and level control needs to know the level, is there one transducer, or is there one transducer per control --

MR. POPPEL: We had a slide for that, which was deemed to be too complicated, believe it or not. The reactor trips on level. It has four divisions of level transmitter for reactor trip. ECCS initiates --

MR. WALLIS: Four transducers or one transducer?

MR. POPPEL: Four transducers, one per division, connected only to the reactor trip system or I should say to the reactor trip systems RMU. ECCS, the SSLC ESF initiates on reactor level. It has its own level transmitters that are not the ones used by the reactor trip system.

MR. WALLIS: So it has different transducers?

MR. POPPEL: Different transducers, four of them.

MR. WALLIS: So when you say transmitters, I think you're talking about the electronics?

MR. POPPEL: No, I should say transducers.

ATWS/SLC fires off on low level. It has its own four transducers, okay? Reactor level control has --

MR. WALLIS: So this with all these transmitters?

MR. POPPEL: Yes, it is. But it's more than 12 because we have wide range, narrow range. But per function, they're all separate.

MEMBER STETKAR: For example, like whatever controls the level three range or the level two --

MR. POPPEL: We did not believe we could get away --

CHAIRMAN CORRADINI: Excuse me. We're having conversations that I think we want on the record that are not getting there.

MR. POPPEL: We did not believe we would achieve the correct amount of diversity by having different controllers all operating from the same transmitter. So the transmitters are just as diverse as the controllers.

MEMBER BLEY: So how many times have you stuck the pig in terms of piping to do all this? Are you having a tap for every one of these?

MR. POPPEL: If you look at the reactor vessel, if you look at a plan view of the building,

each safety division is in a quadrant, okay? Let's just talk about narrow range level. So a narrow range level signal will come down for div one to an instrument rack in this quadrant. The reference leg and the variable leg will go here. Similarly, a separate set of reference and variable legs to the division two, division three, division four. So there's four instrument racks. On the instrument racks, we have multiple transmitters, okay?

MEMBER BLEY: But each rack has one set of taps?

MR. POPPEL: Yes.

MR. MILLER: Per division.

MR. POPPEL: Yes, one per division, so there are four sets of taps. So the transducers are the same, but the instrument column, the transducers are different but the instrument columns are the same per division.

MEMBER BROWN: So the reference legs are the same for all 12 detectors?

MR. POPPEL: No. The reference legs are the same for all the detectors in one division.

MEMBER BROWN: Okay, per division.

MR. POPPEL: Per division.

MEMBER BROWN: Okay.

MR. POPPEL: And, if you will, per non-division because the non-safety systems measure now a range level also.

MEMBER BLEY: Off of the same four taps?

MR. POPPEL: Yes.

MEMBER BROWN: Okay. Let me restate that. Division one of the RPS has four level sensors. No, there are four level sensors that feed the RPS system. There are four separate taps and reference legs for those. The same taps and reference legs are then used for the four separate detectors for the ESF functions that require level. So the holes to plug into the different pipes coming out, is the reference leg the same for all the detectors in each division?

MR. POPPEL: Yes. There's only four reference legs.

MEMBER BROWN: Okay. That's enough.

MR. MILLER: The reference legs are an extension of the vessel.

MEMBER BROWN: Yes, that's fine.

MR. POPPEL: So an individual transducer failure can't do more than one out of four, whether it's active level control --

MR. WALLIS: They're all four physical links?

MR. POPPEL: But when you made the question unless it leaks, putting aside the question about sump levels and all the rest of it, basically a div one and div two and div three and div four might say 30 inches, 30 inches, 30 inches, and 20 inches. And the common reactor level controller will receive 30, 30, 30, and 20. Their validation algorithms will say, "Hey, that 20 doesn't agree with anything. Throw it out. I'm controlling on 30 inches." The safety systems will say, "Hey, this must be a legitimate 20-inch thing; I'm going to trip. But I'm only one division. I need two divisions per parameter un-bypassed to trip." So, of course, the first thing the operator is going to do when he learns there's a leaky instrument line is put div one in bypass, meaning that trip decision will no longer contribute to the two out of four, okay? So in other words, we're going to get an alarm and nothing is going to happen.

MEMBER BLEY: So I think I got it. In one division, a hanging Rosemount will only affect that one transmitter, but a leaking bellows might affect the whole division?

MR. POPPEL: It might affect the whole division, but only that division.

MEMBER BROWN: For ESF, RPS, and whatever

the third set of --

MR. POPPEL: Yes. And we have bypass switches for the sensors to say those are the joystick fibers which is that say you only bypass one division at a time, and so I have determined that div one is bad for whatever reason, so neither -- and we have separate sensor bypasses, "Hey, ECCS, don't pay attention to div one," "Hey, RPS, don't pay attention to div one," and the level control system will automatically not do that, but we have a bypass also.

MEMBER STETKAR: Since you mention bypasses, you can bypass a full division of sensors and a division of, a different division of logic simultaneously; is that correct?

MR. POPPEL: Yes.

MEMBER STETKAR: So I can have division one sensors all bypassed and let's say division two logic channel bypassed?

MR. POPPEL: Yes, for the trip system.

MEMBER STETKAR: Okay.

MR. POPPEL: But there is no combination of bypasses available to the operator in the control room that will ever degrade this system to less than two out of four like un-bypassed parameters. No bypasses that he can do in the control room that will

do that.

MEMBER BROWN: Well, you just mentioned if you bypass -- correct me if I'm wrong in thinking here. But a whole set of sensors and then I bypass in one of the other divisions the trip logic, I have effectively taken two divisions out of service, and I have two left.

MR. POPPEL: And the logic is any two un-bypassed like parameters will scram. So if I've got two divisions left --

MEMBER BROWN: But I've bypassed both of them physically, and now I'm down to two out of two.

MR. POPPEL: Well, no. But the point is those two are now un-bypassed and presumed good. So if you get an actual level trip and the two un-bypassed logic, un-bypassed sensors, you will scram.

MEMBER BROWN: Let me phrase this a different way because I don't think I'm understanding. I've got two of four divisions now effectively unable to do a trip?

MR. POPPEL: No.

MEMBER BROWN: Well, I've taken the sensors out of one division --

MR. POPPEL: No, no, now wait. When you take the sensors out in div one --

MR. WALLIS: You get a trip in that circumstance?

MR. POPPEL: No, no. When you take the sensors out in div one, what you're telling the trip logic units is in div one, in div two, in div three, in div four, don't pay any attention to the div one level. That's what you're saying. However, both div one, div two, div three, and div four, all four divisions still have access to div two, div three, and div four levels. So each one of those systems is still capable of making a two out of four, one of which is no longer contributing, decision on trip. And so, therefore, all four divisions, if you get two reactor level trips in any of the remaining three divisions, you're going to get a --

MEMBER BROWN: If I bypass the trip logic in the second division, you're saying the signals that tell its own division to trip will still go to division one through trip logic, theoretically, since you can't bypass that.

MR. POPPEL: So you still have --

MEMBER BROWN: So you still have three. Okay, all right. Thank you.

MR. WALLIS: So you've got four signals of reactor level and you get one which is different, you

say there's something wrong with that sensor when it could be telling you something about the thermal hydraulics of what's happening in the vessel. The fact that one of them reads something different from the other might tell you something about what's going on in the vessel. You're sort of assuming that it's a bad signal.

MR. POPPEL: No, I'm not assuming --

MR. WALLIS: No, but that's the way you're talking. Ignore it. You want to say, "Look, something is strange."

MR. POPPEL: No, no, ignore it is bad, okay? I mean, it can only come in to you as an analog value. For the reactor protection system, the analog value will be it's tripped or it ain't tripped. That's your only two choices: it's above the trip or below the trip as determined by the logic. You can tell that logic please ignore that signal, but you can only tell it in one division, okay? And so separately we have, you know, proven to ourselves at least that three divisions or two divisions of level measurement, which, incidentally, is what an awful lot of BWRs have --

MR. WALLIS: The thing I'm concerned about is, if you see that you've got four signals and one is

different, it may be telling you something real that's happening.

MEMBER STETKAR: In our scenario, it told you you had a leak.

MR. WALLIS: There maybe some three-dimensional flow pattern or something which makes the level --

MR. POPPEL: In our non-discussion of self diagnostics, in terms of -- first of all, this will happen in several ways. In terms of the reactor protection system, basically you've got 30, 30, 30, and 20. Immediately, you will get an alarm from the tech spec monitor that says you have an inconsistent level. So whatever happens, it's not silent. And so now it's up to the operation staff to determine what the importance of that might mean, whether it be bypassed or not.

MR. WALLIS: I am concerned about them having a mind set that if they get one out of four it's immediately discounted. That's the only thing I'm worried about.

MR. MILLER: Rich Miller. There will be operating procedures that occur, okay, that you cover that alarm --

MR. POPPEL: Well, and then on the non-

safety side for example, the reactor level control system will also alarm and say, "I have inconsistent signals," but probably we could all agree that it's better to control on the consistent signal than the inconsistent signal. And so, therefore, in that case, it will be ignored, okay?

CHAIRMAN CORRADINI: But there would have to be other action taken if there were other associated alarms that showed a different sort of behavior. I mean, if you're going to have --

MR. POPPEL: I mean, what we want to do is control level no matter what with the best information we can, and we're not constrained like the reactor protection system. We can set up the system to control -- I mean, if signals are inconsistent, it's easy to tell. If there's only two signals left and they're different, it's hard to tell, but we can control on the average. We can also, since 99 percent of the time the way transmitters fail is they go down scale, so that's another way to say the reactor level control might react a protection. We can say, okay, we know this one is bad because it's hard down scale and alarms in any case.

MEMBER BROWN: By down scale you mean?

MR. POPPEL: The transmitter went to zero

milliamps instead of -- we have a live zero, 4 to 20 milliamps. So if the power supply failed, unlikely, or the transducer itself failed, most of the time they failed to below four milliamps. There are failure possibilities hard above 20 milliamps, both of which we detect in both the safety and the non-safety system. The safety system says, hey, trip. The non-safety system control says ignore. But it's rare to have a transmitter fail like I described, 30, 30, 30, 20. That's rare. Now, you can imagine leaks and stuff like that; it's hard to imagine leaks unaccompanied by alarms or reactors making their rounds in the buildings. So I think we're pretty well covered for that.

MR. MILLER: There's also on these instrument lines excess flow check valves that basically detect a leak and give you a signal to close and fail the transmitter to zero.

MEMBER BROWN: On the sensing lines?

MR. MILLER: Yes, the sensing lines coming out of the vessel.

MEMBER BROWN: You have a flow detector --

MR. MILLER: Excess flow check valves that we usually use on those sensing lines, and it's got a differential around it. That differential closes that

valve and, therefore, isolates the leak and, therefore, the sensor has noted that changed state in a safe direction so that you ignore that transmitter. If I alarm, the operator would have a procedure to follow to check it.

MEMBER BROWN: You know, one of the interesting things that falls out of this discussion is, again, there's words in the text which allude to the discussion but no figure showing the arrangement or the actuation of these concepts as to how, you know, the two things can go into different places, yet you still have two out of three. There's no examples, figures, details that allows that to be discerned from the DCD, which leads to the conclusion that if you pass this on to somebody that's got to design the system and we've certified it, how do you know they will execute it in the manner in which it's described in the DCD? There's nothing, the detail is so lacking that maintaining the configuration control of the design process as you go forward actually designing and building something from this stage, from the certification stage, it's difficult to get comfortable with that that's the way it's going to happen. Well, I mean, if the information is not in there, and that's one of the difficulties. There's some good comments

that have fallen out of this discussion which is all very illuminating but . . .

MR. WALLIS: I'm just trying to think this through. If you get a regional instability, I'm not sure that transducers on both sides will measure the same level.

MR. POPPEL: On the core or on the --

MR. WALLIS: The transducers simply measure pressure, and momentum and stuff could be going on as well, and you're not quite sure what you're measuring. So it seems to me there are modes of operation where you might get, forcing those different for good hydraulic reasons. So it's not just the logic of --

MR. POPPEL: We have not observed such instabilities in -- we have observed isolation and level signals, not different isolations around the vessel, but we have seen that in flux because the cores are so big that they're like infinite cores. But that stability detection is in the neutron-monitoring system, but GE doesn't think that looking at reactor level is a good way to --

MR. WALLIS: I don't want to prolong it. Sometimes when you get signals which are inconsistent, it's telling you something. That's all. That's all

I'm trying to say.

MR. MILLER: If there are signals that are inconsistent, they'll be alarmed; and, basically operators have to follow procedures.

MR. POPPEL: Several other things on this chart is, as I said, the closed loop control is self-contained in the control room. The reason I'm saying that is when you ask questions about data storms here on, quote, the network, which is really five networks, which is really five redundant networks, they don't affect the closed loop control. What they will affect is the operator's ability to manually control stuff, but the autonomous control reactor pressure, reactor level, etcetera, will continue based on the last known set point. That's the first comment.

The second comment is part of this built-in isolation cyber security, etcetera, etcetera, this is not a connection to the network like you may be used to with a traditional commercial network. I don't really mean to be too technical, but it's not a TCP/IP protocol to the network. This is ethernet global data and too many buzzwords, but the bottom line is these controllers cannot be told. They are programmed to ask for data. So other controllers could put data on a network which these controllers

will go look for, but they cannot be told stop what you're doing and listen to me. That's not possible with the EGD protocol.

MEMBER BROWN: How does an operator then take a manual action to tell it to stop or start?

MR. POPPEL: Because that's one of the things that it's looking for. It's been told to look for a specific operator command with that kind of anti-corruption protocol on it.

MEMBER BROWN: I mean, what's the data flow --

MR. POPPEL: But it's not like you say, "Hey, I'm pinging you, answer me back." There's not an interval. He's been told to look for a reactor set point, and if he doesn't get it it's still controls. So the point is even if data storms got on this network or bad guys got on this network, that works, which is highly unlikely, it doesn't affect the controllers. It doesn't affect the safety controllers, and it doesn't affect the plant controllers.

MEMBER BLEY: Let me just ask a question here. You've talked about this a number of times. Given I want to carry out one action, which we talked about earlier, there's this specific pair of

authentication codes that you have to match up. But how many different sets of authentication codes are there? I mean, the chance of hitting a specific one is extremely low. Are there tens, hundreds, thousands of these?

MR. POPPEL: Millions.

MEMBER BLEY: Because the chance of hitting one, even though you don't know what it is, is small, as we've been talking.

MR. POPPEL: Yes.

MEMBER BLEY: So it's on the order of millions out of a 64-bit scheme?

MR. POPPEL: Yes.

MEMBER BLEY: Okay. So that's still pretty small. But it's millions of codes that are --

MR. POPPEL: Very specifically, because it seems to be an issue, in the communication protocol, as you can imagine, there will be a sending address and a receiving address, so everything has an address. That's pretty standard, so just so everybody knows. So that has some uniqueness by itself. In addition, it has a sequence number. This is the first time this thing has communicated with that thing. When the communication has been deemed successful, the sequence number changes to two. So that way, the receiving

controller, if it got a one the last time and now gets a three, it knows it missed something or knows it's coming from the wrong place. And so the sequence is unique per communication between two devices. And so that makes it kind of unique.

Then you have this cyclic redundant -- there's a few other things in there too, but the cyclic redundancy check is you add up, you know, all the ones and zeroes, divide by the 64, and put the remainder in the message as a cyclic redundancy check. And then the receiving controller does its own cyclic redundancy check, and if it doesn't match it's not an authentic message. So address, sending, receiving, sequence number, cyclic redundancy check twice in a specified time interval.

MEMBER BROWN: So that's a data validity issue, which you addressed, but it's still a land type operation where you can overload it with data, commands, whatever, unless it's a very dedicated, whether you've limited the loading you can put on that bus such that you don't end up with collisions that don't allow stuff to get places. I mean, the last thing you want is to command something to stop doing something and the message does not get there in a timely manner.

MR. POPPEL: We need to make sure exactly what we're talking about. Yes, anything to do with a timely manner, meaning a human being is in terms of seconds, because basically all of our instructions say put your hands in your pockets until you know what's going on and then try to --

MEMBER BROWN: I'm not talking about the human reaction. We can turn a switch and tell something --

MR. POPPEL: In a timely fashion, yes. First of all, this display is on this switch which talks to, say, the PIP A controller. It's not the PIP B display, and it's not the PIP B controller, okay? If this controller fails, if this network switch fails, it has nothing to do with the other network switch. It has nothing to do with that other communication path. First comment.

Second comment is I said these were network-managed switches that are far more than traditional switches. In addition to the kind of thing that says, "Who are you? I'm not going to let you talk," the switches can also monitor traffic. So for example, if one of these controllers -- the controllers are all dual-ported, so there's always two switches in a segment. So if one of these controllers

went crazy, it could happen, and just flooded one of those switch boards, the switch would turn it off. It wouldn't let it flood the network.

So strangers can't get on. You can't have a data storm from a controller failure. An outside world thing can't get in there in the first place, and the controller can't be told to ignore what you're doing and listen to me. That makes it pretty robust.

Now, it does mean that we do need the network or at least one network to tell something what to do when we need it to be functional. The chances of both switches in a redundant network times PIP A and PIP B going down simultaneously are pretty remote. This is non-safety. The safety stuff doesn't use the network managed switches; it's completely autonomous. We haven't talked about that work yet to address your question. But the point is we believe we're almost immune to data storms, and we believe we're almost immune to the kind of attacks that might go on there, assuming that the firewall over here let it through in the first place.

MEMBER BROWN: But your monitors, your VDUs still require the outgoing data from all of the divisions of all of the stuff to hit those networks and then get into the VDUs. There's got to be --

MR. POPPEL: Yes.

MEMBER BROWN: So that's a ton of data that's being constantly updated at a whatever, your 25 millisecond type time frame is.

MR. POPPEL: Actually, data in front of operators is typically once a second. A busy screen might have a hundred hunks of data on it. Most of our human factor folks would say that's too much. But pick a hundred. So a hundred, you've got maybe 30 screens, that's 3,000 data. That's not going to flood it. It's not even going to come close. This is stuff which is talking about, these switches are a hundred megabit links and one gigabit uplinks, 15,000 message packets a second. And we're talking about 10 to 20 message packets a second.

MEMBER BROWN: So are you using a second for VDU updates for data?

MR. POPPEL: That's up to the HFE folks, but, nominally, most people think updating more than a second just flashes numbers in front of the operators and annoys them.

MEMBER BROWN: I just asked that because when we did it in programs I was with we used the blink of an eye rule, which is another quarter of a second. When I say rule, it's not a rule. It's kind

of a rule of thumb, if nothing else.

MR. POPPEL: Well, whatever HFE determines is the best way to do it. It's not going to be the networks which is controllers that are limiting it. It will be how much HFE wants because it's capable of far more than an operator can absorb.

CHAIRMAN CORRADINI: We should move on --

MR. POPPEL: Yes.

CHAIRMAN CORRADINI: -- or we're going to -- okay.

MR. POPPEL: All right. This is, I'm going to try to address very quickly your comments about the reactor trip system and data path. The individual chassis that you saw in the DCD, the remote multiplexer, the digital trip module, the trip logic unit, etcetera, are connected on a dual redundant ring called a scram net ring and then utilizes shared memory. So if you will, at a fixed pace, I'll say 25 milliseconds, it will be wrong but look close, the RMU says here's reactor level, puts it into a shared memory in the RMU itself, and on the other side of the shared memory is this ring, okay? And then also on that same ring is the DTM, which happens to need reactor level. So it is a function of the ring to say something has changed in shared memory. I have no

idea how that reactor level got into that memory location. I don't know where it came from, but any time this memory location changes I'm going to send it around the ring. So between 5 and 20 microseconds later, everything on the ring knows in its own memory location what that level was and pressure and etcetera, etcetera, etcetera.

MEMBER BROWN: And that's a fixed process?

MR. POPPEL: It's a fixed process. But in terms of the how often you look versus how often it gets around is over a thousand to one speed check. So in other words, having measured level every 25 milliseconds it appears, as if by magic, in all the other boxes almost instantaneously. So, essentially, every box is getting a reactor level of 25 milliseconds. So the DTM box looks in its shared memory and say, "I have no idea how that reactor level got here," although we know it was shared memory and the ring, "so I'm going to go look at my box every 25 milliseconds and go see what that shared memory says about level and I'm going to run a little algorithm that says is level greater than or less than X. And then I'm going to help put a trip, and then I'm going to put the level trip back into shared memory and put it on the ring." And so that trip decision gets to

the trip logic unit virtually instantaneously, and the trip logic unit, which is getting that, plus information point to point --

MEMBER BROWN: You just shifted from the RMU DTM to the DTM trip logic.

MR. POPPEL: Yes. But my point is all of these boxes are not connected, they're connected by the ring. So all the boxes know everything, including diagnostics, about all the other boxes on the ring --

MEMBER BROWN: So the TLU is on the ring?

MR. POPPEL: Yes.

MEMBER BROWN: It's not a DTM to TLU ring?

MR. POPPEL: No. It's all on the ring. And if you will, that's this ring here that we very crudely call the safety ring. That's the ring that's needed to do the function. We also have a non-safety ring, but all the data that goes to the non-safety ring -- I don't want to make it sound like it's non-safety. It's a fiber ring attached to the safety component and the shared memory isolates it, no idea how it got there, it's just there, and sends it all to a box here, which has the rings from the other division, so that this box knows everything about div one, two, three, and four basically instantaneously. And so this ring can go down, and all that's affected

is isolated data transmission to the non-safety. If this goes down, if the RMU isn't putting information on the ring, the DTM assumes all of the information coming from the RMU is tripped. It's the fail safe program in the DTM, not in the RMU.

MEMBER BROWN: Where's the description of all this in the DCD?

MR. POPPEL: That's a general question that I'm sure will come out of --

MEMBER BROWN: No, that's a specific question.

MR. POPPEL: Well, no, no, no, I mean we will have to discuss how we're going to deal with what information goes in the DCD as a general thing about how specific it has to be.

MEMBER BROWN: Well, based on the figures in there, I had a totally different concept of how this thing operated, not even close in terms of how information was transmitted from RMU to DTMs to TLUs to OLUs out to zero information relative to that entire data transmission path and how that would occur. Zero. I mean, don't take my comments negatively. I'm not objecting. The purpose if it is not to object, it's to try to gain an understanding and to have that understanding documented in a manner

in which we have it, you know, that we have to certify, and it's not there. And that's a key, that whole process is a key element in how the protection system, ESF, that whole, all of those, I presume they all operate the same, in a similar manner. Am I wrong?

MR. POPPEL: All of the NUMAC stuff operates the same, yes.

MEMBER BROWN: All the NUMAC, and so the TRICON, and there's no discussion of the TRICON, whatever that concept is, because the general flow in the ESF of the RMUs and getting data from sensors, it's not in there either. And how in the world, I mean, literally, if I had agreed and said, yes, this makes sense to me, it was on a totally different scale from what --

MEMBER BLEY: There's another side to this, and I guess later when the staff comes out I'd be interested in hearing if you did audits or how you got to this level of information and if you had this level of understanding and if that level of understanding is part of what you see and what you're certifying or if you think the DACs that you have really cover the information that might be needed here to have confidence, and I guess I'd like to hear about

those, too.

MR. MILLER: This is Rich Miller. Yes, we have Table 7.1-1 that basically identifies the requirements for each system for 603, etcetera. We're complying with the requirements, okay? Our hardware and software, our architecture, our platforms, our networks, and so forth will meet the requirements. They're required by regulation that are defined in the DCD, and that's covered by DAC for I&C.

MEMBER BROWN: There is no information that goes from one point to the other. I mean, your discussion in the chapter says we will confirm to reg guide, whatever it is, or a triply standard 603 requirement 5.6, you know, which I guess is independence and something else, and that's all it says. And then the DAC says go look at that and see you comply, but all these other factors relative to independence, determinism, the matter of how this thing goes around, collects data, you need that knowledge or at least we need that knowledge to understand how this functionally is going to do that because, otherwise, you're saying, "Trust us." You're giving me a block and saying, "I've got data coming in and there's something going out, and we're going to meet the requirements within the block, and you don't

need to know," and I've got a hard spot with that.

MR. POPPEL: We don't --

MEMBER BROWN: I may get speared in the chest or something, but I've got a hard spot with not knowing what I'm agreeing with.

MR. POPPEL: We don't mean for you to trust us but --

MEMBER BROWN: That was not supposed to be pejorative.

MR. POPPEL: No, no, no. I mean, we have a process, so if anybody came and said, "What did you do with the reactor trip system?" we will be able to show you, as the design proceeds and through the process, design requirements documents, etcetera. So we say you're going to scram in 60 milliseconds after, you know, so that will be a requirement. And then you might ask where did that come from, and we'll say from the analyses in Chapter 15, and it will be a documented requirement. Presumably, we could meet that anyway we wanted to as long as you met that functional requirement because that's what the analyses show is safe for the reactor.

Now, it's not that we're adverse to describing all of this stuff. Given the state of how CNI stuff changes, you know, in the industry nowadays,

we want to leave ourselves some flexibility.

MEMBER BROWN: But this doesn't have anything to do with the microprocessor or the platform. This is strictly the architecture that you stick this platform within, and all the touch points and where it sits in this ring is irrelevant if you don't care what that architecture looks like. The architecture is what defines the overall operation and the methodology of achieving those end goals of the requirements. You probably want to tell me to shut up and move on.

