Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:Advisory Committee on Reactor SafeguardsDigital Instrumentation and Control Systems

Docket Number: (n/a)

Location: Rockville, Maryland

Date:

Monday, April 4, 2016

Work Order No.: NRC-2299

Pages 1-311

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

	1
1	
2	
З	
4	DISCLAIMER
5	
6	
7	UNITED STATES NUCLEAR REGULATORY COMMISSION'S
8	ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
9	
10	
11	The contents of this transcript of the
12	proceeding of the United States Nuclear Regulatory
13	Commission Advisory Committee on Reactor Safeguards,
14	as reported herein, is a record of the discussions
15	recorded at the meeting.
16	
17	This transcript has not been reviewed,
18	corrected, and edited, and it may contain
19	inaccuracies.
20	
21	
22	
23	
	NEAL R. GROSS
	COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.
	(202) 234-4433 WASHINGTON, D.C. 20005-3701 www.nealrgross.com

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

MONDAY

APRIL 4, 2016

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 1:04 p.m., Charles

H. Brown, Jr., Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR. Member

DENNIS C. BLEY, Member

JOY REMPE, Member

JOHN W. STETKAR, Member

ACRS CONSULTANT:

MYRON HECHT

1

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

ANDREA D. VALENTIN, Executive Director, ACRS

ROSSNYEV ALVARADO, NRR/DE/EICB

GORDON CLEFTON, Public Participant*

SAMIR DARBALI, NRR/DE/EICB

JOHN LUBINSKI, NRR/DE

SCOTT PATTERSON, PG&E

MARY JANE ROSS-LEE, NRR/DE

KEN SCHRADER, PG&E

RICHARD STATTEL, NRR/DE/EICB

MICHAEL WATERS, NRR/DE/EICB

KATE WILLIAMS, PG&E

*Present via telephone

AGENDA

Opening Remarks4
Introductory Remarks on Diablo Canyon PPS
System
Overview of the Diablo Canyon Process
Protection System (DCPP) System LAR17
Project Status Update
Summary of the Safety Evaluations
Conclusions56
Lessons Learned on the Digital I&C Licensing
Process
Digital I&C Action Plan Development
Activities178
Conclusions and Path Forward
Closing Remarks
Adjourn

	4
1	PROCEEDINGS
2	1:04 p.m.
3	CHAIRMAN BROWN: The meeting will come
4	to order. This is a meeting of the Digital
5	Instrumentation and Control Subcommittee. I am
6	Charles Brown, chairman at the Subcommittee
7	meeting. ACRS members in attendance are Dennis
8	Bley, John Stetkar, Joy Rempe and our consultant
9	Myron Hecht. Christina Antonescu of the ACRS is
10	the Designated Federal Official for this meeting.
11	The purpose of the meeting is for the
12	staff to provide a presentation on the Diablo
13	Canyon replacement digital process protection
14	system license amendment request, its design and
15	the staff's safety evaluation conclusion.
16	Specifically during the meeting staff will provide
17	a refresher for the Subcommittee members of the
18	design as it looks today.
19	They will address again how
20	independence is maintained, deterministic
21	processing is achieved. Control of access is not
22	susceptible to compromise from external surfaces,
23	how D3 is achieved and include a summary of the
24	safety evaluation conclusions that are relevant to
25	these types of concerns.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

Identify issues that arose during the development and testing of the final design and how they were resolved and addressed in the safety evaluation. Since this was a pilot program for ISG-06, explain how it worked and what lessons were learned that could improve the replacement application approval process.

staff 8 Also, the will provide an 9 overview of the draft integrated DI&C regulatory 10 infrastructure modernization action plan, in 11 response to the Commission's February 26, 2016 SRM 12 regarding the proposed 10 C.F.R. 50.55(a) rule change to incorporate by reference IEEE 603-2009, 13 14 with additional conditions.

15 Subcommittee The will gather 16 information, analyze relevant issues and facts, 17 formulate proposed positions and actions as 18 appropriate for deliberation by the full committee. 19 The rules for participation in today's meeting have 20 been announced as part of this notice -- of the 21 notice of this meeting, previously published in the 22 Federal Register on March 23rd, 2016.

The meeting will be open to the public attendance with the exception of portions that may be closed to protect information that is

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

(202) 234-4433

5

	6
1	proprietary. We have received no written comments
2	or requests for time to make oral statements from
3	members of the public regarding today's meeting.
4	To preclude interruption of the
5	meeting, the phone line will be placed on listen-in
6	mode during the presentations and committee
7	discussions. Also, the bridge line will then be
8	opened at the end of the meeting to see if anyone
9	listening would like to make any comments.
10	A transcript of the meeting is being
11	kept and it will be made available as stated in the
12	Federal Register notice. Therefore, we request
13	that participants in this meeting use the
14	microphones located throughout the meeting room
15	when addressing the Subcommittee. The participants
16	should firs identify themselves and speak with
17	sufficient clarity and volume so that they may be
18	readily heard.
19	Also, now the most cogent announcement
20	of the day. Would you all please silence your cell
21	phones, pagers, iPhones, iPads and all other
22	electronic devices that could beep during the
23	meeting. We will now proceed with the meeting and
24	I call on Ms. Mary Jane Ross-Lee, the Deputy
25	Director in Division of Engineering in the Office

(202) 234-4433

	7
1	of Nuclear Reactor Regulation, to make some
2	introductory remarks.
3	Mary Jane? Press the little button at
4	the bottom. If you're green, you're good.
5	
6	MS. ROSS-LEE: Great, thank you. Now
7	if I can figure out how to make this work. All
8	right, thank you. Today we will be presenting the
9	Diablo Canyon license amendment to upgrade the
10	digital process protection systems. This has been
11	an extensive and complex review effort for the NRC
12	staff.
13	The draft safety evaluation report was
14	provided to the Subcommittee members in advance of
15	this meeting. We hope to address any comments or
16	concerns you may have regarding this evaluation
17	during today's presentation. It's our
18	understanding that a follow-up presentation will be
19	provided to the ACRS full committee for the purpose
20	of developing a letter to the staff describing the
21	ACRS reviews on the amendment.
22	We'll begin with a presentation of the
23	license amendment request by the licensee, Pacific
24	Gas & Electric, and I believe today we have Mr. Ken
25	Schrader, Kate Williams and Scott Patterson

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	8
1	present. Actually, I think this is in reverse
2	order. Mike Waters will go first, who will briefly
3	describe, sorry
4	CHAIRMAN BROWN: We're flexible.
5	MR Thank you. Don't follow my script
6	just hopefully I'll catch up. So Mike Waters will
7	briefly describe the regulatory history of the
8	license amendment, which will then be followed by
9	Pacific Gas & Electric's presentation. Rick
10	Stattel, Rossnyev Alvarado and Samir Dabali, who
11	are all sitting in the rows behind you, are the
12	principal technical reviewers of this evaluation.
13	They will describe the regulations,
14	relevant regulatory guidance and the technical
15	evaluations performed on the topics shown on the
16	slide in front of you. Now I'll turn this
17	presentation over to Mike.
18	MR. WATERS: Good afternoon. It's a
19	privilege to be here. Thank you. In October 2012,
20	Pacific Gas & Electric submitted a license
21	amendment request to replace the existing Eagle 21
22	visual process protection system (PPS) for Diablo
23	Canyon Units 1 and 2. The NRC accepted that Diablo
24	Canyon request for review in January 2012.
25	The new, improved system is comprised

(202) 234-4433

two subsystems, one of which is based on 1 of the 2 Invensys Tricon platform and the other based on the 3 Westinghouse Advanced Logic System (ALS). The 4 Tricon system is а computer-based PLC system. 5 Staff has separately reviewed and approved the topical report for the Tricon B10 platform in May 6 7 2012. The ALS is full programmable array base 8 system which includes features to address the needs 9 of the new protection system. 10 The NRC has also reviewed and approved 11 the topical report for ALS in October 2013. Our 12 review has focused on many key technical areas such as the deterministic performance software, software 13 14 documentation, equivalent qualification testing 15 plans and set point methodologies. We'll hear more 16 about that from Rich and the team. 17 We also conducted four audits of the 18 vendor facilities of Westinghouse and Invensys. Ιt 19 is also important to note the role of interim staff 20 guidance ISG-06 about the licensing process. ISG-21 was issued in early 2011. It was developed in 06 22 our early licensing experiences part from with 23 Oconee and Wolf Creek visual upgrades. 24 This Diablo Canyon licensing review is 25 considered a pilot application for ISG-06 and again

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

9

	10
1	you'll hear from Rich and the team using ISG-06.
2	At this time, PG&E has responded to all audit
3	questions with only one remaining open item
4	regarding size and qualifications.
5	We have developed a draft safety
6	evaluation report which is still pre-decisional.
7	At the end of the day, as time evolves, I will be
8	happy to talk about next steps in our license
9	review. In summary, the entire industry review
10	team has performed a high quality review of this
11	complicated amendment, as documented in the draft
12	evaluation report.
13	There were some pauses in the review
14	and multiple amendment supplements. That happens
15	during the license review period, but we can only
16	consider ISG-06 to be successful in clarifying
17	staff's acceptance criteria and review procedures
18	for digital amendments, and we have identified
19	additional lessons learned for continual further
20	improvement of this guidance. Unless there's any
21	questions, I'll be happy to turn it over to the
22	licensee next.
23	MEMBER STETKAR: Mike, you mentioned
24	and it's on the SER that there's only one, whether
25	you want to call it one open item or two open items

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	11
1	related to the in-cabinet response vector to the
2	seismic analysis. I want to make sure that I was
3	looking at the same version of the SER that you
4	had.
5	In section and this is kind of a
6	heads up that you may want to look at while other
7	people are talking. That's why I wanted to bring
8	it up now. In Section 3.5.4 on the electromagnetic
9	compatibility, there are several referneces made to
10	Open Item 115, 1-1-5, and all the subsections in
11	that are just end with a parenthetical statement
12	saying "See response to OI-115."
13	So I don't know whether I was looking
14	at an earlier version or whether that's indeed what
15	we were supposed to be reviewing.
16	CHAIRMAN BROWN: No, that is the
17	version I had also. I had the same question.
18	MEMBER STETKAR: Okay. You may want to
19	go figure what's going on there, because it seems
20	like an open item, at least as far as what we were
21	given to review.
22	MR. WATERS: Thanks for that. We'll
23	take a look at that. It could be just an editorial
24	item. I'll have
25	CHAIRMAN BROWN: Wait a minute.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	12
1	Editorial is one thing, but the question is
2	MR. WATERS: Yeah, yeah.
3	CHAIRMAN BROWN:what are we given to
4	review?
5	MR. WATERS: I can call Rich up to
6	answer now or if you want to wait for his
7	presentation too.
8	CHAIRMAN BROWN: I don't care. I
9	wanted to give you a heads up in case somebody
10	needed to do some homework. That's the only reason
11	I brought it up now.
12	MR. STATTEL: I can respond.
13	CHAIRMAN BROWN: Just push right at the
14	base toward you. There you go.
15	MR. STATTEL: I've got it, okay. Yeah,
16	I can respond to that. So we sent to you we had
17	completed our safety evaluation about five weeks
18	ago, and we sent what we had documentation-wise at
19	that time, but it was under concurrence review at
20	that time. So there have been changes between that
21	and the issued version that we have sent to the
22	project manager.
23	Regarding the open item, it's actually
24	part of the ISG-06 process and I'll be discussing
25	it during my presentation. But those open item

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	13
1	also have associated RAIs and we kind of used the
2	open items list as a way of facilitating our
3	discussions with the licensee during the process.
4	That terminology will be removed from
5	the evaluation when we issue the license amendment.
6	There are no the open items are now closed.
7	There are no remaining open items, however. I can
8	say that, aside from the seismic issue which we
9	left as an open item.
10	MEMBER STETKAR: What I'm curious about
11	though is the fact that we have a document that has
12	I'll call it an open item because it's called an
13	open item in it. It's Open Item 115. I don't know
14	what it is. It has something to do with oh gee,
15	I can look it up here.
16	MR. STATTEL: EMIR.
17	MEMBER STETKAR: Yeah, right.
18	MR. STATTEL: It's equipment
19	qualification.
20	MEMBER STETKAR: Right. Equipment
21	qualification for interference, and there's a
22	discussion about why that was a concern and all it
23	says is refer to that open item. It doesn't say
24	refer to an RAI. It doesn't say this is closed.
25	It was open at the time. Now if it's been closed

(202) 234-4433

	14
1	since then, okay. There must be some reason why it
2	was closed. Why was it closed?
3	MR. STATTEL: Okay. I guess I have a
4	question for you then. So we last presented this
5	evaluation to you in 2014, and at the time we
6	presented the entire design and the status at that
7	time. At that time, the design had not been
8	completed and they had not built the system.
9	We were asked by the ACRS to come back
10	once we had completed our evaluation, but prior to
11	the issuance of the safety evaluation. So this is
12	that window of time that we're speaking right now.
13	MEMBER STETKAR: Oh.
14	MR. STATTEL: All right. So our
15	evaluation is complete. The documentation is not
16	finalized, right. We will be issuing our plan
17	is and we'll discuss this at the end of the
18	presentation, our plan is to issue the license
19	amendment later this year. Let me also offer, we
20	can look at that specific section on the break and
21	make sure it is clear.
22	MEMBER STETKAR: All I'm concerned
23	yeah, I understand that there's a moving target,
24	and I understand that we're looking at the snapshot
25	in a moving target. If that snapshot that two open

(202) 234-4433

15 items, one related to electromagnetic compatibility 1 2 and another one related to seismic, I'm fine with 3 that. 4 MR. STATTEL: Again when you look at it, I believe the clarification is that the safety 5 6 evaluation is complete except for the open item for 7 seismic-only. If we need to clarify something in 8 the documentation --9 MEMBER STETKAR: Well, you certainly 10 need to clarify how all of the electromagnetic 11 compatibility issues were resolved, because the 12 documentation just simply says see response to OI-That's a verbatim quote from the draft SER. 13 115. 14 Again, you're looking at MR. STATTEL: 15 a draft version of this SER, and that has changed 16 during the last month, during the concurrence 17 reviews, and it will change between now and when we 18 issue the safety -- the license amendment. 19 MEMBER BLEY: When you actually get up 20 will you be to talk, walking us through the 21 difference between what we saw and the current 22 status? Well, 23 STATTEL: it's draft MR. а 24 document. If you wanted to see the final document, 25 have waited until after the license we could

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	16
1	amendment was issued. But we were specifically
2	told
3	MEMBER BLEY: When we have a partial
4	document and then you move ahead, that's very
5	reasonable. But we would expect when you come here
6	that you would tell us, you know, we've closed out
7	one item and here's how we closed it when you give
8	your presentation.
9	MR. STATTEL: Okay.
10	MEMBER BLEY: So I'm hoping you're
11	going to do that.
12	MR. STATTEL: Okay.
13	MEMBER STETKAR: Also, this is more
14	important, because this is only a Subcommittee
15	meeting so and we're used to actually dealing
16	with things that are in a state of flux, because we
17	try to get typically the Subcommittees involved
18	earlier rather than later on some technical issues.
19	Certainly when you come to the full
20	committee, whenever that is, the SER ought to be a
21	self-contained coherent document, not in a state of
22	flux. Don't this is just my personal
23	recommendation. Don't bring it to the full
24	committee and expect a full committee voter that
25	might say something like this, that we're viewing

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

17 something that's incomplete and therefore can't 1 2 reach a conclusion on something. 3 Well, MR. STATTEL: it's not а finalized document until we issue the 4 license 5 amendment, and that will be after the full 6 committee meeting. 7 MR. WATERS: Let me clarify. I believe 8 based on timing that the seismic issue will not be 9 closed at this time. We will have an updated draft 10 SE that should hopefully be more clear on the open 11 items. If we need to clarify we'll do that and 12 provide that. That's what we plan on providing for 13 the full committee meeting. 14 MR. STATTEL: One final statement I'll 15 make is we will not issue a license amendment to 16 allow installation of this system until all of the 17 open items are closed. 18 MEMBER STETKAR: Thanks. 19 Are there other questions for Mike? MR 20 (No response.) 21 So seeing none, are we turning it MR 22 over? Do we need to change --23 (Pause.) 24 MR. SCHRADER: Do you want me to come 25 up or speak from here? Okay.

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	18
1	(Pause.)
2	MR. SCHRADER: Okay, I've got a green
3	light. Can everybody hear me? Okay. Good
4	afternoon. I'm Ken Schrader. I'm a principal
5	engineer in Regulatory Services, so the licensing
6	area at Diablo Canyon plant for PG&E, and I'm
7	responsible for this license amendment request and
8	obtaining NRC approval. I also have Kate Williams
9	here today. She's sitting back there, and Kate is
10	the project manager for this project.
11	Finally, I have Scott Patterson here
12	next to me. Scott is retired from PG&E. He worked
13	for over 30 years at Diablo Canyon in the I&C area,
14	and Scott was responsible for the I&C obsolescence
15	program at Diablo Canyon, and really was one of the
16	major designers of this protection system upgrade.
17	So I have Scott here to provide a little more
18	detail on the change, because he's definitely
19	probably the most PG&E person on this project.
20	Okay. So I'll talk a little bit about
21	ISG-06 and how we're involved in that. We'll give
22	a higher level presentation or discussion of what
23	the process protection system replacement is, kind
24	of how it's designed, and the ISG-06 lessons
25	learned we'll be more than happy to jump in and

(202) 234-4433

	19
1	provide information there when the staff discusses
2	it later on today.
3	Okay, so Slide 3. So Diablo Canyon,
4	this application was the pilot application for the
5	use of ISG-06. ISG-06 was interim staff guidance
6	developed for licensing a safety-related digital
7	upgrade. We were involved in the working group
8	developing ISG-06, so essentially involved since
9	2008 time period. So we're very familiar with the
10	contents of ISG-06.
11	We submitted our license application on
12	October 26th of 2011, and we then provided a
13	supplement on April 30th, 2013. That supplement
14	did include one design change that I'll talk about
15	later on in my presentation. So the basis
16	architecture of the process protection system
17	replacement that we are requesting approval for is
18	composed of two different vendors' architecture.
19	The first is the Invensys Tricon
20	Version 10. That's a PLC-based architecture which
21	comprises triple redundancy. It also contains the
22	Westinghouse Advanced Logic System, which is an
23	FPGA-based system, that it contains both redundancy
24	and diversity. The reason we're using the two
25	architectures was we wanted to be able to provide a

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	20
1	system that could address a common cause software
2	failure without requiring operator actions.
3	Several other prior licensee
4	applications for safety-related digital upgrades
5	required a diverse actuation system in order to
6	address common cause failures. That has some
7	negative aspects that we wanted to avoid. So we
8	were able to provide the diversity on the safety
9	side as part of the protection system.
10	Okay. Just to kind of give you an
11	overview of what the scope is of this, this is not
12	just it's like Oconee where we're almost
13	replacing the entire protection system. We're not
14	doing that here. We're replacing essentially the
15	processing part of the protection system.
16	So if you look at the figure here, this
17	figure kind of gives an overview of the whole
18	entire protection system, and so we're going to be
19	replacing the portion in the red box, which is
20	essentially the part of the system that determines
21	whether we need an reactor trip or an engineering
22	safety feature's actuation signal.
23	That process protection then sends that
24	signal from each of the protection sets, and
25	there's four of them, to the solid state protection

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	21
1	system and the Solid State Protection System
2	actually does the coincident logic to determine if
3	there's an actual actuation and then sends that on
4	the reactor trip system and engineering safety
5	feature's actuation system.
6	So we, as part of this project, are
7	changing what I would say is the heart of the
8	system, the part that processes the incoming
9	signals and determines if a trip is required.
10	Okay. So the figure on page five is a
11	little more detail of the part of the system that
12	we're replacing. So the part that we're replacing
13	is in the dotted circle there in the center of the
14	figure. The box that's above is the solid state
15	protection system that does the coincident logic,
16	that does not run software and that system we are
17	not replacing as part of this. It will remain as
18	is.
19	Also, this project we're not replacing
20	the sensors portion of the system or any of the
21	control systems.
22	CHAIRMAN BROWN: Excuse me. What does
23	the red line which means "stop at the streets"
24	mean?
25	MR. SCHRADER: That's a good question.
	NEAL R. GROSS

(202) 234-4433

	22
1	So what that means is that there's no common cause
2	software failure that can occur in that component.
3	CHAIRMAN BROWN: The FPGA part of the
4	system?
5	MR. SCHRADER: That's correct.
6	CHAIRMAN BROWN: That's kind of an
7	interesting, overarching, completely blanketed
8	statement. I mean is there it might have been
9	in the SE and I missed it. I know there was a
10	discussion of it, but I did not see any other
11	MR. SCHRADER: The staff presentation
12	actually has some detailed slide on how a common
13	cause failure is presented within ALS, the FPGA
14	side. Rich, you'll be discussing that.
15	MR. STATTEL: Yes, I'll be covering
16	that.
17	CHAIRMAN BROWN: Okay.
18	MR. SCHRADER: So this is higher level
19	of the staff's
20	CHAIRMAN BROWN: And the same thing
21	with the SSPS, which is not part of the project,
22	also has a slice. So there's no so there was an
23	that's leftover from before and I guess that was
24	determined to have no common cause failure modes at
25	all.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	23
1	MR. SCHRADER: It does not run
2	software, so there's no common cause.
3	CHAIRMAN BROWN: I understand that.
4	But yeah my mic's on. Am I hearing? Can you
5	hear me? Okay. All right, go on. Thank you.
6	MR. SCHRADER: Okay. So
7	MR. SCHRADER: It was though Ken, and I
8	don't want to go too far astray here though, but as
9	I understand it, one of the reasons for the
10	allocation of specific signals and functions
11	between the ALS and the Tricon platform was
12	apparently to address some concern about common
13	cause failures in the Eagle 21 system that would
14	require manual operator intervention.
15	Those were in the input signal
16	processing part of the Eagle 21? In other words,
17	not the part that has the no common cause failure
18	line through it now?
19	MR. SCHRADER: Okay, so you're correct.
20	Essentially, our current Eagle 21 system, if it has
21	a common cause failure, there's several signals
22	that there's no backup in other parts of the
23	protection system and therefore manual operator
24	action would need to be taken.
25	MEMBER STETKAR: But that, I'll call it

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	24
1	a postulated common cause failure, that postulated
2	common cause failure was within, on this drawing,
3	the dotted black oval shaped sort of thing, not in
4	the upper part of the SSPS; is that correct?
5	CHAIRMAN BROWN: Okay, that is correct
6	John. Within the dotted circle, and so essentially
7	where you see the circle with the slash through it
8	in the ALS, that is where the possibility of a
9	common cause failure is addressed in this new
10	protection system, such that we won't need operator
11	actions any longer.
12	MEMBER STETKAR: Okay, thank you.
13	MR. SCHRADER: And Scott will actually
14	go into that and so will Rich.
15	MEMBER STETKAR: Okay.
16	MR. HECHT: So when you say no CCF,
17	which you really mean is no software CCF?
18	MR. SCHRADER: That's correct.
19	MR. HECHT: Because there could be
20	hardware or other CCFs in there as well?
21	MR. SCHRADER: Yeah, that's correct. I
22	mean you can always postulate a common cause
23	failure. So it does mean software failure, that's
24	correct.
25	All right, so Slide 6. So when we were

(202) 234-4433

first starting on this project, you know, looking at operating experience from several of the prior protection system upgrades, you know, there were areas that caused extensive interactions with the NRC and negotiations and additional, you know, changes to the system in order to obtain NRC approval.