CHAIRMAN CORRADINI: I do.

MEMBER BROWN: Okay, thank you.

CHAIRMAN CORRADINI: I do want to move on. I don't want to tell you to do anything other than just --

MR. POPPEL: N-DCIS control some of these things we mostly discussed. We talked a little bit about the architecture. I do want to say that the N-DCIS, in addition, it is non-safety but it does provide automatic injection and suppression pool cooling functions that do not require operator input. Those are important things for a long-term cold shutdown. I just wanted to mention that they were there.

The big control systems are triply redundant. All the rest are dual redundant. The big control systems are segmented, so there's not one box controlling reactor level pressure, control rod position, etcetera, etcetera. Many of these things have analogs in Lungmen, not all of them. ABWR, meaning we control reactor level and reactor pressure with Mark VI controllers. We have a rod control system for the FMCRDs that, other than the chain, are too detailed. But the bottom line is is that we are very confident that they can be built with the equipment that we have picked out now and in the architecture.

MEMBER STETKAR: Let me stop you a minute. Steam bypass and pressure control, on the ESBWR, the turbine stop-valve closure and turbine control valve closure reactor scram signals are interlocked with a number of turbine bypass valves that are more than ten percent open within some, I don't know what the time period is and it doesn't make any difference. And apparently that number that is required to open is controlled by the reactor power. In other words, higher power, more valves obviously have to be open. And I don't care what that algorithm is right now. Where is that algorithm developed?

MR. POPPEL: Algorithms. The reactor protection system has an algorithm, actually it's the same algorithm, same program, if you will. But implemented in reactor protection system is something that says based on this reactor power level you need to have X number of bypass valves opened by this time. Totally separate in steam bypass and pressure control, they say, based on reactor power level, this is the number of bypass valves you need to open.

MEMBER STETKAR: Where do the turbine bypass valve status signals come from?

MR. POPPEL: The status signals from the reactor protection system that say they're ten percent open are, in fact, reactor protection system signals --

MEMBER STETKAR: So those are safety related.

MR. MILLER: Those are safety related.

MEMBER STETKAR: Okay. That was what I was curious about because in nothing that I've read did I find that information. I was looking for that because I'm familiar with other designs where those signals come in. They're safety-related signals and --

MR. MILLER: Rich Miller. I think that's

being clarified in the --

MEMBER STETKAR: I missed them, and I missed them, there were a couple of statements in the SER that said, that seemed to say that the turbine, everything related to turbine bypass was completely non-safety related and had no impact on anything.

MR. MILLER: Yes, we make those limit switches on those valves safety related --

MEMBER STETKAR: That's the way I've seen --

MR. MILLER: -- and they're part of the --

MEMBER STETKAR: Fine. Thank you.

MR. POPPEL: Okay. A very quick slide to say just like the safety side, all of our N-DCIS equipment is supplied with two or three uninterruptible power supplies and can run appropriately with power supply failures. So, again, this is just another way of saying there aren't any single failures in the power or the controls for the non-safety DCIS.

This is the thing that's majorly different in the ESBWR versus other plants. We talked about the diverse protection system in terms of what functions it has to do, and it has a subset of scram functions, a subset of isolation functions, a subset of ECCS

functions, and SLC initiation also does some other things I don't want to quite get into now. But this is a stand-alone triply redundant controller, a Mark VI, and all the sensors that it needs to do those backup scrams and isolations, etcetera, are its own sensors acquired with its own RMUs that are not the same as the safety system sensors either trip system or ECCS system. No, this is a Mark VIe control. In the broadest sense, it's a programmable controller, but it's a very highly reliable industrial control system.

MEMBER BROWN: But it's a microprocessor?

MR. POPPEL: Three microprocessors.

MEMBER BROWN: That's fine.

MR. POPPEL: Actually, lots and lots of microprocessors because there's intelligence all through it.

MEMBER BROWN: It's software-driven as opposed to --

MR. POPPEL: But since it's only one thing and the one thing had access to things like squib valves, we determined that that one thing itself needed to be very, very reliable in terms of the inadvertent actuation. And because this is a backup to a backup to a backup, we don't really expect too

many common-cause safety-related failures. This isn't fail safe. It's fail as-is, if you will, and thoroughly alarmed so that everybody knows that it's, you know, broken.

Different operating system, different hardware, different software than either the ATWS/SLC, ECCS, or reactor trip system. And, incidentally, it has, just like those systems, the operator can manually do stuff on BPS like it can in the safety systems but not on the safety system screens. You can't talk to the safety systems with DPS. You can control DPS with this, but you can't control anything in the divisions with this, okay? And those displays are different displays than the safety displays in terms of hardware/software platforms. So we find it very unlikely that you would simultaneously fail the DPS manual capability at the same time as the safety manual capability coming through those screens.

Plant investment protection and RTNSS you guys have seen in a lot of other context, but from the DCIS point of view is, essentially, everything you saw where there was an A and B thing, like ARWCU, BRWCU, CRD, A electric building age back, b electric building age back, those are separately controlled with a mound of PIP A controllers and a mound of PIP B

controllers that each have their own dual network managed switches that each have their own displays connected to those switches such that, normally, you can control anything from anywhere, but if you lose one whole thing of the loss of the entire PIP B DCIS system will not affect the operator's ability to operate PIP A from either the main control room or the remote shutdown valve.

The main control room -- we're almost at the end now. The main control room has four displays here, one per division, and four displays here, one per division. Those are the only ways you can talk to the divisions. In other words, the only way you can talk to a div one and tell it to do anything is with either that div one display or that div one display or the div one display on the remote shutdown valve.

MEMBER BROWN: One is ESF, and the other one is?

MR. POPPEL: No. Basically, you don't control reactor trip and neutron monitoring. They don't need controlled. They just scram you and trip you. But you do have the bypasses. Those are hard joystick fiber switches. And as I said before, the manual scrams switches are manual scram software pre-switches. So, generally, you don't control reactor

trip or neutron monitoring generally. There are some things too detailed for this meeting yet, but all the ECCS stuff, manual initiation of the ICs and GDCS, etcetera, is done from the div one. But the only thing that div one screen will control will be, for example, all the way through the logic to the div one squib initiator on that valve. It has nothing to do and no connection with the div two squib initiator on the same valve. No electrical or data connections between divisions other than the two out of four logic we described.

And so, you know, we don't have prioritization modules. We don't have sometimes it's okay for non-safety to talk to safety. It doesn't happen. It's not in the design. And, of course, as we mentioned before, should these displays be lost for whatever reason does not affect the autonomous operation of the safety systems or the manual operation from the remote shutdown plant.

Here, we've grouped a cluster of displays that are basically for manual control or for the diverse protection system, just convenient to the safety stuff. You can't see it here, but these panels are compartmentalized between divisions and separately powered and all the rest of that stuff. This is,

broadly, all of the non-safety displays. You can't see the segmentation between PIP A and PIP B in balance of plant, but it's there. But, normally, the operator can do anything on those displays, anything non-safety on those displays, nothing safety. And we have a shift supervisor position. We have a few other things.

The general thought is that surveillance type stuff be done here because that way he doesn't have to stand in front of the operator at the main bench board, so the operator has his displays to do anything while surveillance can be done over here without being in his way. Non-safety surveillance are done over here.

This wide display panel, the technology is changing but the intent is to have important, basically, BWR control systems permanently available so you can always see what reactor level is and reactor pressure is. One number. So you see a single reactor level, which is the combination of all ranges, all divisions, all non-safety as a bar graph appropriately human factored and with an indication to say to the operator whether or not two transmitters agree that this is, in fact, this case. So it's not only telling you the level, it's telling you how good

it thinks the level is because operators are almost always told don't do anything unless you get two transmitters to agree that that's the case.

We have variable areas of -- this is all part of human factor, so I don't want to make it sound like this is design. But the intent is that these are displays. They're just really big displays. So whether or not big displays are up there permanently or they're variable depending on plant modes or whatever is an HFE decision, but the intent is that anybody sitting any place in the control room has a line of sight view to that and will be able to grasp an overview of plant condition simply and quickly.

MEMBER STETKAR: Are all sensory input to the operator visual?

MR. POPPEL: If you mean do we have audible alarms, yes, we do.

MEMBER STETKAR: But are they distinguishable?

MR. MILLER: You might have 70,000 signals. So the wide display panel gives you a big overview. If you have an alarm, that would come up on your non-safety display, and the operator procedures would direct the operator on how to handle that.

MEMBER STETKAR: There must be some

important alarm.

MEMBER STETKAR: It's the displays, basically. The importance of alarms are prioritized and filtered based on mode and so forth, and that's based on our HFE process.

MR. POPPEL: Alarm management is probably a 22-day meeting that we could have. But suffice it to say, our human factors folks and us and INC are trying, the many, many plant alarms are going to be, I don't know whether to use the word suppressed or filtered based on plant conditions versus events or events such that we do not flood the operator or overload it. That's an important, very careful task that has to be done. It requires a lot of work, but, essentially, we don't want to give the operator more alarms than a single human being or three human beings can handle versus the task analyses that are designed per system. So there's a formal HFE process we haven't talked about here, but the intent is alarms are just as much a part of the operator interaction as the displays are. And so, you know, for example, we're not going to have the low potable water level alarm in the middle of a LOCA. That one is easy; some of the other ones are a lot harder to determine.

MEMBER BLEY: Just at a simple level, do

you have different audible for ECCS and reactor trip than for other things?

MEMBER BROWN: You mean sound? Different sound?

MR. POPPEL: If you're saying could we, the answer is yes. If you're saying are we, the answer is HFE.

MEMBER BLEY: You've already done this for an ABWR. Are you starting from scratch over here?

MR. POPPEL: The HFE rules have changed and become a lot more formal since then, but there's no distinguishing between what's causing the level. The alarm is driven by all the levels in the plant, and it is an audible alarm. That's an easy one because there's reactor level, and there's probably nothing more important.

MEMBER BLEY: Are you going to work with each buyer such that ECCL might get a different HFE arrangement?

MR. POPPEL: No, it's a standard plant, and it's a standard HFE.

MEMBER BLEY: But not yet.

MR. POPPEL: Not yet, but it's certainly what our customers want. They want the same, you know, operating procedures, the same alarm response

procedures. We haven't discussed it, but the CNI supports having you got this alarm and you'll be able to say, okay, for that alarm, what alarm procedure, you know, as text, should you take to deal with it, okay?

MEMBER BLEY: And at this point, all we have are the process documents that you've agreed to follow for carrying that out?

MR. POPPEL: Yes. And in our defense, I mean this is designed, I mean there is an alarm filtering system in place for the ABWRs in Japan and a better one in place for the alarm filling stuff in Lungmen, not because we're smarter than Japan, it's just later. So you learn more, you do more, etcetera. We expect the ASBWR to be better than that. But the intent is, functionally, don't overload the operator and don't give them information you can't do anything about and don't give them information that's less important than something else that is more important.

So the control room, I mean that's what our control room looks like. It's intended to be --

MEMBER BLEY: I'm sorry. I just want to follow that up with a question. I understand what you told me about what you want and what you think your customers want. But the way this process works, the

process for getting from here to there is what's part of the certification. So that process could be implemented alternative ways in the future for other - -

MR. POPPEL: Why not? First of all, our customers are happily ensconced in Wilmington to help us with the alarm management system and provide, you know, the task analysis insofar as it's associated with the system. But the point is it's delivered as, there will always be a few plant unique systems, circ water, say, may be one of them. But all of this stuff that you might consider, like FAPCS, CRD, will be the same from ESBWR to ESBWR, including its alarms and its procedures and its filtering.

MR. WACHOWIAK: This is Rick Wachowiak. We covered this in the Chapter 14 presentation a few weeks ago. The way that we intend to close these back are one issue, which would be this HFE control room, one review, one position. And so when we close this for the first, for the reference plant, the way we've described this in the DCD is we would write a topical report that all of the customers can reference to close that same issue in the DAC.

Now, we recognize that since this is DAC that this may change, but it's not intended to be

changed plant by plant by plant by plant. The way we would see this is if 10 or 15 years after the first set of ESBWRs are built and operated and we gain sufficient operating experience in this HFE area, we would modify that DAC LTR and it would be re-certified as a DAC closure and then subsequent plants to that could reference that one. So, yes, it's flexible enough to do more than one time, but the intent is that we really only solve this issue once, get it approved once, and everyone implements the same thing. And we described that in the tier one section a few weeks ago.

MR. POPPEL: The mechanical stuff associated with this, like will it fit in the room, in the main control room, and the layout and all the rest of it on the sidelines have, in fact, been checked.

MEMBER STETKAR: Ira, in the DCD and the topical reports, I get mixed up between them, in many places there's a generic term called the main control room back panel area. I've been interpreting that as other rooms in the control building. We're not really talking about panels behind --

MR. POPPEL: No. In fact, those are the Q-DCIS rooms and the N-DCIS rooms.

MEMBER STETKAR: Yes, okay. I just wanted

to make sure I was correctly interpreting that phrase.

MR. POPPEL: Yes. The remote shutdown system, unlike previous plants, it's not a system, it's an auxiliary control room. We basically have, we have two panels in the reactor building that you can quickly reach from the main control room, okay? They're in separate fire zones and separate from the main control room fire zone. And on each panel is a div one display, a div two display, for want of a better term a PIP A and a PIP B non-safety display. So if there is offsite power available, you can run any system in the plant, balance a plant so you can use their, you know, circ water system and main condenser to cool down the plant. If, in fact, you don't have offsite power but have the diesels, you can use any of the PIP A or B systems: reactor water cleanup, you know, FAPCS, CRD, etcetera. You can utilize those systems.

If you don't have any diesel power available, those same 72-hour batteries that run the safety system will also support those displays, and you can run anything in div one or then div two, okay? The connections do not go through the main control room. These are just like the main control room. It's fiber back to the appropriate Q-DCIS and N-DCIS

room, just like there's fiber from the main control room. So when you work it through, if I lose a single RSS panel, I can still use the other one. If I lose the main control room, I can use either one. If I lose a single Q-DCIS room I lose that division, but I can utilize the other divisions in N-DCIS and any of the other locations, okay?

So it gives you far more capabilities and maybe even more importantly is the operator interface to it is exactly the same as you would have in the main control room. However, the operator DAC system in the main control room is a display he's going to see in the remote shutdown plant.

MEMBER STETKAR: Are the RSS panels normally online, or when you abandon the control room do you have to transfer control to the RSS?

MR. POPPEL: We can do it either way, but online is --

MEMBER STETKAR: I'm asking you how --

MR. POPPEL: Well, again, so far that's considered to be an HFE decision.

MEMBER STETKAR: Okay. Because in the SER it states point blank that no transfer is required, so I was curious where that information came from.

MR. POPPEL: Oh, no, no, let me rephrase

that. Transfer in the traditional way you're talking about remote shutdown systems, there's the switch and says ignore the main control room and listen to me. We don't have those switches; you can't transfer them. What you can do is have a display that normally can't do anything but you have to log into to enable. That's not transferring control because the control remains in the N-DCIS rooms.

MEMBER STETKAR: Taking transportation, it could be a bicycle or it could be a truck. An operator must actively do something to take control from RSS; is that correct? If I walk up to an RSS panel, the plant is operating 100- percent power, and I want up to an RSS panel and I say, "Initiate DPV," just arm fire, can I do that without doing anything else? I know --

MR. POPPEL: Because so far, it's determined to be an HFE decision. So if they say we think you should do something active, because remember the two rooms are going to be locked; that's for sure.

MEMBER STETKAR: The only reason I raise this, it will come back to the staff, I wanted to make sure I understood. Your position is you could do it either way, but you haven't necessarily made that decision yet, and that's --

MR. POPPEL: But our equipment will support either --

MEMBER STETKAR: Yes, I wanted to understand whether there was --

MR. MILLER: Rich Miller. The equipment will support either decision, but if you're controlling in the control room on a VDU there, you can't control at the remote shutdown --

MEMBER STETKAR: You can or cannot?

MR. MILLER: Cannot. Whoever has the control at the VDU --

MEMBER STETKAR: So if --

MR. MILLER: So if I stop controlling it, it logs out on that VDU, and I go to remote shutdown panel and I open a VDU and bring up some displays, whoever has brought up those displays will control that.

MEMBER STETKAR: He's got to actively log in onto the remote shutdown panel.

MR. MILLER: That hasn't been determined yet. It's still --

MEMBER STETKAR: Okay, thanks. That's enough.

MEMBER BROWN: Now, he said log off. Do you have to log off --

MR. POPPEL: No, no, no, automatic.

MEMBER BROWN: That's what you said.

MR. POPPEL: But let's just be clear. What you cannot ever do is have two operators, wherever they are, call up the same display and one guy say on and the other guy say off. The first guy who gets it, if you will, for that display, for that control, locks out everybody else.

MEMBER BLEY: So it's not, as of now, that the primary controls are in the control room. It's whoever gets it first by whatever process you go by.

MR. POPPEL: We don't force the guy to log in, but obviously it would lead to chaos if you could simultaneously control from two screens, even if they were next to each other in the control room. And so the system is proofed against that, okay? But you go down to remote shutdown panel and unlock the door and open it. Whether or not we're going to force the operator to log in before he can do anything at those screens, meaning, in your term, they will be transferred off, or not. The reason they consider that an HFE decision is because, obviously, going down to the remote shutdown panels under the circumstances you would normally think is a pretty stressful situation. And, therefore, saying to the guy we think

you should log in before you can deal with the plant, some of the HFE people don't think that's a good idea.

MEMBER BLEY: I don't know. If he can't figure out how to log in . . .

MR. MILLER: Apparently, it's an HFE task analysis type, you know --

MEMBER BLEY: So the question on this, and I think you told me the answer, but you could, if they wanted you to, arrange it so you have to log in on the remote shutdown panel. And I suppose if they wanted it, it could allow the main control room to block that log-in from somewhere else. If they wanted that, you could do that?

MR. POPPEL: We could do that. Interfering from different locations brings up interesting cyber security and stuff like that.

CHAIRMAN CORRADINI: Let's move on.

MR. POPPEL: We feel we can support whatever is determined to be optimal. Okay. I should have also mentioned that from either of these panels you can manually scram the plant or manually isolate the plant in a software-free way.

These are the last slides, the firewall. We mentioned before that the firewalls are all over the plant, but the firewall that everybody thinks of

as traditional, this is also explains a little bit about shared memory. So imagine two processors we call the internal processors. The two is because of redundancy and reliability. But imagine an internal processor on that plant data highway network and that processor knows everything there is to know about the plant. It's got all the data. Everything is sending information to it, etcetera, etcetera. These processors know everything there is to know about the plant; they have all the information.

Then there's the shared memory. So the job of the internal processor, the only job, is to put information into the shared memory. So its shared memory is, if you will, write only, never read. Very easy to verify and check. And so this thing is scarfing up data all over the plant and dumping it into the shared memory.

On the other side of the shared memory we have external, I don't mean external physically but external from the shared memory, that basically says, "I have no idea how this information got into these memory locations. I didn't ask for it, I can't talk to anybody on the other side and tell it to put it in. All I can do is read it." So that processor says, "No, what I have to do is verify that he's just

reading and not writing." Of course, even if he did write, the other processor isn't designed to read in any case. And so, basically, the external processor now also knows everything about the plant without any idea or control or any memory address, any nodal address, anything associated with the plant.

So now we have this external processor which you can now think of as a more traditional firewall. This thing will be set up so that, you know, who's a legitimate person to talk to me, nuclear data link, technical support center, etcetera, etcetera, so that, basically, we have to actively decide what information we're going to put through the shared memory because that's the only information the outside world is ever going to have. We'll probably just dump everything, but, you know, and then that thing will determine who can call me up, who can listen. That thing will include the utilities, engineering networks. That will include the data link, the simulator, business processors, anything you want. And all they will be able to do is to destroy those external processors. They can spoof them, bring them to the ground, data flood them, unlikely even with a commercial firewall. But the point is that's all they can do. They can't get to the other side.

That's the shared memory concept that safety is using to talk to the non-safety ring, that the safety systems are using to talk to each other, etcetera. And so it's a very, very powerful concept in terms of data isolation and cyber security.

So the net result of all of this is we believe nobody can get in. If they can get in, they can only get to the plant data highway, which has no control function. And the network managed switches on the plant data highway will basically say, "Who the heck are you? I'm not going to listen to you."

Then it has to go through what's called a bridging station between the unit data highway and plant data highway to get to the control networks. The control networks are all on the same network managed switches that say, "Who the heck are you? Are you trying to flood me? Are you trying to do this?" etcetera. And then even if you did flood that, the controllers won't listen to it. I mean, they won't listen to commands other than what they've been pre-programmed to listen to. And so, therefore, it's very hard to alter their functionality. And it's more or less the same thing but going backwards through shared memory and stuff like that to get to the safety system, but it's layer upon layer upon layer upon

layer to get through. So this firewall is the biggie that everybody looks at, but all through the system . . .

There's other little things that we haven't talked about much. For example, all of our DCIS cabinets have door switches which are an input to the data acquisition system. So we believe the self diagnostics are such that nobody should ever open a door. But, more importantly, if they do open a door, they're going to know it. So the way that this is going to happen in the main control room is some self diagnostic alarm goes off and says, "Hey, we need to call somebody to fix it," so when the guy goes in to ask the shift supervisor for the key he's not going to give it to him unless he's had a previous alarm that says something broke. Then when he gives them the key and he goes down to the room and opens the cabinet, if he opens up a different cabinet that's going to be a, you know, "Hey, we didn't tell him to open that cabinet, we told him to open that cabinet."

So we basically tried to design the system so that there's no knobs or tweaks or screwdriver adjustments or anything in these DCIS cabinets. There's no reason to be in them unless they're broken, and we hope we'll be able to tell you when they're

broken.

So that's also part of, if you will, cyber security. The network switches not only have switches and all that stuff on that, they're in a cabinet with a locked door. And so the guy who's going to come in with a laptop, which is going to be ignored in any case, has to first open the door to even plug it in, and that will be an alarm. And this goes to the stuff in the field cabinets, too. If the guy in the service water building opens up a remote multiplexer there, we will know that.

So, anyway, I almost hate to ask if there's any questions, but that's the presentation.

MEMBER BLEY: I have one that you haven't talked about at all, but I want to check my understanding and maybe you'll get to this later on. Looking through tier one at the DAC, it appears that the primary DAC for INC are 14 of them associated with IEEE compliance confirmation, a couple on DPS, and then a few on various distributed systems; is that right?

MR. POPPEL: Actually, this would be a good time to segue way into Steve's conversation.

MR. MILLER: Yes. DAC is the next, like, five slides or so.

CHAIRMAN CORRADINI: Okay. So let's hold that question, but let's move on then.

MR. MILLER: I think we're complete here, unless there's any questions.

CHAIRMAN CORRADINI: No, let's move on.

MR. MILLER: Okay. We're going to switch over to Steve Kimura, who has a presentation on DAC.

MR. KIMURA: I don't know if I want to follow all that. My name is Steve Kimbura of GEH, and I'm here to present the DCD design detail and the relationship of DAC to the amount of detail that's shown in the DCD.

And I really have a, you know, a hard time sometimes talking to mixed audiences of INC folks and non-INC folks because we get to this problem of scale. And by that, we sort of went through ten orders of magnitude of various levels of detail on describing the INC system. And where someone would say 25 milliseconds is a very short period of time, there are people in this room who would say, "Well, that's 25 million nanoseconds," and on the scale of the chips on the board, that's an enormous amount of time.

So when we look at that as far as the DCD is concerned, I'm looking at a design that takes, say, ten to the three or ten to the four pieces of paper

and try to compress that down into a document that has ten to the two pages in it and present all the information that everyone wants to hear and everyone wants to see within this various levels of documentation that spans multiple orders of magnitude.

So what the DCD does is provide you design basis. Those are the things that the control system absolutely has to do. And one of the things that it has to do, it has to scram the reactor under certain conditions. And those conditions aren't esoteric conditions. Those conditions are very basic. They've been well documented throughout the history of BWRs and PWRs, and we know that there are certain conditions that are indicative of when we need to shut down the reactor.

And so the DCD presents these conditions that says, "Well, at level two I'm going to have to start initiating some protective actions, and at level one I have to start initiating some other protective actions. Under conditions of ATWS, I have to do slightly different things."

So one of the things that we do is we commit to following codes, standards, regulations, regulatory guides, some of which are very prescriptive and some of which are, in fact, very confusing. You

can have an ASME code that says, "Do a design and present me your design details at the end, and then someone will evaluate them and see if those are good enough."

In the INC world we have things like IEEE Standard 603, design criteria for safety systems for nuclear power plants. And that standard says these are the good things that a bunch of people have determined are those things that are the minimum that a control system or a protection system really has to do to protect your power plant.

One of those is meet the single-failure criteria and which applies to the safety function, the protective function that that system has to do, so that you may use a series or a combination of redundancy or other means to make sure the single failure way upstream, let's say a failure of one sensor, doesn't cause you to prevent you to ultimately make this decision to scram the reactor. So we apply those criteria to the control system, and we follow the industry guidance and the standards that are set forth in the DCD.

Some of this detail we bring down into topical reports. Again, the topical reports, if there is enough detail, provide a good source of

information. For the control system, we're at a quandary because the control system has so much detail in it and so much things that change as you make decisions that if you pick one set of chips today and it takes three years to design this platform or even three years to get it approved through regulatory space and then I go and try and build the first prototype based on the design I had three years ago, I'm going to have significant changes to that design when I go to build it. Now, does that mean I have to go through licensing again and get it re-certified? We would hope not.

So the process to address that we call DAC, and DAC is a process. It's a design process. So what you certify is the process of doing the design, which is, in fact, for many systems, many complex systems, more important than just looking at the final product because it's very hard to tell how good a final computer system is from another computer system just by its surface appearance.

So DAC, the way we've defined it, starts with the software with the life cycle development process. The software life cycle development process starts off with planning, making sure that I can complete the design of that safety system. It has

several parts to it. It has the software management program manual part, and it has the software QA program manual part. The management program manual part is the design. That's under the control of the designers. They're setting the requirements for the design. The software QA program manual sets the requirements for the people who verify and validate that the design followed the process. So we've split those things into two parts, but both are required to adequately complete the process and accurately complete the design.

The way we control this is by using what we call a baseline review process. At each baseline of the life cycle phase, the planning phase, there's a point in time at which the designer says he's done, we're done with planning. We have a review. We gather the design team. We gather an independent review team. We have space available to include in the review team customers to get their input, regulators, depending on the need and the desire of people involved of what they want to do.

So as we go through these baseline reviews, we look at all the requirements that led up to saying that we're done. Did we meet the requirements? Did we have all the documentation that

we had already said we needed for that baseline phase? Is that documentation complete? Is that documentation adequate? Did it allow us to move into the next phase of the life cycle?

So at that point, you have to meet all the phase requirements before you can pass on to the next development life cycle. And as I said, these review points provide natural places to where we can conduct audits or you can conduct audits and say are we following the process. We said we're going to do this, we said we did it, you come in and audit us and you verify that we're actually following those processes.

This process is actually an extension of a process that GEH uses in the normal development. It's not something that we invented just for this project. It's something that a lot of folks at GEH had been using. There are certain details of the process that have a big history of success. You know, it's not that this is something that we think might work; we know it works.

CHAIRMAN CORRADINI: So can I ask you a question? Because this is somewhat high level philosophy. I want to get down to for the ABWR versus the ESBWR, at what point do they deviate in design

that you could not simply say, let's say reactor protection, that this is the same functional logic that ought to behave with one machine as to the other machine? Let's take reactor protection. So that what you learn from ABWR you can immediately instill into ESBWR to explain what the functional logic is that you want to control with. My reason I'm saying this question is just to preempt my colleagues. Where we're getting heartburn is is we feel that you're up here and you can be a few more steps down into detail so we can understand and get an appreciation and confidence into what you're choosing to do.

MR. KIMURA: The level of detail that exists at Lungmen and the RPS system functionality is very close to what we would require to scram a reactor for ESBWR on a large functional level. Implementing that design and hardware right now, because there are issues with obsolescence of the chips --

CHAIRMAN CORRADINI: What I guess I'm trying to ask is, and I'm the least qualified of the committee to understand this from an INC standpoint, but it just seems when I read through Chapter 7 you were at such a high level that I did not have confidence and you couldn't have gotten more detail and still not have gone into the worry about what

software or hardware do you have to pick. Rather, you could have gotten more detail into the logic of how the design would work, independent of what box you buy or computer program you choose to write.

MR. KIMURA: We have a set of simplified logics that we have sent to the staff. They are not right now on the docket as part of the DCD. That simplified logic is derived from a large part from what was developed for Lungmen.

CHAIRMAN CORRADINI: So staff has something that wasn't in the DCD we've seen?

MR. KIMURA: Right. Now, that logic will go into a lot of details of how a lot of these pieces interact with other pieces but on a very large scale.

MEMBER STETKAR: Now, let me follow up a little bit on this and try to cut to the chase a bit. I've looked at INC designs for probably, I don't know, 25 currently operating plants. I don't care whether they were relay implemented or toggle-switch implemented; it doesn't make any difference. What I've found is that until you look at the design at a, I'll call it a middle level of detail, but in an integrated sense you cannot make a reasonable determination about whether that design, and I'll use this word carefully, is prudent. Every design I've

looked at has met all of the design criteria. Every single design criteria. It is absolutely prose, poetry, verse. It meets all of the criteria.

Many features of the designs are not prudent. I can give you many examples that's not prudent to do that for this meeting. If you want to discuss them, I can tell you later off the record.

The purpose I thought, naively, of the whole DCD of the whole design certification process was to allow the staff and the ACRS as an independent committee to have some time at this middle level of detail. I don't care what chip set you use. In the relay, I don't care whether it's a six-contact relay or a four-contact relay, whether it's a GE relay or a Westinghouse relay. That's fine structure detail. At a medium level of detail within a decent time frame, not under the pressure of construction deadlines and things like that, to look at the design and, number one, it must meet the criteria absolutely, but all the designs do. There's no doubt that your design will meet the criteria. You will certainly meet the criteria.

But at that next level to see whether the design is indeed prudent from a safety perspective. That requires some time and it requires some thought

and it requires much more, not much more information than in the DCD. The information might be available in those simplified logic diagrams that you alluded to that we've not seen. I don't know that because we've not seen that. It's certainly not available in the DCD right now.

So that's I think a couple of our, we've had a lot of discussions about this, a couple of our concerns. And I was curious about why you can't, number one, at that middle level of detail, why you can't incorporate that into the DCD?

MR. MILLER: Rich Miller here. We did I guess a lean session step two three years ago, and we looked at what we did on Lungmen ABWR and the processes we used. We noted on Lungmen that we found mistakes in our logic doing our simulation testing, and that fed back to the logics. And then we had to rework the logics, and it caused our cycle to stretch out.

So we decided on the ESBWR to use a simulated engineering tool so that we develop our logics in a simulation tool so we can have that test fed as we do our logics to test the zeros and the ones and so forth as we go forward. It also minimizes our factory acceptance test phase because we have less

errors because we found them up front versus at the mid-cycle of our development.

So prudent-wise, I guess, we have cut off a good amount of rework by finding things up front in our logic. Not that we will because we have in the past, for example RPS, done testing on it. We're actually almost repeating the RPS logic on the ESBWR, except for minor changes. But we feel we have a very prudent method in using this simulation engineering tool to develop our logic diagrams and to use it as a test bit to correct errors and things up front.

MEMBER STETKAR: I think we still may be talking a different levels of details. And let me give you an example of something that I read. I'm going to say it a little bit back from the detail, but in many cases you have to talk about specific things. Apparently, in the logic there is a 30-minute interlock that prohibits automatic or manual actuation of the GDCS equalizing lines. Thirty minute. And it says in words automatic or manual. That says that if I'm an operator I cannot open those -- somebody made a decision.

Now, it says that in words, but I can't see that in a real diagram to see whether or not that's simply a poor use of the English language or

whether that is actually the logic. That, to me, I don't care how it's implemented, I don't care how you do that. To me, that's kind of interesting. And in terms of prudency, can I think of situations, if it actually does lock the operator out, can I think of situations where that might not necessarily be all that prudent to do? Follow me? That's the level. And if I could see a logic diagram that indeed says automatic signal comes in at point A, manual signal comes in at point B, it's an or logic with a lockout time delay in series with those. That would indeed confirm how the system works at that function --

MEMBER BLEY: It might implement it in many different ways.

MEMBER STETKAR: It could be implemented in probably an infinite number of ways.

MR. MILLER: That is stated in the DCD. The logic diagrams would have that on it and show the implementation.

MEMBER STETKAR: Well, but in many cases, because the DCD is just verbiage and it's not a precise document.

MR. MILLER: I would say there is vagueness in that.

MR. KIMURA: And the safety analysis of

that one event would be in Chapter 6 or Chapter 15. So the details of why that interlock exists is not something that the control system is really, you know, really concerned about. The fact, the requirement, to have that interlock is important.

MEMBER STETKAR: Well, the first time I heard about it was when I read Chapter 7. So a bit of the problem that we have here is that, for example, the first time I recall hearing about the valves that cross connect the equipment storage pool with the ICCP pools was in Chapter 7. I don't remember hearing about those valves before. I don't remember hearing about the battery -- were there any other parts? I missed.

MS. CUBBAGE: Excuse me. This is Amy Cubbage. If you want to hear from the staff, I think we do need to move on. If there's a concern about the simplified logic guide or what GE provided on the docket, I think we're also going to need to have a conversation with GE about whether those need to be referenced through the DCD. So we'll need to just take that and move on.

MEMBER BROWN: Aside from the logic diagrams, you made the observation that because of the technology issue for some reason you can't lay out

what the architecture is. And I fundamentally just disagree with that thought process period because that is simply something that processes data. That is what that package is that's you're putting in there. You can program it. Functionally, you want a certain logic array. How that's programmed in that platform is irrelevant to the overall architecture, and I would amplify that with, until I saw your diagram up here, how the RPS, the protection system, reactor protection system, operated and how your rings, you know, with your various functional attributes, you know, the RMU, the DTL, the TLU, blah, blah, blah, all that stuff on that ring, didn't fall out at all. None of that information is available.

Now, you can tell me, well, gee, it doesn't matter to you. Well, in fact, it does matter to us because it's different from other stuff. I don't know whether I want to use the word prudent or not, but why is that equivalent to, as good as, or sufficient based on past experience of how we've done things? When the data comes into the RMU, I guess, correct me if I'm wrong because I'm going to use a slice specific, there's sensors. A sensor come into the RMU. I presume, in each division, if there's four sensors, there will be a pressure sensor, there will

be a temperature sensor, maybe a couple of them for different functions where they're replicated.

So there's a number of pieces of sensor data coming in to the RMU. Is there an A to D converter for every one of them? Is it just signal conditioned and then something grabs each of those condition signals in a multiplexing manner, processes it through a single A to D converter, and then dumps it into the shared memory? How is the shared memory, are there allocations to the shared memory in terms of how you partition it?

Some of it may be too far down it, but it's irrelevant to the platform. The technology doesn't care. I mean, in my experience, I started doing this stuff in 1978 with Z80s, and if you think about no capability with Z80s. And we spent millions of dollars because technology changed, and we ended up coming up with platforms where we could put them in the functionality, how the architecture stayed the same, not "I changed one thing, one card, and I took care of all technology changes for the most part," there are always exceptions.

So the idea the technology, you can't define the architecture of your protection system or your safeguards functions doesn't stick. You can't

access what you've got in terms of goodness or prudence based on the detail we've got.

MR. MILLER: I think what you're saying that we can't say what our architecture is, but we might have one chip designed today and three years from now we might use a different chip --

MEMBER BROWN: It doesn't matter.

MR. MILLER: And we use the same process --

MEMBER BROWN: Exactly. The process is fine, but the chip, it's irrelevant to the chip.

CHAIRMAN CORRADINI: I think you sense our, I think you sense where we're coming from.

MR. MILLER: Some of that information were in LPRs specific to NUMAC, specific to TRICON. TRICON has an SER, okay? We have SERs on our old RPS designs, our neutron monitoring system designs. We had LTRs --

MEMBER BROWN: But that's all on this other stuff. I mean, do I want to go down into the bowels of the NUMAC internal processing? I could care less. I wouldn't understand it if I read it. It's just, it's how you put data in, you get data out, it processes stuff and sends it off to do something.

CHAIRMAN CORRADINI: But I think you get

our point.

MR. MILLER: We get your point, yes.

CHAIRMAN CORRADINI: Okay. So I'm going to encourage you to, we'll not say anything, but to finish, you know, a couple more slides, and then we need to hear from the staff because we want to hear from the staff.

MEMBER BROWN: I think he's finished.

MR. KIMURA: Well, a lot of that design detail we have actually gotten into some level of detail and what we found was that the level of detail that we had presented, which actually got down to like specifying DTMs different from TLUs, was at a level where, in hardware space, it wasn't going to be implemented that way. So how can we commit to saying this level of architecture is sufficient --

MEMBER BROWN: You got it. It's there. There's an RMU that feeds data in, goes to a DTL, goes to a TLU, goes to an output logic unit --

MR. KIMURA: But the DTM and the TLUs can be one thing.

MEMBER BROWN: I don't care. It's all right. They're blocks. You run through a loop within the thing. That's the level of detail.

MR. KIMURA: And that level of detail is

in the DCD.

MEMBER BROWN: No, it's not. It's a straight line. There's no rings in there. There's no discussion of the data rings or the communication rings. There's no discussion of communications at all except that it's a distributed whatever. There's no discussion at all.

CHAIRMAN CORRADINI: Go ahead. Let him finish.

MR. KIMURA: In 7-2 we describe the RPS system as --

MEMBER BROWN: And by the way, that was generic. So if you go look, the fact is if you look at your diagram it looks like the nuclear monitoring system never, ever gets to the RTIF, whereas some of your figures that has a line going out to an RTIF. Look at your major diagram, and it's got to go up into the network and come back. There's no other way to get there, whereas on the RPS, the other function, you show them going up, you know, and into the RTIF functions for all the other parameters, but not nuclear monitoring. It's totally divorced, yet all the things that has to feed to make it do anything are over in the RTIF boxes that you show in your big diagram. So if you don't show a system-by-system

application, even though it may be the same thing, it may be being executed by the same piece, but system-by-system execution and how they communicate is important so we know that, number one, is it independent; two, is it deterministic? It's obviously you've got enough train for redundancy. Nobody is complaining about that. I'm sorry. I had to amplify my thought process.

MR. KIMURA: And Section 7.2 actually tells MNS feeds RPS.

MEMBER BROWN: I know it says that, but it's not showing the figures.

MR. KIMURA: Figure 7.2-1 I believe actually shows the line that goes out.

MEMBER BROWN: 7.2-1 doesn't address -- you're right. I don't want to argue about it.

CHAIRMAN CORRADINI: You finish, and then we'll turn to the staff.

MR. KIMURA: So the DAC process is actually part of an integrated process that ends with the final ITAAC to demonstrate that the control system actually has been not only designed but constructed, installed, and tested to show that it meets the requirements. The DAC process itself is projected to complete three years after the start of detail design.

At that point, you'll have all the details of the system requirements for the standard reference plant, and every plant that uses the standard design will have to fall to that level of detail to the operation of the control system, the design of the control system.

So that's what this figure is trying to show. That completion here, and we have a bunch of activities that deal with planning and software requirements, software development and testing, software integration into the hardware platforms, acceptance tests, the installation phase, and then the site acceptance tests of the entire control system.

MR. WALLIS: So you're going to procure hardware before you complete the DAC?

MR. KIMURA: Procurement of the hardware is part of the, it actually occurs right there.

MR. WACHOWIAK: Those three circles on the graph are where the DAC elements are completed. So we procure after the three elements of DAC have been completed.

MR. WALLIS: But before the HFE?

MR. WACHOWIAK: Right. So those three circles with the asterisks there should be the ones that identify closure of the DAC.

MR. KIMURA: Yes. So the software DAC, the requirements are necessary to go forward. We know what the system has to do.

MR. WALLIS: How can you procure the hardware if you don't know what your HFE --

MR. MILLER: Your HFE requirements are determined up front, and then you get into your HFE testing phases and hardware --

MR. KIMURA: Once we know what these features are, what the basic requirements are that we have to do, we can start the procurement of the hardware phase. There's a lot of time involved in just ramping up the hardware design effort.

CHAIRMAN CORRADINI: Keep on going.

MR. KIMURA: The last thing I was told to talk about was do a brief overview of the set point methodology because GEH has what they call the red book, which was a set point methodology that was issued NEDC-31336A-P, which is used by the fleet currently, but it did not address certain things that the staff had issued in regulatory information summary reports, 2006-017 and 2005-020. So we added those issues and addressed those concerns in a revised set point methodology, NEDE-33304P. And it clarifies the difference that a limiting trip set point that

satisfies Reg Guide 1.105 is more conservative than the nominal set point compatible with operational needs.

So we have kind of clarified where the final nominal trip set point will be in relationship to the limiting trip set point and to the analytical limit and the safety limits. It complies with the Reg Guides 1.105, and it complies with the branch technical position, and it complies with the industry standards used by everyone, ISA S67.04.01 and 67.04.02.

MR. MILLER: Any questions at this point?

MEMBER ABDEL-KHALIK: Is the application of the set point methodology a part of the DAC?

MR. MILLER: There is an LTR, number NEDE-33304P, and there is a DAC for set points.

MEMBER ABDEL-KHALIK: So at what point will you have the opportunity to see how the specific set points have been --

MR. MILLER: The calculations will be done based on the methodology and after we obtain hardware. That hardware is an input for us doing our calculations, so normally after the procurement cycle.

MR. WACHOWIAK: The set points should be ITAAC.

MR. KIMURA: The set points are ITAAC. IEEE 603 requires that you use a methodology. The methodology is this LTR 3304 which is under review. Until we get approval of the LTR we really don't have an approved methodology at design certification. So to divorce it from design certification we've made it part of the DAC.

MEMBER ABDEL-KHALIK: So this says 3304P. I guess it doesn't have an A next to it so --

MR. MILLER: P stands for proprietary.

MEMBER ABDEL-KHALIK: Right. I understand.

MS. CUBBAGE: Let me just clarify that. The topical report was submitted. The staff is reviewing it. They will not get a certification until that separate methodology is approved. Implementation of that methodology to develop the set points is something that's done later, and it's also controlled by the set point control program that's going to be in the tech specs.

CHAIRMAN CORRADINI: Okay. Let's move on. Thank you very much.

MR. MILLER: We're done. NRC staff's turn.

MR. GALVIN: My name is Dennis Galvin.

I'm the ESBWR project manager. The first four slides cover the topics, list the topics in the SER, list the reviewers, gives an outline of the presentation, and lists the key regulations which I'm sure you're already familiar with. I'll make two brief comments. As it says, we've had about 276 REIs, and 70 REIs remain open. The staff position is most of these remaining open items are clarifications and consistency-related type issues, and also there's no safety or technical issues that need resolution. There's topics that need to be addressed, but we don't consider them to be safety significant.

And with that, I will go to the technical staff. We'll start with Hulbert Li.

MR. LI: My name is Hulbert Li, and I'm one of the ten reviewers. And as GEH presentation, basically there are two parts: safety-related INC platform and non-safety related INC platform. Staff review has focused mainly on the safety-related platform, that including reactor trip. Regarding the non-safety related platform, the staff's only concern any failure of those control on non-safety related system will not impact toward the safety-related function. And we still have an outstanding question in the Chapter 7 area on the GEH to document these and

make sure that's the case, no failure on the control system will impact the safety system.

Our review guidance basically follows similar -- I guess bring the hard copy of Chapter 7. It is a big book and lots of detail guidance within these books. And so we use these sort of like a bible for review of these applications. Most of this guidance come from the IEEE standard endorsed by Reg Guide. The only IEEE 603 is the regulation. The part of IEEE standards are just guidance.

The main area of concern is how this ESBWR INC system comply with the regulation, that means comply with IEEE 603 requirements. We have many questions on this area. And GE proposed in the section 2.2.15 address how to verify how their design comply with the IEEE 603 requirements. But those tables in revision four of DCD is not quite complete, so we raised the question in our SER many, many times and tried to make sure the DCD would fully document a compliance with the IEEE 603 requirements.

Another key INC is related to the design process. That is documented in Chapter 3.2. And in four, we also have many questions, so it's still ongoing and GEH recently provide some response to update those --

MR. WALLIS: So can I ask you something? I read the list in the figure. There's a ritual you go through about compliance with IEEE 603, blah, blah, blah, blah, blah. Is there any point where you consider the prudence of what they're doing that John talked about here? Is there any point where you step outside this for the rather routine cranking through the compliance and say does this make sense what they're doing?

MR. LI: In our mind, compliance show the quality of the final product. So we --

MR. WALLIS: If they say they're going to comply, I'm sure they're going to comply. But is the design now safe?

MR. LI: Our question mainly to see how they complying with it, so give more specific, we want them to document in the DCD how they're complying with each of these requirements.

MR. WALLIS: Do you ever find where you raise a question about prudence or --

MR. LI: Well, it's part of the DAC process. Their design hasn't complete yet, so we have to rely on these DAC and ITAAC to verify. And the next presenter will bring up the life cycle design process, when we can verify those compliance.

MR. WALLIS: Isn't the DAC review part of what you're doing now?

MR. LI: The language in the DAC, but completion of the DAC is two years from now.

MR. WALLIS: So if their design, whatever it is, meets the DAC, you're satisfied?

MR. LI: In that --

MR. WALLIS: So are you sure that the DAC detail is appropriate?

MR. LI: Right. Right now, we are doing whether the language in the DAC is --

MR. WALLIS: Because what concerned me was I read all this stuff, and they're going to have a DAC and it's going to be, they assure you that it will comply with all the criteria. But until you look at the details of what's in the DAC, are you really sure that it's okay? I didn't see that at all in the review.

MR. LI: Well, they proposed --

MR. WALLIS: There is a DAC. There is a DAC.

MR. LI: Baseline review document and we have another chance to review and will write SER.

MR. WALLIS: There's another stage.

MR. LI: Right.

MS. DUDES: Now, excuse me. This is Laura Dudes, Deputy Director for the Division of Engineering. What they're approving in the DCD is the DAC and will be verified through ITAAC. And as they say, it meets the regulations; and, therefore, by definition or the Commission's definition, is safe. So they don't necessarily do a formal prudency review. However, I think if you look at the times that they've looked at this design, the number of questions that they've asked, the number of meetings that they've had, I think that, although we don't regulate the prudency, I think the questions have been asked. I understand your point, and, in the interest of time, if there's a follow-up question on prudency, we can answer that. But I'd like to let them --

MR. WALLIS: I was concerned about the statements of a DAC doesn't exist --

MEMBER BROWN: No, the DAC is here. There's a DAC.

MR. WALLIS: But not in every case.

MEMBER BROWN: Well, no. If you look at the reactor protection system, there is a --

MR. WALLIS: Oh, there is a --

MEMBER BROWN: -- there's a list of numbers for the reactor protection system, and it says

how they're going to go do it. And part of that -- well, it's got an item-by-item, number-by-number things in there. And I just lost one of the ones I wanted to see for the reactor --

MR. WALLIS: So it makes sense.

MEMBER BROWN: Well, no, I didn't say that. I just said there is a DAC and ITAAC.

MR. WALLIS: There is. Yes, that's right.

MEMBER BROWN: And I'm trying to give you an example to answer your question.

MR. WALLIS: There is a DAC, but is the DAC good enough? That's the question.

MEMBER SHACK: And that was just the answer you got.

MR. WALLIS: No, no. Well, she gave an answer, which I don't necessarily agree with.

MEMBER SHACK: Well, that's an answer. I mean, there is the presumption from the staff that there is sufficiency for the criteria.

MS. CUBBAGE: Let's just make it clear we have not decided that DCD Reg 5 is sufficient for anything, okay?

MEMBER BROWN: That's the one I reviewed, by the way. That's the only one I had.

MS. CUBBAGE: It only gets decided --

MEMBER SHACK: I understand that. I understand.

MS. CUBBAGE: We have significant questions with the DAC and the ITAAC in Chapter 7 that are all open, and you're going to hear from the staff about what those open items are.

MEMBER BROWN: But we were told that they were basically procedural. That was the statement that was made as the opening is that, you know, there are no safety-significant open items.

MS. DUDES: Safety-significant issues with the design as we have seen it, but we still have significant open issues with the documentation which includes the quality and completeness of the DAC.

MEMBER BROWN: Or the, in my mind, the completeness, not necessarily because of the definition or the description of the systems as they are proposing them.

MS. CUBBAGE: And we heard that that's your concern.

MEMBER BROWN: Yes, okay. And it deals with several of the items within 603 relative to independence. Physical and electrical independence comes across pretty clearly. Communications independence does not come across very clearly at all

or doesn't come across period. The system descriptions they went through today lead toward some of that, but, yet, they are not, if you look at the way the DAC and the ITAAC are formulated, they don't address, they just said, "We're going to go inspect and test that to see that it meets 5.6." That's it. There's nothing from which to draw what are the criteria, what are the figures, what are the connections, how do we know what the nature of that data is, the characteristics of it, etcetera, etcetera? And that's all missing.

MS. CUBBAGE: I think we've got that concern --

MEMBER BROWN: I've got an old habit of repeat it once, repeat it twice, maybe six times. I'm sorry.

MS. CUBBAGE: Let's let that go. I didn't do the review. Let's let that go.

MR. LI: The next slide. The design process --

MEMBER STETKAR: Let me stop you on 7.1, though, just to kind of reinforce a little bit of the stuff because there are statements in the SER that do make technical conclusions about the design. You read the SER, and there are indeed several statements in

there that make active technical conclusions accepting portions of the design. One of them is a statement that says the main control room fire will not actuate any DCIS controls other than trip the main generator. The main control room fire does not result in the loss of offsite power or the loss of the diesels. That's a positive statement. I was quoting from the SER there, and I was curious how you reach that conclusion without any information about what is actually in the main control room. That's a technical conclusion in the SER. That is a statement. It is not a request for additional information. It's a statement, and I didn't read that statement anywhere in the DCD or the topical report, so I was curious how you reached that.

MR. LI: DCD, Chapter 19.

MEMBER STETKAR: Chapter 19?