8 So we tried to start out right from the 9 beginning to make our system design as simple as 10 possible. So some of the attributes that we have -11 - or design requirements that we included in this 12 protection system upgrade were we don't use anv cross-channel communications, and that's consistent 13 14 and I'll show you on the next slide here, with our 15 current design.

16 have four different protection So we 17 and there are communications going sets no on 18 between those protection They're sets. kept 19 isolated from each other. The other attribute is 20 is there's no two-way safety communications going 21 from safety to non-safety or non-safety to safety 22 within this design, while the system is required to 23 be operable.

24 Obviously when it's in maintenance, 25 there's communications going on, but it's out of

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

(202) 234-4433

25

	26
1	service. It's inoperable. Finally we have no
2	within the process protection system there's no
3	voting of the signals between the different
4	protection sets or within the protection sets.
5	That voting will continue to be done by
6	the Solid State Protection System, which we are not
7	changing.
8	CHAIRMAN BROWN: Okay. Let me I
9	guess no signal voting of channels. I understand
10	the voting in the SSPS. That's where your
11	coincidence is generated and that's where you
12	generate your final either reactor trip or
13	Safeguards or whatever is required. Are you
14	referring to go back, which diagram? I'm trying
15	I think you're working on the Oconee stuff that
16	you had to deal with and there, if my memory serves
17	me right and that may not be serving me right,
18	there was some communication between channels to
19	determine signal goodness.
20	MR. SCHRADER: That is correct.
21	CHAIRMAN BROWN: Richard's shaking his
22	head over here, so I'm probably shooting off. But
23	is that that's my understanding. This is a
24	seven year old memory, okay, and at my age that's
25	very suspect. So that's why I'm

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	27
1	MR. SCHRADER: Yeah, I understand. So
2	yeah. So we within each of the protection sets,
3	sorry. Pardon me, I said it wrong. Between the
4	different protection sets there's no within the
5	change that we're making here, there's no loading
6	happening, you know, between each of the protection
7	sets.
8	CHAIRMAN BROWN: Okay. Even within a
9	protection channel, you're taking the signals from
10	the sensor through the signal conditioning and it's
11	processed as if it is a valid signal? I mean it's
12	not evaluated for goodness or badness?
13	MR. SCHRADER: It does do that, right?
14	CHAIRMAN BROWN: I mean, hold it. Let
15	me clarify. It may be out or range, high or low,
16	that's one thing. But in terms of within a channel
17	saying well gee, if my pressurizer pressure is such
18	and such and my loop pressure is such and such and
19	they deviate by some amount, therefore something's
20	suspect.
21	MEMBER STETKAR: You pick you're
22	picking the Tricon. You pick the middle of the
23	three or you do some sort of voting from the
24	Tricon. I don't remember what it is. But there is
25	some sort of comparison and selection process

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

	28
1	there, because you've got three inputs
2	MR. PATTERSON: Yeah, we do that for
3	MEMBER STETKAR:for three outputs,
4	whatever you want to call them.
5	MR. PATTERSON:for a control system,
6	we do a median signal select. For the protection
7	system, there's nothing like that.
8	MEMBER STETKAR: How do you select from
9	the three processors in the Tricon which signal to
10	pass through to the output?
11	MR. PATTERSON: Internal to the Tricon?
12	Yeah, there is some voting going on internal to
13	that.
14	MR. SCHRADER: So let me just
15	(Simultaneous speaking.)
16	MR. SCHRADER: This statement is
17	referring to between
18	MEMBER STETKAR: Between channels.
19	CHAIRMAN BROWN: Okay, between
20	channels.
21	(Simultaneous speaking.)
22	MEMBER STETKAR: That is true. You
23	have to pick something to send through.
24	MR. SCHRADER: In that, some of the
25	previous digital upgrades, that was not the case
	NEAL R. GROSS

	29
1	and that caused a lot of interactions.
2	MEMBER STETKAR: Okay, thank you.
3	MR. SCHRADER: All right. So a final
4	point on this slide that we've already discussed.
5	With this design, if we have any type of common
6	cause software failure that is, you know, just
7	assumed to occur, with this system we will be able
8	to still get automatic actuation and we won't need
9	a manual operator action, and we designed it that
10	way so that we didn't have to have manual operator
11	actions required to deal with a common cause
12	software failure.
13	MEMBER STETKAR: Ken, let me stop you
14	there. I was going to wait, but I might as well,
15	since you have a bullet for it here. Two years
16	ago, I went back and looked up my notes, and I
17	looked at the system design and we had a
18	discussion. The ALS platform is the only platform
19	that gives me a Safeguards actuation from the LOCA.
20	Now the assertion is there cannot be common cause
21	failures in the ALS platform. So you're saying
22	that the operators don't need to do anything for a
23	LOCA because there can't be common cause failure,
24	software failures in the ALS platform.
25	The Tricon platform is the only

(202) 234-4433

	30
1	platform that gives me auxiliary feedwater
2	actuation, with a successful reactor trip
3	condition. Not ATWS, but with a successful reactor
4	trip, and it's the only platform that I can find
5	that gives me main scheme isolation for a steam
6	line break outside of the containment.
7	I brought these three things up two
8	years ago. At that time my notes say well, we
9	don't postulate software common cause failures in
10	the ALS because of what we're going to hear about
11	later. So I'll accept that for now and we'll ask
12	the staff about that.
13	We had some discussion regarding the
14	auxiliary feedwater actuation with respect to your
15	ATWS mitigation, the AMSAC logic, and I don't have
16	the drawings to show the logic. I just took notes
17	and the notes that I have say that there's a 240-
18	second time delay, that the AMSAC logic remains
19	armed, and if you get low level in three of the
20	four steam generators within that 240 second
21	period, that auxiliary feedwater will be actuation
22	from AMSAC.
23	In a lot of plants that I've seen,
24	AMSAC also requires that the if the reactor trip
25	breakers are open, AMSAC doesn't do anything. In

(202) 234-4433

	31
1	other words, it requires a coincidence that a
2	reactor trip breaker must be closed and these other
3	things happen.
4	So because I don't have the AMSAC
5	logic, I wanted to sort of pulse the fact that that
6	240 second period that will actuate auxiliary
7	feedwater is valid regardless of the status of the
8	reactor trip breakers, whether they're open or
9	closed.
10	I know that's a lot of detail, but if
11	it's not contingent on the reactor trip breakers'
12	position, then I don't know how AMSAC will give me
13	that backup automatic auxiliary feedwater for a
14	successful reactor trip, for a successful reactor
15	trip.
16	(Off mic comments.)
17	MEMBER STETKAR: We've got time.
18	MR. PATTERSON: AMSAC is not even
19	armed, I don't believe, until you get to
20	MEMBER STETKAR: It's 40 percent power
21	that arms it. So let's just take a condition we're
22	above 40 percent, 100 percent power.
23	MR. PATTERSON: Right.
24	MEMBER STETKAR: We get a loss of main
25	feedwater. The reactor successfully trips. There

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	32
1	is a software common cause failure in the Tricon
2	platform. It's gone. Now what automatically
3	actuates auxiliary feedwater under those
4	conditions? Loss of all main feedwater, reactor
5	successfully tripped, software common cause failure
6	in Tricon.
7	Just that take that away. Don't try to
8	answer it real time because you need to
9	(Simultaneous speaking.)
10	MEMBER STETKAR: I wrote my notes and I
11	said gee, that's kind of neat but I've seen some
12	AMSAC designs and I don't know how Diablo's is.
13	The second question though, I didn't get an answer
14	two years ago, and that is what automatically
15	isolates the main steam line for a main steam line
16	break outside containment, outside containment, and
17	a common cause failure in the Tricon logic?
18	Does a backup signal for a steam line
19	break inside containment because it contained high
20	pressure comes through the ALS logic and we'll get
21	you there. I couldn't figure out anything for
22	downstream. Now I'm not I just the reason I
23	bring these up is that you've taken care of some
24	manual operator actions that had a potential
25	vulnerability for some postulated common cause

(202) 234-4433

	33
1	failures.
2	You may have introduced other operator
3	actions for other types of common cause failures.
4	That doesn't necessarily mean that the new system
5	is worse than the old system; it's just different.
6	However, if there are manual operator actions
7	required, that last bullet on this slide, that it
8	eliminates the need, is not a correct statement.
9	That's why I'm trying to pulse this,
10	because that statement up here is throughout the
11	license submittal and throughout the staff's SER,
12	kind of parroting back. So that's the only reason
13	I'm trying to understand that statement.
14	MR. SCHRADER: I think the answer to
15	both of your questions is in the diversity and
16	defense indepth topical report that we submitted
17	prior to this.
18	MEMBER STETKAR: He's actually on.
19	MALE SPEAKER: It is on.
20	(Off mic comments.)
21	MEMBER STETKAR: Yeah, he's on.
22	MALE SPEAKER: Just move forward.
23	MEMBER STETKAR: Just pull your mic
24	toward you a little bit. They're real sensitive.
25	Don't hit it with the paper now, but now it will

(202) 234-4433

	34
1	cause other problems.
2	MR. SCHRADER: The diversity and
3	defense indepth topical report that we submitted
4	prior to the license amendment went through all the
5	different scenarios.
6	MEMBER STETKAR: I raised these
7	questions originally when I read through that D3
8	report, so I didn't get the answers in that report.
9	MR. SCHRADER: All right.
10	MEMBER STETKAR: Look them up. I mean
11	that's as I said, we can't do it real time here
12	because it requires some signal tracing.
13	MR. SCHRADER: Okay. So Slide 7. So
14	I'll just so this is just a depiction of the
15	current Eagle 21 protection system. I just want to
16	put out a few things here and then I'll turn it
17	over to Scott to give some more detailed
18	explanation of the upgrade.
19	But we have this slide here just so you
20	understand what we have today, and so the Eagle 21
21	protection system and it is a digital system, we
22	have four different protection sets and they are
23	independent. Today, they don't communicate between
24	each other and each of them has a dedicated
25	maintenance work station.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433
35 The output of the Eagle 21 system is to 1 2 Solid State Protection System that does the the 3 That pathway is hard wired and then the voting. what actually performs the coincidence 4 SSPS is 5 logic to determine, to actually send the actuation to trip the reactor breakers or to actuate an SFAS 6 7 (phonetic) component. 8 So now I'm going to, unless you have 9 any questions, I'm going to turn it over to Scott 10 to give a little more detail of how the protection 11 system is designed. 12 MR. PATTERSON: You want to go to Slide 13 10? Okay, here we go. 14 MR. SCHRADER: Do you want take over from there? 15 16 MR. PATTERSON: I was going to start. 17 MR. SCHRADER: Oh, you were going to 18 Can you go to 10? Okay. So I'll have start. 19 Scott start at Slide 10. 20 MR. PATTERSON: So the next few slides 21 are to kind of give you an idea of how we split the 22 functions between the Tricon and the ALS and why we did that. 23 24 MEMBER STETKAR: You're not going back 25 to simple cartoons that you skipped over, the

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	36
1	right? The only reason I was going to ask a
2	question were you got
3	MR. SCHRADER: That would be fine.
4	(Simultaneous speaking.)
5	MEMBER STETKAR: A lot of what I read
6	or what I read in the SER said that a lot of the
7	information that the staff reviewed was specific to
8	Protection Set 1, and that it's inferred that the
9	other three are the same. It's pretty apparent
10	that they're not all the same, from what I can
11	read, because if nothing else Protection Sets 1 and
12	2 have more stuff in them, in the sense they have
13	more cabinets and I looked at a couple of the
14	analyses that refer to the fact that they're the
15	more limiting sets in terms of looking at what was
16	done in the timing analyses.
17	So what's the difference among the four
18	sets, at a fairly high level not you know, what
19	does 1 and 2 do that 3 and 4 don't do?
20	MR. PATTERSON: There are several
21	functions that are 2 out of 3 and not 2 out of 4.
22	For example, RCS flow, there's only three channels
23	for that.
24	MEMBER STETKAR: Oh okay.
25	MR. PATTERSON: Containment pressure
	NEAL R. GROSS

(202) 234-4433

	37
1	safety injection is only three channels. Wide
2	range temperature channels, there's four of them
3	but they're on in Sets 1 and 2. Wide range
4	pressure is in 3 and 4. So there are some
5	differences there.
6	Set 4 has pressurized vapor space.
7	That's the only one. There's only one channel of
8	that. So there's different channels based on 2 out
9	of 3 coincidence, 2 out of 4 coincidence and then
10	some of the other post-accident stuff.
11	MEMBER STETKAR: Okay, that helps.
12	Thanks.
13	MR. SCHRADER: Slide 10.
14	MR. PATTERSON: So this slide just
15	shows you the inputs to Eagle 21. I think on the
16	copies it's gray, but the top four blue boxes on
17	the slide are reactor trip functions. The bottom
18	two pink boxes are your engineered safety feature's
19	functions, and then the purple boxes are a
20	combination of reactor trip and ESF functions.
21	Then on the right side of the diagram
22	shows you the actual ESF functions and the reactor
23	trip, reactor trip being at the top. So one of the
24	objectives for the whole project was again, as Ken
25	stated, was to remove some of the operator actions

(202) 234-4433

	38
1	that we were taking credit for, and those were
2	based on three functions: reactor coolant flow,
3	containment pressure and pressurizer pressure.
4	So if you go back to the diversity and
5	the defense indepth analysis that we had performed
6	and then submitted as a topical report, we
7	identified those three functions. The rest of the
8	functions had some sort of an automatic backup for
9	a common cause failure in Eagle 21.
10	Then we go to the next slide. So the
11	top box in the middle is your Tricon and the second
12	box in the middle is your ALS platform.
13	Next slide. This slide shows you the
14	functions that are associated with the Tricon. The
15	ones that have a T on them are just the Tricon, the
16	ones that have an AT are both ALS and Tricon, and
17	the ones that just have the A on the left are the
18	ALS functions. Same on the right. You can see
19	that some of them are combinations of both.
20	Go to the next slide okay. This is
21	just a little bit more detail showing some of the
22	functions. Your OP Delta T, OT Delta T.
23	MR. HECHT: The functions that are
24	indicated as A, you know, we've been concerned what
25	happens when the Tricon goes. But what happens if

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	39
1	the ALS goes with respect to those functions that
2	are A?
3	MR. PATTERSON: That's the circle with
4	the slash in it, no common cause failure thing
5	right. So there's two
6	(Simultaneous speaking.)
7	MR. HECHT: Well, I guess my question
8	is if there is a failure in the ALS system, what
9	happens?
10	MR. PATTERSON: Are you talking a
11	common cause failure or just a failure?
12	MR. HECHT: Well, I guess let's just
13	say a simultaneous failure. Does that mean that
14	the that you can't do that reactor trip?
15	MR. PATTERSON: So there's four
16	divisions and four protection sets of equipment,
17	and then in each one of those divisions or
18	protection sets there's two ALS chassis, and
19	they're diverse from each other. So you actually
20	have redundancy in a set of four redundant
21	channels. So you would have to have all those fail
22	at the same time.
23	MR. HECHT: Okay. So in other words,
24	the ALS is responsible for those two functions
25	exclusively, and not the Tricon?

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	40
1	MR. PATTERSON: Correct. Reactor
2	current flow is just in the ALS platform itself.
3	There's not anything in the Tricon and then the
4	pressurizer pressure does go to the Tricon, but
5	it's for OT Delta T not pressurizer pressure,
6	safety injection or reactor trip or anything like
7	that.
8	MR. HECHT: Thank you.
9	CHAIRMAN BROWN: Just to make sure I
10	understand it, I understand you do have two
11	redundant, diverse ALS sections and they both do
12	process each of these signals. So it's not
13	they're not isolated, one goes through one. So you
14	have redundant processing of those in the two
15	diverse ALS applications?
16	MR. PATTERSON: Correct.
17	CHAIRMAN BROWN: Change, processing
18	change in each processing channel. Okay, thank
19	you.
20	MR. SCHRADER: It had to be designed
21	that way to address a common cause failure and be
22	able to still perform the function.
23	MR. PATTERSON: And that's worked
24	together, so either one can cause the trip.
25	CHAIRMAN BROWN: I'm truing to remember

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	41
1	from reading in the SER or in part of the system
2	description. When you say "diverse," it's the same
3	is it the same hardware but they are programmed
4	differently? In other words, in developing the
5	logic flow through the FPGAs? Is that that's
6	what my memory is clicking around in here.
7	MR. SCHRADER: They're forced to be
8	programmed differently as part of the design
9	CHAIRMAN BROWN: Yeah, yeah, two
10	different folks, different layout, different
11	programming implementation?
12	MR. SCHRADER: That's correct, yes.
13	CHAIRMAN BROWN: Okay, all right.
14	MR. PATTERSON: Two separate design
15	teams with two separate
16	CHAIRMAN BROWN: I got it. Thank you.
17	MR. PATTERSON: So yeah. This is just
18	the Tricon function allocation with a few more
19	details put in the middle that describe some of the
20	functions like OP Delta T and OT Delta T for the
21	neutron flux. One of the other advantages that we
22	had for not replacing the Solid State Protection
23	System is the nuclear instrumentation system
24	actually bypasses Eagle 21.
25	There is neutron flux coming in, as you

(202) 234-4433

	42
1	can see here on the top left-hand blue box there.
2	That's upper and lower flux for the OP Delta T and
3	OT Delta T trips. For high flux trips, the nuclear
4	instrumentation system goes straight into the solid
5	state protection. So that's a diverse function
6	that we took credit for in our diversity analysis.
7	By keeping SSPS or Solid State
8	Protection System and having the nuclear
9	instrumentation feed directly into that, that's all
10	analog systems. We could use that as a diverse
11	automatic backup function for some of these
12	scenarios.
13	Give me the next one. This slide shows
14	you the breakdown of the ALS functions like we
15	talked about, the reactor current flow. It
16	currently has a manual operator action that we take
17	credit for loss of coolant flow in a single loop.
18	I believe that's about a five minute operator
19	action time or is it ten minute operator action
20	time, and then containment pressure and pressurizer
21	pressure safety injection, there's an operator
22	action that we take credit for currently now.
23	With this system, with it being on the
24	ALS, again as we talked about being diverse, we can
25	not have to take credit for those anymore.

(202) 234-4433

	43
1	MR. SCHRADER: Yeah. It was a credited
2	ten minute operator action in the prior NRC safety
3	evaluation for the Eagle 21 installation back in
4	the 90's.
5	MR. PATTERSON: Unless there's any
6	questions, I'll hand it back over to Ken.
7	MEMBER STETKAR: Yeah, let me ask you -
8	- let's see if I can figure out how to ask this.
9	There's a lot of discussion well I won't say a
10	lot of discussion, there's some discussion in the
11	safety evaluation, I'll ask the staff about this
12	later but I want to get the input from you, about
13	definition of the output signal safe states what
14	they're called from the ALS platform.
15	In other words, given I don't like to
16	use the term "failure," so I'll use the term given
17	some glitch in the ALS platform, there is some
18	predefined safe state of the output that the cores
19	drive the output to. There's some discussion about
20	specification of those safe states, reviews of
21	those safe states.
22	I would presume, although I may be
23	wrong, that there is an equivalent definition of
24	safe states for the Tricon logic. Is there,
25	because I could find no discussion of safe states

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	44
1	from Tricon or any review of any said safe states
2	or any specification of said safe states from
3	Tricon.
4	MR. PATTERSON: You can define safe
5	states in the Tricon, yes.
6	MEMBER STETKAR: I'm sure you can. I'm
7	asking did someone do that?
8	MR. PATTERSON: For the reactor trips,
9	they're deenergized to trip functions. So the safe
10	state would be reactor trip or deenergized.
11	MEMBER STETKAR: That's easy for you to
12	say and I could say that too. I'm asking in the
13	design and in the specification, were those safe
14	states defined such that they're traceable and
15	reviewable?
16	MR. PATTERSON: I believe so, but I'd
17	have to go back and look.
18	MEMBER STETKAR: Okay. Could someone
19	please check on that, because I found no discussion
20	of it? I can guess what a safe state for a reactor
21	trip could be. A safe state for a Safeguards
22	actuation function in some cases is not so simple,
23	because it depends on the event scenario.
24	Sometimes I like to isolate auxiliary
25	feedwater because it's feeding a faulted steam

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	45
1	generator. Most of the time I like to keep it
2	going. Sometimes I like to isolate certain
3	containment penetrations like reactor coolant pump
4	seal injection, component cooling water, thermal
5	barriers because I have a Phase B containment
6	isolation. Most of the time I like to keep it
7	going.
8	So sometimes the defined safe state
9	requires some judgment on the part of the people
10	who specify the particular application for a
11	particular plant. That's I'm more concerned
12	about the Safeguards safe states than the reactor
13	protection quite honestly.
14	But if they weren't defined that is a
15	question about why. So I'd like to some follow-up
16	on that. As I said, I'll follow up with the staff
17	because they did the review. They should have
18	looked at that. Thank you.
19	MR. SCHRADER: All right. So I'm on
20	Slide 16 now. So I think you'll see when the staff
21	gives their presentation, that they did an
22	extensive review of our application. So as a
23	result of the review, we did actually make one
24	design change ot the protection system. It wasn't
25	we weren't required to. It was a PG&E decision

(202) 234-4433

	46
1	to make that change.
2	But what it relates to was the
3	maintenance work stations. So originally our
4	original design for each protection set, we were
5	going to have one maintenance work station that had
6	the ALS software and the Tricon software on it, you
7	know, and it would be shared.
8	We received many questions about how if
9	we did a software update of one vendor's software
10	on that maintenance work station, how was that
11	going to affect the other software? How would you
12	know if it affected the software? What kind of a
13	procedure are you going to have to do the testing?
14	So it would have been pretty difficult
15	to come up with a procedure that could be done in a
16	timely manner, to make sure that there were no, you
17	know, unwanted interactions. So we made the
18	decision to essentially use a separate computer
19	core for each of the systems.
20	So each protection set will have a
21	computer with the ALS software and a computer with
22	the Tricon software on it, and we will use a, you
23	know, common monitoring keyboard and mouse through
24	a KBM switch. So that change was a change that did
25	result based on the NRC review.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

47 There were a couple of other I would 1 2 say minor changes that we made as a result of while 3 we were going through the review. For example, we 4 originally were going to have a printer in the cabinet and each protection set. 5 We determined, you know, with all the digital technology and PDF 6 7 files and everything that we did not need to have a 8 printer actually inside the cabinet. So we removed 9 that from the design. 10 MR. HECHT: Question. 11 MR. SCHRADER: Yes. 12 I wanted to verify, is that MR. HECHT: 13 KBM switch totally mechanical, because some KBM 14 switches are now designed that they're basically 15 they're networked to the processors network, and 16 control is accessed through when software not 17 through hardware? 18 MR. SCHRADER: Oh, it's not totally 19 mechanical. I'll let you do that. 20 MR. PATTERSON: No, it has USB ports on 21 it, so it does have some software internal to the 22 KBM. 23 And was that analyzed? MR. HECHT: It's a non-safety part 24 MR. PATTERSON: 25 looked of the system, it was at from а SO