MR. LI: Yes. That they, basically, they don't have any power circuitry, a circuit breaker in the control room, only the low level signals. So there's no --

MEMBER STETKAR: That's all you have in any control room is low voltage signals. It's just in a lot of other control rooms there are push buttons or switches, not VDUs. I've never lived in a control

room that had any more than 125 volts of DC in it for good reason. So it's all low voltage.

MR. LI: Q-DCIS cabinets are outside --

MEMBER STETKAR: And all of our protection control cabinets were outside of the control room, and, yet, you could trip offsite power and you could do a lot of things from our control room, as you can from any other control room. So I was curious why in this control room it cannot happen. It has nothing to do with voltage. It has nothing to do with locations of cabinets, it's all of the controls are in there. Anyway, I just wanted to highlight two or three things and ask you about them.

Another section states that the IC PCC pools have no active components and do not require INC functions to perform their safety-related function of transferring heat to the atmosphere. Accordingly, because the ultimate heat sync cooling water does not require any INC functions, the staff finds that the requirements of GDC 44 are not applicable to the ESBWR and design. What about the INC that's required to open the valves that communicate from the equipment storage pool to the IC PCC pools, which are apparently required for some types of accidents. Otherwise, they wouldn't be there. That's a positive statement that

says there's no requirement for INC to support long-term cooling through the IC PCC pools, yet in the DCD I read about requirements to open those valves for certain accidents. I don't know what those accidents are. I didn't go back and actually look at Chapter 15 to find out what accidents they required. So I was curious how you drew that conclusion.

MR. WACHOWIAK: Can you read that statement again? I think they were talking about 72 --

MEMBER STETKAR: No, there was no 72-hour limit.

MS. CUBBAGE: Can we get a page number on that?

MEMBER STETKAR: I don't have the page number. It's Section 71136. But I don't have my computer with me, so I can't quickly find the page number. It's probably one of those long sections. It's under sub-item 21 GDC 44 cooling water. So if you find the section --

MS. DUDES: Okay. I'm not going to pretend to find that section and answer this now.

MR. LI: It's the passive nature.

MEMBER STETKAR: It's a passive nature except in the DCD it says for certain accidents

there's a requirement to open those communication valves. And as I said, I don't know what accidents they are. I didn't do the homework to go back and look at Chapter 15 or close the loop to see what accidents those valves must open under. But, apparently, under some accidents, and I'll ask GEH this, is it true that the, I'll call them make-up valves, but the cross-tie valves from the equipment storage pool to the IC PCC pools need to open under some accident conditions and even I'll ask it pre 72 hours, so I'll give --

MR. WACHOWIAK: Pre 72 hours, if there's no active cooling systems, those valves must open to have enough water to boil off for 72 hours in the decay heat --

MEMBER STETKAR: And no --

MR. WACHOWIAK: However, this SER was based on rev 4 of the DCD, and I believe on rev 4 of the DCD those were rupture disks rather than squib valves.

MEMBER STETKAR: This SER is rev 4 of the DCD? Because it makes reference to an awful lot of rev 5 things.

MR. MILLER: Rich Miller, but I'll let you speak for it.

MR. GALVIN: It's primarily based on rev 4 in the, you know, as we've discussed, in some places where -- 76 and 75 and 77 in particular we had an opportunity to revive those sections based on DCD rev 5 just because the development process took a fairly long time.

MEMBER STETKAR: So it's a four plus? Okay.

CHAIRMAN CORRADINI: So just to make sure I understand this one particular point, the one where it was reviewed, it was rupture disks and not valves, and that has since been changed in the design?

MR. WACHOWIAK: In rev 3 and 4, it was an option for rupture disks, which we thought was the best way to go with that. And when we finally got to rev 5, we determined that it probably wasn't the most prudent way of implementing that, so we changed it to a squib valve, primarily a squib valve operation. So our primary means in the earlier revs we thought was going to be rupture disks because they introduced some other failure modes that we didn't want to have to deal with.

CHAIRMAN CORRADINI: And that's Rick Wachowiak.

MEMBER STETKAR: There are a few others,

but in time consideration --

MR. WALLIS: Can I ask some of the -- you make a statement about inadequate core cooling, which is a very important issue. The indication of inadequate core cooling, there's a whole section on that. And you make a statement the RPV level is the only issue to be considered. Now, if you have an indication of RPV level, it's a collapsed level, whether or not the core is cool has to be determined by analysis. Just because you know there's water there doesn't mean the core is cool. When the water level, the collapse level may be such that in certain regions you get superheated steam coming out of the core. It would be very useful to have an indication of whether or not to superheat steam. And you indicated cooling temperature can be determined entirely from the reactor pressure. Well, if you have superheated steam, you don't know the temperature just from the pressure, so I would think you would have asked the question why is having a level indication the only thing we need to worry about about whether or not the core is being cooled properly? But you don't seem to question, you just seem to accept the statement that it's okay just to measure level. I would think you'd want to measure exit temperature

from the core or something that tells you whether or not you've got superheated.

MS. CUBBAGE: We'd have to take that back for our reactor systems.

MR. WALLIS: Oh, they are. I mean, there's a statement here that it's okay.

MS. CUBBAGE: But they can't answer the question.

MR. WALLIS: It's the same thing that maybe concerns some of my colleagues. You question these statements, not just accept them, because --

MS. CUBBAGE: I'm not discounting your question. I'm saying that we don't have people here to answer it.

CHAIRMAN CORRADINI: Go ahead.

MR. TANEJA: Basically, you know, since our review had a lot of focus on the process, the design process, we looked at GE's software QA management plan and their software QA plan and software QA management plan, and it's in line with our branch technical position assignment 14, which, essentially, is a development life cycle process. And this, you know, part of our SRP, it provides a process to assure a quality development of a digital INC system. So if it's followed and it's verified that

this process is followed that it assures that at the end of the process that we would end up with a high quality product.

So, you know, I don't know. We just put this in. This is from our branch technical position. Assignment 14 is the different stages of our life cycle process. Basically, you know, just like what GE went over is the planning activities as the first phase, followed by the department's activity, and then the design activity. Now, basically, what we're seeing is that the end of each, what GE is proposing is that the end of each life cycle process they're going to write a baseline summary report, which would be available to us and we choose to review that and evaluate that. And, essentially, all the requirements are captured in the ITAAC DAC right now, which is complying with the 603 requirements, criteria requirements. They need to be all spelled out for each of the platforms in the requirement specification. Again, when they're going through the development process and at the end of each activity, be it planning activity, at the end of each activity we should be able to review that and verify that they have actually captured all the requirements that are in the DCD.

So, essentially, you know, so really there's a big emphasis on following the process, and that's where we looked at their software QA plan and software management plan, which is in line with the branch technical position assignment 14. And what we did on the, you know, as for the question was on the adequacies on the DAC and ITAACs, you know, SRP Chapter 14.3 I think it is for why is the guidance on the, you know, types of ITAAC that need to be captured for the INC area, especially for 603 compliance. And we, basically, verified the DAC ITAACs and they were in compliance with the SRP Chapter 14.3.

MEMBER BROWN: But a point on that is when I tried to look at 603, a couple of the criteria that you went through, I then looked at those requirements and said, okay, what can I go look at in the DCD to say does the design meet those requirements? It wasn't there. So in terms of seeing that the design in its present state or how it was at least described couldn't do that relative to a list of, I mean a couple of them you could, many of them, maybe most of them, you couldn't. And so that was kind of the genesis of my comments from that standpoint. And if you're going to use a DAC and ITAACs approach, you need enough description of the design as it has been

certified to be able to know that when they develop the plan to go look for those that the information is there and that they're going to be certifying stuff that we've seen, you all have seen, and the Committee members have agreed with.

MR. TANEJA: You know, I agree with you. We do have some open items --

MEMBER BROWN: I know you do. I'm just giving you the thought process I had. I'm not saying, I'm not saying, I'm not trying to be picky on any one thing. I'm just trying to give you the idea of where I -- and I think, I'm not going to speak for John, he's got some of the same thoughts I think, relative to his comments.

CHAIRMAN CORRADINI: Can I just ask a general question again? Because I'm not understanding the details of this. But I sense the staff, as Amy has said and others have said, that you have a lot of open items and still more information is coming. But I sense that in the conversations with GEH in the developing of the current open items and closing certain ones, you have much more information than we have seen in the DCD rev 5. Is that a fair statement?

MR. TANEJA: Well, you know, just like what GE presented right now, you know, in our meetings

we basically --

CHAIRMAN CORRADINI: Clearly, today I've seen a lot more than I saw in the DCD.

MR. TANEJA: Exactly. So the thing is there is a certain, in the blinders that we have to put on, we have to look at the document as it's presented on docket. You know, we're evaluating that. And really most of the open items are in that area that, you know, listen, we know a lot more about the system and it would be nice to have it properly documented, and that's why we are saying that those open items in the area, maybe it's a level of detail, maybe it's inconsistencies between different things.

MEMBER BROWN: Well, let me --

CHAIRMAN CORRADINI: Just let him finish.

MEMBER BROWN: Oh, I'm sorry. I apologize.

MR. TANEJA: Right. So those open items, and we've gotten a response on some of the RAIs, which have really, you know, I would say considerably changed. For example, tier one, what is that table for the 603? 2215 is redone totally, okay? So when you look at it now, it has a different flavor all together as to looking at the process. You know, the way the ITAACs are documented or the DAC ITAACs are

documented, and now if you look at it it really provides a more defined process with very little wiggle room to be able to implement that process.

MS. CUBBAGE: On that note, I just wanted to mention that there has been such a significant change to tier one in these areas that GE is going to be sending us basically a rev 5 plus version sometime at the end of the month or in January time frame that's going to roll up all of the changes that they've made in tier one that respond to staff RAIs.

CHAIRMAN CORRADINI: Okay. That's very helpful.

MR. GALVIN: I think it would be important to point out, in Section 3.2, the technical content -- this is Dennis Galvin -- of the DAC is changing significantly. That's the software, the DAC ITAAC for the software development activity. The main focus of the RAI is to make sure we can understand how they're going to actually close the DAC and that it addresses all the requirements because the way it was laid out, it was not clear that they were going to address all the requirements. So 3.2, I think we're going to see a significant change in the content of the actual criteria.

MEMBER BROWN: But that's software.

That's software as opposed to the architecture issue that's meeting certain requirements.

MR. GALVIN: 603, I think the format and the way it addresses the platforms is going to change. But as far as the level of detail in the actual criteria for 603 staff has not had a whole lot of questions on. So, more or less, what you see, it's going to change in the format. They're going to add some criteria that they didn't have before, but the level of detail, and there is, more or less, consistent with the SRP and we don't have --

MEMBER BROWN: In the DCD Chapter 7?

MR. GALVIN: No, the ITAAC. And Section 2215, the level of detail --

MEMBER BROWN: You're talking a change is what you're saying.

MR. LI: Well, Table 7.1-2 they have a cross reference to address each 603 requirement discussing DCD and which section. So that table will keep the, how they --

MEMBER BROWN: Is that the one with the systems across the top and the criteria down this and just put an X in a box?

MR. LI: No, that's Table 1. That's the --

MEMBER BROWN: No, this is in the DCD chapter.

MR. LI: The DCD 7.1-2. It's a cross reference to how they comply with the specific section of the 603 requirements.

MR. TANEJA: It basically provides a roadmap to the different parts of the DCD.

MEMBER BROWN: I know exactly which table you're talking about. I saw it and I looked at it, and it was a matrix and had 603 item whatever, Section 4 or 5.1 through there, and it had systems across and then put an X in the box whether he had to confirm it or not.

MR. TANEJA: No, see, that's a different thing. That's a tier one document. That is truly a multiplier for your DAC ITAACs. So if you see, you know, for example, requirement number, you know, and there's a bunch of Xs, that many DACs are there.

MEMBER BROWN: What was it? Seven --

MR. LI: 7.1-2. I think it's the roadmap for that. They cross referenced many DCD section numbers.

CHAIRMAN CORRADINI: Keep on going. Why don't you proceed, please?

MR. TANEJA: Okay. So, you know,

essentially what we looked at also, you know, the level of detail question came up, just like what's coming up, and we went back looking at our position on why the DACs are there and how much information we need. So, essentially, what we were looking for is, you know, high-level system design information and then a clear process for implementing that system design. So that's really where the focus was in looking at the adequacy of the DACs and looking at the definition of the DACs that they're very specific.

So, you know, that's the open items. We'll see that. Like I said, that is a major change that's already happened. I think we'll see the next revision and we'll see them.

MEMBER BROWN: All I thought you really had was a process that says they will design the system and then they will inspect it to a set of diagrams that they generate and they will confirm that it complies with 603 in these various areas and they'll write a report that says it complies. A little sarcastic, okay? I'm not meaning to be pejorative or a smart aleck or anything. But that's the way it comes across. I mean, we'll develop a block diagram, we will review the block diagram, we will determine that it meets the criteria, and we'll

submit you a report that says it meets the criteria.

MR. TANEJA: Well, let's go back a little bit. Now, the thing is the high-level design concept, you know, it's there, in a sense, that, first of all, the DCD is far from neutral. Now, we are hearing about TRICONIC and NUMAC and all that. Okay. That is neutral, right? But we do know that there are four divisions of RPS, okay? Now, they're independent of each other.

MEMBER BROWN: That's not clear. No, you can't tell how some of the data goes between them.

MR. TANEJA: No, no, that's a requirement. See, this is what I'm saying. The IEEE 603 requirement of independence is invoked. That's one of the DAC items, right? Now, if it's a DAC item, those four divisions need to be independent regardless. Now, how you, you know, prove that is part of the DAC closure. I don't have the detail design. I cannot verify that. Until I see the DAC closure, I cannot verify the compliance of that requirement.

MEMBER BROWN: But what do you expect to see as a DAC closure?

MR. TANEJA: What am I expecting to see a DAC closure? I'm expecting to see detail that would say that how did they meet that requirement, the how

part. Right now, they're committing to meet it and this is the process, but how do they meet it is going to be part of that DAC closure.

MEMBER BROWN: So you get to design what it looks like so they can tell you how they verified the design? So you're going to get more design details?

MR. TANEJA: Exactly.

MS. DUDES: Let me just help explain a little bit about the ITAAC process in general and what is required in that. I mean, each of these items, as we know, is not complete, and the whole purpose of ITAAC is to verify the as-built plan and its inspections, tests, analysis, and acceptance criteria. So what is required by the regulations is that the licensee will submit under oath and affirmation to the Commission that they have completed because it is their responsibility to do a 100-percent verification that this facility has been built in accordance with its license. But then there's an entire inspection program built around going out and actually -- I understand, and I think we all have challenges with some of the wording. I will agree with you that when you read some of the ITAAC associated with the DAC it can feel a little, there's a report, it exists, it

concludes this, there's a diagram, and it doesn't give an engineer perhaps as warm of a feeling. But there is a full-blown inspection that will take place. It's not necessarily that submission of that report --

MEMBER BROWN: I'm not worried about the inspection. I understand that part. After a design is --

MS. DUDES: Which is conducted by these --

MEMBER BROWN: Yes, but you've got to have a design to which you're going to do the inspection and you've got to know what that design looks like before you can inspect to it. I'm sorry.

MS. DUDES: No, that's okay. I understand the concern. I think in terms of DAC and ITAAC, especially with INC, these conversations are quite understandable because the staff continues to have them with the applicants.

MR. TANEJA: We went through the same frustrations of lack of detail, you know, trying to understand how much detail is adequate if you're going to use this DAC process.

CHAIRMAN CORRADINI: So can I try something there since I'm, again, totally out of my element? So if I were in your shoes, I might go back and ask how did this compare to the past

certifications and the DAC confirmation for acceptance criteria on the ones that you already have certified on a relative basis? And you've done that.

MR. LI: The ABWR better than --

CHAIRMAN CORRADINI: Excuse me?

MR. LI: The current documentation in ESBWR is better than when we certified the . . .

CHAIRMAN CORRADINI: And ABWR?

MR. LI: ABWR is a pioneer. In fact, I don't really know how to expect the ITAAC, but we kind of tried to improve our process.

CHAIRMAN CORRADINI: Okay. So you used that as a relative basis and decided that the DAC, if the acceptance criteria for the DACs were of at least equal specificity and compliance that you felt comfortable with?

MS. CUBBAGE: I will say that we have taken lessons learned from all of the previous certified designs and applied them here. We had inspectors review the ITAAC in addition to the technical review team, and we're making sure that they are legal and that they are something that's inspectible. So that whole process has taken place. And as Laura alluded to, the construction inspection program, the whole office down in Atlanta, in addition

to the team here that's working on the program, and the licensees are going to be required to have an enormous amount of documentation to support the closure of each and every ITAAC. And in the case of DAC, it's going to be a voluminous amount of information that needs to be made available to the staff so that we can agree or disagree with the licensee that they have completed the DAC.

MR. JUNG: This is Ian Jung, chief of the INC. The whole topic of how much detail is somewhat subject, and we had the same question previous times. And it's a fact that, you know, we did not intend, the DAC I think was recently only meant to be platform-specific area. The reality of where GE belongs in this life cycle stage, this life cycle stage is not necessarily solid by itself. Eventually, hardware and software has to be integrated. GE's life cycle stage is some there in the planning and the requirement stage, sometimes with some design activity because we have high-level design information.

So what we are expecting, just like in previous cases, some of the design details that Mr. Brown is talking about, although our wish is to get as much information now, when we ask that information through the topical reports, the NUMAC, application of

NUMAC and TRICON, when those information was provided, there were a lot of concurrent processes that are not all through their design stage. We are at the stage of creating enormous amount of RAIs. There's no way we could go through the review process. That was one of the challenges. And that's why we relied on, them tell us through your life cycle stages, develop your requirements, and develop your detailed design, and they will go through the DAC verification stage that we have another opportunity to verify that, not as a licensing opportunity. We're going to make a safety finding at this stage, but with the commitment in the DAC. But DAC verification is extremely important. That's why it keeps coming up.

MEMBER SHACK: The question keeps coming back to why you feel the DAC are complete enough. I mean, when you do the final acceptance and review, you will review to the DAC criteria. You won't be able to ask for anything more than they've committed to. You can ask them to meet that, but you can't go further. Now, what gives you the confidence that you've got sufficient --

MR. JUNG: One is, from a regulatory perspective, INC area, fortunately we kept up with the regulatory criteria, acceptance criteria, the industry

guidance. The requirements traceability, we're not talking about just a 603. If we get down to industry standards that are endorsed, GE is saying there are 9,000 or 10,000, that range, of acceptance criteria they have to meet and trace it through the life cycle practice. Plus, also, when you look at this chart, at the bottom part of it, there are built in within the processing each side of it, and then each output has to be verified. And then our INC's verification activities cannot go on top of that, and we realize it's going to be a process because, as they go on, they'll learn some lessons, "Oh, we should have done it this way or that way."

But at the end, after this, you should look at the validation stage, integration stage. They're going to be additional testing requirements that are coming along, individual platforms, and then the factory acceptance testing, site acceptance testing, and then Chapter 14.2 that shows start-up testing and pre-operational testing. There are multiple layers that they're coming along.

So we feel, even though we are sort of focusing on 603 and some of the requirements, all these pieces together, you can put together, you know, if GE follows this process and if they demonstrate

clear compliance and conformance with the industry guidance and standards and regulation and design criteria, I think we have a strong belief that they'll get there. I think some of the challenges we've seen is not necessarily their complying with those things or not. Sometimes it's the implementation. They are not actually implementing the way they are supposed to be implementing in these processes. That's why we have some concerns. Those are being dealt with in terms of schedules and other vehicles at this point.

But I think we, in the INC area -- another thing I didn't mention is also INC DAC and ITAAC, INC in general is a software system. So we have also, you know, ITAAC related to the very specific systems themselves. Those systems have to perform the requirements listed in the DCD. So we are, those are very important, too. Eventually, at the end of the game, those GDCS functions have to function as it is intended. It has to have demonstrated INC's part of that demonstration, and we are building additional, all these requirements to make sure they follow the process.

MEMBER BROWN: The observation, I'll use the GDCS as an example, and you say it's a support system. But, in fact, it's not a support system, it's

the thing that takes the problem and actuates the solution. And if it doesn't actuate or you don't understand the design in its configuration so that it will actuate, I don't view it as a support system. It is the brains, the know center, and the monitoring information to know what the plant is doing. All the rest of the stuff is just hunks of metal and valves and water.

CHAIRMAN CORRADINI: Don't forget the water, don't forget the water.

MEMBER BROWN: I mean, it's blacksmith technology. I mean, squib valves, you're blowing up valves to make water going into the plant. I mean, you can't get anymore blacksmith than that, okay? We could use 400 AD gun powder and do this and it would do the same job. I'm trying to inject a little humor into this discussion, serious discussion. The point being is what I feel like when I look at the INC systems, the way they're displayed, and I've sat through meetings on some of the mechanical systems and GDCS is one of them, and it was like sucking blood out of rocks to go through the slope of lines and then you're going to have air binding. I mean, good questions, all good stuff to look at. What's the design configuration to allow this passive system that

you can't test, it's got to be done right design-wise to make sure you don't have it bind up and a lot of the tension is -- I would view this, if you applied to DAC to it, you'd get a box that said here's the pool of water, here's some control valves, here's a box up here that's going to tell you to open these things, and we'll give you some DAC to show that it's going to work okay. That's the way I would view that if you applied DAC to this process. That's what I see being applied to the INC system: a very generalized, generic design applied across multiple systems with little detail about how and what the character of communication between divisions is that you have to have to get the trip signals there.

I mean, on your little diagram that you showed with the little rings and everything floating around, there's one line coming out that says two out of three voting. What is it? Time out, I'm sorry. So what I'm telling you is the bottom line is I guess I don't really agree with you right now that you have sufficient information to be able to confirm that the design is going not be confirmed by the ITAAC that you have to have to verify whether the design is that has evolved. That part is easy. Once it's designed, the ITAAC is clear. You have your drawings, you're going

to make sure that the --

MS. CUBBAGE: I see that you disagree that we have sufficient detail, but I think we need to move on. And if you all want to put it in a letter to us, you can do that.

CHAIRMAN CORRADINI: I have the sense that words are being formed at this point, so let's move on.

MR. TANEJA: In the SER Section 7.1-2, you know, we evaluated the software management program manual and the software QA program manual that we received from General Electric. You know, we used our SRP branch technical position 714 as a guidance to evaluate these manuals. It really is a digital system platform development process because, essentially, within that process is where you are coming out with your specifications for your platform, your hardware. And it is part and parcel of the whole system. The title may be misleading, but we reviewed it, you know.

Essentially, like I said earlier, their process follows our branch technical position pretty much, you know, the life cycle process. As far as the SER open items, you know, we've asked the question on the SER open item is that they had the DAC, this is where they're call captured in Tier One 3.2, and we've

seen the response in a draft form right now. Essentially, what it was is the DAC ITAACs are now broken out for each of the platforms separately, where, you know, the implementation would be done platform-by-platform basis. So once that platform is done, the DAC goes out, our DAC evaluation is going to be done platform-by-platform basis. I think that was the major change in that. So that is an open item that we are working through with GE right now to get that resolved.

CHAIRMAN CORRADINI: Keep on going.

MR. LI: The defense in depth in diversity is a major concern for the digital systems. GE submitted a topical report to address their strategy and then how to comply with the BTP 7-19. BTP 7-19 provides the guidance how to perform the assessment of the system, and staff reviewed this topical report. They conform with the BTP 7-19.

The only open issue in this area is some inconsistency because DCD revision 5 makes some change in Chapter 15, but it's not reflected in the topical report, so we had a question, so we required the topical report to be updated to be consistent with DCD.

The next area is the set point methodology

thing we already discussed. We have one open issue and a discussion. It's related to the, in staff's view, when they perform a certain methodology, but it's still in discussion.

MEMBER BLEY: Can you say that one again? I didn't . . .

MR. LI: We still have one open issue related to this how to determine --

MS. CUBBAGE: We can't get into too much detail in an open session, correct?

MR. JUNG: GEH responded to a staff question on demonstrating 95.95, and they responded, and we are not fully comfortable at this point regarding -- in our view, there might be potentially some reduction in the margin that maybe it might be okay but maybe not. We are trying to conform that right now.

MS. CUBBAGE: If you'd like, we do have --

MEMBER BLEY: Okay. So that's enough for now. Thanks.

MR. LI: The data communication of each platform. So when we reviewed the data communication, it's part of the DAC process. When we reviewed the platform back closure, we're also covering this data communication system.

MR. JUNG: Mr. Brown, this is an area that our main review is, essentially, in the communication.

MEMBER BROWN: Did you finish it? Is your conclusion that it's okay?

MR. LI: Well, it's a back process. We will defer to the DAC closure base because it's part of this platform design.

MEMBER BROWN: I'm going to keep the meeting moving right now.

MR. JUNG: Yes, we don't really have detailed design information. We --

MEMBER BROWN: I agree with that.

MR. TANEJA: All right. In the SER Section 7.2, basically we, you know, we evaluated the reactor trip system. In the ESBWR design, the reactor trip system consists of the reactor protection system function, separation cool temperature monitoring function, and the neutron monitoring system platform provides the input for the, neutron monitoring system provides reactor trip signal.

In this design, you know, essentially, under Chapter 7.1, we evaluated the platform generically. This thing is going to resolve on the RTIF platform and the NMS platform. These are the two platforms that contain the reactor trip system. And

we basically reviewed the section, Section 7.2 guidance, and, essentially, again, there are a few open items that are still being worked, and they are all, again, going back to the DAC and clarification of the DACs, so the process is well laid out for the DAC closeout and evaluation of their design. And that's where we are.

As for the high-level design is concerned, you know, I think they provided, the logic was in words, not in figures, as was the, you know, the documentation is concerned. But there's enough information there for us to be able to, you know, develop the adequacies of the ITAACs and DACs.

Section 7.3, the EESF systems, in the ESBWR, essentially, it's the ECCS, the leak detection and isolation functions of the other system, minus the MSIVs, the control room have ability systems, and the reactor breaker isolation functions. Similar to 7.2, the SSL, this, you know, the EESF system runs SSLC/ESF platform. It's technology neutral. It's basically an as-is platform, as opposed to the reactor trip which is a fail safe platform. We looked at that under 7.1 generically, the whole platform. Here, we looked at the specific functionalities of the ESF system, systems I should say. And SRP 7.3 guidance was

followed for that one. And the open items are, again, they are really, there's not really any technical because there aren't any details of the design.

MR. WALLIS: Can I ask you a question?

MR. TANEJA: Sure, go ahead.

MR. WALLIS: I'm quoting from page 132, which says that SRP appendix 7.1-A states that the staff review should evaluate the INC system contributions to design module for reactor core and reactor cooling systems. Well, I don't know what that means, but what it could mean is that when you look at 2200 degrees F for EECS success, the INC system is worth so many degrees. What's its contribution to design module? I don't understand how you do this. How do you look at the contribution to design module from the INC system, and what do you use as measure as design module with regard to reactor cooling system?

MR. TANEJA: It's basically, what we're looking at is, one thing, this is our 603 criteria again, going back to it. We're looking at the accident analysis. Analyzing Chapter 15, right? In there, you have set points. Well, these are analytical limits or these are certain design parameters that are assumed for the analysis, along with some timing functions, that these functions have

to occur within a given time frame.

MR. WALLIS: But that's part of the design of the cooling system to me. That's not the INC. The INC is how it all works through the controls.

MR. TANEJA: Right. The INC system needs to assure that we are able to perform those functions within those defined time margins. Just like we were talking about, you know, the scan rates and deterministic and non-deterministic. Essentially, if there is a function that needs to be performed in X milliseconds based on the actual analysis, my INC system should be designed in such a way that we are able to get that function performed without invoking our --

MR. WALLIS: So it's nothing to do with reliability? It's just time?

MR. TANEJA: Reliability is also part of it because we have these redundant and diverse systems in order for us to be able to get the function -- well, it's deterministic, I would say. I mean, you know, this is our criteria. This is our design criteria and regulation.

MR. WALLIS: So what is the contributions of design module from all of this? Is it so many degrees in terms of the temperature of the --

MR. TANEJA: INC systems should not be contributing to design margin. It should be ensuring that we are not violating any of the design margins.

MR. WALLIS: That's right. That's why I was puzzled by this statement that you quote on page 132.

MR. TANEJA: Well, that's our SRP, and that's the way some of these things are written. But, you know, in essence, the INC system is, again, it's a support function. It really is there. It's not a thermal hydraulic system. You know planning itself is designed in such a way --

MR. WALLIS: Hydraulic system doesn't work either.

MR. TANEJA: Exactly, exactly. I agree with that. So when we look at our regulation, the compliance to 603 requirement assures that high reliable INC system, I shouldn't say digital period, when it's called upon to do its work, it does its work predictably and repeatedly.

MR. WALLIS: Okay. A few pages later you say design to assure an extremely high probability of accomplishing the safety function.

MR. TANEJA: Exactly.

MR. WALLIS: Now, what is that high

probability, and did it --

MR. TANEJA: Well, that's why we have the regulation guidance, right? See, you know, the assumption is this, you know, if the design meets these regulations and the regulatory guideline and criteria, by meeting those things we assure that it's a high probability of achieving its function. You know, we have four trains to do the same thing. We measure reactor level with four separate instruments for reactor protection and --

MR. WALLIS: Lousy instruments then the result is lousy.

MR. TANEJA: But that's where the qualitative and evaluation gets into it, you know, that we have these requirements, your appendix B requirements --

MR. WALLIS: You have four different channels, but there's no requirement on the reliability of each channel?

MR. TANEJA: Yes, it is.

MR. WALLIS: There is?

MR. TANEJA: It's one of the criteria of 603.

MR. WALLIS: So someone is going to give a measure to this probability at some time?

MR. TANEJA: Well, we are actually, you know, the INC design is not really a PRA. It's really a deterministic design.

MR. WALLIS: Nothing in life is deterministic.

CHAIRMAN CORRADINI: Let's move on.

MR. LI: Okay. The next section, GE has presented, I think the staff finds that design in compliance with GDC 19. They have a control room and a remote shutdown station to perform a safe shutdown if called upon. The open item in these areas similar to 7273. It's inconsistency in the documentation area.

MEMBER STETKAR: Hulbert?

MR. LI: Yes?

MEMBER STETKAR: To follow up on what I asked GEH earlier about this transfer, there was quite a long discussion in the SER about feeding criteria or concerns about the transfer to the remote shutdown systems. And your conclusion is that because there's no transfer required the design, the INC design of the remote shutdown system is fully acceptable. Is that conclusion consistent with what we've heard today saying that somebody has to do something some place to enable control from that location? A transfer switch

or something like that.

MR. LI: When we prepare SER, in my operating plan, you have to have some switch in a certain location you have to go to. So in their design with the digital capabilities, so --

MEMBER STETKAR: That switch doesn't make sense, but there's a requirement, as I understand it, to actively enable control. And I don't know the concerns, but the location of that enabling, is it the best thing to have it in the remote shutdown location itself? Should it be in a third location?

MR. MILLER: Rich Miller. There is no enabling it yet. At this time, it's only HFE analysis that the operator has to take these actions and include that into your design. So right now there is no enabling to get access to a system.

MEMBER STETKAR: I understand that, but the staff's conclusion that the design is acceptable is based, apparently, on the assumption that absolutely no action is required, and that's different than saying you aren't sure how it will be implemented.

MR. MILLER: I think that, you know, the field transfer switch and digital IT might require that to be re-evaluated. We'll go back and look at

that issue.

MR. LI: The Section 7.5 information system important to safety, most systems are related to the GMI action plan items. The post- accident monitoring system is the most important system in this session, and GEH complied with revision four of this 1.97. That involves the human factor engineering design process to determine these tests. It's a part of this bank process in Section 3.7. So the manual clarification and consistency when GEH update a revision, a DCD revision. It's not a major concern.

Section 7.6 as a specific item on this interlock. This interlock is not like a separate system interlock. It's mainly for prevent the half pressure damage to low pressure line and for RHR system. GEH only identify one interlock in their system, and because the failure of that interlock were not affecting the safety functions, they categorized that as a non-safety system. But they will be considered part of the litmus program. So the only open issue related to that is the Chapter 19, the litmus program table should include these items to be make it consistent.

MEMBER BROWN: You didn't take issue with their decision about it's not a safety --

MR. LI: Their analysis we find satisfactory, yes.

MEMBER BROWN: Okay.

MR. LI: 7.7 is a control system. As I mentioned earlier, our focus is mainly just make sure the failure of the control system will not impact the safety function and the action or inaction of the control system will not create a challenge to the protection system. So we still have an open item --

MR. WALLIS: They didn't say much about the neutron monitoring system.

MR. LI: It's kind of --

MR. WALLIS: Yes, but it's very important for the stability analysis in the control --

MR. LI: No, that's just for calibration of this label of this --

MR. WALLIS: Just for calibration.

MR. LI: Yes.

MR. TANEJA: There are two parts to the neutron monitoring system. There's a safety portion, you know. So, basically, what it is is that this part of the system does not have adverse impact to the safety side of the neutron monitoring system, essentially. So that, you know, on your neutron flux that it generates a trip signal.

MR. MILLER: Same thing for NBS.

MR. TANEJA: Right. Nuclear boiler system has --

MEMBER BROWN: Is this the AFIB card, the calibration where you come in under certain circumstances and calibrate the --

MR. LI: Yes. The next section is the diverse instrumentation and control system. And Chapter 7.1, we already discussed the diversity and test strategy. And this section mainly documents how they design and implement this ATWS mitigation system to satisfy Regulation 56.62 requirement and also the diverse protection system to deal with the common-cause failure in the --

MR. WALLIS: This is the section where you talk about defense in depth?

MR. LI: Right.

MR. WALLIS: Did you get to the usual question of is there any measure of what's adequate defense in depth?

MR. LI: Well, I think the, yes, the --

MR. TANEJA: 63-03 is really the guidance.

MR. WALLIS: Does it give you a measure of defense in depth? No, it just talks about ways to achieve it.

MR. LI: It's a deterministic approach from INC's point of view. So they propose diverse protection system, so we consider that acceptable.

MR. JUNG: Yes, this is Ian Jung. There's a research effort on adequate diversity dealing with the different types of human diversity, hardware, equipment diversity. Some of you might have seen the chart, I think. They're developing a new reg to demonstrate the degree of adequacy of the diversity, and we expect that new reg sometime early next year. We'll see that. But from our staff's perspective, we have basically new reg 63.03 which provides a process and strategy, and the BTP 7-19 has the acceptance criteria specifically related to 10 CFR 100 for postulated and AOs. We can eventually verify that through the DAC we have.

MR. LI: In summary, we followed the review plan, Chapter 7, to review the high-level functional requirements and Section 14.3 to verify the design commitment in the tier one. And the major area for INC's IEEE 603 criteria compliance in life cycle design process, set point methodology, diversity, and defense in depth, and data communication system.

MEMBER BROWN: Is that the 1992 version? The reason I ask that is because there's several

places in the chapter where it refers to criteria 4.1. The only copy I had was the 1998 version, and there were no --

MR. LI: The `91 is --

MEMBER BROWN: -- ABCDE, and so I had to go through and do a -- so I'm just asking is it 1993 to which they're making reference in here?

MR. LI: Yes, 10 CFR 5055, but we haven't changed the regulation, so it's still referenced --

MEMBER BROWN: IEEE 603 1991?

MR. LI: Yes.

MS. CUBBAGE: That's the one that's the law.

MEMBER BROWN: Okay. That's the one I don't have.

MR. JUNG: We can get you a copy.

MEMBER BROWN: I'm sure I will get some more paper or some more electronic information somewhere I'm sure.

MR. JUNG: To make it clear, 1991 and what we endorse is there's also 1995 with a little bit of modification for correction. The difference between the `91 and the 1990 version is very minor. It really doesn't even --

MEMBER BROWN: I figured it was.

MR. LI: So as we mentioned earlier, the many open items is for the clarification and consistency-related issues and documentation. Our goal is to make sure the DCD and have correctly identified the requirements, so when we're doing the DAC closure we can use the traceability metrics to follow up all those requirements. So no other significant safety technical issue.

CHAIRMAN CORRADINI: Thank you. Before we thank GEH and the staff, I'm going to go around the table to see if there's other questions from the members. Comments I think I'm going to get anyway, so I'm just looking for the questions. Well, I have that funny feeling, yes. Let's turn to the consultants.

MR. WALLIS: I don't have a question.

CHAIRMAN CORRADINI: Our mature set up in front.

MR. WALLIS: I'm trying to think about what my comments are going to be. I tend to agree with my colleagues on the other side of the table there, so you'll hear from me.

CHAIRMAN CORRADINI: I'm sure I will. Tom?

MR. KRESS: I have no questions, but you'll hear from me.

MEMBER SHACK: No questions.

MEMBER BROWN: I've articulated enough.

MEMBER ABDEL-KHALIK: I have one question, which relates to the firewall and whether or not the information that is available to see.

MR. POPPEL: It is not impossible, but, for example, the answer to your question is, yes, it could be corrupted. There are many, many ways to make that very, very unlikely. For example, it can be done over modem and they can pull it up and then the firewall can pull them back so you know that they're the right people. The data going to the display controllers in the technical support center, the EOF, those messages have the same kind of authentication features that the control room stuff does so that we can say that when it left it was good and when it's displayed it's good, okay? And, of course, they always have the ability to call up the control room. But aside from the authentication techniques, all the other stuff is like commercial firewalls because it's outside the ability to manage the plant.

MR. MILLER: But that's not to say that somebody could not.

MEMBER ABDEL-KHALIK: So you consider that to be outside your design certification process all

together, assuring that the information --

MR. POPPEL: The facilities and the requirement to meet 0696 is a requirement of the ESBWR. So we are providing it with the ability to get the information and the ability to display the information, and you're asking a very detailed question about can the information be corrupted. And the minute I say absolutely not --

MEMBER BROWN: It can always, there is no -- it's external. I mean, it will corrupt itself. It will. I mean, it just happens. Software does that.

MEMBER ABDEL-KHALIK: The point I'm trying to make is that this is very important because if this information can be corrupted you negate the function of these.

MR. POPPEL: The statement that you made is true. I don't think it's unique to the ESBWR, but it's certainly --

MEMBER ABDEL-KHALIK: But you're the one we're reviewing right now.

MR. POPPEL: I understand. But if you follow through and read the Chapter 7 thing and go through, we had our design basis accident, we've blown all our squibs, we re-pressurized the reactor, we've kept the core completely covered. You know, GDCS

pulls their drain, and there the reactor is. Now you're in a condition of, depending on which direction you want to go, cooling down or just maintaining it that way by filling the coolers with water. And so under those circumstances, I believe it's fair to say that the technical support center, EOF or ESBWR, have much less advice to offer the operators because there's not much left for them to do.

MEMBER ABDEL-KHALIK: I think it's emergency planning is what --

MR. POPPEL: Yes, I agree, but, again --

MR. MILLER: I fully understand what your concern is. We'll take it back offline because it's associated with emergency planning and it's getting the information out to the public, and then in the emergency, when we get into severe accident guidelines, many plants transfer command and control to the GDC, and that would be an impact there.

CHAIRMAN CORRADINI: Now, thank you to GEH and the staff, and I guess we'll all be back together tomorrow morning.

MR. WACHOWIAK: Isn't it tomorrow morning now?

MS. CUBBAGE: There is one action that I know I can do, and that's I can get the Committee to

copy the simplified logic diagrams that were submitted by GEH on the docket. Beyond that, I think there were some questions, if possible, we could get back to the Committee in the morning, but I think --

CHAIRMAN CORRADINI: No, that was the main one. I think that was the main one. There were some other clarification questions, but I think that was the main thing that you had mentioned that I think we'd appreciate.

MR. GALVIN: I would offer, I don't think the staff really reviewed those diagrams because they're not part of the design certification.

MR. LI: Yes, it is the sample. It's not really refractive ESBWR design itself, so it's just the logic diagram.

CHAIRMAN CORRADINI: Wait a minute, wait a minute. Let's back up. What did you say?

MS. CUBBAGE: We are not reviewing and approving them. They were submitted on the docket for information.

MEMBER STETKAR: But what Hulbert just said sounded like they aren't really the real ESBWR --

MR. MILLER: No, the SLDs are developed based on the DCD. So whatever is in the DCD wording, developed with simplified logic diagrams for one

division.

MEMBER STETKAR: From the DCD?

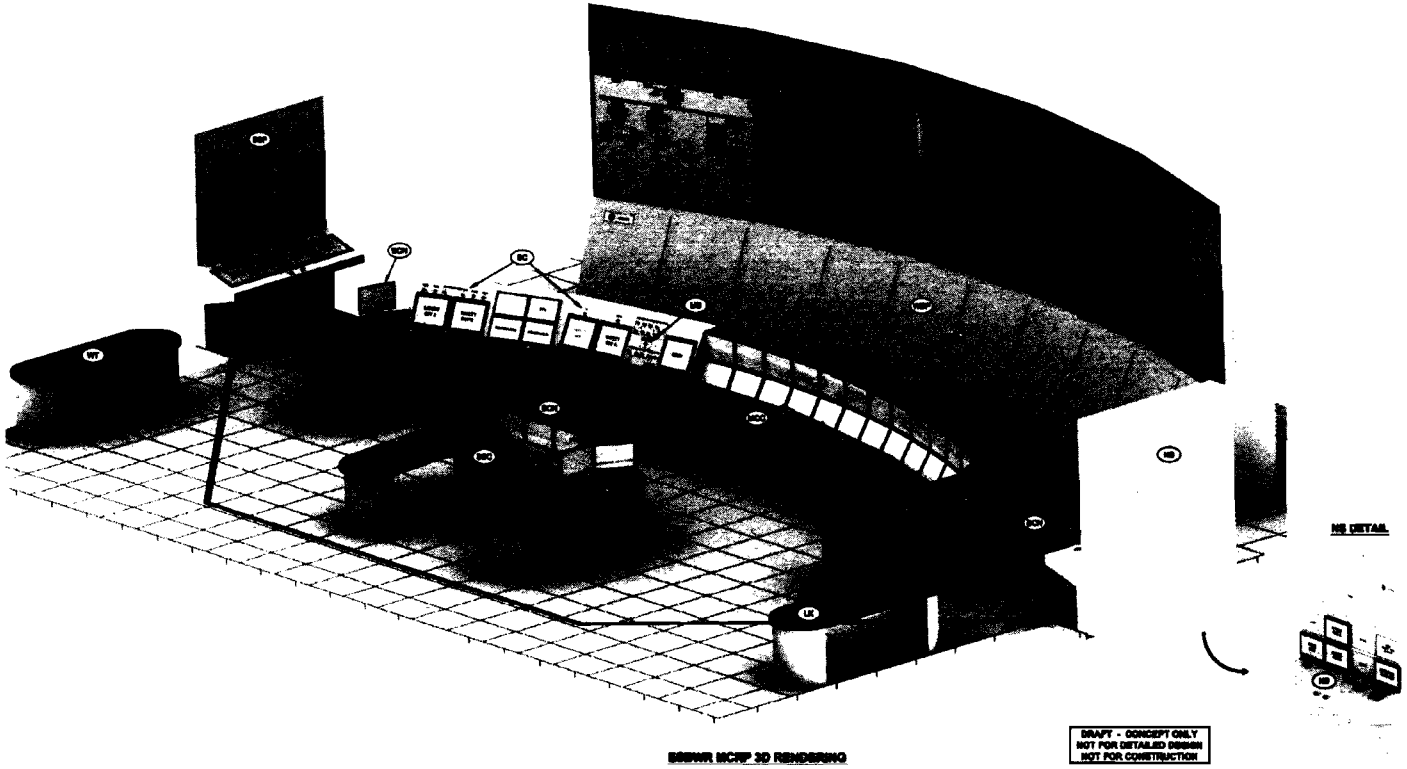
MR. MILLER: From the DCD. So we're up to DCD rev 5. I think the one they have right now is rev 6.

CHAIRMAN CORRADINI: Okay. Thank you all. We'll see you in the morning.

(Whereupon, the foregoing matter was concluded at 6:10 p.m.)

ESBWR DCD Chapter 7 DCIS Overview

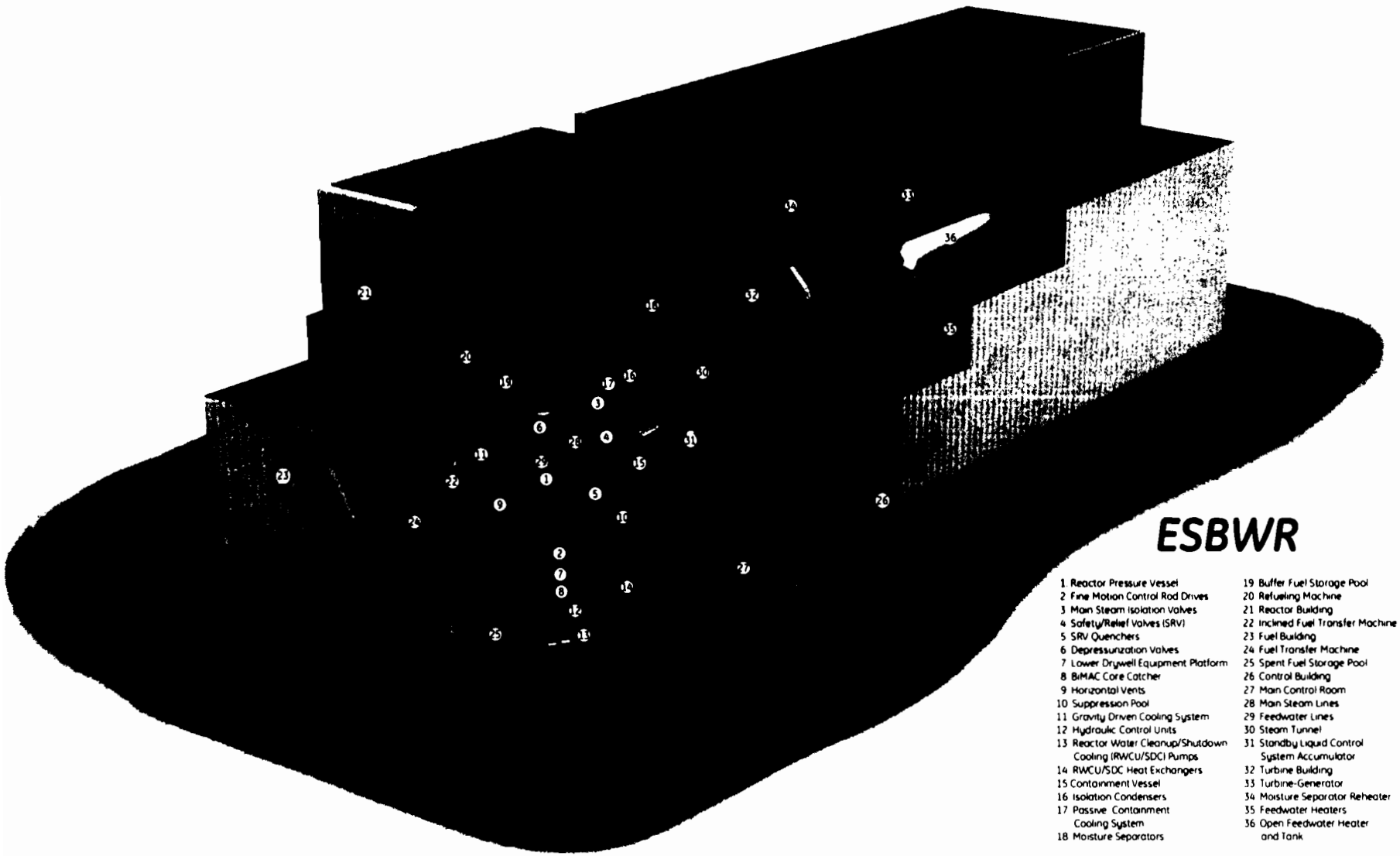
Full/Subcommittee ACRS Meeting



Rich Miller
Ira Poppel
Steve Kimura
Dec 3-4, 2008

HITACHI

ESBWR 3D Cutaway View

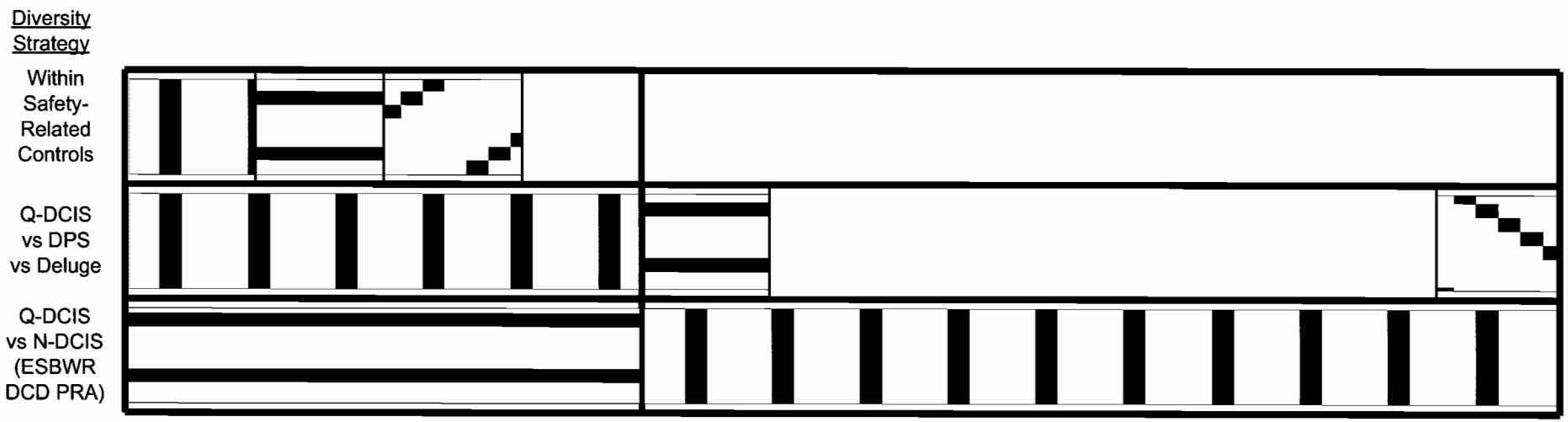


ESBWR

1 Reactor Pressure Vessel
2 Fine Motion Control Rod Drives
3 Main Steam Isolation Valves
4 Safety/Relief Valves (SRV)
5 SRV Quenchers
6 Depressurization Valves
7 Lower Drywell Equipment Platform
8 BiMAC Core Catcher
9 Horizontal Vents
10 Suppression Pool
11 Gravity Driven Cooling System
12 Hydraulic Control Units
13 Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) Pumps
14 RWCU/SDC Heat Exchangers
15 Containment Vessel
16 Isolation Condensers
17 Passive Containment Cooling System
18 Moisture Separators
19 Buffer Fuel Storage Pool
20 Refueling Machine
21 Reactor Building
22 Inclined Fuel Transfer Machine
23 Fuel Building
24 Fuel Transfer Machine
25 Spent Fuel Storage Pool
26 Control Building
27 Main Control Room
28 Main Steam Lines
29 Feedwater Lines
30 Steam Tunnel
31 Standby Liquid Control System Accumulator
32 Turbine Building
33 Turbine-Generator
34 Moisture Separator Reheater
35 Feedwater Heaters
36 Open Feedwater Heater and Tank