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	48
1	perspective of cybersecurity, but not as affecting
2	like a safety function or anything.
3	MR. SCHRADER: Yeah. It's in a part of
4	the non-safety part of the system and signals from
5	that. While the system is operable, an operation
6	cannot get to the protection system.
7	MR. HECHT: It wasn't clear from
8	when I was looking at the documentation and
9	admittedly I may not have read enough. But it
10	wasn't clear to me whether the maintenance work
11	stations could be attached to the either of the
12	computers during operation.
13	MR. SCHRADER: Oh yeah.
14	MR. PATTERSON: Well, there's two
15	maintenance work stations, one for the Tricon and
16	one for the ALS, and they are connected one-way
17	communications all the time. So data comes out of
18	the Tricon and the ALS and goes into the
19	maintenance work station for monitoring alarm
20	functions, diagnosis, things like that.
21	The only way you can talk back into the
22	safety systems, on the ALS you have to actually
23	connect a physically cable. On the Tricon, there's
24	a switch and then there's also a there's a key
25	switch and then there's also an out of service

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	49
1	switch that you have to throw, which is a safety-
2	related switch.
3	MR. HECHT: Okay, but what if how
4	are you sure that you're not getting alarms that
5	you do need to get on the maintenance work
6	stations, or is it not safety so it doesn't matter?
7	MR. SCHRADER: That's correct. It's
8	not we don't our operators won't need to get
9	an alarm on the maintenance work station, you know.
10	This is contained down in the cable spreading
11	room, locked area below the control room. All the
12	required indication for the operators will be in
13	the control room, just like it is today.
14	MR. HECHT: So then why do you need the
15	maintenance work stations connected?
16	MR. SCHRADER: Because with the
17	maintenance work station, the maintenance I&C
18	technicians can get much more detailed information
19	if a fault occurs. They can get, you know, more
20	detailed diagnostic information from the Tricon or
21	the ALS, in order to diagnose what the problem is
22	so that they can quickly
23	MR. HECHT: So it's acting as a data
24	logger if you will?
25	MR. SCHRADER: In a sense yes, it does

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	50
1	have data logging capabilities, yes. But again,
2	while the system is operable in operation, there's
3	no information, there's no information going
4	through the maintenance work station to the safety
5	side.
6	MEMBER STETKAR: On the Tricon side
7	with the key switch, is it physically impossible
8	for the maintenance work station to communicate
9	with the application software when the key switch
10	is in the run position, I mean physically
11	impossible, because there's some statements in
12	there saying that there's internal software that
13	looks at the key switch and makes internal
14	determinations of what can be done, depending on
15	what the software thinks the key switch position
16	is?
17	(Off mic comments.)
18	MEMBER STETKAR: So what I'm asking is,
19	is it possible to alter the software internal to
20	the Tricon platform, such that with the key switch
21	in the run position it thinks it's in the program
22	position and somebody can get in? I'm talking
23	about cybersecurity here.
24	MR. SCHRADER: I think Rossnyev's going
25	to answer.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	51
1	MEMBER STETKAR: Okay.
2	MS. ALVARADO: This is Rossnyev
3	Alvarado. I'm with the staff, and I will talk
4	about communication. But yes, there are certain
5	functions, not all of them, that if you have the
6	key switch in the wrong position you can modify
7	the variables. But there are specific functions,
8	not all of them, that you can do that.
9	MEMBER STETKAR: You know, I was very
10	careful. I asked about the application software.
11	I did not say variables, because I know you can go
12	in and modify set points and variables.
13	MS. ALVARADO: Yes, there are certain
14	some functions that you can modify. There are some
15	points like variables and that that you can modify
16	when the program is in run.
17	MEMBER STETKAR: Okay, thank you. I
18	was aware of that. That's not answering the
19	question that I asked. When the key switch is in
20	the run position, is it physically possible to be
21	able to access the application software and make
22	changes to that software? Can that be done? Can
23	the system be spoofed?
24	MR. PATTERSON: No, I don't believe so.
25	That's part of the
	NEAL R. GROSS

(202) 234-4433

	52
1	MEMBER STETKAR: That's one of the
2	things I was looking for, because there was this
3	sense, the sense of the software looks at the key
4	switch position and then determines internally what
5	can be done. I don't care if people are modifying,
6	you know, parameter values or set points or things
7	like that. That's I'm relying on safe steps to
8	take care
9	MR. PATTERSON: That was part of the
10	Tricon-specific, you know, approval, that
11	MEMBER STETKAR: But I didn't think
12	about it until I started, you know.
13	MR. SCHRADER: And, you know, we are
14	relying on that.
15	MEMBER STETKAR: You are relying on
16	that?
17	MR. SCHRADER: Yes. The NRC approval
18	of the when the switch is in run that you can't
19	make modifications.
20	MEMBER STETKAR: You cannot make
21	changes to the application software. That's what I
22	was looking for. I hope that's true.
23	MR. SCHRADER: But there was a very, I
24	mean detailed response from Invensys on how that
25	key switch works that, you know.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

53 MEMBER STETKAR: You know 1 what I'm 2 looking at is somebody getting in and modifying 3 whatever routine determines what position the key switch is in internally, such that when it's in the 4 run position it can be spoofed to think that it's 5 in the program position, and then somebody can go 6 7 in and make allocations such as while it's in the 8 run, and the operators don't know that it's being 9 done. 10 MR. SCHRADER: Okay. Well let me two 11 things. So whenever the key switch it out of the 12 run position, it alarms in the control room. Okay, but it's not out 13 MEMBER STETKAR: 14 of the run position. It's in the run position. 15 MR. SCHRADER: Okay. Well so we have 16 to deal with that for cybersecurity, and let me --17 I don't want to get into the details. 18 MEMBER STETKAR: Yeah no. you 19 MR. SCHRADER: I will tell that 20 there are multiple barriers to prevent that from 21 happening. 22 MEMBER STETKAR: Okay. 23 MR. SCHRADER: Okay multiple, because 24 that's part of cybersecurity and also SDOE as well. 25 Yeah, okay, okay. MEMBER STETKAR:

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	54
1	Thank you.
2	MR. SCHRADER: And the staff has
3	reviewed those aspects.
4	MEMBER STETKAR: Okay, good. Bear with
5	me. There was something in the SER that talks
6	about the and this is again Tricon, the remote
7	RXM, and I've forgotten what RXM is an acronym for.
8	MR. PATTERSON: It's Remote Expansion
9	Chassis.
10	MEMBER STETKAR: Thank you. It says
11	"The purpose of the remote RXM is to acquire and
12	transfer input and output non-safety related
13	signals to support functions that are not safety-
14	related PPS functions, such as signals to various
15	main control board indicators." Two is the
16	operative thing.
17	"It represents an expansion chassis to
18	be located several miles away from the main
19	chassis." Ha. That causes me pause because if
20	there's something several miles away that can
21	change signals to the main control board, I as an
22	operator are a bit concerned about. So could you
23	explain to me what that is?
24	MR. PATTERSON: I think that's the
25	capability of the remote expansion chassis, is you
	NEAL R. GROSS

(202) 234-4433

	55
1	could put a fiberlink a couple of miles away. In
2	Diablo's case, it's in the same room. I mean it's
3	
4	MEMBER STETKAR: There will not be
5	remote expansion chassis out somewhere else beyond
6	the site boundary?
7	MR. PATTERSON: No.
8	MEMBER STETKAR: No.
9	MR. PATTERSON: It will be in the same
10	room.
11	MEMBER STETKAR: Okay, thanks. That's
12	all I was looking for. Again, inside the fence I
13	don't care.
14	MR. SCHRADER: For cybersecurity
15	purposes, everything is going to be in the same
16	room.
17	MEMBER STETKAR: All right. I'm happy.
18	What I was concerned about is some remote link to
19	an emergency operations facility or something like
20	that that could get feedback in and change things
21	that the operators are looking at.
22	MR. SCHRADER: Right.
23	MEMBER STETKAR: Thank you.
24	MR. SCHRADER: All right. So just in
25	conclusion, so the process protection system

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	56
1	replacement design, when we replace it it's going
2	to provide significant improvements in safety,
3	reliability and human factors for operators.
4	So we have designed this system using
5	the latest NRC guidance, ISG-04 for communications,
6	ISG-06 for licensing. We also used ISG-02 for the
7	diversity defense indepth analysis.
8	Both of these platforms that we're
9	using are currently, you know, recently approved
10	platforms from the NRC. As I think we've talked
11	about multiple times already with this design for
12	the process protection system, you know, a portion
13	of the protection system, if common cause failures
14	were to occur in that system, we still will be able
15	to have an automatic actuation to perform the
16	required protection system function, such that
17	operators will not have to perform a manual action.
18	Finally, as part of this design, we
19	implemented lessons learned and operating
20	experience from those that went before us and also
21	from applications for each of our vendors'
22	platforms at facilities.
23	MR. HECHT: Can I ask one final
24	question? With respect to the one-way data
25	communications outside to the non-safety systems, I

(202) 234-4433

	57
1	assume that that means that there's also no
2	acknowledgment, there's no hand-shaking, so that if
3	the safety system or if the non-safety if the
4	receiver misses the data, it's too bad for the
5	receiving system, right?
6	MR. PATTERSON: For the ALS platform,
7	that's correct. It's just a one-way broadcast of
8	information. On the Tricon they have what they
9	call a PCM card. It's a communication module, and
10	it does have handshaking. But that PCM card is
11	your boundary, safety-related to non-safety related
12	boundary.
13	So it handles all the communication by
14	itself. It doesn't affect any of the processors
15	for the safety system.
16	MR. HECHT: So what happens if the
17	buffer on the PCM card gets full?
18	MR. PATTERSON: Then it doesn't
19	communicate.
20	MR. HECHT: There's no interrupt on the
21	bus to the rest of the Tricon
22	MR. PATTERSON: Correct.
23	MR. HECHT: Okay.
24	(Phone signal.)
25	MEMBER STETKAR: Just ignore that. It

(202) 234-4433

58 1 goes away. 2 HECHT: So that is kind of using MR. 3 PCM DCPI/PI guest, that card talking to the outside? 4 MR. PATTERSON: I don't remember. 5 Т don't know. 6 7 CHAIRMAN BROWN: Is there any more on 8 that? Are you --9 MR. SCHRADER: Yeah, I'm sorry. 10 CHAIRMAN BROWN: Okay. Are you 11 finished or are you still --MR. SCHRADER: I'm done. I'm done. 12 13 CHAIRMAN BROWN: Okay. 14 MR. SCHRADER: Thank you. 15 Did you have anything CHAIRMAN BROWN: 16 else on this? Any other questions from the members 17 on this particular segment? 18 (No response.) 19 CHAIRMAN BROWN: Okay. We're a little 20 ahead of schedule, so I would suggest we go ahead. 21 Richard, is that okay with you? I think there's 22 some break points in the NRC presentation. Is that satisfactory with you guys? Any problem? 23 24 (No response.) 25 CHAIRMAN BROWN: No? Okay.

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	59
1	(Pause.)
2	MR. STATTEL: Okay. I'm Richard
3	Stattel and I'm lead reviewer on this license
4	application. I don't know what's going on here.
5	Anyway, the next topic is diversity and defense
6	indepth, and I know we've covered some of this area
7	already. But I'll try to give you some
8	perspectives from the staff. I can describe some
9	of the RAIs, some of the interactions we've had
10	with the licensee in order to assure that they meet
11	the criteria.
12	The first line here just shows the
13	current requirements for diversity for digital
14	safety systems. There are three primary documents
15	that are listed here. They're all based on the
16	direction provided by the Commission in staff
17	requirements memorandum 93-087, which I think most
18	of you are familiar with.
19	Okay, the first one is NUREG-6303.
20	This document simply describes a method for
21	analyzing CCF. Diablo Canyon, the licensee in this
22	case performed a D3 analysis back in '93 on the
23	Eagle 21 system and they updated it for this
24	particular modification for the digital system.
25	They used 6303 as the process for performing that

(202) 234-4433

	60
1	analysis.
2	The second document is BTP-719, which
3	is direction to us, the staff, for evaluating the
4	D3 analysis. The final document is ISG, Internal
5	Staff Guide 02, which is actually now defunct
6	because we have incorporated its guidance into BTP
7	in the latest version, Version 6 of BTP-719.
8	But I do list it here and it is it
9	remains important and relevant to this review,
10	because at the time when the D3 analysis was
11	evaluated by the staff, the BTP had not been
12	updated yet. So we used the guidance directly out
13	of ISG-02, and I point that out because there were
14	some changes made when we incorporated that into
15	the branch technical position.
16	Now when we performed the current
17	evaluation that we're looking at, the application
18	evaluation, we did use BTP-719, okay.
19	The next slide. Okay. So BTP-719
20	requires that a coping strategy be developed for
21	digital safety systems to address the effects of a
22	software common cause failure when the potential
23	cannot be otherwise eliminated.
24	Back in 1993, when the Eagle 21 system
25	was put in, really the guidance for diversity was
	NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. (202) 234-4433 WASHINGTON, D.C. 20005-3701 (202) 234-4433

	61
1	just being developed at that time. But the
2	licensee at that time did perform an analysis, and
3	they postulated a software common cause of the
4	Eagle 21 system and it postulated that failure, the
5	postulated failure would result in a loss or
6	failure of all PPS functions to actuate.
7	That is, a failure of the PPS system to
8	perform all of its associated and assigned safety
9	functions. They went through the analysis, through
10	all of the accidents that were that were in the
11	plant safety evaluation, and they basically play
12	those through. Well, what would happen if you
13	don't have the PPS functions available, and what
14	they determined was they had a number of backup
15	functions that were available through other
16	systems.
17	I think Scott mentioned the nuclear
18	instrumentation system was independent. That was
19	one of them. But there were three cases, as was
20	mentioned earlier, those were for containment
21	pressure, reactor coolant flow and pressurizer
22	pressure. The analysis was it had to credit manual
23	operator actions as a means of coping with those
24	failures, okay.
25	This modification, as was mentioned by

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

the licensee, will eliminate the reliance on manual operator actions to cope with software or logic implementation common cause failures. The licensee did the update to the previous analysis tables. It involved the postulation of common failures for all plant accidents and anticipated operating occurrences described in the Diablo Canyon UFSAR safety analysis.

9 As you've seen in the previous slide, 10 the safety functions associated with those three 11 parameters, and they're show on this slide here, 12 have been allocated to the ALS portion of the new 13 PPS system. Now I want to make a point here, 14 because I think there's a couple of misstatements 15 previous.

The detailed analysis does not make a 16 17 case that software common cause failure of the ALS 18 subsystem is not possible or not credible, okay. 19 and we had a lot of discussion, but we were So 20 really not -- in the past we have not been willing 21 to accept an argument that just because a system is 22 FPGA-based that it's not subject to software, 23 because software is not running in that system 24 during operations.

Our reason for that is because software

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

25

1

2

3

4

5

6

7

8

(202) 234-4433

62

	63
1	is used to develop the logic that is implemented
2	within the FPGA designs. So we had this discussion
3	with Diablo Canyon when we did this analysis back
4	in 2010 time frame, and what we concluded for this
5	particular system is they have implemented this.
6	They've used two separate design teams,
7	and I'll talk a little bit about the diversity
8	features that are part of this system, and they've
9	implemented this in a way where they have diverse
10	teams developing different sets of logic for the
11	system, and therefore when we say the CCF is
12	possible, but when the CCF occurs it only affects
13	one of the chassis that's performing those
14	functions, and they both perform those functions in
15	parallel. I have some figures
16	MEMBER STETKAR: Rich, when you say
17	chassis, you mean one of the cores?
18	MR. STATTEL: No. There are actually
19	four cores. There's a figure here that will really
20	lay this out, and I think will help you understand
21	that.
22	MEMBER STETKAR: Yeah okay, okay.
23	MR. STATTEL: Okay.
24	MEMBER STETKAR: A-1, A-2
25	MR. STATTEL: It's coming up, right.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	64
1	A-1, A-2, B-1, B-2.
2	MEMBER STETKAR: I think that the 1 and
3	the 2 is the same, but that's okay.
4	MR. STATTEL: But before I get to that,
5	I do want to talk about the Tricon, okay. So the
6	Tricon, as the name implies, contained three
7	separate layers of redundant input.
8	MEMBER STETKAR: Rich, before you get
9	down in this detail, unless I don't think it's
10	going to come up. You heard I'll wait, I'll
11	wait until later.
12	MR. STATTEL: You can bring it up.
13	MEMBER STETKAR: No, you're on a roll.
14	Go on.
15	MR. STATTEL: Okay, on a roll.
16	MEMBER STETKAR: I'll get to you later.
17	MR. STATTEL: I do have some answers
18	for a couple of your questions.
19	MEMBER STETKAR: Yeah, okay. No,
20	you're on a roll. Go, go, go.
21	MR. STATTEL: But when you get a good
22	breaking point let me know, and I'll try my best to
23	respond to that. Okay. So the Tricon system, as
24	the name implies, has three separate layers of
25	redundant input, processing and output components

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	65
1	for each of the PPS system protection sets.
2	In essence, this establishes like a 12-
3	way or layers of redundancy for the Tricon
4	subsystem. I will mention even though it has three
5	sets of inputs, there's only one sensor generally
6	going into each channel, and it's just jumpered
7	into the three inputs. So it processes three
8	different times, but it is just one sensor here,
9	okay.
10	So all of this redundancy is expected
11	to result in a highly reliable and fault tolerant
12	system, and those characteristics were evident to
13	the staff when we reviewed the failure modes and
14	effects analysis document, and the reliability
15	analysis documents that the licensee provided to
16	us.
17	In actuality, I would expect to see a
18	very small amount of LCO time or out of service
19	time due to system maintenance or surveillance
20	testing following this system upgrade for those
21	reasons. These system characteristics do not,
22	however, address the issue of software-based common
23	mode error because all of the redundant processors
24	within the subsystem will be executing common
25	software components.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

66 Now I heard mentioned earlier that each 1 2 protection set does run different software, and 3 we're aware of that and we have reviewed all four 4 of those protection sets, the documentation 5 associated with those. However, they're all using 6 common components, right. So basically we 7 determined early on that there was no argument that 8 could be made for the Tricon system, that it would 9 not be vulnerable to a software common cause 10 failure, okay. 11 So as a result of this fact, the D3 12 analysis that was performed postulates the complete failure of all functions performed by the Tricon 13 14 and it identifies alternate means of subsystem, 15 maintaining reactor safety for each of the events 16 evaluated or analyzed in the Diablo it Canyon 17 analysis. 18 Richard, when you say CHAIRMAN BROWN: 19 the all functions, that means all four protection 20 Is that what you -- they all sets, process sets? 21 fail? 22 MR. STATTEL: That's correct. Any 23 safety function that's allocated to Tricon, you saw 24 the figure earlier. 25 CHAIRMAN BROWN: In other words it's

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	67
1	all but it happens
2	MR. STATTEL: Just assume they don't
3	work.
4	(Simultaneous speaking.)
5	MR. STATTEL:for a non-safety
6	system.
7	CHAIRMAN BROWN: But in every one of
8	the channels, all four channels. So you have
9	Tricon
10	(Simultaneous speaking.)
11	CHAIRMAN BROWN: I just wanted to make
12	sure I understood.
13	MR. STATTEL: That's right. So since
14	it's common cause, even though we have three layers
15	of redundancy in here, it's really above and
16	beyond, and granted Tricon has a pretty good track
17	record of having very reliable system. However,
18	we're really not crediting that in the regulatory
19	world for eliminating the potential for a common
20	cause failure here, okay.
21	Okay. At this point, I want to address
22	one of the questions that you had regarding the
23	fail-safe states, okay. So there are fail-safe
24	states generally fail to a deenergized state, which
25	in the case of SFAS functions is not actuate for

(202) 234-4433

	68
1	the channel, and in the case of a reactor trip
2	function, it actuates to the trip, and that is
3	really driven by general design criteria.
4	Now there is a discussion that's
5	specific to the ALS system that defines failed
6	states for particular failure detection, for
7	particular failure modes. There is not an
8	equivalent discussion in the Tricon because it
9	doesn't work the same way. So I'm going to get to
10	this in the next slide when I talk about the ALS,
11	so I just want to give you a heads up on that.
12	MEMBER STETKAR: You brought out the
13	shovel, so we'll be digging the hole. I don't want
14	to confuse the two for the moment, so let's keep on
15	the Tricon. You said it doesn't work in the same
16	way. It's kind of like I don't care whether I have
17	a diesel engine or a gas engine or a Wankel engine
18	or whatever in my car.
19	When I press on the accelerator, I
20	expect it to increase, and when I press on the
21	brake, I expect it to stop and those are kind of
22	fundamental things that I'd like, in terms of
23	specifying what I'd like a vehicle to do.
24	So you were careful. You said well in
25	general it fails to deenergized state, but in

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	69
1	general doesn't mean always.
2	MR. STATTEL: Well, let me try to
3	explain. What I'm trying to get at is there's a
4	fundamental difference between the technologies and
5	how they work. The Tricon system is a
6	microprocessor. So it's running, it's performing
7	equations, it's running in a cyclic fashion and
8	it's processing inputs, performing its calculations
9	and sending the outputs, and it's constantly doing
10	that.
11	So the failure modes that we postulate
12	in these cases are either that it halts operation.
13	That's one potential failure mode, or it performs
14	something that it's not supposed to do, it's not
15	programmed to do, in which case that would be the
16	common cause or the software error, the software
17	common cause failure.
18	Now typically so Tricon does use
19	watchdog timers. So if the processors do fail to -
20	- basically if the cycle stops, it will identify
21	that and it takes appropriate action. But in the
22	case of an FPGA, the FPGA technology, you don't
23	have a similar type of cyclic operation running.
24	Now there are frames so that it runs
25	through processes in a similar manner, but it's not

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	70
1	the same. So we don't have we can't just
2	monitor the same way, monitor performance in the
3	same way we do with the microprocessor. So the
4	figure here shows you that we have two logic
5	implementations
6	MEMBER STETKAR: You're back to ALS
7	again.
8	MR. STATTEL: I'm on it. I'm on ALS.
9	I'm talking about ALS.
10	MEMBER STETKAR: Yeah, but you're back
11	to ALS again. I want to keep you on Tricon.
12	MR. STATTEL: Okay.
13	MEMBER STETKAR: I understand that
14	there's a difference between a Wankel engine and a
15	diesel engine. What does the Tricon output do if
16	steam generator level input signal says it's plus
17	9,000 percent wide range? What does the output
18	signal from the Tricon do for auxiliary feedwater
19	in that case? What does it do? It's plus 9,000
20	percent, way out of scale, high out
21	MR. STATTEL: Well, in that case the
22	signal is validated. It goes through a validation
23	routine
24	MEMBER STETKAR: Yep, and it's invalid.
25	(Simultaneous speaking.)
	NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. (202) 234-4433 WASHINGTON, D.C. 20005-3701 (202) 234-4433
	71
----	--
1	MR. STATTEL:just being in an
2	invalid state.
3	MEMBER STETKAR: And what does then the
4	output signal for auxiliary feedwater actuation
5	from that Tricon protection set do?
6	MR. STATTEL: So okay. So are we
7	saying that all three of the redundancies and all
8	four of the protection sets are reading the same
9	thing?
10	MEMBER STETKAR: We've already
11	established that there's one steam generator level
12	signal into Protection Set 1.
13	MR. STATTEL: Correct.
14	MEMBER STETKAR: And I'm saying it's
15	9,000 percent of wide range. What does the output
16	signal from the Tricon Protection Set 1, I don't
17	care about 2, 3 and 4, 1 do under that condition?
18	MR. STATTEL: It would not initiate the
19	auxiliary feedwater.
20	MEMBER STETKAR: It would not initiate
21	the aux. So the fail safe state is to not initiate
22	auxiliary feedwater under that condition.
23	MR. STATTEL: That's correct, and
24	that's the same as the current Eagle 21 system as
25	well. That's the current licensing basis