ESBWR DCIS

Safety Category	Safety-Related				Nonsafety-Related						
	Q-DCIS				N-DCIS						
Platform/ Network Segment	RTIF NMS	SSLC/ ESF	Independent Control platform	other	GENE		PIP A/B	BOP		PCF	
architecture	divisional	divisional	divisional	note 1	Triple Redundant (DPS)	Dual Redundant	Dual Redundant	Triple Redundant	Dual Redundant	Workstations	PLC (Deluge)



Note 1 – RSS provides operator workstations at appropriate diverse locations outside the main control room in accordance with GDC 19. See DCD section 7.1.3.2.3.2

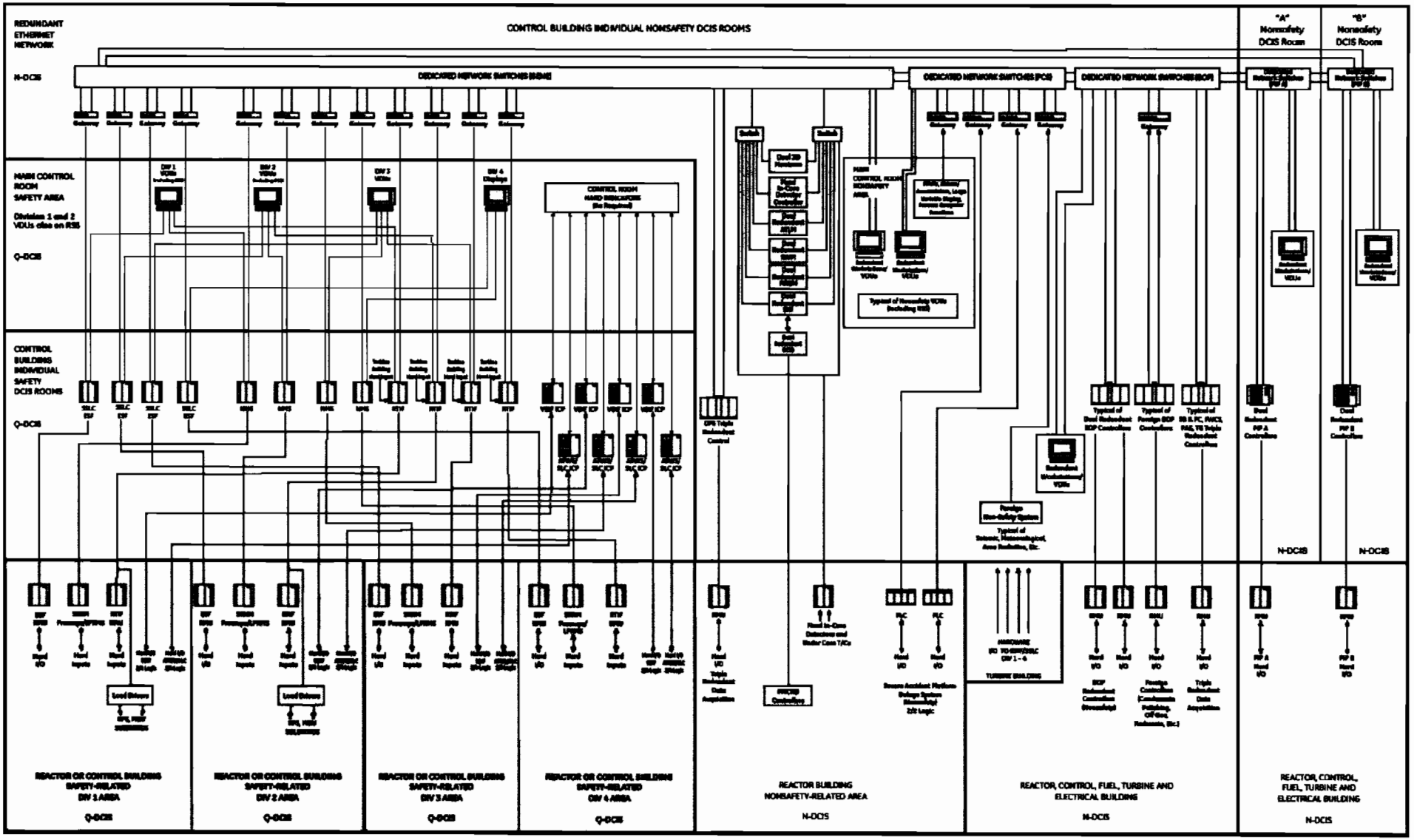
Note 2 – Crosshatching denotes different platforms or networks

Presentation Content

- Distributed Control & Information System Overview
- DCIS Function
- Q-DCIS (Safety-Related DCIS)
- N-DCIS (Non Safety-Related DCIS)
- MCR/RSS (Main Control Room/Remote Shutdown System)
- Severe Accident

ESBWR DCIS

ESBWR Distributed Control and Information System (DCIS) Functional Network Diagram



ESBWR DCIS Organization

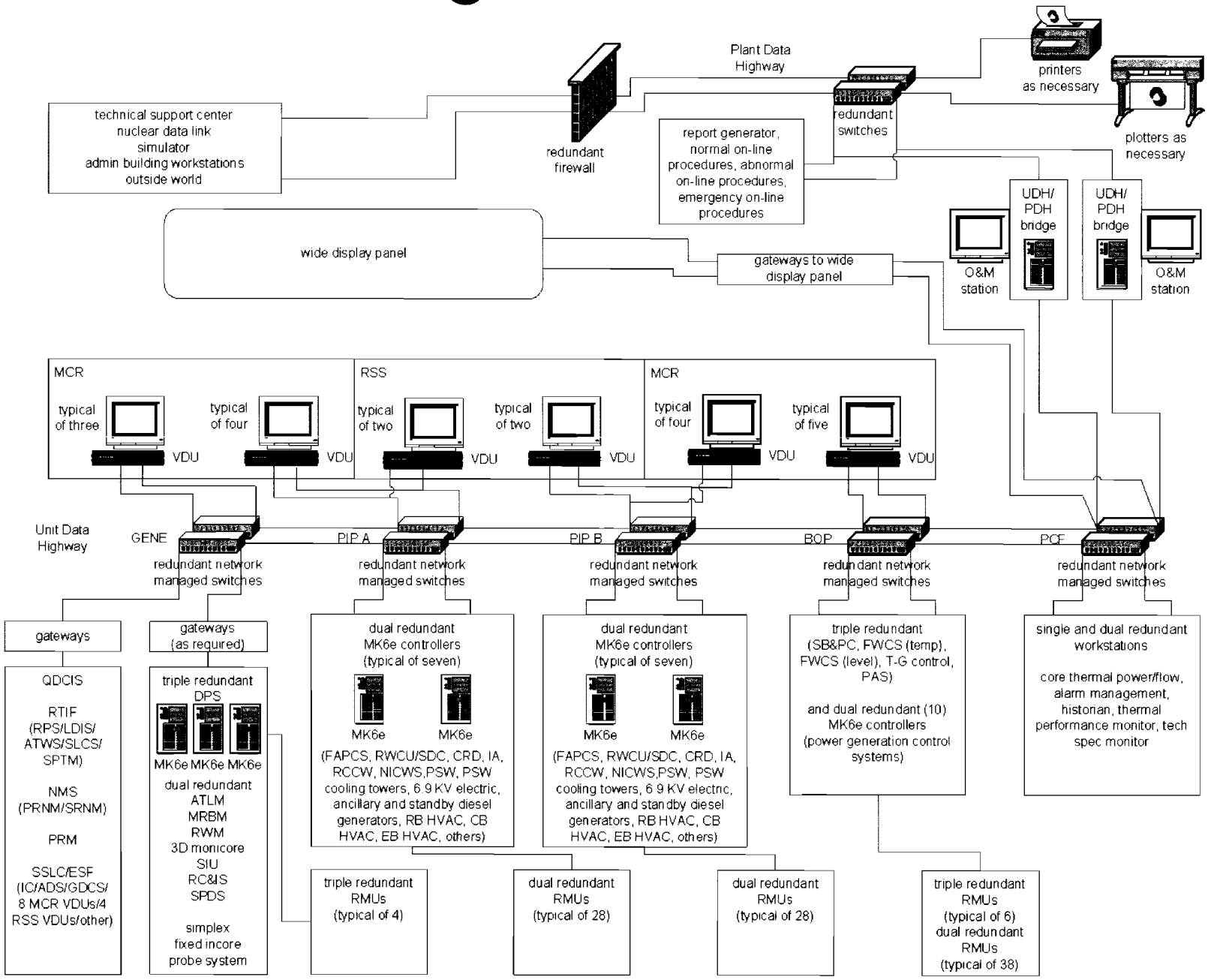
ESBWR DCIS organized around:

> Q-DCIS

> N-DCIS

- Network (managed) switches
  - GENE Network (includes gateways, Diverse Protection System, ATLM, RWM, MRBM)
  - PIP A Network (contains RTNSS)
  - PIP B Network (contains RTNSS)
  - PCS Network (contains alarms, recording)
  - BOP Network (power generation)

ESBWR DCIS Organization - Continued



HITACHI

ESBWR DCIS Functions

- ESBWR DCIS meets requirements applicable to new units and to existing plants
- DCIS capabilities allow for more reliable reactor control and protection than existing designs
- ESBWR DCIS supports "hands off" 72 hour coping

DCIS Organization – Safety-Related

- ESBWR Safety-Related DCIS (Q-DCIS) is designed with four divisions
  - Supports 2 out of 4 logic
- ESBWR Q-DCIS (RTIF/NMS and SSLC/ESF) retains all safety –related functionality with one of four divisions out of service and a random single failure in the remaining three divisions
- ESBWR Q-DCIS is specifically designed to allow a divisional safety-related battery to be taken out of service for maintenance or surveillance (load testing) indefinitely

DCIS Organization – Safety-Related

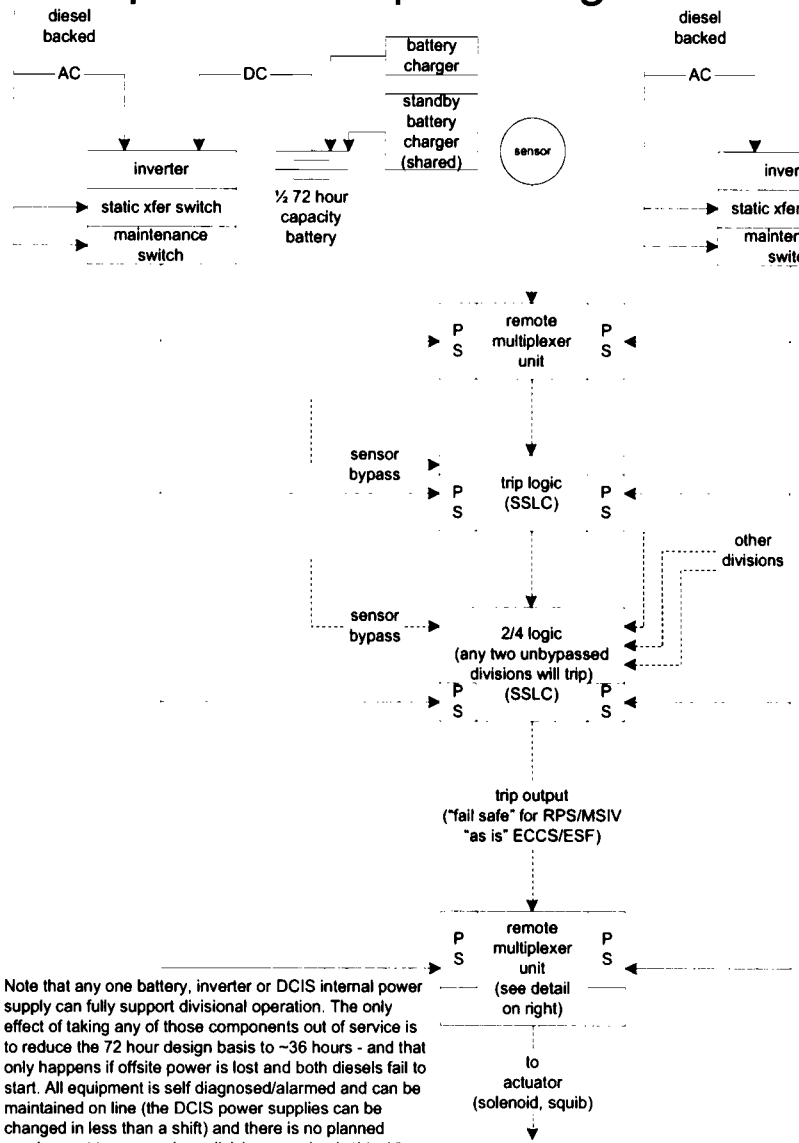
- Q-DCIS is deterministic
- RTIF/NMS and SSLC/ESF functions implemented on diverse hardware/software platforms
- N-2 can be more easily achieved in a passive plant because safety actuators are not "divisional"
  - > An ESBWR pneumatic valve or explosive operated valve (squib) can have multiple divisional actuators
  - > Unlike an active plant MOV or motor, the ESBWR valves do not lose functionality with loss of a division.

Q-DCIS Support

- Q-DCIS normally actively cooled but can operate continuously for DBAs with passive cooling
- Each Q-DCIS division supplied with redundant uninterruptible power for 72 hours, redundant on site non safety-related diesel generators and either normal or alternate preferred offsite power

Q-DCIS Power

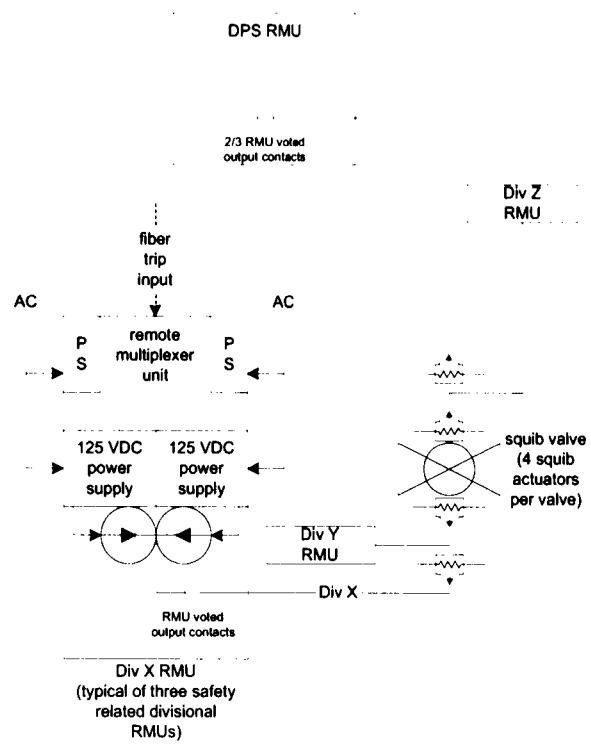
per division power/logic



Note that any one battery, inverter or DCIS internal power supply can fully support divisional operation. The only effect of taking any of those components out of service is to reduce the 72 hour design basis to ~36 hours - and that only happens if offsite power is lost and both diesels fail to start. All equipment is self diagnosed/alarmed and can be maintained on line (the DCIS power supplies can be changed in less than a shift) and there is no planned requirement to ever make a division completely "black".

per actuator

Typical of SRV solenoids, DPV valves, GDCS valves, equalizing valves; any one (of three) squibs (divisions) or DPS will open the valve.
Lines with two isolation valves in series use two solenoids per valve; lines with one isolation valve in series with a check valve use four solenoids.
Per division, any one of two AC inputs (inverters/batteries), allows the squib to fire.
Overall scheme allows any division to be taken out of service, incur a DBA and accept a single additional failure and still open all valves.



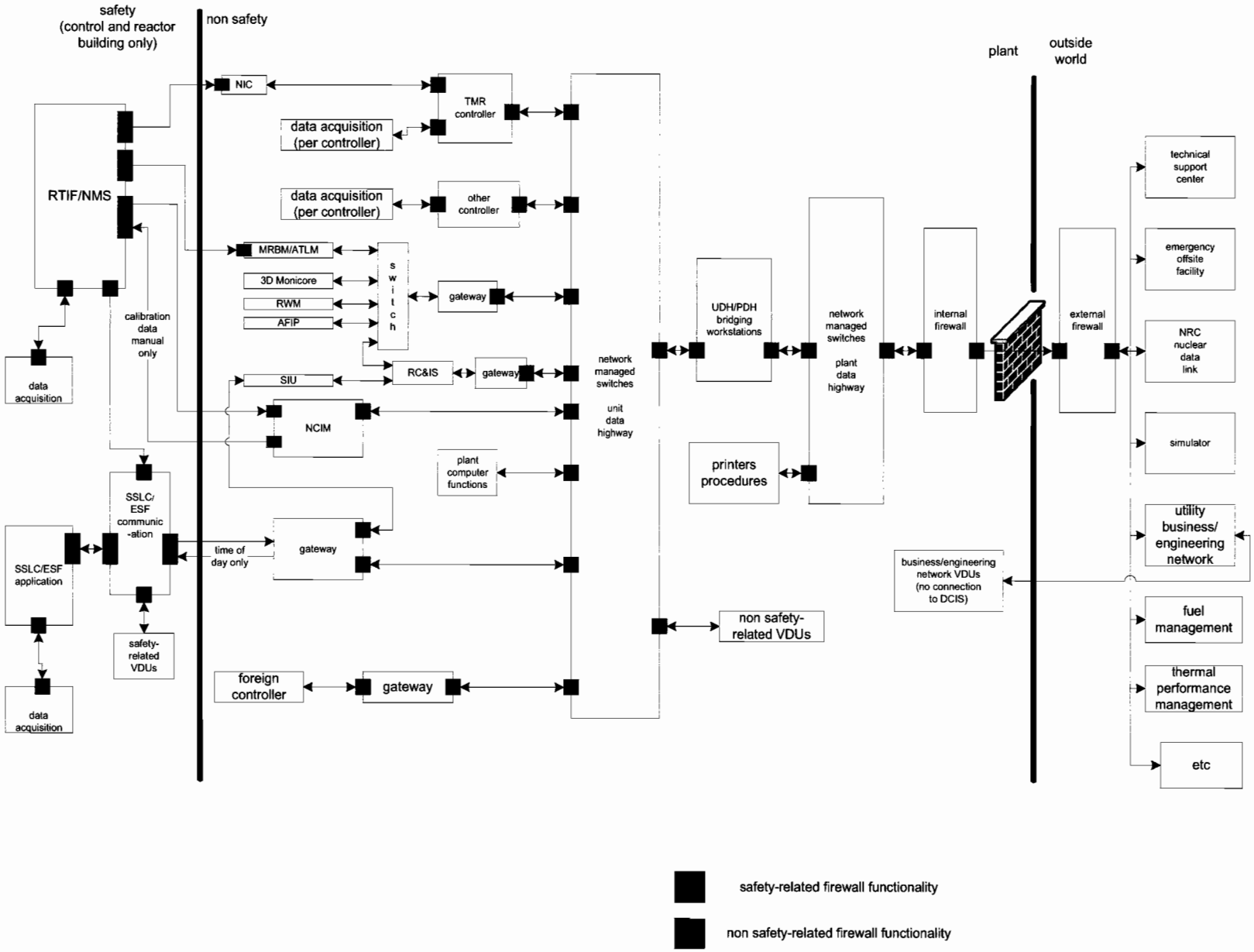
Q-DCIS Configuration

- RG 1.75, IEEE 603 independence, cyber security "baked into" the design
  - > Not an add on
  - > No changes in DCIS configuration anticipated with future cyber security regulation

Q-DCIS Configuration - Continued

- No copper wire between divisions or between divisions and non divisions
- Q-DCIS divisions in physically separate areas/fire zones
- Data Isolation/Cyber Security addressed per communications path
  - > Communication between divisions limited to 2 out of 4 logic
  - > No non safety-related VDU or component can communicate with or control Q-DCIS
  - > No safety-related VDU can communicate with or control another division of Q-DCIS

ESBWR Communication Paths



HITACHI

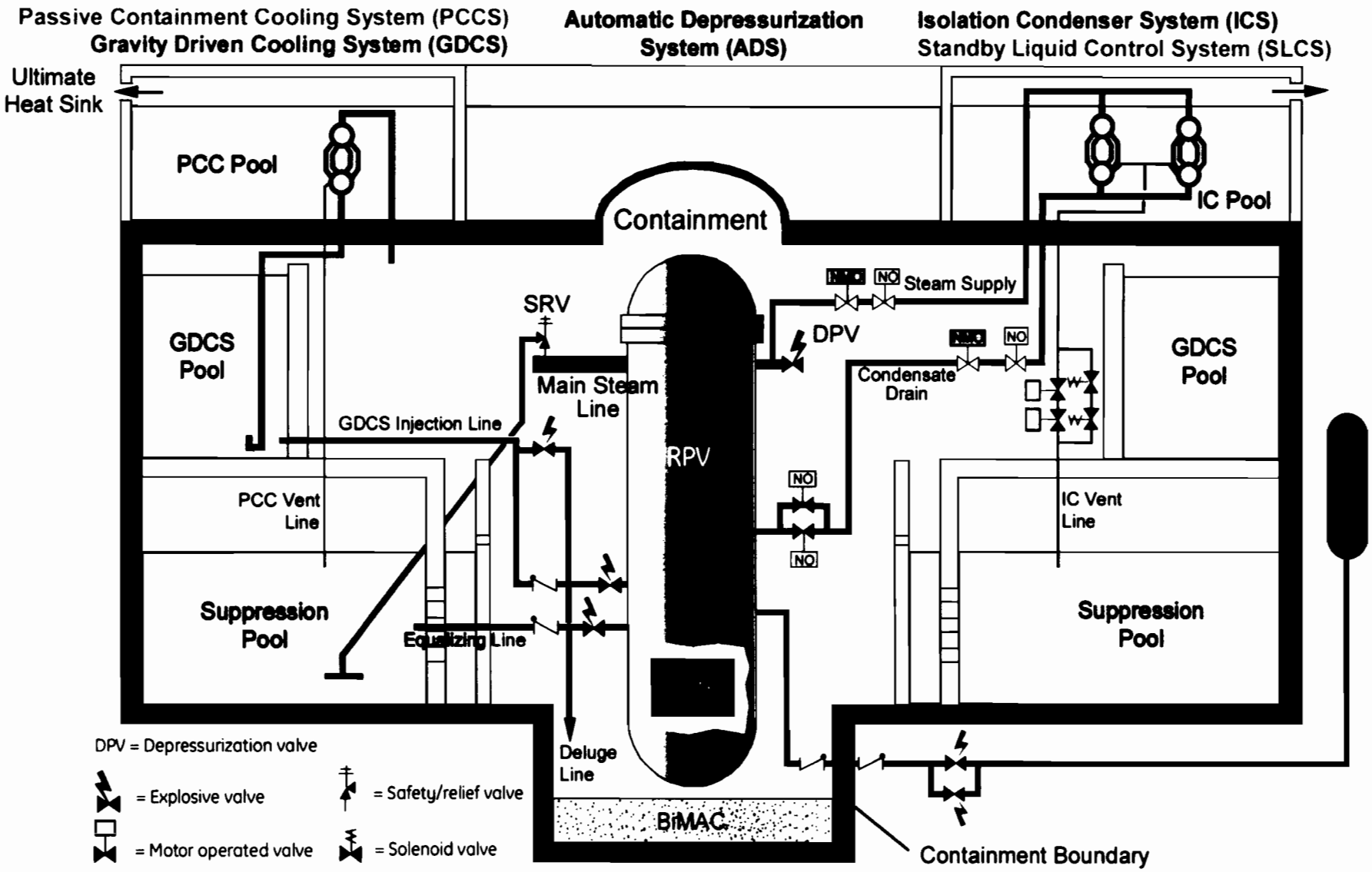
Q-DCIS Configuration - Continued

- Controllers (GEH-NUMAC/Invensys-TRICON) in centralized and divisionalized DCIS rooms
- Data acquisition (in or out) both local (in controller cabinet) and field (Reactor Building)
- Connected via redundant fiber
- Some functions on independent logic platforms (no operating system, no multiplexing, "black box" testing)
  - > ATWS/SLC (Anticipated Transient Without Scram/Standby Liquid Control)
  - > VBIF (Vacuum Breaker Isolation Function)

ESBWR RTIF/NMS

- RTIF/NMS is fail safe and N-2
- ESBWR can be manually scrammed (and isolated) without software
- DPS can scram the reactor
- Backup scram (safety-related) or ARI (non safety-related) can scram the reactor
- FMCRDs support "motor" scram if hydraulic scram fails
- ATWS/SLC can shutdown reactor without control rods using Boron