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	72
1	MEMBER STETKAR: Is that hold on.
2	Let's not. I'm trying to establish a fundamental
3	design specification here, and that is a lot of
4	attention is paid over here on the thing that you
5	want to drag me to on ALS of safe states, and I'm
6	not hearing the same confidence in either the
7	design specification or the implementation of a
8	design specification establishing those safe states
9	for the output of the Tricon platforms. I'm just
10	not hearing that.
11	MR. STATTEL: Well, all of the failure
12	states of the Tricon platform are postulated and
13	they're documented in the failure
14	MEMBER STETKAR: I'm not talking about
15	I'm not talking about failure states, FMEAs.
16	I'm talking about what does the thing do, actively
17	do, I will do this given an input parameter of thus
18	and such, or I will do this if two of my three
19	internal whatever mechides (phonetic) stop doing
20	whatever they were doing?
21	MR. STATTEL: Those are functional
22	requirements, and those are in the functional
23	requirements document.
24	MEMBER STETKAR: Okay, and that's what
25	I'm and that's what I'm asking about. Do the
	NEAL R. GROSS

(202) 234-4433

	73
1	functional requirements specify that given an out
2	of range condition on each input signal, for
3	example, that's an easy way to start thinking about
4	it, what is the desired output state from that
5	processing logic?
6	MR. STATTEL: Yes. I can't
7	MEMBER STETKAR: I hope they do, but if
8	they don't, because the answer you gave me is not
9	necessarily the answer that I'm in other words,
10	if the input signal has failed out of range high,
11	that's a judgment call about whether I want to not
12	initiate aux feedwater or initiate aux feedwater
13	from that channel, because those are the two my
14	two output conditions.
15	So obviously it's a fairly complex
16	system, especially when we're talking about the
17	number of redundancies with the Tricon system. I'm
18	not going to be able to state from memory exactly
19	what the system response is to any particular
20	failure and any particular failure mode.
21	However, I do know, from my experience
22	over the last several years of evaluating this
23	system, I know exactly where I would go to to find
24	the answers for a particular failure.
25	So the first place I would start would

(202) 234-4433

	74
1	be the functional requirements specification, which
2	it has a section that basically describes what the
3	signal validation routines do. So an out of range
4	signal or a high signal that's still within range,
5	for example. Those functional requirements are
6	described in there.
7	Now from there, we have a requirements
8	traceability matrix, and that traces over that
9	will point me over to the implementation documents.
10	Those, for instance, the software description, the
11	software document, SDD, it has a very detailed
12	description of how that functional requirement is
13	met.
14	We have quite a bit of experience. We
15	spent a lot of time during the vendor audits and
16	even time back here in the office of pulling
17	threads on just this type of thing. So we
18	postulate a situation or a scenario for the system
19	and we pull that thread. We go through the
20	functional requirements.
21	We go to the system design description,
22	the software design description and we find out how
23	that's being implemented, and then we actually have
24	in the latter audits, we pull that thread through
25	to the actual tests that are performed to verify

(202) 234-4433

75 that the system responds in that particular manner. 1 2 So it's -- like I said, it's a complex 3 process and there's hundreds and hundreds of states 4 that can be postulated for it. I'm not going to 5 sit here and say that we tested every one of the 6 possible states of the system. However, those 7 functional requirements are well defined. 8 MEMBER STETKAR: But Rich, I'm not 9 talking about the internal, whether I have a Wankel 10 engine or a diesel engine or a gas, you know, The 11 piston engine. internal states are the 12 I'm talking about the fundamental internal states. 13 outputs, from I either get a signal to actuate 14 auxiliary feedwater from Protection Set 1, or I 15 don't get a signal to actuate auxiliary feedwater 16 from Protection Set 1. 17 Ι either signal trip the get а to 18 don't signal trip reactor or Ι get а to the 19 I mean those are my output states. reactor. Those 20 are --21 MR. STATTEL: My point is --22 MEMBER STETKAR: I don't care how I got I care about does the functional -- do the 23 there. 24 functional requirements specify a desired set of 25 safe state conditions from that processing logic?

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	76
1	MR. STATTEL: And my answer is yes.
2	The documentation is in place to find the answers
3	to any particular situation that you can postulate.
4	MEMBER STETKAR: Did the staff review
5	that for the Tricon, because the reason I came
6	across this is there's quite some discussion.
7	(Simultaneous speaking.)
8	MR. STATTEL: I know exactly what
9	you're talking about.
10	MEMBER STETKAR: But I started reading
11	that and I said whoa, wait a minute. I'm seeing
12	this big discussion about ALS. I'm not seeing the
13	comparable discussion on the Tricon platform. In
14	fact, I didn't see any mention of something called
15	default states or safe states or any kind of states
16	for Tricon.
17	MR. STATTEL: Right.
18	MEMBER STETKAR: That's what started me
19	asking.
20	MR. STATTEL: Well, it's a difficult
21	question to answer because of the complexity and
22	the number of redundancies and the number of
23	possible iterations for any particular failure
24	mode. What I will say is the documentation is in
25	place for us to find the answers to any specific

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

S

1

2

3

4

5

6

7

8

scenario that's posed.

I started the discussion by trying to describe the differences between the FPGA and the microprocessor. So in general, when we're dealing microprocessor, we expect it to with а be operating functioning and and executing the software correctly, and the failure is it fails to do that. It stops doing that.

9 So what becomes the fail ___ what 10 happens to the outputs when that occurs? In these 11 systems, the outputs, the functional requirements define where 12 those do outputs qo to in that scenario, in the total fail scenario. 13 For the 14 FPGAs, it's a little bit different because the 15 systems have -- the process, I'm sorry the cores 16 are comparing signals to each other in intermediate 17 states.

18 something called So we have а 19 redundancv checker in the FPGA design. So 20 basically the two cores are comparing calculations 21 on the way. If there's a difference between those, 22 it forces the finite state to be a fixed value, and that's where the other, the alternate discussion 23 24 occurs in the ALS system.

So I don't think it's -- I don't think

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

25

(202) 234-4433

77

	78
1	that there's anything missing from the
2	documentation. I think the documentation trail is
3	all there. I think we spent a little bit more time
4	discussing this in the safety evaluation for the
5	ALS, because it's a little bit less understood
6	phenomenon the way this design works, and how the
7	cores how we ensure that the cores come up with
8	the same answers.
9	So we did spend a little bit more time
10	discussing that phenomenon. So shall I go to ALS
11	now?
12	MEMBER STETKAR: Yeah. I'm writing
13	notes on what you've said. Thanks.
14	MR. HECHT: Can I follow up on that?
15	MR. STATTEL: Sure.
16	MR. HECHT: You said that there were
17	I thought I heard you say that you needed to define
18	those safe states in the event of a miscompare
19	between Core A and Core B.
20	MR. STATTEL: That's correct.
21	MR. HECHT: And then I thought I heard
22	you say something else about you needed to know in
23	general when the algorithms are executed what the
24	safe state needs to be, irrespective of whether
25	there were one or two cores. Are both those

(202) 234-4433

	79
1	statements true or did I misinterpret the second
2	one?
3	In other words let's just say there was
4	both of them agree and for some reason there's
5	some anomaly in the calculation for those, you
6	know, for the containment spray let's just say.
7	MR. STATTEL: Right, okay. So let me
8	try to put this in simple terms. You've got two
9	brains given the same input parameters, deciding on
10	a solution, right.
11	MR. HECHT: In each channel. Right now
12	we're talking about
13	MR. STATTEL: Right, exactly. But
14	let's just keep it simple. So one comes up with
15	one answer, one comes up with another answer and
16	they should be identical.
17	MR. HECHT: Right.
18	MR. STATTEL: Theoretically, they
19	should be identical. If they 're not the same
20	answer, what do you do? Do you pick one, do you
21	pick the other? Do you go to a fail state? What
22	exactly do you do, and that was the question
23	that was the fundamental question that the staff
24	was asking to the licensee.
25	We wanted to understand that with the

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	80
1	ALS system, particularly where we have two we
2	have two sets of cores. We have basically four
3	cores. So now we have four brains coming up with
4	potentially four different answers to the same
5	problem, right. How do I know they're exactly the
6	same? How do they
7	Now with Tricon there's voting that
8	happens. So you calculate it three times. You do
9	a voting and you do you do like a, what is it
10	called, triple mode redundant I think was the
11	terminology they used for Tricon.
12	MR. HECHT: Modular.
13	MR. STATTEL: Triple modular
14	redundancy. So it's basically a voting logic. Now
15	the FPGAs don't work that way, right. So we don't
16	have any voting that's taking place between Core A-
17	1 and Core A-2 logic. What we do have is we have a
18	redundancy checker that's comparing the results of
19	those, and unlike with a microprocessor, you can
20	have slightly different results.
21	With the finite state machines, they
22	are always identical results at the identical time,
23	because they're basically operating synchronously,
24	unlike with microprocessors.
25	So the redundancy checker is what we

(202) 234-4433

81 review efforts 1 concentrated our on, in 2 understanding how that redundancy checker operated, 3 and we wanted to know what the defined states were 4 going to be when we had different answers coming from these four different brains. 5 And that's what -- that's the extensive 6 7 writeup that you're referring to within the safety 8 evaluation. 9 MR. HECHT: And I got that, and I 10 understand that, and I know why --11 MR. STATTEL: Okay, okay. You're 12 looking for the equivalent for Tricon. 13 MR. HECHT: I'm looking for the 14 logically equivalent thought process in the Tricon 15 platform. 16 MR. STATTEL: Understood, yes. 17 MR. HECHT: I know why you pulled all 18 I thought gee, this is really good. that. That's 19 me thinking about backwards for what got the 20 Tricon. 21 MR. STATTEL: Right. Okay. 22 MR. HECHT: I appreciate that parallel 23 or whatever you want to call it. 24 MR. STATTEL: I guess I can take an 25 and maybe I could write a paper assignment and

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

82 explain that in a little more detail of how --1 2 But it's kind of why MEMBER STETKAR: 3 didn't you need something like that on the Tricon? Why didn't you need to do it that way? That way it 4 It's something that -- what I think 5 seems clear. about is we don't postulate common cause failures 6 7 of hardware. So I won't postulate a common cause 8 failure of hardware. 9 But suppose three of my steam generator 10 level signals for some reason or another, because 11 of some stuff all fail out of range high, they're 12 all pegged high, and I mean pegged high, what does the Tricon platform do in that kind of situation? 13 14 Because now I've got -- now I've got several 15 channels affected. I've got all three, you know, 16 three out of four protection sets affected. Does 17 it, you know, what does it do? 18 So it kind of -- it MEMBER BLEY: 19 ought to know this doesn't make sense --20 (Simultaneous speaking.) 21 MEMBER STETKAR: I'm sure it knows it 22 make doesn't I've signals, sense. got input 23 signals that all out of range in are some 24 direction. 25 Okay. I'm going to give MR. STATTEL:

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	83
1	a little logistical explanation for why the
2	writeups are somewhat different. Back when the
3	platforms were reviewed, the Tricon platform was
4	reviewed by Steve Wyman and during that review, he
5	basically established safety conclusions and he did
6	not require any follow-up actions at the
7	application level, right.
8	MEMBER STETKAR: I've got some more
9	questions in the back end of the SCR that I think
10	are
11	(Simultaneous speaking.)
12	MR. STATTEL: In the ALS platform,
13	Bernie Dittman (phonetic) did that evaluation and
14	Bernie put a specific, a specific hook in there.
15	MEMBER STETKAR: Yep, yep.
16	MR. STATTEL: He basically gave me
17	direction when I review the application to make
18	sure that these states are established as part of
19	the design. And that's and it's not an excuse,
20	but it's another reason why the writeups look
21	different, okay.
22	Okay. So the ALS subsystem was
23	designed with two important diversity features
24	considered in our evaluation. They are core
25	diversity and as implemented in the Diablo Canyon

(202) 234-4433

	84
1	application, it generates two redundant logic
2	implementations for placement within each FPGA
3	board for each standardized circuit board.
4	The second form of diversity is
5	embedded sign diversity, and it provides an
6	additional level of diversity. Embedded diversity
7	requires the production of two versions of
8	hardware, descriptive language files for each
9	standardized circuit board. Now the hardware is
10	the same, but basically if you look at the A side
11	of the diagram here, that's developed by the A
12	team.
13	So they have a team of engineers that
14	is developing that, the code that generates this
15	logic, and then a separate code is developed by the
16	B team. So they are diverse.
17	MEMBER STETKAR: Rich, as I always do,
18	I'm going to be a thorn. The A team and the B team
19	all collect paychecks that have a Westinghouse logo
20	on them today?
21	MR. STATTEL: Yes, they do.
22	MEMBER STETKAR: Okay, and those teams,
23	because they all work for the same company, are
24	subject to the same kind of engineering training as
25	they come into the company, sort of guidelines

(202) 234-4433

	85
1	about how we do business?
2	MR. STATTEL: That is true, and for
3	that reason the evaluation team spent a lot of time
4	working with the V&V manager and the V&V management
5	team, because we wanted to understand how the A
6	team was diverse and was coming to different
7	decisions from the B team, right.
8	So they each have a baseball team;
9	neither one can win, right. So there are different
10	ways to do that, they do have different sets of
11	procedures. Rossnyev can speak to this a little
12	bit. We did review those procedures. They are
13	cewrtainly different, we could see that.
14	Now they're basically programming the
15	same boards, right. So there's similarities,
16	right. But they are certainly different. They are
17	different people. They don't have the same person
18	who's on the A team helping out or programming on
19	the B boards.
20	MEMBER STETKAR: Let me ask you this,
21	from kind of a practical implementation. Did you
22	look at the results from these teams and see
23	MR. STATTEL: Okay. One of the
24	questions
25	MEMBER STETKAR: I don't want to say
	NEAL R. GROSS

(202) 234-4433

fundamentally different, because they can't 1 be 2 Fundamentally different --3 And that's one of MR. STATTEL: the 4 questions I had, okay. So in my experience, good 5 engineers think alike and they come up with the 6 same answers the same way. So what is to prevent 7 them from coming up with the identical solution 8 that has the identical problem, right. 9 And so my question to Westinghouse was 10 how do you make sure in the end, you know, you put 11 all these things in place, different procedures, 12 different people. How do you know in the end that 13 the product, the end product is different, right, 14 because theoretically they could come up with the 15 same answer? 16 And the response was they have a V&V 17 activity that they perform, and they actually take 18 implementation and that final logic they put 19 eyeballs on it, and the V&V manager they actually 20 verify that they're different, that they're 21 significantly different from each other. 22 Now we reviewed those. We did take a 23 Α little bit difficult gander at those. to 24 understand the detail but we had them walk us 25 through that, and it was pretty obvious to us that

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

86

	87
1	they were developed in different ways. It was very
2	obvious to us.
3	So we were very insistent. I don't
4	think they may not have had that originally,
5	that idea in mind of verifying the outcome. But we
6	were very insistent and we ensured that they do
7	have that instituted as a V&V activity.
8	MEMBER STETKAR: Good. I mean that to
9	me would be a confidence-builder at least.
10	MR. STATTEL: Yeah.
11	MR. HECHT: Can I ask a
12	MR. STATTEL: Certainly.
13	MR. HECHT:implementation question?
14	As I was looking at that, I realize that there's a
15	distinction between the Core A-1 and A-2 logic.
16	MR. STATTEL: Yes.
17	MR. HECHT: And between the FPGA
18	designs, and does that mean that one's an Actel
19	chip and one is another chip? Is that what Core A-
20	1 and Core A-2 means?
21	MR. STATTEL: No, that's not what they
22	mean. It's essentially they have they use a
23	software tool that basically develops the logic.
24	It does place and route and it develops the logic
25	that gets put onto the FPGA itself. They set the

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	88
1	directive different for the Core 1 and for the Core
2	2.
3	MR. HECHT: I see.
4	MR. STATTEL: Now remember, this is all
5	within the A team that's doing this, right. So the
6	A team has procedures, and those procedures tell
7	them to set the directives one way for Core 1 and a
8	different way for Core 2. So that results in a
9	certain level of diversity, even though it's done
10	by the same team. It's a level of diversity that's
11	achieved just within the A chassis.
12	This was the same concept that was used
13	for Wolf Creek application. Now Wolf Creek didn't
14	have the B chassis. They only did the Core A-1 and
15	A-2 diversity. The other the embedded diversity
16	adds the second chassis to the design.
17	MR. HECHT: Okay. So putting it in
18	other ways, you have the VHDL which is basically
19	written; you have the synthesizer program and you
20	used different directives on the synthesizer
21	program?
22	MR. STATTEL: That's correct.
23	MR. HECHT: Because you really didn't
24	do a complete verification of the synthesizer
25	program, or was this

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	89
1	MR. STATTEL: There was a review of the
2	synthesizer program and some of this gets into
3	detail that is proprietary. So I would kind of
4	hold off there on that discussion. That was not
5	evaluated as part of this application. That was
6	evaluated as part of the ALS platform evaluation.
7	MR. HECHT: I see. So it would be
8	analogous to if I had two ADA (phonetic) compilers
9	like they do on the
10	MR. STATTEL: Well right. So you write
11	code, and let's say you're using C and you write
12	the code, and you have two different compilers and
13	you run it and you set the directives of those
14	compilers differently. So the final binary file
15	that gets put out of the compiler that goes on to
16	the chip, it's going to be different right.
17	So you're basically forcing diversity,
18	not through human diversity, right. You're not
19	developing two sets of code. You're just letting
20	the software tools develop the final binary files
21	in a different way.
22	Move on, so I think I discussed the
23	embedded diversity, so I'll go on to the next
24	slide. This is just really a demonstration. So
25	this figure shows the functional architecture for

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	90
1	the ALS portions of the system. You can see where
2	you have the core logic A and B chassis in each
3	protection set. So that's the eight boxes you see
4	on top, and those provide input directly to the
5	SSPS coincidence voting.
6	This shows the effects of what a logic
7	implementation error or common cause malfunction
8	would look like on the B cores, and you can see you
9	maintained the safety function via the A cores, the
10	diverse A cores. Conversely, this is what a logic
11	A common cause function failure would look like.
12	Okay. Spend a couple of minutes
13	talking about the AMSAC system. The staff did a
14	review and so for the ATWS system, it is
15	implemented at Diablo Canyon via the AMSAC, which
16	is ATWS mitigation system actuation circuitry
17	system, which trips the main turbine, starts
18	auxiliary feedwater.
19	Actually, this goes to a previous
20	question, because you were asking about the
21	initiation of auxiliary feedwater in the case of a
22	Tricon malfunction.
23	MEMBER STETKAR: Right.
24	MR. STATTEL: I wanted to say
25	something, but I decided to hold off. But the
	NEAL R. GROSS

(202) 234-4433

	91
1	AMSAC system does actuate auxiliary feedwater.
2	MEMBER STETKAR: I know that.
3	MR. STATTEL: Okay.
4	MEMBER STETKAR: But in some, and I
5	don't know how the Diablo AMSAC system is wired up.
6	In some plants that I have seen, and I haven't seen
7	theirs, the AMSAC system, if the reactor trip
8	breakers are open, meaning the reactor ought to
9	have tripped, the AMSAC system doesn't exist
10	anymore.
11	It doesn't care, because it's only
12	there for an ATWS, and it doesn't look at, you
13	know, did the rods actually insert into the core.
14	It's off of some auxiliary contacts on the reactor
15	trip breakers basically.
16	MR. STATTEL: Okay, I understand. So
17	there could be a follow up
18	MEMBER STETKAR: There could be a
19	follow-up on that, because if it's only triggered -
20	- in other words, if it's bypassed or taken out of
21	the logic if the reactor trip breakers are open,
22	then I don't see how Tricon I don't see how
23	auxiliary feedwater is actuated given a successful
24	reactor trip and failure of the Tricon.
25	MR. STATTEL: Okay, and again, I think

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	92
1	the documentation is in place. If I had all the
2	documents in front of me I could kind of look at
3	MEMBER STETKAR: I'm sure it is and I
4	didn't
5	(Simultaneous speaking.)
6	MEMBER STETKAR: But two years ago when
7	we had the Subcommittee meeting, we had this
8	discussion and they said oh, AMSAC will initiate
9	it.
10	MR. STATTEL: We postulated very
11	similar situations during our evaluation. So but
12	the purpose of this slide is to just demonstrate
13	what the staff looked at. We were looking to make
14	sure that the new system was going to remain
15	diverse from the existing AMSAC system, right.
16	So this figure shows it. You can see
17	they're completely different systems. They do
18	share a same sensor. However, it's an analog
19	device and it's isolated through a qualified
20	isolation device.
21	And we showed you at the last
22	presentation that there's a whole lot of different
23	aspects of diversity that we looked at, as far as
24	this part of the evaluation, and we found that the
25	AMSAC system, it's really a lot different than what

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	93
1	the new system is. It's very diverse. I'll just
2	leave it at that. It is written up in the safety
3	evaluation if you want to look at the details of
4	that.
5	MEMBER STETKAR: I read it.
6	MR. STATTEL: Okay, okay. A word on
7	manual operator action, okay. So the new system
8	will eliminate the need for manual actions as a
9	means of coping with software or logic
10	implementation CCF within the PPS. However, and
11	the staff made a point of this, the modification
12	does not affect the ability of the operators to
13	perform those manual actions of the safety
14	functions.
15	The existing component and division
16	level actuation capability is being retained, and
17	these capabilities will not be changed as a result
18	of this upgrade. We have spoken with the licensee
19	about potential procedure changes that they will be
20	making, and in these cases, so earlier Myron I
21	believe you postulated, you know, well what if the
22	ALS just fails, right, and you're left with those
23	functions not being performed in spite of the
24	diversity that we've credited here?
25	Well, the real answer to that is the

(202) 234-4433

procedures aren't changing and the procedures right now credit the manual operator actions, and it's been shown that the operators do have the time available to perform those actions. We're talking beyond design basis in this case here, because you know, we've already established that there are diverse cores in play.

8 MR. HECHT: Okay, but I was just 9 relating to that statement that you made about 10 eliminating operator actions.

MR. STATTEL: Well, it's not -- it's not -- the operator action is available and we know the operators can perform that. That's their current licensing basis. It's not credited; it's not required because we know that a common cause failure would not result in the loss of those safety functions.

18 within the design basis of the So 19 don't credit those system, we manual operator 20 actions, after the upgrade. Currently we do.