Passive Safety - ECCS



ESBWR ECCS

- Major safety-related ECCS systems operated by SSLC/ESF include:
  - > GDCS
  - > IC
  - > ADS (nuclear boiler)
  - > Non MSIV Leak Detection and Isolation (process isolation)
- Other safety related SSLC/ESF functions include:
  - > VDU/operator control and monitoring interface
  - > Main Control Room Habitability
  - > Post Accident monitoring/1.97
  - > Non detector part of Process Radiation Monitoring
  - > Containment Monitoring System
  - > Process alarming/self diagnostics/communication isolation

ESBWR ECCS - Continued

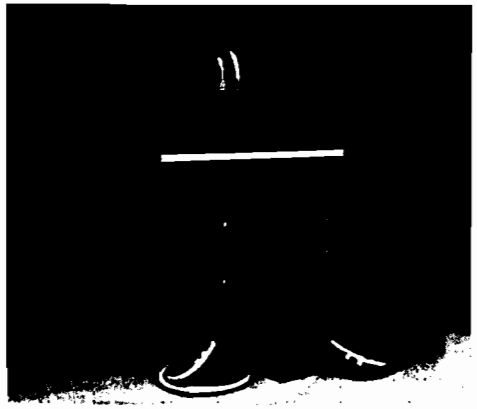
- ESBWR requires safety-related DCIS for ECCS functions (SSLC/ESF) to be highly reliable to initiate ESF when required
  - Manually and automatically
- ESBWR incorporates depressurization via one-shot explosive squib valves
  - > it is equally important to have high confidence that inadvertent actuation will be avoided
- ESBWR SSLC/ESF must provide a highly reliable operator interface for monitoring functions (including NMS and RPS/LDIS) as well as for ECCS functions.
- ESBWR SSLC/ESF must provide highly reliable interdivisional communication for the 2 out of 4 initiation logic.
- ESBWR SSLC/ESF must provide highly reliable and isolated safety-related/non safety-related communications while accepting non safety-related time of day signals for display and data time tagging
- Support N-2
- SSLC/ESF not fail safe

ESBWR ECCS - Continued

- ECCS functions are automatic
- ECCS functions can be manually initiated at the system level
- ECCS functions can be manually initiated at the component (actuator) level

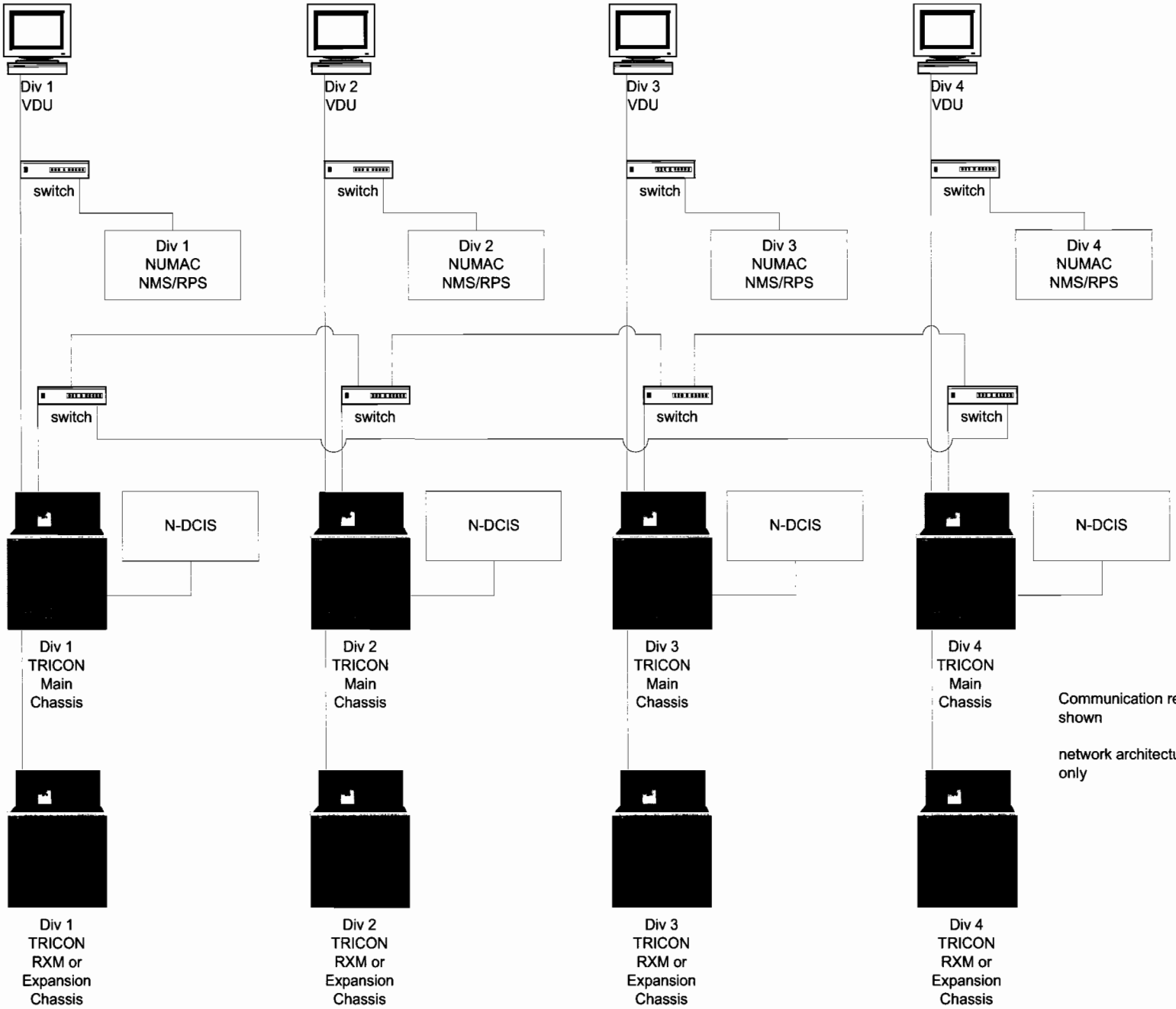
ESBWR SSLC/ESF

- ESBWR SSLC/ESF vendor is the Invensys TRICON platform (HW/SW)
  - > Triple Modular Redundant
  - > No single point of failure
  - > Full internal diagnostics, self testing and self calibration



- Designed to maintain operation with multiple failures, properly report failures, and allow on-line repairs

ESBWR SSLC/ESF Architecture



Communication redundancy not shown

network architecture functional only

HITACHI

TRICON Squib/Solenoid Actuation

- Inadvertent actuation of any squib valve (DPV, GDCS) requires the simultaneous failure of three processors or three independent voted 2 out of 3 discrete outputs
- Inadvertent actuation of any solenoid valve (SRV) requires the simultaneous failure of three processors or two independent voted 2 out of 3 discrete outputs
- Per division discrete outputs are within two widely separated cabinets
  - Addresses hot short concerns
  - Addresses fire concerns
- Squib/solenoid power is grounded (not floating) and will use shielded power cable

ESBWR Q-DCIS/N-DCIS Displays

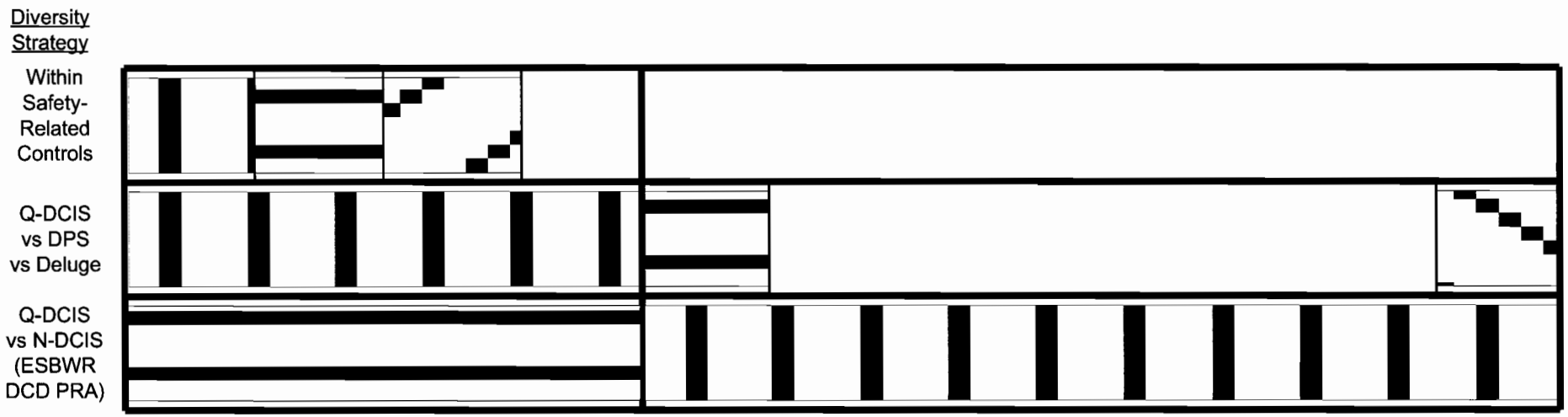
- All Q-DCIS data available at deterministic rates for display
- All ESBWR displays connect to DCIS equipment rooms only via fiber
  - > Fire/smoke does not cause inadvertent actuation
- Main Control Room (MCR) and Remote Shutdown System (RSS) panel areas are in separate fire zones from DCIS equipment rooms
  - > MCR/RSS fire/smoke does not affect DCIS automatic or manual operation
- MCR displays and remote shutdown area displays are independent
  - > ESBWR RSS has same capability as MCR in operating safety-related and non safety-related DCIS

ESBWR Diversity

- Reactor Trip and ECCS hardware/software platforms are diverse
- ATWS/SLC and VBIF hardware platforms are diverse from other Q-DCIS
- DPS hardware/software platform is diverse from all Q-DCIS
- Safety-related and non safety-related VDUs are diverse
- Major control systems diverse from Q-DCIS
- Control systems diverse from ATLM/RWM/MRBM
- Reactor trip, ECCS, ATWS/SLC, DPS do not share sensors or actuators
- Severe accident I&C diverse from everything

ESBWR DCIS Overall Diversity

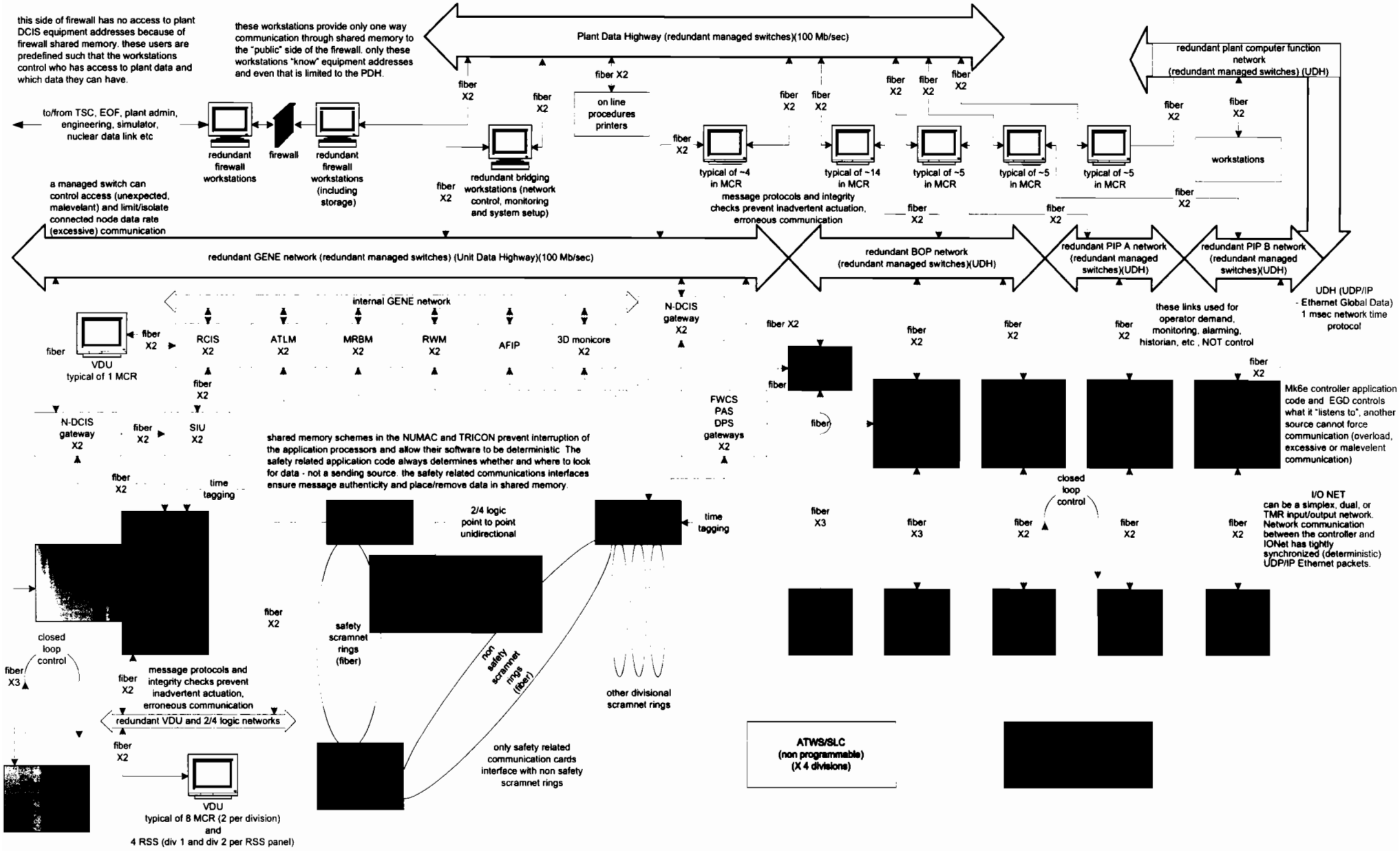
Safety Category	Safety-Related				Nonsafety-Related						
	Q-DCIS				N-DCIS						
Platform/ Network Segment	RTIF NMS	SSLC/ ESF	Independent Control platform	other	GENE		PIP A/B	BOP		PCF	
architecture	divisional	divisional	divisional	note 1	Triple Redundant (DPS)	Dual Redundant	Dual Redundant	Triple Redundant	Dual Redundant	Workstations	PLC (Deluge)



Note 1 – RSS provides operator workstations at appropriate diverse locations outside the main control room in accordance with GDC 19. See DCD section 7.1.3.2.3.2

Note 2 – Crosshatching denotes different platforms or networks

ESBWR DCIS Network Security and Diversity



N-DCIS Controllers

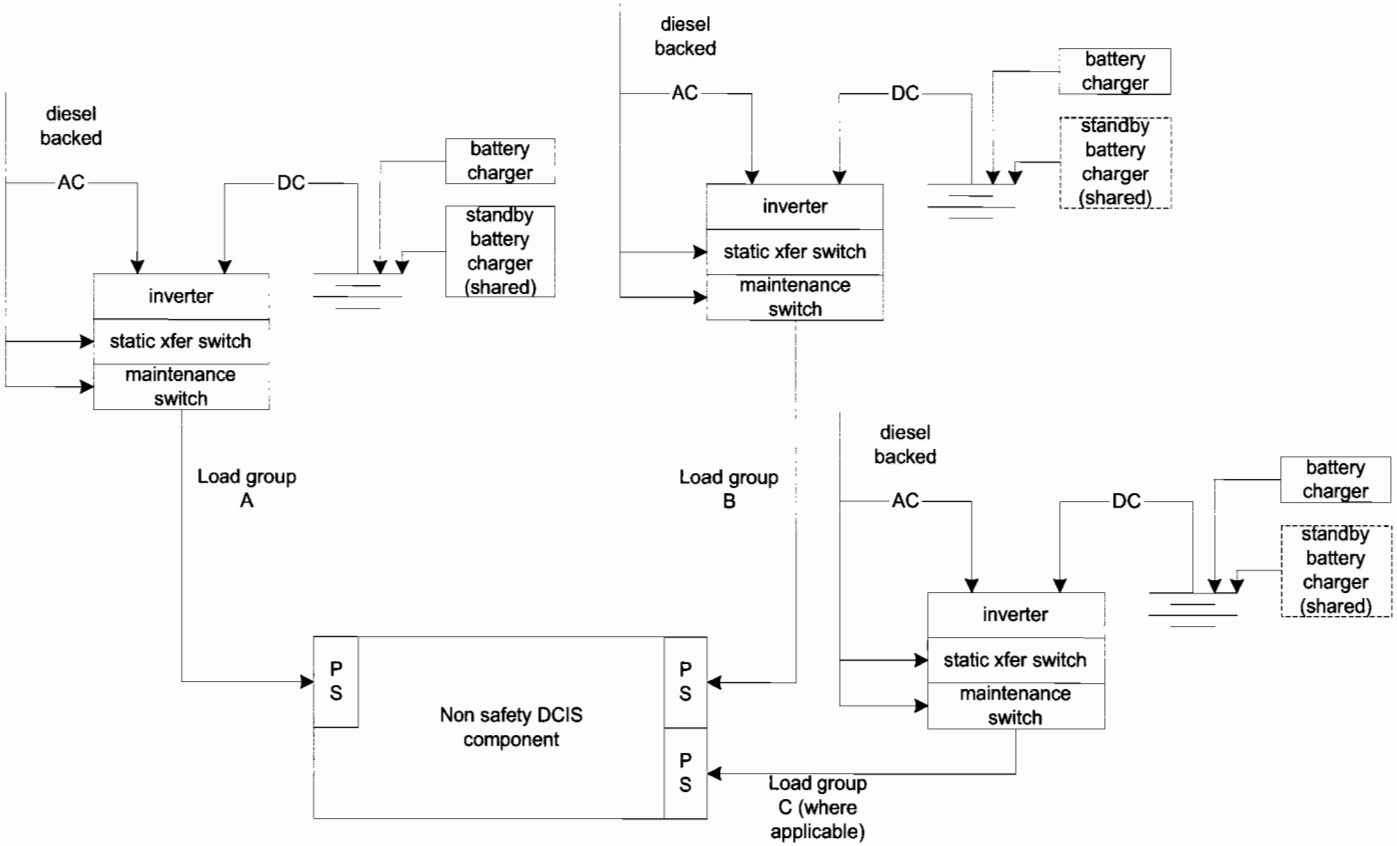
- Network not used for important trips or inter-controller communication
  - > Main turbine, reactor water level, feedwater temperature control, and reactor pressure control
  - > Hardwired/hard fibered and deterministic
- N-DCIS controllers located in A or B N-DCIS rooms
  - > Data acquisition both remote and local multiplexers
  - > Connected by dedicated, redundant fiber
- All N-DCIS automatic control is deterministic by application
  - > Data acquisition is dedicated to controller function
- Plant is designed on safety-related side to not require operator intervention for 72 hours
- Non safety-related DPS provides automatic scram, isolation and ECCS functions
- N-DCIS provides automatic injection (CRD) and suppression pool cooling functions

N-DCIS Controllers (Continued)

- Important N-DCIS control systems are triply redundant
  - > SB&PC, PAS, FWC(level), FWC(temp), Turbine-Generator, DPS
  - > With exception of DPS, triply redundant controllers are for power generation
    - – They are not required for any safety-related function
- Important N-DCIS control systems are segmented into physically separate controllers and cabinets
- All other N-DCIS controllers important to power generation are at least dual redundant

ESBWR N-DCIS Power

- Non safety-related DCIS is supported by three uninterruptible power systems
- Non safety-related DCIS cabinets have two (or three for TMR) power feeds and can operate on either without loss of function



ESBWR Diverse Protection System

- Provides manual and automatic
  - > Backup scram functions
    - (Rx level, Rx pressure, pool temperature, drywell pressure)
  - > Backup MSIV isolation functions
    - (Rx steam flow, Rx level)
  - > backup ADS and GDCS initiation
  - > Backup IC initiation
  - > Backup process isolation functions
  - > SLCS initiation
- Mitigates loss of feedwater heating (SRI, SCRRI)
- Initiates ARI, SRI/SCRRI, all control rod run-in
- Initiates FW runback
- Initiates level 9 FW pump trip

ESBWR DPS (Continued)

- Different hardware/software platform than Q-DCIS
- Can obtain any safety-related data from isolated dedicated data links
- Can obtain any non safety-related data using its own RMUs or the plant non safety-related network
- Triply redundant - reliable against inadvertent actuation
- Non fail safe logic
- On GENE network and can be controlled by GENE control room displays – diverse from Q-DCIS displays

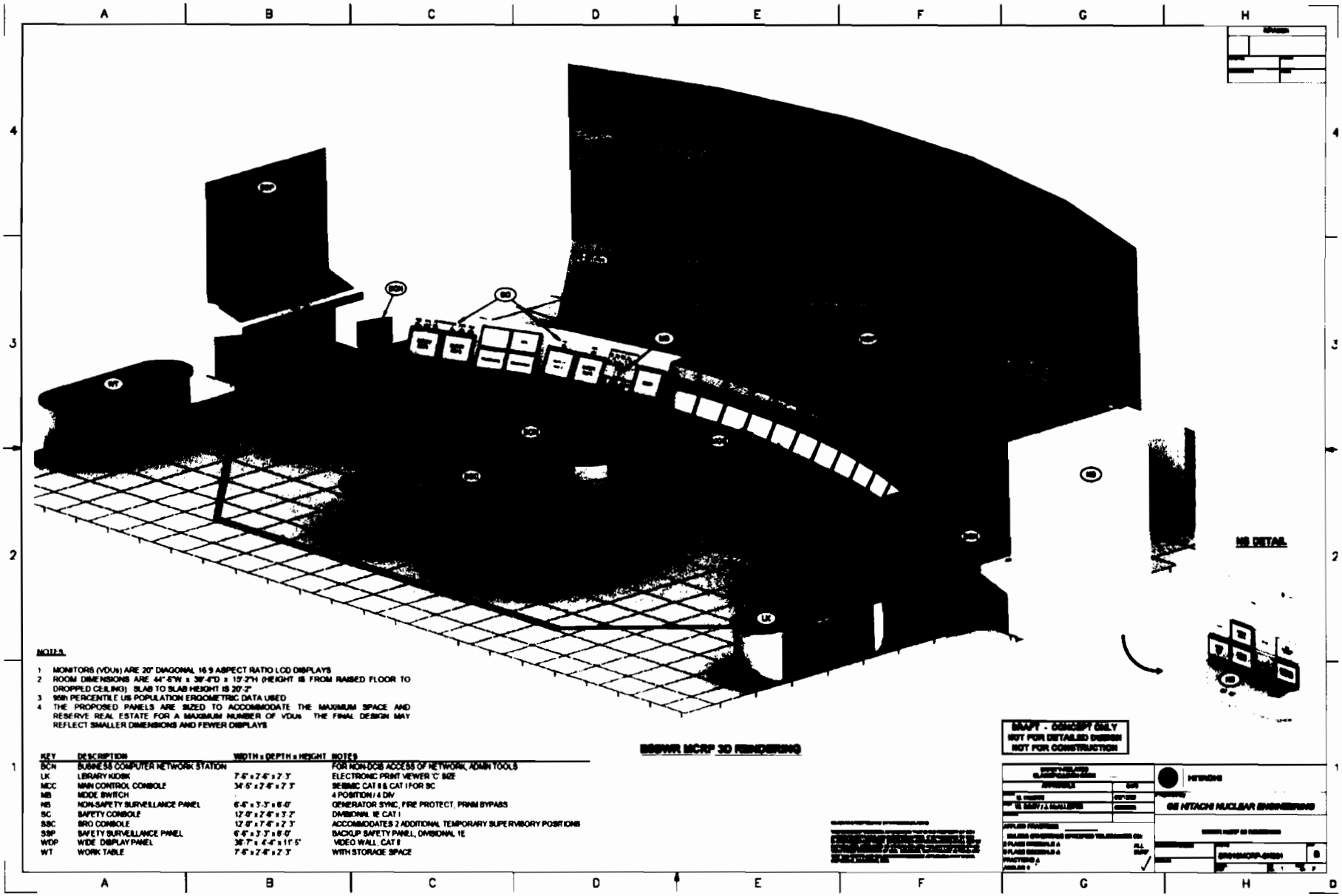
ESBWR RTNSS/Plant Investment Protection (PIP)

- RTNSS and PIP equipment is generally divided into two trains
  - > Each train is powered by a standby diesel generator
  - > Trains are physically separated
- Systems include:
  - > Fuel and Auxiliary Pool Cooling (FAPCS)
  - > RWCU/Shutdown Cooling
  - > HPCRD (High Pressure CRD Injection)
  - > Support systems

ESBWR RTNSS/PIP (Continued)

- ESBWR N-DCIS supports PIP/RTNSS
  - > PIP A and B N-DCIS is segmented – each segment can operate independently
  - > Each segment is configured with seven dual redundant GE MK6e controllers (DCIS is single failure proof)
  - > Major systems are on different controllers
  - > Controllers are redundantly powered