21 MEMBER STETKAR: Let me, I guess they 22 did what -- they're proposing to do what they're 23 proposing to do. You review what they're proposing 24 to do and I absolutely understand this second 25 bullet and the sub-bullets on this slide. And even

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

11

12

13

14

15

16

17

	95
1	if, you know, ALS can go completely belly up and I
2	don't get the safety injection for a LOCA, the
3	operators can still initiate safety injection. I
4	got it.
5	MR. STATTEL: Correct.
6	MEMBER STETKAR: And we talked about
7	AMSAC and whether or not that actually will
8	initiate auxiliary feedwater for a successful
9	reactor trip. I still can't one that I'll ask
10	you to follow up on, that I've mentioned a couple
11	of times, and that's the main stream line isolation
12	for a steam line break outside containment. There
13	also, the operators I will grant you can manually
14	initiate main steam line isolation, because I
15	assume that the switches to close the MSIVs are
16	hard wired somehow to the MSIVs. Actually it
17	(Simultaneous speaking.)
18	MR. SCHRADER:read on the break.
19	MEMBER STETKAR: It only affects
20	everything that I say only affects that first
21	strong bullet, that it's eliminated operator
22	actions.
23	MR. STATTEL: Right, right.
24	MEMBER STETKAR: And what I'm saying is
25	I don't care if it hasn't eliminated operator

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	96
1	actions, as long as it doesn't preclude those
2	operator actions that are that are, you know,
3	are available today.
4	MR. STATTEL: I hope everyone
5	recognizes that this is an improvement in safety.
6	It's a good thing that the licensee wants to
7	eliminate the reliance on manual operator actions.
8	This is a good thing. They didn't have to do this.
9	There's nothing in the regulations that forces them
10	we cannot have manual operator actions.
11	They currently are licensed and are
12	operating with those manual operator actions in
13	place. They could have done an equivalent system
14	and kept the reliance on those manual operator
15	actions. But we actually want them to make these
16	types of improvements.
17	MEMBER STETKAR: Yeah, and I'm not
18	arguing with that. You know, this is a
19	Subcommittee meeting so I can say I. I think this
20	is a really good thing to do. I just don't the
21	only thing I'm concerned about is either the
22	licensee in this case or the staff in publicly
23	available documents, like safety evaluations,
24	making very specific statements like this
25	eliminates all manual operator actions.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	97
1	MR. STATTEL: I don't think that's
2	actually a true statement.
3	MR. SCHRADER: John this is
4	MEMBER STETKAR: That's the concern
5	that I have.
6	MR. SCHRADER: This is Ken Schrader.
7	So no. This change is not eliminating all operator
8	actions to mitigate accidents. Just for example,
9	steam generator tube rupture has four operator
10	actions. It will still have four operator actions
11	after this upgrade.
12	MEMBER STETKAR: Okay. That's let
13	me be very specific with respect to the first
14	bullet on this slide, that is has an NRC logo on
15	it. "The new Diablo Canyon digital process
16	protection system eliminates," means ain't none,
17	"the need to perform manual operator, as a means of
18	coping with a software common cause failure."
19	MR. STATTEL: Within the PPS.
20	MEMBER STETKAR: Within the and what
21	I'm asking about if it doesn't do that for all
22	types of events through the Tricon platform, you
23	can't make that statement. If the operators have
24	to manually initiate main steam line isolation for
25	a steam line break outside containment

(202) 234-4433

	98
1	MR. STATTEL: I think this is a true
2	statement. Within the context of the PPS, within
3	the context of the postulated failure modes.
4	MEMBER STETKAR: Okay. You gave me
5	something to read. I'll read it.
6	MR. STATTEL: Again, so it refers back
7	to the D3 analysis, which we completed that safety
8	evaluation a while back. But in the original D3
9	analysis, there were only those three functions
10	that required manual operator action.
11	MEMBER STETKAR: I understand that.
12	MR. STATTEL: And all three of those
13	have now been allocated to ALS.
14	MEMBER STETKAR: I understand that, but
15	you may have introduced others that weren't
16	required previously, okay.
17	MR. STATTEL: Okay, all right. Fair
18	enough.
19	CHAIRMAN BROWN: The chairman is going
20	to take control of this meeting back, otherwise we
21	will never leave.
22	MEMBER REMPE: Use your mic.
23	CHAIRMAN BROWN: I'll repeat myself.
24	The chairman, now with the microphone on, will take
25	control of this meeting. We will take a I'm

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

99 going to reduce to a 15 minute break. This is a 1 2 break point. We go into response times next if I'm 3 not mistaken. MR. STATTEL: Could I have one more 4 5 slide? Ιt just has our conclusions, safety conclusions. 6 7 CHAIRMAN BROWN: Oh. I thought we had 8 finished that already. 9 MR. STATTEL: Oh no, that's 10 deterministic --11 VOICES: Yeah. 12 CHAIRMAN BROWN: That's why. 13 MR. STATTEL: Actually, this slide is 14 mislabeled. It's the D3 analysis --15 (Laughter.) 16 CHAIRMAN BROWN: Okay. Do your 17 conclusion. 18 Okay. These are the key MR. STATTEL: 19 safety conclusions that the staff reached for diversity defense indepth. That's all I have to 20 21 say. 22 (Laughter.) CHAIRMAN BROWN: We will now recess for 23 ten minutes slash fifteen. 24 25 (Whereupon, the above-entitled matter

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

	100
1	went off the record at 3:02 p.m. and resumed at
2	3:15 p.m.)
3	CHAIRMAN BROWN: I will call the
4	meeting back into order. Richard?
5	MR. STATTEL: Okay, our next topic is
6	System Time Response and Deterministic Performance.
7	Our standard review plan guidance advises the
8	evaluation should confirm the system's real time
9	performance characteristics are deterministic and
10	known.
11	Our Branch Technical Position 7-21
12	discusses design practices to be avoided for
13	computer-based systems. These practices include
14	non-deterministic data communications,
15	non-deterministic computations, interrupts,
16	multitasking, dynamic scheduling, and event driven
17	design.
18	Each of the platform evaluations
19	concluded that there are application specific
20	parameters which could influence the system's
21	ability to perform in a deterministic manner. The
22	staff therefore, this staff therefore reevaluated
23	deterministic behavior characteristics for each of
24	the subsystems within the context of the Diablo
25	Canyon application.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	101
1	So for ALS, the ALS platform of course
2	is a FPGA based design, and it does not embed
3	microprocessor cores or use interrupts. The staff
4	has confirmed that the application of the ALS
5	platform operates on fixed cycles where a
6	deterministic sequence of one, acquire inputs, two,
7	perform logic operations such as compare processed
8	variables against a trip set point to determine
9	partial trip status, and three, generate output
10	signals, is followed without the use of a
11	microprocessor core or interrupts. This is
12	consistent with the ALS platform approved topical
13	report.
14	I might point out that the FPGA
15	technology has evolved somewhat in recent years,
16	and there are versions of FPGAs that actually do -
17	they're kind of hybrids and they do microprocessor
18	type functions, but the ALS system is not one of
19	those systems, so that's another thing that we
20	confirmed.
21	The staff evaluated the deterministic
22	performance characteristics of the ALS during our
23	evaluations. There are parameters which are
24	application specific and required additional
25	evaluation. In this case, only the ALS 102 core

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	102
1	logic boards were subject to application specific
2	response time performance and deterministic
3	behavior variations. So there are, I believe,
4	seven circuit boards that are part of the ALS
5	platform. One would be like an analog input board
6	for example.
7	Most of those boards - well, six of the
8	seven boards are not application specific. You
9	simply, if you're going to take analog inputs, you
10	use an analog input board. The seventh board is
11	the application specific board, and that's where
12	all of the Diablo Canyon specific application logic
13	is developed, so that's the board that we
14	concentrated our review on.
15	Now, the other boards do have response
16	time and I'll explain how we considered that. So,
17	next slide? So there are two timing parameters
18	that are used to establish deterministic
19	performance of the ALS subsystem. They are access
20	time and frame time. The definitions are given
21	here.
22	Although the ALS platform establishes
23	fixed board access time, other aspects, including
24	the number of times a board is accessed per frame,
25	the number of boards accessed per frame, the

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	103
1	sequence of board accesses per frame, and the frame
2	time itself are determined using application
3	specific design - they're done during the design
4	phase, during the development of the design.
5	All of these design aspects established
6	a fixed interval for each safety function
7	performed. The NRC staff evaluated these
8	application specific attributes for Diablo Canyon
9	design and found them to be acceptable and within
10	the established system performance criteria for
11	response time. The results of this evaluation are
12	documented in Sections 3.17 of the safety
13	evaluation report.
14	Now, the Tricon system, the triple
15	redundant architecture is designed so that input
16	processing, application function performance, and
17	output signal processing are performed by redundant
18	sets of components operating in parallel to provide
19	highly reliable safety functions.
20	The Tricon uses a custom system
21	executive to run the processor card and host the
22	safety application, in this case the PPS
23	application. A system executive is an operating
24	system used to cyclically run a predetermined list
25	of tasks.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

Tricon has three prioritized tasks controlled by three prioritized interrupts. There are no event driven interrupts in this system. So every microprocessor uses interrupts, but in this for this particular design, there case, are on event driven interrupts.

The scan structure guarantees that this Tricon scan cycle is predictable and repeatable from one scan to the next. The background task always runs, but it is the lowest priority task. Every - periodically, the communication interrupt is asserted to kick off the communication task.

communication task 13 The is a higher priority and it runs for a fixed amount of time, then the background task is allowed to run again. 15 16 The background and communication tasks cycle back and forth like this until it is time to start the 18 next scan.

19 The start scan interrupt is asserted to start the next scan cycle. The scan task is the 20 21 highest priority task and can only be interrupted 22 the watch dog, and it contains all of the bv 23 functions that are critical to the safety function. 24 In order, it resets the watch dog timer. It reads 25 fresh inputs. It runs the algorithm and writes the

> **NEAL R. GROSS** COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

8

9

10

11

12

14

17

outputs, then determines when to start the next scan cycle. That's the end of the scan's task.

When the scan task ends, functionality back to the cycling communication reverts and Deterministic background tasks. behavior is assured through synchronizing of application scans which guarantees a new set of inputs and a new set of outputs for the IO modules are established during every application scan in each of the separate processors.

Okay, like the ALS platform, the Tricon characteristics dependent performance are on 13 application specific design. As part of the development process, a timing analysis calculation 15 application program is performed after the is 16 written to determine what the expected execution times will be for the application.

18 The input variables for the calculation 19 include the number of input and output parameters 20 used by the application, the number and types of 21 function blocks that are used in the application, 22 and the architecture of the designed system.

23 An example of this was we mentioned the 24 use of the RXM chassis which is, again, we said it 25 was in the same room. It's in the cable spreading

> **NEAL R. GROSS** COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

8

9

10

11

12

14

17

(202) 234-4433

105

	106
1	room, but that's a chassis that processes
2	non-safety related input and output. Using that
3	takes a little bit more time for the application to
4	execute the necessary software.
5	So in other words, the more things that
6	your application is doing, the more complicated the
7	application, the more calculation intensive it is,
8	the more time - the more basic time it's going to
9	take to execute. It's just a fact of life.
10	CHAIRMAN BROWN: I'm sorry, let me try
11	to phrase this.
12	MR. STATTEL: Okay.
13	CHAIRMAN BROWN: When you started off,
14	you talked about background, a background
15	processing, a communication processing of some
16	sort, and then the scan time, and what I'm trying
17	to do is put this into the term of reference of an
18	overall operating cycle period.
19	And from my past experience, we had
20	something. I didn't call it the same, but there
21	was - you read inputs, this part of your scan.
22	MR. STATTEL: Right.
23	CHAIRMAN BROWN: You perform the
24	application, then you had a period of time with
25	miscellaneous tasks being performed that - you can

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433
	107
1	call them background tasks, self-diagnostic tasks,
2	etcetera, and then you had to transmit data out,
3	and that overall period established what we
4	referred to as the overall cycle time.
5	MR. STATTEL: Yes, that's the base time
6	of your system.
7	CHAIRMAN BROWN: Yeah, but -
8	MR. STATTEL: This is similar.
9	CHAIRMAN BROWN: But it incorporates
10	all of those things you talked about.
11	MR. STATTEL: Right.
12	CHAIRMAN BROWN: So the scan time, the
13	more functions you had to accomplish during the
14	scan time, and in our times the taking data, doing
15	your algorithms, generating some output but still
16	having - that might take more or less time during
17	any cycle depending on what functions you were
18	executing during that cycle, that overall cycle, so
19	background could be less.
20	MR. STATTEL: So in general, you're
21	describing what's performed by the scan task.
22	What's different here, and the reason why I
23	broadened this discussion a little bit to include
24	the background task and the communication task, is
25	in this particular design, those tasks are not

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	108
1	performed as part of the scan task, okay?
2	CHAIRMAN BROWN: And that's what I was
3	trying to get to.
4	MR. STATTEL: They're separate tasks.
5	So the background tasks, the diagnostic functions,
6	things like that, they're not - they're really -
7	they segregate them. And this was just a design
8	decision that was made by Tricon way back when,
9	when the system was developed, so that's why my
10	discussion has to be a little bit broader than what
11	you're discussing. However, these are the three
12	fundamental tasks that are run by - within the
13	operating system.
14	CHAIRMAN BROWN: Okay, let me expand my
15	- or at least move on with my - so the scan - what
16	I'm - so if the scan - you're saying what I've
17	talked about encompasses your scan section?
18	MR. STATTEL: And the communication
19	too, I would say.
20	CHAIRMAN BROWN: Okay, all right, scan
21	and communication, right?
22	MR. STATTEL: Right.
23	CHAIRMAN BROWN: The background is kind
24	of formulating along over here.
25	MR. STATTEL: Right.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	109
1	CHAIRMAN BROWN: Is the scan period run
2	at the exact same frequency throughout operation or
3	can it be delayed because of this executive sitting
4	over here deciding, "Oh, I don't want to run the
5	application. I don't want to run that scan right
6	now because I am doing some important/non-important
7	stuff"?
8	MR. STATTEL: Right.
9	CHAIRMAN BROWN: "And so instead of
10	repeating this every 100 milliseconds, I'm going to
11	save it for 150 or 175, and I'm just going to live
12	with the result."
13	MR. STATTEL: So the answer to that
14	question is I described what the scan task
15	performs, and the last thing it does, it determines
16	when to start the next scan task, okay? So the
17	scan task, once the application is developed, it's
18	very predictable what the scan time is going to be.
19	That's a result of a calculation. We have reviewed
20	those calculations. We know what the application
21	is doing. We can predict what the scan time is
22	going to be.
23	Now, we don't set the cycle time for
24	this system to be equal to the scan time, and we
25	don't let the system run as fast as it can, okay?

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

110 Because it could, theoretically, run at the program 1 2 scan time, but then there would be some variation 3 depending on various things. So instead of doing that, we calculate 4 5 what the program scan time is. We specify а response - well, we know what we are required to 6 7 perform, what our required time response is, and we 8 this program scan time to be shorter than set 9 what's required, so it's going to be faster - it's 10 going to operate faster than what's required, but 11 it's going to be slower than what it's capable of 12 doing. 13 So it's very - the answer to your 14 question is yes, it's very predictable. It's a 15 fixed scan time, and it's determined during system 16 development. 17 CHAIRMAN BROWN: Okay, but my -18 MR. STATTEL: So when we started this 19 review, we didn't know what that time, what those 20 numbers were going to be. 21 CHAIRMAN BROWN: I understand that. 22 MR. STATTEL: Okay. 23 CHAIRMAN BROWN: That's not a problem. 24 That's - you have to deal with that with every 25 system you develop.

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	111
1	MR. STATTEL: Right.
2	CHAIRMAN BROWN: My question is -
3	MR. STATTEL: Different platforms work
4	on different cycles and different conduct.
5	CHAIRMAN BROWN: My question is does
6	the scan time run within a fixed cycle every -
7	MR. STATTEL: Yes, it does.
8	CHAIRMAN BROWN: So I mean, I can say
9	here is time zero. At some point 200 milliseconds
10	later, the scan time will be run. 200 milliseconds
11	later, it will be run again. 200 milliseconds -
12	MR. STATTEL: That's right.
13	CHAIRMAN BROWN: Regardless of what
14	happened, where your background communication scan
15	- application code, it always runs with a fixed
16	cycle time?
17	MR. STATTEL: That is correct.
18	CHAIRMAN BROWN: And that cycle time
19	cannot be interrupted by the executive?
20	MR. STATTEL: It can only be
21	interrupted by the watch dog.
22	CHAIRMAN BROWN: That's - in - and
23	that's in the scan time. That's in the scan frame
24	_
25	MR. STATTEL: Right.
	NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	112
1	CHAIRMAN BROWN: - time period?
2	MR. STATTEL: Correct.
3	CHAIRMAN BROWN: Okay, next question,
4	and I may have asked this at the previous meeting.
5	I just don't remember. When you develop your
6	overall needed response time, not what the
7	processors can do, but your needed from your action
8	and analysis, is it considered that a sensor signal
9	output that would generate a trip doesn't get into
10	the - its data is not read until immediately after
11	that cycle occurs so that you have to go through
12	two cycles effectively, okay, in order to generate
13	the required trip?
14	MR. STATTEL: Yes, it does.
15	CHAIRMAN BROWN: Because I didn't see
16	that in any of the documentation.
17	MR. STATTEL: It is in some of the
18	supporting documents that were provided.
19	CHAIRMAN BROWN: Yeah, I didn't have
20	them, so -
21	MR. STATTEL: The references are in
22	there. They did some conversation assumptions, and
23	in some cases - as a matter of fact, with this
24	particular application, they ended up lengthening
25	the program scam time. The vendor lengthened the

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	113
1	program scan time because of - some things would
2	require two cycles to complete the execution,
3	right, to complete - to ensure that we had a fresh
4	set of data every - during every cycle.
5	CHAIRMAN BROWN: Let me rephrase this
6	slightly. Since the systems I dealt with is a
7	little bit - they ran a little on a different
8	format -
9	MR. STATTEL: Sure.
10	CHAIRMAN BROWN: - than you talk about,
11	what we assumed was a cycle time started, and
12	momentarily after that, all of the stuff it read
13	changed. Now I've got data -
14	MR. STATTEL: It would miss that.
15	CHAIRMAN BROWN: You missed it?
16	MR. STATTEL: Right.
17	CHAIRMAN BROWN: So it runs through its
18	150 or 50 millisecond cycle, whatever cycle you're
19	running at, and it generates no trip?
20	MR. STATTEL: Right.
21	CHAIRMAN BROWN: And then it comes back
22	and, ooh, my God, I now have a low pressure. I've
23	got a high temperature, and dang, I get multiple
24	trip signals, then I run it. Now I actually
25	generate my trip signals after that period. And is

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	114
1	that - my only point being is that - all of that
2	should occur and should have been factored into
3	that overall cycle time within which all of this
4	other stuff you're talking about, the backgrounds,
5	the communications, the scan time, and everything
6	else fits? I was just looking for fixed cycle time
7	and -
8	MR. STATTEL: Really this comes down to
9	some conversation assumptions that are made when
10	the calculations are performed, and in some cases
11	it's assumed, just like you said, it's assumed that
12	we just missed that input, so we're going to have
13	to wait a second cycle in order to ensure that that
14	trip occurs within that. And that really comes
15	down to what's shown on the diagram here, and I'll
16	preface this. The diagram is not shown to scale in
17	any way, okay?
18	CHAIRMAN BROWN: That's obvious.
19	MR. STATTEL: So the calculation
20	results in basically that calculated response time,
21	and theoretically that's what we would expect that
22	system to operate at, at that calculated response
23	time if you were to just let it run free, let it
24	run free. However, it doesn't - if
25	you were to run it that way and you were to program

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	115
1	your scan time at that, it would not guarantee that
2	that trip would occur, or the right calculation -
3	the complete set of calculations would occur on
4	every program cycle.
5	So to ensure that happens, we set a
6	program scan time which is a greater time than what
7	the system is capable of, right? And it's a
8	significant amount of time greater than what the
9	system is capable of.
10	Now, we step back. The way we - the
11	staff performs our evaluation, we then step back
12	and we really want to know what the system needs to
13	do as far as response time, and we looked to the
14	accident analysis for this.
15	Now, the accident analysis, it tells
16	you times, and oftentimes it's like start - the
17	safety injection pump has to pump water within 20
18	seconds of this parameter exceeding this value.
19	Generally, they're a lot longer times than the
20	cycle times we're talking about with these types of
21	processors. So we start with the accident analysis
22	required response. Now, that response,
23	the system, the PPS system really is only a portion
24	of that. Some of it is going to be the timing of
25	the breaker that starts the safety injection pump.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	116
1	Some of it's going to be just the time it takes for
2	the pump to get up to speed. So there's a lot of
3	other variables that come into the assumed response
4	times than from the accident analysis.
5	Now, with a system like the process
6	protection system, we have a really good starting
7	point because we have the Eagle 21. We know what
8	its required time response was, and it's a licensed
9	system. It's operating. So we could have just
10	said, "Oh, well, it's at least as fast as the Eagle
11	21, therefore we know it's within their licensing
12	basis." However, I was not satisfied
13	with that because I wanted to see how it - how it
14	played out with respect to the accident analysis
15	time response. So I went back to the FSAR. I
16	looked at the accident analysis. And for each of
17	these functions, I confirmed that the allocation,
18	you know, the time required just for the PPS was
19	reasonable with respect to what was being specified
20	within the functional requirement specification for
21	the PPS system.
22	So you can see the green line. That's
23	what you're going to see in the functional
24	requirement specification is the green line. What
25	the system is actually performing at, what we

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	117
1	program it to perform at is the blue line below
2	that, the program scan time. And I would ignore
3	the pink line because that's just the theoretical
4	fastest time that this thing can cycle, but there's
5	no guarantee that it will perform all of the
6	required safety functions in that amount of time.
7	Now, the accident analysis time
8	response, the top line there, the purple line,
9	really that's just the portion that's allocated for
10	the PPS. So if there was 15 seconds to get a
11	safety injection pump pumping water, there might
12	be, you know, a 500 millisecond allocation of that
13	15 seconds to the PPS, and that's the number I'm
14	verifying there, okay? So that's essentially what
15	we validated for the PPS system. So -
16	CHAIRMAN BROWN: Just restate to make
17	me feel comfortable then. This scan time that does
18	all of your algorithms and calculations is on a
19	fixed cycle?
20	MR. STATTEL: Yes, it is.
21	CHAIRMAN BROWN: Okay.
22	MR. STATTEL: And we do know the
23	number.
24	CHAIRMAN BROWN: And that fixed cycle
25	is satisfactory to always ensure that you capture
	NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. (202) 234-4433 WASHINGTON, D.C. 20005-3701 (202) 234-4433

	118
1	data appropriately and can generate a trip within
2	the accident analysis time response or the PPS
3	specified time allocation?
4	MR. STATTEL: Yeah, and we do know
5	those numbers. They are - I believe they're in the
6	safety evaluation, and we also reviewed the factory
7	acceptance test results, so we satisfied ourselves
8	that they are actually performing to that
9	specification.
10	CHAIRMAN BROWN: All right, thank you.
11	MR. STATTEL: So just in summary on
12	this slide, the calculated response is what the
13	system is theoretically capable of doing. The
14	program scan time is the cycle time set for the
15	application. If someone makes a decision, this is
16	what the cycle time is going to be. And the
17	specified response time allocation is the response
18	time the system is guaranteed to meet.
19	Now, this diagram, I know you had had
20	some comments on this before, Charlie, because
21	you're looking for this type of circuit on an
22	architectural diagram, right? So in response to
23	your comment, I drew this up real quick and it's
24	really just a picture from my talking points just
25	to understand that. It's not any specific design.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

119 So failure 1 to perform 2 deterministically, so this was another aspect of 3 the PPS system that we were concerned about. So 4 both the ALS and the Tricon platforms include 5 features to detect and monitor the system's 6 performance during operation, and to initiate 7 alarms if either system fails to perform 8 deterministically and within the required time 9 frame. 10 So the platform designs include the use of watch dog timer functions to detect conditions 11 12 would affect the deterministic performance that 13 characteristics of the system. These features are 14 specified at the generic platform level of the 15 design, and therefore are not dependent on any 16 application specific design, so it's built into the 17 platform. 18 licensee, So the PG&E, when they 19 decided to use this platform, that's just the -20 it's basically a feature that comes with that. 21 It was evaluated by the staff when they platform. 22 performed that platform evaluation. 23 So because these monitoring functions 24 are included as the inherent part of the platform 25 they are not part of the application designs,

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	120
1	software or logic in either one of these platforms.
2	They are therefore independent of the system
3	architecture, so that's why we don't see them on
4	the system's architecture diagram.
5	CHAIRMAN BROWN: They are software
6	based though?
7	MR. STATTEL: No, they are not.
8	CHAIRMAN BROWN: They are hardware
9	based, and you said yes?
10	MR. STATTEL: Yes, they are hardware
11	based. Now, okay, I'll leave it at that. So based
12	on a specification analysis - specifications,
13	analysis, deterministic performance
14	characteristics, and the system response time
15	performance test results, the NRC determined that
16	the PPS system meets all of the requirements for
17	safety system response time performance. This is
18	the safety conclusion reached by the staff. Any
19	other questions on diversity, or deterministic
20	performance, or time response?
21	Okay, next, the next topic will be
22	independence and Rossnyev will present that.
23	MS. ALVARADO: Okay, my name os
24	Rossnyev Alvarado. I was responsible for reviewing
25	the independence and system communication for

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	121
1	Diablo Canyon. This is a slide that you can see
2	now. It pretty much lists the guidance that we
3	have to evaluate system communication, and that's
4	the guidance that I used for my evaluation.
5	This drawing that we have represents
6	the system communication architecture for our
7	protection set. It's the same communication
8	architecture for each protection set. As mentioned
9	before, the Tricon and the ALS do not communicate
10	with each other. I know in the drawing it looks
11	like they communicate on the left, the red squares,
12	but I tried to draw that purple line to separate
13	them because they are not connected.
14	The green - the red line that you see -
15	I'm sorry, sorry, wrong line. The red line shows
16	the separation between each protection set. The
17	green line that you see to the left of the red
18	squares shows an analog signal that is processed in
19	the ALS and is used in the Tricon system to perform
20	our power differential temperature and other
21	temperature differential temperature reactor trip
22	safety function.
23	Within each protection set, again we're
24	talking about the red line, the PPS incorporates
25	safety to non-safety communications with the plant

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

computer system which you can see on the bottom right, the maintenance work station which I drew as - just two squares to the right, and the Tricon remote RXM non-safety tasks which is not shown on this side.

6 MEMBER STETKAR: Rossnyev, before we 7 get into too much details on the communication, I 8 wanted to wait until we get to this slide. The 9 temperature signals that come out of ALS and go 10 into Tricon, everybody mentions the, whatever it 11 is, over power delta T and over temperature delta T 12 Those signals are actually trip signals. 13 used for other things though, aren't they? Don't 14 they generate the T av, average temperature signal that's used for main feed water isolation? 15 And 16 also I found a reference to a delta T signal that 17 was used as a surrogate for reactor power for some 18 protection signal interlock, so it's not only those 19 two trip functions.

20 MS. ALVARADO: Right, I was just trying 21 to show that there is no communication between the 22 ALS and the Tricon, but I wanted to show the ALS is 23 processing that analog signal and sending it to the 24 Tricon.

MEMBER STETKAR: I know, but -

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

25

1

2

3

4

5

	123
1	MS. ALVARADO: But yes, you're right.
2	MEMBER STETKAR: I just wanted to make
3	sure you thought about those other functions.
4	MS. ALVARADO: Yes, those were like
5	examples.
6	MEMBER STETKAR: Okay, thank you.
7	MR. STATTEL: I'll just throw something
8	in here because those functions that rely on the
9	temperature signals, they require processing by
10	both the ALS and the Tricon.
11	MEMBER STETKAR: When you did your
12	timing and your -
13	MR. STATTEL: The timing analysis.
14	MEMBER STETKAR: I know, I read that
15	and that was good.
16	MR. STATTEL: Okay.
17	MEMBER STETKAR: No, I read that.
18	MS. ALVARADO: We evaluated these
19	communications from safety to non-safety and
20	confirmed they met the guidance provided in ISG-04.
21	Both the Tricon and ALS communicate data to the
22	plant computer system. The plant computer system
23	is part of the existing system, and was not part of
24	the scope for this amendment.
25	Communication with the plant computer

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	124
1	system is one way. The Tricon transferred this
2	data through the port aggregator tap which I'm
3	going to discuss later, and the ALS does it through
4	the transmit TXB communication port.
5	Even though this is not shown in this
6	slide, there are other plant data information that
7	will be provided in the main control room for
8	indication. This data will be provided through
9	hard wired direct connection.
10	MR. HECHT: Rossnyev?
11	MS. ALVARADO: Yes?
12	MR. HECHT: I'm sorry.
13	MS. ALVARADO: That's okay.
14	MR. HECHT: I had asked the question
15	earlier during the PG&E presentation about the
16	ethernet connection to the non-safety systems, and
17	that's shown here in the top line through the
18	maintenance work station, to the port aggregator
19	tap, to the media convertor, to the fiberoptic
20	cable.
21	And the statement was made that there
22	is a card actually within the Tricon that's
23	involved in doing the hand shaking. It's kind of a
24	buffer card. Have you done any tests - or not have
25	you. Have you required testing of what happens

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	125
1	when that buffer card is overflowed?
2	MS. ALVARADO: Yes, you're talking
3	about the TCM card. This is the card in between
4	that is separating the maintenance work station
5	from the Tricon. This was evaluated during the
6	Tricon safety evaluation of the topical report and
7	they did tests. They also did tests during Diablo
8	Canyon when they did the factory acceptance tests
9	to confirm that if this card, the TCM card fails,
10	the Tricon continues to operate, so the Tricon will
11	continue to operate if the TCM card fails, yes.
12	MR. HECHT: Well, it's a fail silent
13	thing. It's just the fail -
14	MS. ALVARADO: In communications.
15	MR. HECHT: Well, the issue is that
16	there is a buffer - I mean, there is some hand
17	shaking going on -
18	MS. ALVARADO: Right.
19	MR. HECHT: - across the ethernet
20	connection, and if for some reason the receiver is
21	a little bit slow and the data is accumulating
22	within the Tricon, the Tricon is basically going to
23	dump the bits on the floor or something like that.
24	It's not going to keep them and wait and stop the
25	rest of the processing.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	126
1	MS. ALVARADO: Well, they have the
2	DPRAM, the dual ported access memory, that they are
3	using for collecting data coming from the outside,
4	and keeping it, and using buffers. But if I - I
5	think that would provide other information if I
6	went into detail to explain how the buffers work.
7	MR. HECHT: Well, I guess the question,
8	just to follow up, is if that dual ported memory
9	gets filled -
10	MS. ALVARADO: Right.
11	MR. HECHT: - nothing bad happens to
12	the Tricon?
13	MS. ALVARADO: No.
14	MR. HECHT: It continues operating?
15	MS. ALVARADO: Exactly, exactly.
16	MR. HECHT: That data gets overwritten?
17	MS. ALVARADO: Yes.
18	MR. HECHT: Okay, thank you.
19	MS. ALVARADO: Okay, on the right side,
20	you can see the maintenance work station shows as
21	the maintenance work station for the Tricon and one
22	for the ALS. The maintenance work station are
23	separated and they cannot communicate with each
24	other. Also, the maintenance work stations cannot
25	communicate with maintenance work stations in other

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

The 1 protection sets. maintenance work 2 stations are stand-alone computers that do not 3 connect to the internet, or with the plant computer system, or with the plant network. 4 To use the 5 maintenance work station, Diablo Canyon is going to use a KVM switch to provide access to a keyboard, 6 7 displays, and mouse for the authorized video 8 personnel to perform maintenance and calibration 9 activities. Only one KVM will be used for each 10 protection set. This will be located inside a 11 cabinet, and it will have administrative procedures 12 to access the cabinet. 13 This slide is a carton representation 14 made with the communication for the ALS that I 15 It's the same communication for all of the system. 16 Ι mentioned before, there ALS. As are no 17 communications between the protection set in the 18 ALS portion, so the ALS in protection set one does 19 not communicate with ALS in protection set two. 20 communication with For one way the 21 maintenance work station and the plant computer 22 system, the ALS uses the transmit information to the TXB ports. 23 You can see there is a TXB one and 24 TXB two for each one of the ALS. The ALS subsystem 25 does not require a port tap device to enforce one

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

127

	128
1	way communication to the plant computer system.
2	Instead, constant communications for
3	the TXB ports, as I mentioned before, are
4	configured to only transit data through these
5	connections. Communication for the TXB port is
6	unit directional and doesn't require the use of
7	hand shaking signals. They are physically and
8	electrically incapable of receiving information
9	from external sources.
10	CHAIRMAN BROWN: Rossnyev, isn't that
11	because there's a, I don't want to call it a
12	jumper, but there's a hard wired connection where
13	you don't use this terminated in some form?
14	MR. STATTEL: The circuitry doesn't
15	exist.
16	CHAIRMAN BROWN: That's what I thought
17	I remembered from the previous information I read
18	in your SCR, that it's like an open circuit. Okay,
19	that hasn't changed.
20	MS. ALVARADO: Right, no. We confirm
21	it, and actually I even reviewed the code for this
22	communication. For testing the maintenance of the
23	ALS, Diablo Canyon will use the Test ALS Bus, or
24	TAB, which you can see on the right on top, that is
25	to connect to the maintenance work station. This

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	129
1	TAB will provide two-way communication for
2	maintenance activities.
3	Normally the TAB is physically
4	disconnected from the ALS system. When maintenance
5	and calibration is required, the Diablo Canyon
6	operator will use the TAB and connect to only one
7	of the cores. This will be physically connected to
8	the ALS, and a digital input signal will be active
9	allowing two-way communications between the ALS
10	maintenance work station and one of the ALS core.
11	There is no software associated with
12	connecting or disconnecting this data link. That
13	connection is provided for each core, as I
14	mentioned before. Only one core can be connected
15	to the maintenance work station at a time. This
16	will be a procedure requirement for Diablo Canyon.
17	The diverse ALS subsystem connected to
18	the TAB will be taken out of service with the
19	exception of the RTB signals processing function.
20	These are the temperature signals that we talk
21	about, which will remain operable during specified
22	surveillance tests performed on other ALS
23	functions.
24	The diverse ALS subsystem whose TAB has
25	not been enabled will continue to perform its

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

safety function without impact. Whenever the TAB
is connected to the ALS and the maintenance work
station, an alarm will be annunciated in the main
annunciated system.

Then in this next slide, I'm showing the communication architecture for the Tricon. This is the same communication architecture for the Tricon in other protection systems. Again, as I said, there is no communication between the Tricon portions of the PPS.

All of the Tricon communication with 11 12 devices is the Tricon external communication 13 module, the TCM, and the Tricon RXM. The TCM I 14 didn't put it, but it's inside the Tricon box, but 15 you can see the primary RXM on the drawing. The 16 TCM allows the Tricon to communicate with the 17 maintenance work station through а dedicated You can see it in 18 one-way port aggregator tab. 19 this slide. It's the port tab in purple.

I will talk about the port tab on the next slide, but let me continue with the TCM. As I was asked before, the TCM uses a cyclic redundancy check, hand shaking, and protocol-based functions to ensure data communication integrity. This is a proprietary protocol that they use, so it's no -

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

5

6

7

8

9

10

131 you were asking me if it was TCP/IP, and it's a propriety protocol that they developed, yes. In addition, the Tricon uses dedicated memory allocations for communication. In this manner, there is no direct communication between application processor and the TCM interface that interfaces with the maintenance work station. you lose the TCM, the main processor would continue to function. The TCM handles all communication with external devices, and it has been qualified under the Appendix B program for nuclear application. The Tricon also incorporates a safety

14 related to non-safety related communication link via a RXM chassis. The purpose of this chassis is 15 16 acquire and transfer IO non-safety related to 17 signals to support functions that are not safety 18 related to the PPS functions. Such signals go to 19 control board, to the main control the board 20 indicators.

21 This represents an expansion chassis to 22 located - that can be located several miles be 23 But like Rich explained, this is inside the away. 24 - in the control room. There is no data exchanged 25 between the RXM chassis and other protection sets.

> **NEAL R. GROSS** COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

8

9

10

11

12

13

the

If

The use of the RXM communication was described in the Tricon platform topical report and the staff approved these. The only application specific action item was for the staff to confirm that all data received from non-safety mode RXMs must not be relied to perform the required safety function, and we confirmed that there were no signals coming to be used for safety functions through the RXM.

10 MR. HECHT: Rossnyev, I know this is a 11 simple block diagram, but you have two-way 12 communication indicated on that block diagram. Is that true? 13

14 MS. ALVARADO: Well, okay, I will try 15 to explain this and try not to get into proprietary 16 information, but, yes, because what happened is 17 between the primary and the remote RXM, it's like a 18 master/slave communication, so what happened is 19 like they have separate communication lines.

So when the primary sends a request to the remote RXM, it has to go through the line to request, and when the remote is sending back the data, the IO data that is collected, it has to send it through a separate line. That is why there is two-way communication. It's just for the command

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

8

9

	133
1	signal to go there.
2	MR. HECHT: So I guess my same
3	question, between the Tricon and the primary RXM,
4	if the remote RXM gets busy and the primary RXM
5	fills up, is there - what happens to the Tricon?
6	MS. ALVARADO: The Tricon will continue
7	to operate. And remember, the RXM is not using any
8	IO signals for safety functions, so it doesn't
9	really matter. It's just indication.
10	MR. HECHT: How do they -
11	MS. ALVARADO: But yes, the Tricon will
12	continue to function. It would just fail.
13	MR. HECHT: How does the Tricon
14	communicate with the RXM?
15	MS. ALVARADO: It's a protocol
16	communication that I have. It's called IO Com.
17	It's in the safety report.
18	MR. HECHT: I see.
19	MS. ALVARADO: Yes.
20	CHAIRMAN BROWN: You commented that the
21	Tricon primary RXM does not perform any safety, but
22	in the PG&E system description figure 4.5, there is
23	- it says, "Tricon primary XM chassis," and it's
24	got a number of inputs and it shows, "trips to SSPS
25	discrete," and so I'm a little curious.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	134
1	MR. STATTEL: Can you tell me where
2	you're referring to?
3	CHAIRMAN BROWN: Figure 4-5 of the
4	enclosure to PG&E letter DCL 13-043, which was the
5	supplement to license amendment request 1107,
6	process protection system replacement which was a
7	fairly large system description.
8	MS. ALVARADO: Yes, the remote one.
9	CHAIRMAN BROWN: No, this is not the
10	remote. This is the primary.
11	MS. ALVARADO: Yes, the primary is
12	safety related.
13	CHAIRMAN BROWN: Okay.
14	MS. ALVARADO: The remote is the one
15	that is not safety related.
16	CHAIRMAN BROWN: Okay, all right.
17	MS. ALVARADO: Yes.
18	CHAIRMAN BROWN: I misunderstood what
19	you said then. I apologize for that.
20	MS. ALVARADO: No, that's fine. The
21	remote is the one that we're using for IO signal.
22	CHAIRMAN BROWN: I understand that, and
23	that shows on this chart only one-way
24	communications from primary to the remote, whereas
25	your diagram shows bidirectional.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	135
1	MS. ALVARADO: Because, like I said,
2	it's just the way they communicate to request the
3	signal as the master and the slave is configured,
4	the way they have it configured for the Tricon.
5	CHAIRMAN BROWN: That's a little bit
6	above my -
7	MR. STATTEL: We show this on this
8	figure as a communication link, but in reality, the
9	RXM is really just a remote extension chassis.
10	That was the purpose of it. It was designed for
11	that. When the platform - when Tricon submitted
12	their platform application, they thought that this
13	remote extension chassis could be used as an
14	isolation barrier for non-safety related - between
15	safety and non-safety related.
16	So because of that, I mean, it really
17	wasn't designed for that, but because of that, we
18	performed a pretty extensive evaluation during
19	that. I went to the vendor. I reviewed the actual
20	coding that's involved with the bus protocols.
21	There is actually circuitry involved.
22	It is very propriety so I can't get
23	into a lot of the details, but that was - all of
24	that was evaluated as part of the platform designed
25	for Tricon, and we concluded that the RXM setup,

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	136
1	where you see the primary as being safety related,
2	and the secondary being non-safety related, we
3	qualified that as an approved isolation device
4	between safety and non-safety for communications,
5	for the purpose of communications.
6	Now, in the Diablo Canyon application,
7	it is a two-way communication because the RXM does
8	receive does receive inputs, and the RXM does send
9	outputs to drive indicators on the control board,
10	and it drives alarm outputs to the annunciator
11	system, the Diablo Canyon annunciator system, so it
12	is two-way.
13	MEMBER STETKAR: That's what I was
14	going to ask. You're very careful, both in the SCR
15	and here as saying those are not safety related
16	indications or information from your purpose.
17	MR. STATTEL: Right.
18	MEMBER STETKAR: If I'm an operator
19	sitting in the main control room, maybe I'm
20	interested in them, so could you give me some
21	examples of what signals are actually processed
22	through that template?
23	MR. STATTEL: So what I'm trying to
24	describe is the RXM is really just a bus extension.
25	So if you want to have a remote IO that's ten miles

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	137
1	away, you can do that.
2	MEMBER STETKAR: Yeah, I got it, yeah.
3	MR. STATTEL: So to approve it as a
4	safety to non-safety boundary, we didn't have any
5	control over the - you know, we're reviewing the
6	platform, so we didn't have any control over what
7	the application would be.
8	So we knew certainly you could write a
9	safety application where the safety function is
10	dependent on some piece of data that was coming in
11	on the RXM link from the non-safety side. It's
12	theoretically possible to do that, so obviously
13	that would compromise the isolation characteristics
14	of the system.
15	Therefore, we wrote an application
16	specific action item into the Tricon evaluation and
17	for the application level, and this is what
18	Rossnyev has done. She looks at every signal that
19	is configured to be input or output over the RXM
20	chassis and makes sure that there's nothing in the
21	safety-related side that relies on that signal to
22	be valid or even there, right?
23	MEMBER STETKAR: Yeah.
24	MR. STATTEL: So there's no reliance on
25	those functions.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	138
1	MEMBER STETKAR: And I got that. I was
2	asking the question though if I'm an operator in
3	the main control room and something goes - I'll use
4	the technical term - belly-up in the Tricon
5	platform, what non-safety related function
6	indications do I lose?
7	MS. ALVARADO: Delta T indicator.
8	MEMBER STETKAR: What?
9	MS. ALVARADO: Delta T indicator.
10	MEMBER STETKAR: That's it? That's the
11	only one?
12	MS. ALVARADO: No, there are more. You
13	asked for one example. You asked for one example.
14	I have one example.
15	MEMBER STETKAR: Do you -
16	MR. STATTEL: It's comparable - like it
17	drives the alarm, the main alarm system outputs for
18	the system.
19	MEMBER STETKAR: So there's a lot of
20	stuff that's processed?
21	MR. STATTEL: Yes, there is actually -
22	MEMBER STETKAR: Okay, okay, that's
23	what I was trying to find out -
24	MR. STATTEL: - quite a bit of signals.
25	MEMBER STETKAR: - whether it was a lot

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	139
1	or a little.
2	MR. STATTEL: So, you know, the Eagle
3	21 drives alarms -
4	MEMBER STETKAR: Okay.
5	MR. STATTEL: - also, you know, a
6	similar alarm system, trouble alarms. So basically
7	they're repeating that functionality that's in the
8	Eagle 21.
9	MEMBER STETKAR: That's what - see, I
10	don't know the system design. I didn't know if
11	they had a separate, you know, a completely
12	separate status monitoring system and alarm
13	generation or if everything comes through this.
14	Okay, thank you.
15	MS. ALVARADO: This slide shows the
16	port aggregator tab that is used with the Tricon.
17	This tab is a hardware device that provides a
18	bidirectional communication path to the Tricon
19	maintenance work station, and a one-way hardware
20	enforced communication path to the plant computer
21	system. It doesn't rely on software to perform
22	this function.
23	It has three ports, Port A for
24	communication with the TCM in the Tricon, Port B
25	for communication with the maintenance work

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

1 station, and Port 1 for communication with the 2 plant computer system. Ports A and B are for 3 two-way communication, and Port 1 is for one-way 4 communication.

The port tab was previously evaluated and has been approved as an acceptable means of isolating safety system, and specifically the NRC performed accident analysis of this device. The result of this analysis showed the amplifiers were not capable of passing electrical signals in the reverse direction under any condition, so data cannot flow from Port 1 to Port A.

13 So this slide shows the conclusion 14 regarding independence. The NRC staff reviewed the 15 design and functionality of the communication 16 for the ALS and the Tricon process systems, 17 examined the hardware and software used to 18 and concludes implement this communication, the 19 Tricon and ALS complies with the guidance provided 20 in ISG-04. Specifically, the ALS and Tricon do not 21 depend on any information or resource originating 22 or residing outside its own safety division to 23 accomplish its safety function.