ESBWR Main Control Room



KEY	DESCRIPTION	WIDTH x DEPTH x HEIGHT	NOTES
BCN	BUSINESS COMPUTER NETWORK STATION		FOR NON-DCIS ACCESS OF NETWORK, ADMIN TOOLS
LK	LIBRARY KIOSK	7'-6" x 7'-6" x 7'-3"	ELECTRONIC PRINT VIEWER 'C' SIZE
MCC	MAIN CONTROL CONSOLE	34'-5" x 7'-6" x 7'-3"	SEISMIC CAT II & CAT I FOR SC
MS	MODE SWITCH	-	4 POSITION / 4 DIV
NS	NON-SAFETY SURVEILLANCE PANEL	6'-6" x 3'-3" x 6'-0"	GENERATOR SYNC, FIRE PROTECT, PRNM BYPASS
SC	SAFETY CONSOLE	12'-0" x 7'-6" x 7'-3"	DIVISIONAL 1E CAT I
SSC	SRO CONSOLE	12'-0" x 7'-6" x 7'-3"	ACCOMMODATES 2 ADDITIONAL TEMPORARY SUPERVISORY POSITIONS
SSP	SAFETY SURVEILLANCE PANEL	6'-6" x 3'-3" x 6'-0"	BACKUP SAFETY PANEL, DIVISIONAL 1E
WDP	WIDE DISPLAY PANEL	36'-7" x 4'-4" x 11'-5"	VIDEO WALL, CAT II
WT	WORK TABLE	7'-6" x 7'-6" x 7'-3"	WITH STORAGE SPACE

ESBWR Remote Shutdown System (RSS)

- ESBWR RSS not really a "system" – instead two auxiliary control rooms with RSS panels located in Div 1 and Div 2 quadrants of the Reactor Building
- GDC 19 RSS requirements are met by the manual scram and isolation switches on the panels
- With offsite power available, either RSS panel can operate BOP normally for plant shutdown
- With only diesel power available, either RSS panel can operate PIP A or PIP B systems for plant shutdown
- With only safety-related batteries available, either RSS panel can operate division 1 or division 2 systems for plant shutdown

ESBWR Firewall

- Plant firewall is the only port from the DCIS to the outside world
- Firewall is used by TSC (physically inside plant boundary), EOF, NDL, Simulator, plant engineering servers outside controlled area, any other approved user
- Conceptual design of plant firewall uses shared memory between two pairs of workstations

Firewall (Continued)

- "Internal" workstations obtain plant data from all sources on the Plant Data Highway (PDH)
  - > generally put onto PDH by the bridging workstations
  - > only these workstations "know" internal plant node addresses on the PDH
  - > data put into shared memory
- "External" workstations respond to predefined legitimate users by supplying predefined per user data from shared memory
  - > "external" workstations have no control over or knowledge of how data gets into shared memory
  - > these workstations do not know any internal plant node addresses on the PDH and cannot otherwise communicate with internal workstations, control systems or safety-related systems

ESBWR Severe Accidents

- GDCS deluge lines use squib valves that use different pyrotechnic technology and independent logic for operation from that used for design basis events
  - > Logic is redundant, diverse from all other hardware/software platforms and independently powered separately from all other DCIS
  - > Logic requires safety-related lower drywell temperature switch permissive
  - > Valve opening is signaled by high temperature in Lower Drywell, measured by a number of imbedded thermocouples
  - > GDCS pool water flows directly to designed core catcher in Lower Drywell (BiMAC)
  - > Passive Containment Cooling System (PCCS) operation to remove decay heat would continue as in the design basis case

GE Hitachi
Nuclear Energy

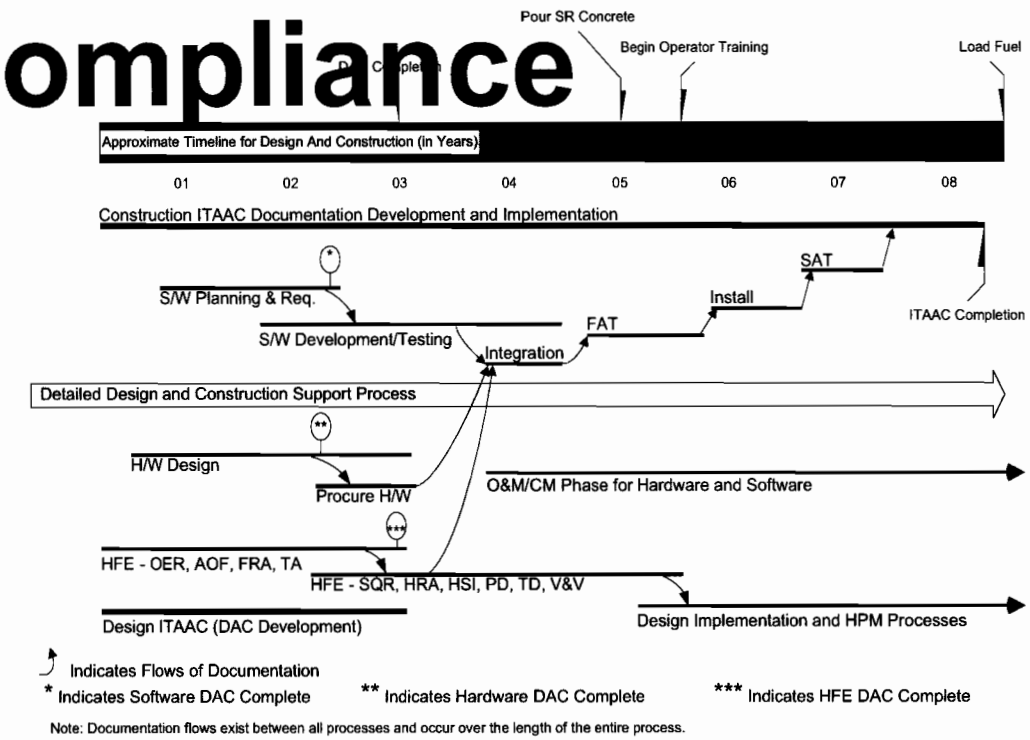
ACRS ESBWR Chapter 7 SER w/OI
DCD Design Detail and DAC Regulatory Compliance Digital I&C

December 3, 2008

Stephen Kimura

Ira Poppel

Rich Miller



HITACHI

Design Detail in DCD vs DAC

The DCD

- **Provides commitments to design systems in accordance with recognized codes, regulatory guidance, and industry standards**
- **Defines the important design bases to be used as acceptance criteria for the detailed design**
  - Defines all safety-related functional requirements
  - Defines important nonsafety-related functional requirements
  - Defines normal and DBE environmental conditions
  - Defines intersystem interfaces and communication pathways
  - Incorporates applicable requirements from previous plant designs
- **Defines the design processes for detailed design**
  - By reference to topical reports

HITACHI

Design Detail in DCD vs DAC

DAC

- **Provides access to the design process in key areas**
  - Used where existence of final product is not indicative of overall quality
  - Utilizes DCD design processes to develop sufficiently detailed designs to address NRC staff inquiries
  - Demonstration divided into multiple step process: design requirements, design reconciliation, and as-built tests
- **Addresses concerns about software development**
  - Whitebox (source code)
  - Blackbox (function)
  - Integrating hardware and software systems
- **Addresses concerns about equipment obsolesce**

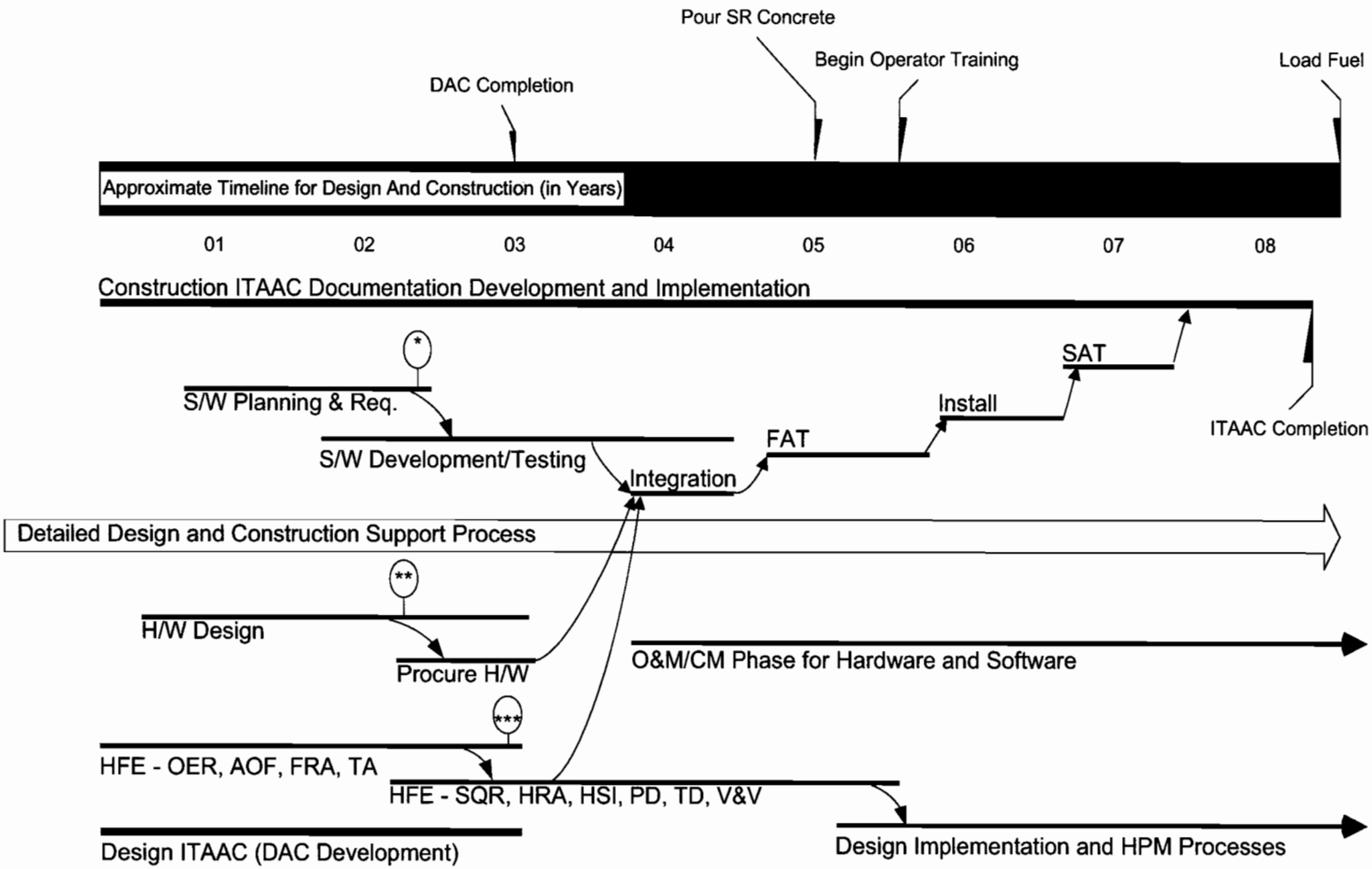
HITACHI

Digital I&C Software Development Process

- Uses lifecycle development process
  - Defined by the SMPM and SQAPM LTRs
  - Design process controlled by baseline reviews for each lifecycle phase
  - Phase requirements need to be met before development can continue
  - Baseline reviews provide natural audit points for the design process
- Is an extension of existing product development processes
  - History of success (both nuclear and commercial)
  - Adjusts to product complexity (safety-related and nonsafety-related)
  - Adjusts to different platforms
- Applied to each platform by software project
  - Where platform types differentiate hardware architectures
  - Where platforms can be independently configured depending on need

HITACHI

Proposed S-R I&C Development Timeline



Indicates Flows of Documentation

* Indicates Software DAC Complete ** Indicates Hardware DAC Complete *** Indicates HFE DAC Complete

Note: Documentation flows exist between all processes and occur over the length of the entire process.

HITACHI

GE Hitachi
Nuclear Energy

ACRS ESBWR Chapter 7 SER w/OI GEH Setpoint Methodology

December 3, 2008

Stephen Kimura

Ira Poppel

Rich Miller

HITACHI

GEH Setpoint Methodology

- Revised GEH Setpoint Methodology, NEDE-33304P
  - ➢Updates GEH setpoint methodology NEDC-31336A-P used by BWR fleet
    - Complies with Regulatory Information Summary (RIS) 2006-017 and 2005-020
    - Clarifies the difference between a LTSP that satisfies RG 1.105 and more conservative NTSP compatible with operational needs
  - ➢Complies with RG 1.105 95/95 acceptance criteria
  - ➢Complies with guidance from BTP HICB-12
  - ➢Complies with industry standards, ISA S67.04.01-2006 and S67.04.02-2000

HITACHI

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Presentation to the ACRS Subcommittee

ESBWR Design Certification Review

Chapter 7,"Instrumentation and Controls"

December 3, 2008

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Chapter 7

Purpose

- Brief the Subcommittee on the staff's continuing review of the ESBWR DCD Application Sections
  - 7.1 "Introduction"
    - Software Development Activities
    - Diversity and Defense-in-Depth Assessment
    - Setpoint Methodology
    - Data Communication Systems
  - 7.2 "Reactor Trip Systems"
  - 7.3 "Engineered Safety Features Systems"
  - 7.4 "Safe Shutdown Systems"
  - 7.5 "Information Systems Important to Safety"
  - 7.6 "Interlock Systems"
  - 7.7 "Control Systems"
  - 7.8 "Diverse Instrumentation and Control Systems"
- Answer the Committee's questions

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Chapter 7 Review Team

- Project Manager
  - Dennis Galvin

- Technical Reviewers
  - Hulbert Li, Lead
  - Leroy Hardin
  - Sang Rhow
  - Royce Beacom
  - Dinesh Taneja
  - Joseph Ashcraft
  - Kimberley Corp
  - Eugene Eagle
  - Thomas Fredette
  - Jack Zhao

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Chapter 7 Presentation

Outline of Presentation

- Applicable Regulations
- RAI Status Summary
- SER Technical Topics of Interest
  - Key I&C DAC/ITAAC Items
  - Key SER Open Items
- Discussion / Committee Questions

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Chapter 7

Key Regulations

- 10 CFR 50.55a(a)(1), 10 CFR 50.55a(h)(3), 10 CFR 50.34(f)(2), 10 CFR 50.62, and 10 CFR 52.47(b)(1)
- 10 CFR Part 50, Appendix A, GDC 1, 2, 4, 10, 13, 15, 16, 19, 20, 21, 22, 23, 24, 25, 28, 29, 33, 34, and 35

Principal Review Guidance

- SRP Section 7, including Branch Technical Positions
- SRP Sections 14.3 and 14.3.5
- Regulatory Guides 1.22, 1.47, 1.53, 1.62, 1.75, 1.97, 1.105, 1.118, 1.151, 1.152, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, 1.189, 1.204, and 1.209
- SRM on SECY-93-087 and SECY-92-053

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Chapter 7

RAI Status Summary: SRP Chapter 7

- Original number of RAIs = 276
- Number of RAIs resolved = 206
- Number of Remaining Open Items = 70

ACRS Subcommittee Presentation
ESBWR Design Certification Review
SER Section 7.1.1

Distributed Control and Information System – General Description

- Q-DCIS safety related platforms
- N-DCIS nonsafety related platforms

Method of Review

- SRP Chapters 7 and 14

Key I&C DAC/ITAAC Items

- IEEE-603 Criteria Compliance (Tier 1 – 2.2.15)
- Software Development Activities (Tier 1 – 3.2)
- Human Factors Engineering (Tier 1 – 3.3)
- Post Accident Monitoring Instrumentation (Tier 1 – 3.7)
- ITAAC for Environmental Qualification (Tier 1 – 3.8)

Key SER Open Items

- RAI 14.3-265 requests GEH to address all IEEE-603 criteria in DCD Tier 1.
- RAI 14.3-415 thru 420 request GEH to document platform specific software plans and associated DAC/ITAAC closure activities.

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Life Cycle Process from SRP BTP 7-14

Life Cycle Activity Groups	Planning Activities	Requirements Activities	Design Activities	Implementation Activities	Integration Activities	Validation Activities	Installation Activities	Operation & Maintenance Activities
	Software Management Plan Software Development Plan Software QA Plan Integration Plan Installation Plan Maintenance Plan Training Plan Operations Plan	Requirements Specification	Design Specification Hardware & Software Architecture	Code Listings	System Build Documents		Operations Manuals Installation Configuration Tables Maintenance Manuals Training Manuals	
	Software Safety Plan Software V&V Plan Software CM Plan	Requirements Safety Analysis V&V Requirements Analysis Report CM Requirements Report	Design Safety Analysis V&V Design Analysis Report CM Design Report	Code Safety Analysis V&V Implementation Analysis & Test Report CM Implementation Report	Integration Safety Analysis V&V Integration Analysis & Test Report CM Integration Report	Validation Safety Analysis V&V Validation Analysis & Test Report CM Validation Report	Installation Safety Analysis V&V Installation Analysis & Test Report CM Installation Report	Change Safety Analysis V&V Change Report CM Change Report

Design outputs

Process implementation

Process planning

Note: A separate document is not required for each topic identified; however, project documentation should encompass all of the topics.

ACRS Subcommittee Presentation
ESBWR Design Certification Review
SER Section 7.1.2

Digital I&C System Life Cycle Design Process Review

- Review TR NEDO-33226 – Software Management Program Manual
- Review TR NEDO-33245 – Software Quality Assurance Program Manual

Method of Review

- SRP Ch 7 BTP 7-14

Key I&C DAC/ITAAC Items

- Software development activities (Tier 1-3.2)

Key SER Open Items

- RAI 14.3-415 thru 420 request GEH to provide
  - DAC/ITAAC coverage for the templates
  - Clearly relate the template to the project-specific implementation process
  - Clearly identify which activity is related to DAC and which activity is related to ITAAC

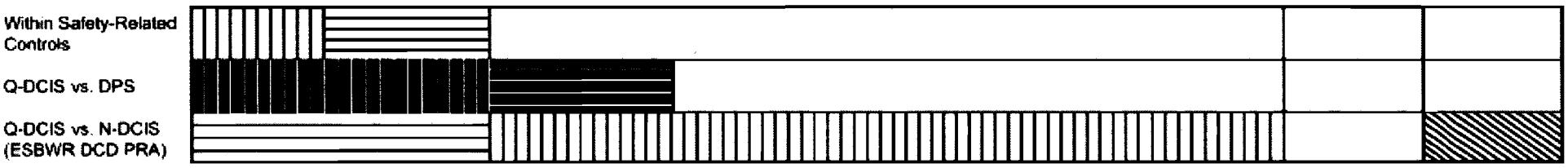
ACRS Subcommittee Presentation
ESBWR Design Certification Review

From DCD Figure 7.1-4. ESBWR Hardware/Software (Architecture) Diversity Diagram

Safety Category	Safety-Related		Nonsafety-Related						
	Q-DCIS		N-DCIS						
System Families	RTIF NMS	SSLC/ESF	GENE		BOP SYSTEMS		PIP SYSTEMS	PCF	SEVERE ACCIDENT
Architecture	Divisional	Divisional	Triple Redundant	Dual Redundant	Triple Redundant	Dual Redundant	Dual Redundant	Workstations **	PLCs
Systems/ Subsystems	RPS LD&IS (MSIV) NMS ATWS/SLC* VBIF** CMS* (SPTM)	ICS ADS (SRV/DPV) GDCS SLC LD&IS (Non-MSIV) CRHS CMS*	DPS (RPS ECCS Backup)	3D Monicore RC&IS ATLM RWM MRBM SPDS Logic	FWCS, PAS (Automation) SB&PC, TGCS	Turbine Generator Auxiliaries Electrical System CIRC TCCWS Chillers	PIP A, PIP B CRDS RWCU/SDC FAPCS RCCWS Electrical System SDGs Chillers	HMI Histonan AMS PMC Functions PCD	Deluge System (GDCS Subsystem)

* Diverse (Discrete Programmable Logic)
* Diverse Sensor Inputs
** Dual redundant as necessary
** VBIF Vacuum Breaker Isolation Function (Discrete Programmable Logic)

Diversity Strategy



Note: Crosshatching denotes different system families and architectures. Within RTIF, ATWS/SLC logic and VBIF use hardware diverse from the RTIF, NMS, and SSLC/ESF system families as indicated above.
Shading is for readability only.

ACRS Subcommittee Presentation
ESBWR Design Certification Review
SER Section 7.2

Reactor Trip System (RTS)

- Reactor Trip and Isolation Function(s) (RTIF) platform
  - Reactor Protection System (RPS) function
  - Suppression Pool Temperature Monitoring function
- Neutron Monitoring System (NMS) platform
  - NMS function

Method of Review

- SRP Section 7.2

Key I&C DAC/ITAAC Items

- RPS Design (Tier 1 – Section 2.2.7)
- IEEE-603 Criteria Compliance (Tier 1 – Section 2.2.15)

Key SER Open Items

- RAI 14.3-265 requests GEH to address all IEEE-603 criteria in DCD Tier 1.
- RAIs 7.1-99, 7.1-100 and 7.1-101 request GEH to ensure consistency within and between DCD Tier 1 and Tier 2 documents.

ACRS Subcommittee Presentation
ESBWR Design Certification Review
SER Section 7.4

Safe Shutdown Systems

- Safety-related systems for automatic shut down in natural circulation mode from full power to a subcritical condition in response to design basis event
  - Isolation Condenser System
  - Gravity-Driven Cooling System
  - Standby Liquid Control
  - Passive Containment Cooling System
- Design allows nonsafety-related system performing cold shutdown when not in LOCA event
  - Reactor Water Cleanup/Shutdown Cooling

Method of Review

- SRP Section 7.4 and GDC 19

Key I&C DAC/ITAAC Items

- IEEE-603 Criteria Compliance (Tier 1 – Section 2.2.15)

Key SER Open Items

- RAI 14.3-265 requests GEH to address all IEEE-603 criteria in DCD Tier 1.
- RAIs 7.1-99, 7.1-100 and 7.1-101 request GEH to verify consistency within and between DCD Tier 1 and Tier 2 documents.

ACRS Subcommittee Presentation
ESBWR Design Certification Review
SER Section 7.5

Information Systems Important to Safety
- Post Accident Monitoring (PAM)
- Containment Monitoring System
- Plant Alarm System
- Process Radiation Monitoring System
- Area Radiation Monitoring System
- Pool Monitoring Subsystems

Review Method
- SRP Section 7.5

Key I&C DAC/ITAAC Items
- IEEE-603 Criteria Compliance (Tier 1 – Section 2.2.15)
- PAM design (Tier 1 – Section 3.7)

Key SER Open Items
- RAI 14.3-265 requests GEH to address all IEEE-603 criteria in DCD Tier 1.
- RAIs 7.1-99, 7.1-100 and 7.1-101 requests GEH to verify consistency within and between DCD Tier 1 and Tier 2 documents.

ACRS Subcommittee Presentation
ESBWR Design Certification Review
SER Section 7.6

Interlock Systems

- A nonsafety-related HP/LP interlock identified in DCD Tier 2, Section 7.6

Method of Review

- SRP Section 7.6

Key I&C DAC/ITAAC Items

- None for this section.

Key SER Open Items

- RAI 7.6-3 request GEH to document the HP/LP interlock function in the Regulatory Treatment of Non-Safety Systems program.

ACRS Subcommittee Presentation
ESBWR Design Certification Review
SER Section 7.7

Control Systems

- I&C Non-Safety Related Systems for Control and Indication
  - Nuclear Boiler System (NBS)
  - Rod Control and Information System
  - Feedwater Control System
  - Plant Automation System
  - Steam Bypass and Pressure Control System
  - Neutron Monitoring System
  - Containment Inerting System

Method of Review

- SRP Section 7.7

Key I&C DAC/ITAAC Items

- Most control systems have ITAAC to verify design

Key SER Open Items

- RAI 7.7-10 requests GEH to transfer description of safety-related NBS I&C from Section 7.7 to 7.2.
- RAI 7.7-14 requests GEH to adjust Table 7.1-1 to create Separate Columns for Safety and Non-safety portions of NBS and NMS

ACRS Subcommittee Presentation
ESBWR Design Certification Review
SER Section 7.8

Diverse Instrumentation and Control Systems (DICS)

- DPS
- ATWS mitigation systems

Method of Review

- SRP Section 7.8 and BTP 7-19

Key I&C DAC/ITAAC Items

- Verify DICS design (Tier 1 – 2.2.14)

Key SER Open Items

- RAI 7.8-8 requests GEH to document equipment quality assurance program to follow ATWS equipment QA guidance GL 85-06 in DCD Tier 2 with regard to DICS equipment.
- RAI 7.8-9 requests GEH to update TR NEDO-33251 in light of DCD Rev.5 design information changes.
- RAIs 7.1-99, 7.1-100 and 7.1-101 request GEH to verify consistency within and between DCD Tier 1 and Tier 2 documents.

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Chapter 7 Summary

The staff followed SRP Chapters 7 & 14 Guidance to review high level functional requirements and design commitments for:

- IEEE-603 criteria compliance
- Life-cycle design process
- Setpoint methodology
- Diversity & Defense-in-Depth
- Data Communication

ACRS Full Committee Presentation
ESBWR Design Certification Review
Chapter 7 Summary

RAI open items status

- Most of the remaining open items are clarification/consistency related issues
- No safety significant technical issues that need resolution

ACRS Subcommittee Presentation
ESBWR Design Certification Review
Committee Questions

Discussion/Committee Questions