In addition, safety functions performedby each system are protected from adverse influence

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

5

6

7

8

9

10

11

12

(202) 234-4433

140

	141
1	from outside each protection set, and failure of
2	the non-safety devices will not affect the
3	functions of the safety systems. This concludes my
4	presentation. Is there any questions? So, next is
5	Samir Darbali.
6	MR. DARBALI: Good afternoon. Today
7	I'm going to be talking about control of access.
8	The staff evaluated how the licensee and the vendor
9	should address the control of access clause of IEEE
10	603-1991 for the PPS replacement design.
11	This clause states that, "The design
12	shall permit the administrative control of access
13	to safety system equipment, and that these
14	administrative controls shall be supported by
15	provisions within the safety systems, by provision
16	in the generating station design, or by a
17	combination thereof."
18	The staff evaluation of control of
19	access is based on the staff's review of Secure
20	Development and Operational Environment or SDOE,
21	and configuration management. The guidance for
22	SDOE is found in Reg Guide 1152 Revision 3, and the
23	guidance for configuration management is found in
24	Technical Branch Position 7-14 of the Standard
25	Review Plan, as well as in Reg Guide 1.169 Revision

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	142
1	1.
2	Appendix 7.1-C to Chapter 7 of the SRP
3	contains three paragraphs of acceptance criteria
4	for evaluating the control of access clause of IEEE
5	603. This acceptance criteria was addressed in the
6	PPS replacement design that's contained in the
7	following slides.
8	Paragraph 1 of Section 5.9 reads,
9	"Administrative control is acceptable to assure
10	that the access to the means for bypassing safety
11	system functions is limited to qualified plant
12	personnel and that permission of the control room
13	operator is obtained to gain access." The PPS
14	replacement design meets this criteria. Access to
15	the system is administratively controlled by
16	control room personnel.
17	Paragraph 2 reads, "The review of
18	access control should confirm that design features
19	provide the means to control physical access to
20	safety system equipment, including access to test
21	points and means for changing setpoints." The PPS
22	replacement design meets this criteria as there are
23	design features that provide physical access
24	controls to the system.
25	For example, the system will be located

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433
	143
1	in a plant vital area in locked cabinets. Also,
2	changing the Tricon keyswitch to a position other
3	than RUN or connected the Test ALS Bus will result
4	in an alarm. Therefore, access to the system is
5	only allowed to qualified personnel with permission
6	of the control room. Next slide?
7	Paragraph 3 of Section 5.9 reads,
8	"Review of digital computer-based systems should
9	consider controls over electronic access to safety
10	system software and data. Controls should address
11	access via network connections and via maintenance
12	equipment." The PPS replacement design meets this
13	criteria as it does not allow for remote electronic
14	access to the Tricon or ALS systems.
15	For example, there is one Tricon
16	maintenance work station and one ALS maintenance
17	work station per protection set. These maintenance
18	work stations only communicate with the
19	safety-related controllers in that protection set,
20	and are not connected to any other plant system.
21	Also, access to the maintenance work stations is
22	controlled.
23	For the Tricon portion of the system,
24	two-way communication is only allowed between the
25	Tricon communication module and the Tricon

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

maintenance work station by means of the port tab device which was previously discussed in Slide 25.

For the ALS portion of the system, two-way communication is allowed between the ALS and the ALS maintenance work station through the use of the Test ALS Bus which is not connected during normal operation, and is only used in test or maintenance mode. Slide?

9 As I mentioned earlier, the staff's 10 evaluation of control of access is based on the 11 staff SDOE and configuration management reviews. 12 These reviews were evaluated during the Tricon and 13 ALS platform topical report reviews and were found 14 to be acceptable. The staff found that the same 15 and configuration management measures SDOE were 16 maintained for the Diablo Canyon application.

17 For SDOE, the vendors performed 18 vulnerability assessments of their facilities to 19 that the replacement ensure PPS system is 20 protection from unauthorized access or modification 21 safety system life cycle. throughout the The 22 the vulnerability assessments results from were 23 used to establish security control requirements to 24 mitigate and identify vulnerabilities through the 25 use of physical, logical, and administrative access

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

8

(202) 234-4433

144

	145
1	controls.
2	For configuration management, the
3	vendors implemented access control measures to
4	ensure that no unintended or unauthorized functions
5	or code were introduced to the system. These
6	measures include the identification of
7	configuration items, access controls based on work
8	responsibilities, change review, approval, and
9	verification processes, and error reporting and
10	corrective actions program.
11	Finally, to detect and prevent the
12	introductions of unintended or unauthorized changes
13	to the codes, the vendors V&V groups performed code
14	reviews. Next slide?
15	The NRC staff concludes that the Diablo
16	Canyon PPS replacement design incorporates features
17	to administratively, physically, and logically
18	control access to the system, both during
19	development and operation. These features meet the
20	guidance for Secure Development and Operational
21	Environment and Configuration Management.
22	Therefore, the NRC staff determined that the PPS
23	system meets the criteria for control of access.
24	Any questions?
25	CHAIRMAN BROWN: Yeah, I have two. One

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

	146
1	is a request to make sure I understand something
2	and the other one is one your configuration -
3	MR. DARBALI: Sorry.
4	CHAIRMAN BROWN: It's all right. It
5	doesn't bother me, but he may come after you. As
6	part of what you call access controls based on work
7	responsibilities - and I'm trying to, again, relate
8	this to some of the controls that we exercised, our
9	vendors exercised in the program from which I left
10	years ago.
11	The software that's being developed is
12	normally, I don't know what they do, is aggregated
13	in some location, you know, electronically or
14	whatever. With the folks we dealt with, there was
15	a very limited cohort of programmers that had
16	access to making any change to that code at all,
17	and it was very, very tightly controlled.
18	In part of you all's review for access
19	controls, is it down to not just work
20	responsibilities, but here is Person A, Person B,
21	and Person C are the only ones allowed to go modify
22	a specific code?
23	MR. DARBALI: Well, for example, for
24	the ALS, we specifically asked during one of the
25	audits, "Can somebody from the Core A group be able

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	147
1	to modify Core B?" and we checked. They don't have
2	access for that.
3	CHAIRMAN BROWN: Is it a multi-step
4	path to gain that access?
5	MR. DARBALI: You need multiple
6	signatures from management and -
7	CHAIRMAN BROWN: What if he walked
8	through the door, got in, and walked up the machine
9	and decided he was pretty good at hacking into
10	stuff, and got into the computer?
11	MR. DARBALI: Well, you have to
12	remember, there is a record for every change, so
13	you could go back to the changes and see who made a
14	change when and what change.
15	CHAIRMAN BROWN: He has to record that
16	he's making the change or does it -
17	MS. ALVARADO: Besides the record, I do
18	remember because I reviewed a part of the code
19	especially for the ALS. You were not granted
20	access to the network or the server where they have
21	the program. So not only do you need different
22	signatures to get access granted, you also needed
23	to have the right password and access requirements
24	for that. Because we tried to create, like, dummy
25	addresses when we were doing the audit, and we

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	148
1	couldn't do it.
2	CHAIRMAN BROWN: You couldn't do it.
3	Okay, all right.
4	MR. STATTEL: Charlie, can I ask you a
5	clarifying question?
6	CHAIRMAN BROWN: Yeah.
7	MR. STATTEL: Are you referring to the
8	in-plant system operating and access -
9	CHAIRMAN BROWN: No, I'm talking about
10	-
11	MR. STATTEL: - or are you talking
12	about at the vendor?
13	CHAIRMAN BROWN: I'm talking about
14	under your SDOE environment -
15	MR. STATTEL: At the vendor facility.
16	CHAIRMAN BROWN: - at the vendor, yeah.
17	MR. STATTEL: Okay, okay.
18	MR. DARBALI: And you have to
19	understand, access to each - because you said,
20	"What if somebody went to a manager's computer to
21	get access?" Well, you know, they have several
22	layers for logging onto those computers, so -
23	CHAIRMAN BROWN: Okay.
24	MR. DARBALI: It's pretty tough.
25	CHAIRMAN BROWN: Okay, the second one

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	149
1	is I just want to validate my general conclusion
2	here is that external access for control of access
3	is literally not - nobody can get in from the
4	outside right now. You've got - you have - I've
5	never seen, either in the SCR or in any of the
6	other documents that I read, that there were any
7	digital type access back reverse wise. They were
8	pretty hard wired. So I presume if it wasn't shown
9	on your figures, there aren't any?
10	MR. DARBALI: That's correct.
11	CHAIRMAN BROWN: You cannot get in. So
12	control of access is very much the same as it is
13	today when you - in an analog system where if
14	somebody wants to change something, they get an
15	operator supervisor approval. They go down to the
16	cabinets. They open them up, get out the
17	procedure, bang, bang, bang, and make the changes
18	and go. So this seems to replicate that process
19	almost exactly to me. There might be some nuances,
20	but -
21	MR. STATTEL: Yeah, I agree there is
22	nothing in the design. However, we were concerned
23	about, like, portable media, flash drives and
24	things like that.
25	CHAIRMAN BROWN: Yeah, but those have

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	150
1	to be brought in.
2	MR. STATTEL: They have to be brought
3	in, but, you know, we're talking about insiders, so
4	-
5	CHAIRMAN BROWN: I understand that,
6	but, I mean, that's like it is today.
7	MR. STATTEL: Okay.
8	CHAIRMAN BROWN: I mean, if you had
9	internal stuff, I mean, an outsider could come in,
10	or an insider could come in and he could
11	surreptitiously, if he had a key, go down and
12	unlock a cabinet, make a change, and kind of mess
13	up the works. So, I mean, it's a supervisory
14	control that's somewhat similar to which some guy
15	could sneak in obviously with a thumb drive and
16	what have you if that's the way it operated.
17	Anyway, so I just wanted to make sure my conclusion
18	from going through this was valid.
19	MR. HECHT: I'd like to follow up on
20	the previous question and just ask it very simply.
21	Is there any source code control system like SVN or
22	something like that that's used? I was a little
23	bit confused by the comment you made about only -
24	that the programmers are not allowed to access the
25	software depository. I kind of think that if I

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

151 developing code, I'd like 1 to the were run 2 integration testing. 3 MR. DARBALI: Let me clarify. I was 4 saying for the ALS, you have a Core A team and a 5 Core В team, and they're not allowed to So the Core A team members don't have 6 intermingle. 7 access to the Core B code. 8 MR. HECHT: Okay. Let's move to a more 9 general situation or to the application code that 10 might be used on the Tricon device. My concern is 11 -- well, I'm going to ask did you see what kind of 12 configuration control software or what kind of configuration control system is being used? 13 14 MR. DARBALI: We did look at that. Ι 15 don't remember because companies use different 16 But, yes, the software would allow you to brands. 17 check out the product that you're changing, do your 18 changes, and check it back in. 19 HECHT: Okay, all right. MR. That's 20 pretty standard. 21 MR. DARBALI: Right. 22 MR. HECHT: And then there are only 23 certain people who are allowed to check out certain 24 components, make changes, and check in, but other 25 people could check out and could download other

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	152
1	components if they wanted to, check something about
2	integration?
3	MR. DARBALI: Right. So there are
4	software librarians who are in charge of
5	controlling all of that, so some people may have
6	read-only access, whereas other people would have
7	access to make the changes.
8	MR. HECHT: Okay, all right. Thank
9	you. CHAIRMAN BROWN: Any other
10	questions in this subject before we move on?
11	MEMBER REMPE: Okay. So the next slide
12	is talking about lessons learned.
13	CHAIRMAN BROWN: Yes.
14	MEMBER REMPE: So I would like to
15	follow-up on what John asked at the beginning of
16	this session about the Open Item 115, and there are
17	several places, as John pointed out, in the text
18	that refer to that response, and I thought you said
19	that, during your discussion, I think this is the
20	section where you probably would like to tell us
21	how did you resolve it in the updated SE?
22	MR. STATTEL: Yes, I will discuss the
23	open item list. It's kind of an informal process,
24	but it will be something I discuss in the
25	MEMBER REMPE: On the lessons learned.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	153
1	MR. STATTEL: lessons learned.
2	MEMBER REMPE: Okay.
3	MR. STATTEL: Yes, correct.
4	MEMBER STETKAR: Before we get to the
5	lessons learned, and, Charlie, I promise to keep
6	this I've got four things that I want to get on
7	the record so the staff can follow-up on it only on
8	comments on the SER. I don't want to discuss these
9	things. I just want to get them on the record,
10	okay? If you'll allow me that. And I'm going to
11	just rattle off section numbers, and you can find
12	them in the transcript.
13	In Section 3.4.1.6, it's noted that
14	PG&E is going to perform site acceptance tests and
15	design verification tests in which they're going to
16	use a live analog signal from the reactor coolant
17	system all the way through ALS through Tricon out
18	to make sure that everything works okay, so that
19	the integrated ALS Tricon works okay.
20	In Section 3.4.2.4, it describes the
21	testing activities, concludes that all those tests
22	are fine, but those testing activities described in
23	that section are only the individual Tricon and ALS
24	platform testing activities. I see no mention of
25	this integrated PG&E test, and I see no mention of

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	154
1	follow-up in terms of site-specific activities to
2	make sure that that test is done. So that's one of
3	them.
4	The next one is something I brought up
5	earlier in the fact that all four protection sets
6	are not equal. They process different signals. In
7	Section 3.4.2.2.1.3, there are statements
8	MR. STATTEL: Can you read that again?
9	MEMBER STETKAR: Sure. It will be in
10	the transcript, but I'll do it again. 3.4.2.2.1.3.
11	You number them, I only read them. There's a whole
12	discussion about verifying the input and output
13	signal lists, and there's statements in there that
14	says, well, it's noted that only Protection Set 1
15	list was provided. And then the thing that caught
16	my attention, it says, "It is assumed that this
17	report will later be revised to include all
18	implementation activities for all four protection
19	sets." And then the final conclusion is everything
20	is okay, so I'm left kind of dangling on whether or
21	not the safety evaluation is based on an
22	assumption.
23	And then in and this is, I'm
24	assuming, it's just an editorial one, but it's sort
25	of pervasive. Section 3.13.1, and there are other

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

	155
1	sections that kind of refer to the same thing, but
2	there are four plans that are discussed for
3	plant-specific or site inspection follow-up
4	activities: software installation plan, maintenance
5	plan, operations plan, and safety plan. There are
6	references back to other sections of the SER where
7	it says those plans are discussed. In some cases,
8	those sections don't even exist. In other cases,
9	they refer to completely different things. In
10	other cases, it says there aren't such things, you
11	didn't review those plans. I'm assuming that's
12	just a clean-up item.
13	And then, finally, and I think, Rich,
14	you may have hit on it earlier, in Section 3.14.2,
15	under ALS, there are inspection items 13, 14, 15,
16	16, and 17. And I did a cross-check between ALS
17	and Tricon. These are anomalies that are only
18	specified for ALS. They're not specified for
19	Tricon. There doesn't seem to be a functionally
20	equivalent inspection, but there are things like
21	termination of cables, chassis grounding, you know,
22	that kind of stuff that would seem to apply equally
23	for Tricon. So you may want to check that
24	crosstalk between the two platforms.
25	And that's it. Thank you, Charlie.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	156
1	CHAIRMAN BROWN: You're very welcome,
2	as always. Very accommodating. Okay. Ready for
3	the next section? I'm checking right now. I think
4	I had one, and I just lost it. This was cumbersome
5	software.
6	MEMBER STETKAR: If you had a trained
7	operator, it would be okay.
8	CHAIRMAN BROWN: Yes, I very much need
9	a trained operator for this. Oh, yes, okay, here
10	it is. There was a section in your SER that
11	identified that each Tricon subsystem has dual
12	redundant batteries, I think, located on the main
13	chassis backplane such that, if a power failure
14	occurs, these batteries maintain data and programs
15	on the associated main processors for a period of
16	six months, which implied to me that you're
17	non-volatile memory has programs disappear after
18	six months. Am I mistaken?
19	MR. STATTEL: I think that's true.
20	That's my recollection, but I would have to look
21	into that. CHAIRMAN BROWN: But the
22	programs really disappear. Okay. It was in
23	section I don't know.
24	MR. STATTEL: I'm thinking way back
25	when I went to the Tricon training. I believe

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	157
1	that's the case. I believe if
2	CHAIRMAN BROWN: But their non-volatile
3	memory is not really non-volatile. It needs to
4	have batteries to keep it in place. Otherwise, it
5	disappears.
6	MR. STATTEL: Well, the system would
7	have to have no power for six months. But I
8	believe that's correct. I believe it will lose all
9	memory if you let the batteries die. Actually
10	CHAIRMAN BROWN: I'm glad our stuff
11	doesn't do that.
12	MR. SCHRADER: We have no shortage of
13	power.
14	MR. STATTEL: The Applicant actually
15	has a lot of experience with the Tricons in their
16	non-safety applications, and I think the battery is
17	common.
18	CHAIRMAN BROWN: I know I have stuff
19	that sits in a warehouse for two years, and it's
20	still there.
21	MR. PATTERSON: Yes, the batteries
22	definitely hold the program and, once those die,
23	the program
24	CHAIRMAN BROWN: They're gone. Okay.
25	So it's not really non-volatile then. That's fine.
	NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	158
1	I mean, if the batteries died immediately, the
2	software disappears. So that's we're ready to
3	go on to the next one. Thank you.
4	MR. STATTEL: Okay. So the next
5	section I think is going to be a little less
6	formal. We're here to talk about lessons learned
7	from the ISG-06 process, so I'll kick it off.
8	The Interim Staff Guide 06, ISG-06,
9	describes a process that may be used in the review
10	of license amendment requests associated with
11	digital I&C systems modifications in operating
12	plants that were originally licensed under Part 50.
13	This slide shows the key objectives that were
14	considered during the development of ISG-06. What
15	I hope to do here is explain how each of these
16	objectives was addressed in ISG-06, the original
17	concept, and to characterize the degree to which
18	these have actually been achieved now that we've
19	had some experience using the guide.
20	And I'll mention that Diablo Canyon is
21	not our only experience. We've also used ISG-06
22	for several platform evaluations and a couple of
23	other review activities.
24	So I'll start with the tiered approach
25	to grading reviews. That's the top bullet here.
	NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

simple criteria. The criteria was does the design refer to a previously-approved platform and have changes been made to that platform since it was approved by the NRC?

So a couple of thoughts I have on this. First of all, all evaluations, everything we've experienced in the last five years, are essentially Tier 2 evaluations, right? Why is that? Tier 1 evaluations are pretty rare because these platforms are updated on a pretty regular basis, which is not necessarily a bad thing. They're making improvements to these platforms as they go along.

14 So pretty much the amount of time that 15 goes by between when we evaluate a platform and 16 when we get an application review, the longer that 17 time period is, the more deltas, the more changes 18 you're going to have in that platform. And of 19 course, we have a section in our safety evaluation 20 here where we reviewed the deltas. Even though it 21 it was less than a year between the was only, 22 application development and our approval, there 23 still changes. So, basically, everything were comes down to a Tier 2. Tier 1 evaluations are, 24 25 well, they're rare because of that.

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

8

9

10

11

12

13

The

	160
1	Now, we don't really expect a lot of
2	Tier 3 submittals. We have had some in the past,
3	but it was mainly because we didn't have, before we
4	had topical reports that were approved. So Wolf
5	Creek, for example, was a Tier 3 evaluation because
6	the ALS platform had not been approved at that
7	time.
8	So that's just kind of my view. The
9	tier approach, it really doesn't provide the type
10	of grading, I think, that was originally sought
11	after on this.
12	CHAIRMAN BROWN: Some of us probably
13	have forgotten totally. I think I understand what
14	you're saying. But Tier 1 effectively said you've
15	got a platform that is approved and you just get on
16	with it.
17	MR. STATTEL: Yes. So the idea is it's
18	Tier 1, if you have a platform and you're going to
19	reference that and you're going to use that
20	platform, the NRC spends the time, spends the
21	effort, reviews that platform, comes up with as
22	many safety conclusions as it can, albeit a lot of
23	time are going to be application specific, and then
24	it's a much lesser effort when we actually get the
25	applications because all we're looking at is the

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	161
1	application.
2	But as you can see, as you've seen
3	here, these two platforms, they had a lot of
4	application-specific action items. I think there
5	were like 15 - 20 action items on each one, and
6	they were not insignificant.
7	The other thing that I observe is most
8	of these IEEE 603 criteria and the 7432 criteria is
9	really application specific. So if you want to
10	know if a system meets single failure criteria or
11	if it alarms when it's put in bypass, that's a 603
12	criteria. If I don't have an application, I really
13	can't verify that. I can't draw that safety
14	conclusion at the platform level. So that's kind
15	of a misnomer there.
16	Now, I think the platform reviews are
17	useful, and I think they helped us out a lot when
18	we were performing our application review. And I
19	think it does shorten the time that it takes to
20	review the application. But it's not all that
21	significant as what we were hoping for.
22	Now, there are other aspects of grading
23	that were not considered in ISG-06, and that is,
24	the obvious one is the scope of the modification
25	being performed. So if you're performing a

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

modification and you're doing one single simple safety function that's not complex, it's just an input bistable output, that's probably going to take a little bit less of a review effort than replacing an entire RPS SFAS system, and that's not considered here. That's not considered in the ISG-06 process.

8 So, now, it's a little hard to quantify 9 that. You know, how complex is your modification? 10 How simple is it? What's the scope of that 11 modification? But I think that's something that, 12 going forward, want we might to consider in a 13 graded approach. And there are some other 14 characteristics that could be used that we're 15 starting to talk with the industry about, other 16 ways to do a graded approach to performing these reviews. 17

18 the second bullet talks about Now, 19 Annex B of ISG-06. Now, Annex B was kind of the 20 starting point for ISG-06. industry was What 21 basically asking for is, with all of the standard 22 review plan and the guidance criteria that we have 23 in these, we don't know what to submit. We don't 24 know, when we're putting a design together and we 25 want to submit an application to the NRC, we just

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

	163
1	don't know what you want, right? And we want you
2	to define that.
3	So Annex B was developed, and it
4	basically provided a listing of documents,
5	although, you know, different vendors use different
6	titles for documents, so that became kind of an
7	issue, too. So it's a listing of topics, let's
8	say. And it provides reference and provides
9	guidance on what the NRC really wants to see. Now,
10	that part I found to be very helpful, and I'll talk
11	about that in one of the other slides.
12	Now, the third bullet was provide an
13	evaluation process that could be performed in
14	parallel with the development process. So for
15	Diablo Canyon, when they first approached us and we
16	were having Phase 0 meetings, they had not even
17	started really with their design. They just had a
18	design concept. So we've been kind of working with
19	them as we perform our review.
20	At the time of the license amendment
21	request, again, they had not really proceeded very
22	far with the design. They had a functional
23	requirement spec but not a lot more than that. So
24	what I ISG-06 does, it breaks it down into two
25	phases: phase one and phase two. So we define

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

what, you know, the minimum set of documents or minimum set of information that we need to commence a review, and then we understand that we're going to be working side by side with you and that, at a later date, when the design proceeds, we'll get that phase two documentation.

7 Now, I think that's worked fairly well 8 with Diablo Canyon, although, with the project 9 delays, it's really taken a lot longer than we had 10 anticipated. But one observation I have on that is like, for 11 some of the phase two documentation, 12 instance, the factory test results, those really 13 don't become available until really late in the 14 process, in the design process, because they have to design the system, they have to implement it, 15 16 they have to work out the bugs, they have to build 17 the system and test it, and then they get to do a 18 So we're thinking of something, you factory test. 19 know, rather than wait for the long pole in the 20 wait for the last document to come tent, in, 21 probably that we could break phase two into two or 22 different areas more SO we can get the 23 documentation made available to us in а timelv 24 manner.

And then the fourth bullet was

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

25

1

2

3

4

5

6

basically just streamline the licensing process. And I think, to a degree, it's not easy to use, but it's easier than it was before, I would say. It's a relative thing.

So now in the lessons learned, Phase 0, this is the block diagram that's in ISG-06. And, basically, this is the pre-application meetings that we have with the licensee. With Diablo had at least three pre-application Canyon, we meetings. Ι think we had a fourth one, but I couldn't find the report for it.

12 during But those pre-application 13 meetings, there were some concepts that were 14 And some of them were acceptable, floated by us. for instance the ALS diversity concepts that they 15 16 were proposing. They ended up moving forward and 17 into the design. Some of them we had some on 18 issues with, and we had this conversation with the 19 applicant.

20 So, for example, at Diablo Canyon, they 21 have a lot of experience with the Tricon system 22 because they it in many of their use 23 non-safety-related applications. So one of their 24 original ideas in one of the earlv Phase 0 25 meetings, they said, well, we're not going to have

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

5

6

7

8

9

10

11

	166
1	the vendor do the development, we're going to do it
2	ourselves. Okay.
3	Now, obviously, there's nothing in
4	regulation that would prohibit that, right? And we
5	told them that. But we warned them that you could
6	do that, but we would still have to perform the
7	same evaluation we would do as if you were a
8	vendor. So we would be looking for independent B&B
9	activities and, typically, for a safety-related
10	application, this is not the type of resources that
11	we would expect a licensee to even have to be able
12	to do that.
13	So I think after the first meeting,
14	they kind of changed their mind on that. And then
15	we ended up where we're at now.
16	So we didn't really have a design.
17	They weren't really making design changes during
18	these Phase 0 meetings, but they were making
19	decisions that ultimately impacted our review. And
20	I think a lot of those decisions and a lot of the
21	discussions we had helped to avoid a lot of
22	controversy and a lot of requests, RAI requests.
23	So I think they really supported a pretty efficient
24	evaluation.
25	So lessons learned here. So

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	167
1	CHAIRMAN BROWN: So the pre-application
2	part of this was productive?
3	MR. STATTEL: I thought it was very
4	productive, and I've heard similar sentiments from
5	
6	MR. SCHRADER: Yes, absolutely agree.
7	MR. STATTEL: So interaction with the
8	staff early and often in the pre-submittal phase
9	was effective at preparing the licensee and staffer
10	license application.
11	Another thing is we talked about the
12	matrix, the Appendix B matrix, in ISG-06, and we
13	talked about, well, what does this document mean
14	and, you know, where are you going to find this
15	information? So it got the licensee to thinking
16	about that. To their credit, the licensee in this
17	case decided to take that appendix from the ISG and
18	they put it into a spreadsheet format, and they
19	actually mapped it out to documentation and
20	sections within their license amendment request.
21	So it made it very easy for us to find the
22	information that we were looking for when we did
23	our application acceptance review.
24	Okay. And then the second lesson
25	learned on Phase 0, yes, it says they should
	NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	168
1	request a Phase 0 meeting at least six months prior
2	to the submittal. And I think most applicants have
3	kind of come onboard with this. We've had several
4	pre-application meetings, for instance with plants
5	that are doing NUMAC upgrades or doing a MELLA+
6	upgrade. We've also had pre-application meetings
7	for set-point evaluations, things like that. And
8	it really helped out a lot because, once they
9	submit it, it's documented material and it's a lot
10	harder to change than it is at the pre-submittal
11	stage.
12	Okay. The next phase, let's see. This
13	is, oh, Phase 1. So I already kind of mentioned
14	this. The tabulation in Enclosure B was very
15	effective in identifying information that staff
16	needed to start its review. The use of the Phase 1
17	documentation compliance matrix facilitated an
18	efficient acceptance review, and we completed that
19	in I think about three months, which is pretty good
20	for such a large application.
21	Okay. Now, we get into the actual
22	Phase 2, the review. So now here's where we
23	started having some issues when we were doing
24	platform evaluation because ISG-06 is really
25	written to review an application, so it's looking

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

for application-specific stuff. So when we're trying to apply this and all we have is a box of Legos or a platform with no application, there's a lot of things that we're just not able to draw conclusions on.

So one of the things I think would benefit us going forward with the process is to have something, have a separate enclosure that would kind of outline what we expect to see for a platform with no application available. So, in my view, the IEEE 603 criteria, it's pretty much always an application-specific action item anyway, so there's really no point in spending a lot of time on that during a platform review. And I think that would help a lot.

16 Next item, it should be enhanced to 17 remote electronic websites. So promote we use 18 SharePoint with the Diablo Canyon application. Ι 19 found that incredibly useful. Primarily, what we 20 use it for, it gives us access to documents before 21 they're actually put onto the docket. And being 22 able to view those documents, we're able to see, A, 23 if it has the information we need because, 24 otherwise, we're just going off of a document title 25 and we don't know what's in it until after it's too

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

(202) 234-4433

169

late, after it's already docketed, and it kind of avoids unnecessary submittals of documentation. And I already mentioned the Phase 2 All right. lists could be enhanced to acknowledge the unavailability of certain documents until the late stages of development.

Now, the next phase is kind of after submittal. And, obviously, we haven't gotten there 9 yet with Diablo Canyon. But we do have experience with prior applications. Let me catch up on my notes here. So in these prior applications, the inspections we found to be very useful. We have a 13 list of inspections. We have a section in the safety evaluation called "Recommended Inspection 15 Items." The inspectors use those pretty 16 religiously. I mean, for the prior applications, they basically take those recommended inspection 18 items and build them right into their inspection 19 plan.

20 We've also participated, both Samir and 21 I, went down for the site acceptance testing at 22 previous applications, and the regions have told us 23 that that's very helpful because we have the 24 perspective of knowing this safetv evaluation 25 pretty well so we know what the intentions were for

> **NEAL R. GROSS** COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

8

10

11

12

14

17

inspection items. And it 1 those gives us an 2 opportunity to see things we're not able to see So we have not been able 3 during this evaluation. to see surveillance test procedures. We have not 4 5 been able to see actual operating instructions for 6 this system. So it gives us that opportunity to 7 get out there and see those, and the region has 8 been pretty supportive with that. And lesson 9 learned is we feel that it's helpful to have people 10 who performed, who were involved with the 11 performance of the safety evaluation actually as 12 members of the inspection team. 13 MEMBER STETKAR: Rich, do you look at 14 the inspection plans before the region issues them? 15 You get a chance to get feedback into that process 16 Because that's, you know, a couple of at all? 17 Ι brought up is I recognize that they things 18 develop their inspection plans given the marching 19 orders in the SER, if you will. What they may not 20 do is not appreciate things that aren't explicit in 21 there but might have been intended that you folks 22 might know --Well, I'll say this: it's 23 MR. STATTEL: 24 really not proceduralized. There's nothing in the 25 standard review plan that tells us we have to write

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

171

	172
1	recommended inspection items, but we do because we
2	recognize there's things we can't see now.
3	And, likewise, there's no requirement
4	for the region to put us in on the review process
5	for their inspection plans, but my experience is
6	they share them with us and they accept our
7	comments on those inspection items.
8	MEMBER STETKAR: Okay, good. So you do
9	get a chance to feed back before you actually go
10	and observe what was being done.
11	MR. STATTEL: So one issue we've
12	experienced while evaluating these I&C systems is
13	that there are many criteria governing many aspects
14	of the design development and implementation of
15	these systems. Now, ISG-06 derived these criteria
16	from many different sources, including the SRP,
17	general design criteria, IEEE standards, BTPs,
18	etcetera.
19	In some cases, the criteria for a given
20	topic must be derived from multiple documents. So
21	the idea was to get it all in one-stop-shopping,
22	get it all in one document. Well, that created
23	some problems, so what we've seen, we recognize
24	some benefit to doing that, but what we've seen is
25	subsequent changes to those source documents have

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

resulted in duplication of criteria and, in some cases, inconsistent or conflicting guidance between what's in the ISG and what's in the source document.

5 MEMBER STETKAR: I was going to wait until our follow-on session here, but we're getting 6 7 real short on time, so I might as well bring it up 8 One of the problems that I had going through now. 9 this particular SER points exactly to that topic. 10 There's just too much guidance out there, and 11 there's an obligation or an implied obligation of 12 check off each reviewer to the box from each 13 sentence and each paragraph of each of those 14 quidance documents. It was really, really hard to 15 SER because it referred back follow this onto 16 itself several times, and in several places where 17 it. referred back onto itself it was internally 18 inconsistent or there were gaps.

19 Something needs to be improved there, 20 quite honestly. And it's not just the flow of the 21 It's obviously, it's resources from the staff SER. 22 reviewers. It's resources from the licensee who 23 has to answer perhaps multiple RAIs on slightly 24 different-worded sections of different quidance. 25 There almost has to be some master review quidance

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

	174
1	
2	MR. STATTEL: Well, this was our first
3	attempt, and putting it all in one document was the
4	idea.
5	MEMBER STETKAR: Yes, but it apparently
6	didn't work.
7	MR. STATTEL: I don't think it's going
8	to work.
9	MEMBER STETKAR: It didn't work there.
10	Yes, but if you leave it disjoint, it's going to
11	become even worse.
12	MR. STATTEL: So what do you do? Our
13	thoughts right now are just, instead of duplicating
14	the words, just put the proper references in.
15	MEMBER STETKAR: Yes, that might be
16	MR. STATTEL: That's about all we can
17	do right now.
18	MEMBER STETKAR: I mean, there ought
19	to be again, this is subcommittee, so I can say
20	what I think. There ought to be review topics, and
21	there might be several source documents that have
22	guidance under that topic. Hopefully, they're not
23	opposed to one another. But under a review topic,
24	if I'm going to review diversity and
25	defense-in-depth or something, I might have several

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

175 source documents that I'm pointed to, but I don't 1 2 necessarily need to say, okay, I'm now reviewing 3 against this paragraph in this particular source The review guidance might tell me what I 4 document. should review against, from the NRC's perspective, 5 6 using all of that other reference stuff as 7 resources. 8 MR. STATTEL: We certainly recognize 9 that as a problem. I don't think this solution 10 worked too well --11 MEMBER STETKAR: Yes, and --12 STATTEL: and I'd MR. ___ love to 13 entertain some ideas for different ways to go. 14 CHAIRMAN BROWN: Are you talking about 15 the SER, or were you talking about the solution 16 didn't work so I'm trying to --17 MR. STATTEL: Well, this is just 18 lessons learned from having gone through the review 19 process. 20 CHAIRMAN BROWN: Okay. But I'm trying 21 to relate how you would change the SER because I 22 somewhat slightly different perception. have а This is one of the first, I think it's one of the 23 24 first I saw with a table of contents. It really 25 made it easy for me to go find what I wanted to

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	176
1	look at and concentrate on. And there were some
2	places, I would agree, where you went through 603
3	1991 and you went through 7.4.3.2 and you went
4	through and some of the things you do are
5	repetitious, and so you see, well, we already
6	discussed that in the previous one. That becomes
7	cumbersome, not only for you but for the reviewers,
8	because you start to zone out as you go through
9	those and hope you find something new. But other
10	than that, I actually, I mean, a 306-page SER and
11	
12	MEMBER STETKAR: But maybe it could
13	have been 200 pages without the repetition and the
14	
15	CHAIRMAN BROWN: Yes. If somebody says
16	I'm going to do something for
17	MEMBER STETKAR: If you guys can
18	produce a 25-page SER, give it to me. I'll read it
19	in my sleep.
20	CHAIRMAN BROWN: One of the things, if
21	everything is constantly, well, we did this in
22	accordance with Reference 27, well, that's fine.
23	I've got to go back and find it. Well, that's
24	great, but what are the points that you were trying
25	to review against? So, I mean

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	177
1	MR. STATTEL: The actual structure,
2	there's another annex within the ISG that kind of
3	lays out the structure of it, the chapter format.
4	I know there's a lot of sub-levels in that format,
5	but that's actually laid out in ISG-06, and we
6	followed that pretty closely.
7	CHAIRMAN BROWN: Well, I mean, this
8	corresponds pretty much to the sections that you
9	put your stuff in in the SER.
10	MEMBER STETKAR: That's right, except
11	why do I need to have separate discussions of very,
12	very similar guidance under, for example, 6 and 7
13	and 9 and 10, you know, in those chapters? Why do
14	I need to hear the same thing or maybe slightly
15	different things, which is more troubling, in those
16	different chapters.
17	CHAIRMAN BROWN: I agree. I agree.
18	That was cumbersome.
19	MR. STATTEL: It's a challenge. It's a
20	challenge for us.
21	CHAIRMAN BROWN: It was repetitious.
22	MEMBER STETKAR: The reason I bring it
23	up now is we're going to have a little section on
24	the path forward, and the path forward for kind of
25	streamlining these reviews retains some of this

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	178
1	discrete guidance sort of framework. It's got a
2	line item for IEEE 603. It's got a separate line
3	item for IEEE 7432. It's got a separate line item
4	for other additional guidance that's pushed off
5	until later. It's got another line item for maybe
6	integrating stuff later, later, later. Maybe it
7	ought to be pulled together like now, once and for
8	all.
9	MR. STATTEL: So I want to make sure I
10	cover the topic that we talked about earlier, the
11	open item table.
12	MEMBER STETKAR: Yes, I don't even know
13	how late we're going to run. I had to get it on
14	the record.
15	MR. STATTEL: But I do have a way to
16	save a little bit of time here. So the open item
17	table was something we had started with a previous
18	review, and it was basically a way for us to
19	interact with the licensee on a regular basis. We
20	had regular phone calls with the licensee, and
21	these were public calls. They were all noticed.
22	Well, not all of them but most of them. And to
23	facilitate those discussions, we used, basically it
24	was just a Word document table, and we wrote open
25	items. Now, these were not RAIs, and there were a

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433
lot fewer RAIs than there were open items. 1 I'll 2 just point that out. I don't have the exact 3 numbers here. But the idea was if you just have a 4 question as we're performing our evaluation, 5 we would write it down in an OI and allow the licensee 6 7 an opportunity to just respond. If they can answer 8 the question and say go read Section 6 of the 9 license amendment request, you dummy, you know, or 10 whatever, and just point us to the right place, 11 there's really no need to have а formal RAI 12 requesting exchanged because we're really not

there's a significant number of those things.

information for

that

example.

And we also don't like the idea of using RAIs as kind of a learning tool. So I don't understand how this works, so, licensee, go get the information and provide me an explanation of how this works. Well, that's not really a request for information. That's just kind of a learning experience, and we could do that outside of the RAI process.

23 tried to, So as best we could, we 24 restrict the RAIS to only actual requests for 25 additional information, and we tried to limit that

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

13

14

15

16

17

18

19

20

21

22

additional

(202) 234-4433

179

And

180 to a subset of information that we need to support 1 2 our safety conclusions. 3 So that was the function of the open Ι think there were like 4 item list. 63 RAIS 5 actually sent to the licencee in this case. Open there were more than a hundred of 6 items, obviously 7 those. And we have those tables. Those tables 8 pretty much, they're informal. We have shared them 9 with the public. We use them to facilitate our 10 conference calls, so we use them on an ongoing 11 basis. We're using them for several different 12 It's a pretty regular thing that we applications. 13 do. But they all go away when it's all said and 14 done, so when the license amendment is issued the 15 open item table just disappears. So the fact that we're referencing open 16 17 items in the safety evaluation, we recognize that 18 We acknowledge that. as a problem. And we will 19 certainly close those open items before the license 20 amendment is complete. 21 MR. LUBINSKI: Rich, if I can ask you 22 to maybe expand on that. John Lubinski, Director, 23 Division of Engineering. So with respect to that 24 specific open item, I think it was Open Item 115, 25 when we --

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	181
1	MR. STATTEL: I can talk about that.
2	MR. LUBINSKI: Yes, if you could. And
3	let me just get the high level is that at the time
4	the SE was submitted to ACRS, we had closed that
5	open item. We had had adequate answers. We had
6	just not updated that section of the document, so
7	it was an administrative error on not providing the
8	updated section to you.
9	That has been updated now. That item
10	was closed, and Mike was going to talk on the path
11	forward. It probably would be best is the
12	recommendation would be to provide an updated SE
13	that's a red-line version so that you can see the
14	differences between what was provided, and that
15	would have a clear indication of how that item was
16	closed.
17	As of today, the only item that is
18	still open has to do with the seismic issue. So I
19	think that's the short answer to the question.
20	How that item was closed Rich can talk
21	a little bit to
22	CHAIRMAN BROWN: We're running out of
23	time. Let's go ahead and move on through this,
24	okay? Because I do want to get on
25	MR. STATTEL: The next four or five

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	182
1	slides are really just concepts that we're
2	contemplating, that we're thinking about. I can
3	cover these, or you can read them and provide me
4	input separately if you want to go through them
5	CHAIRMAN BROWN: What I'm really
6	looking for is you all have a path you're going
7	to do something with ISG-06.
8	MR. STATTEL: Yes.
9	CHAIRMAN BROWN: Do you have a time
10	frame within which you have a I mean, there's a
11	lot of stuff going on. I mean, is this five years
12	away, or are you going to try
13	MR. LUBINSKI: Maybe we can talk a
14	little bit more during the next presentation how
15	that fits into timing.
16	CHAIRMAN BROWN: Okay, all right.
17	MEMBER BLEY: I really hope not.
18	MR. STATTEL: Let me talk briefly about
19	the concepts, and I can go through the slides
20	CHAIRMAN BROWN: You got five minutes.
21	MR. STATTEL: Okay, got it. So the
22	first concept, I'm on slide number 42, the first
23	concept is the living document concept. So a lot
24	of the documents that we look at and we base our
25	evaluations on, we know they're going to change.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

So the development process is happening as we're
evaluating these documents, so it really makes no
sense to submit revision one of the document and
then two months later two and then three and then
four.
So what we ended up with, and this has

7 happened a few times, we end up with four or five 8 or six submittals of the exact same document, and 9 there's really no point to that, especially because 10 we have a SharePoint. So the idea here is that, 11 during the acceptance review, early in the review, 12 we talk with the licensee, maybe during a Phase 0 meeting, and we decide at what point does 13 this 14 document, is it mature enough where you can docket 15 it and we use it as our safety base, so it only 16 gets docketed one time.

17 Now, in the interim, I can view it on a 18 SharePoint, and I know it's going to be docketed, 19 you know, when it reaches that level of maturity. 20 But that's the concept, right? And even after it 21 gets docketed, I know it might change after that, 22 but I have access to look at it, but I don't need to use it as a basis for my safety conclusions 23 The idea is to limit the amount 24 after that point. 25 of documentation repetition on the docket.

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

11

1

2

3

4

5

6

(202) 234-4433

1 2 3

concept is 2a. 1 The next Phase Ι 2 already talked about that one, so I'm going to move 3 to the next one, conditional letter of regulatory Well, we've gotten a lot of complaints 4 compliance. from licensees that they don't like the fact that 5 we wait until the factory test is complete until we 6 7 issue license amendment or our safety our 8 conclusions. And they say that puts a lot of risk 9 them because they're spending all their on 10 resources developing and building this system, and 11 they don't have any regulatory certainty that it's 12 going to get approved because they don't get the SE until really late in the process. 13 14 Well, the concept here is that, while 15 we can't really issue the safety evaluation but we 16 can give you a letter that kind of tells you, based 17 what we've seen, this is the status of our on

18 review. And this would be similar to a process we 19 use for the acceptance review. It's just on the 20 other end of the evaluation process.

21 Now, I'll just throw in here I kind of 22 with the licensees a little bit on this arque 23 because I think the risk is really on them. If we 24 were to approve the design at completion of design 25 build experience is before they it, my those

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

	185
1	systems undergo a lot of changes, and those changes
2	would invalidate our safety conclusions and they're
3	going to have to come back in with amendments, with
4	new amendments. And that's even more of a
5	regulatory risk, from my experience, because the
6	systems do change quite a bit from completion of
7	the design until the completion of the factory
8	tests.
9	MEMBER BLEY: When you say more of a
10	regulatory risk, in terms of the time it takes to
11	go through that process?
12	MR. STATTEL: Well, they kind of have
13	to start over again. And they may get a different
14	set of reviewers.
15	MEMBER BLEY: The same thing will
16	happen if you have a letter, wouldn't it?
17	CHAIRMAN BROWN: We approve DCDs for
18	new reactor designs when we've approved the
19	concepts for the I&C system, and there's been an
20	approval of that design concept as part of the DCD.
21	It's kind of locked in license-wise as to what it
22	looks like, and that doesn't have any factory
23	acceptance test. It doesn't even have a completed
24	design.
25	MR. STATTEL: That is true; and, yet,

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	186
1	those designs are not up and running yet and there
2	have been amendments to those designs.
3	CHAIRMAN BROWN: And we're still
4	expecting to go through that process with the staff
5	when those
6	MR. STATTEL: That's correct. So
7	that's what we're trying to avoid here. So in my
8	view, waiting until after the system is complete,
9	tested, we have results, gives me a lot more
10	assurance that that system is going to meet the
11	regulatory requirements. And there's a lot less
12	likelihood that you're going to have to come in
13	with an amendment before you start up that system
14	in the plant. That's just my view.
15	Yes, this is just my conclusion slide.
16	So, overall, we think ISG-06 processes have been
17	successful in clarifying the activities needed for
18	a license amendment. It's never going to be a
19	simple process because of the many regulatory areas
20	that need to be evaluated, but we also recognize
21	that further improvements can be made so that these
22	systems and the safety benefits they provide can
23	become a viable way to support the safe and
24	reliable operation of these plants.
25	Thank you for your time.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	187
1	MR. LUBINSKI: All right. Good
2	afternoon. I'm John Lubinski. I'm the Director of
3	the Division of Engineering in NRR, and what I
4	wanted to do was provide a briefing this afternoon
5	discussing the digital I&C integrated action plan.
6	The purpose of the briefing, this is an
7	informational briefing this afternoon to give the
8	ACRS a status where we are. What I want to do is
9	give an overview of the current action plan and, I
10	think most importantly, is to discuss with the ACRS
11	time frames for when we would like to come back to
12	ACRS and talk about more specific issues in where
13	we're going.
14	So from a background standpoint, I
15	guess one thing I do want to say here, it's not on
16	the slide, but I think, as part of today's
17	briefing, you heard that we do have a robust
18	process in place for the receipt review acceptance
19	of digital I&C upgrades, and we've shown that we
20	can do it. What we're looking at here is trying to
21	look at the feedback from the industry, as well as
22	areas where we believe we can increase the
23	efficiency of our processes.
24	The first item on the list talks about
25	SECY-15-0106, and this was a rulemaking, 50.55(a),

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

188 603 2009. 1 incorporate the IEEE That to was 2 discussed with ACRS going through the process, and 3 we did have an ACRS meeting on that. 4 What happened when that got to the is the Commission did ask us for 5 Commission a briefing on digital I&C. 6 The reason for that 7 briefing is the Commission wanted to understand how 8 important was the IEEE 603 to the upgrades at the What they're hearing from the industry is 9 plants. 10 that there are some challenges out there in 11 implementing digital upgrades, and the Commission 12 was trying to understand is 603 going to solve the 13 problem or not? 14 And the Commission direction was they 15 wanted to see the more holistic picture before they 16 could approve 603 to determine how important it was 17 to knocking down those barriers or challenges that 18 there were in the process. So the Commission 19 direction came back and basically said, as written, 20 they did not approve the incorporation of 603 and, 21 instead, directed the staff to put together an 22 integrated action plan in looking at what the 23 regulatory challenges are moving forward. 24 As part of doing that, actually, in 25 time frame, the Commission direction came out an

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	189
1	SRM February 25th of 2016. But we were already
2	working with the industry on a draft action plan,
3	and we had a public meeting on January 20th to
4	discuss that action plan. So we were getting
5	stakeholder input at that time.
6	So when the Commission direction came
7	out, we had a pretty good idea of where the
8	industry was collectively with what I'll call their
9	priorities. And the SRM talks about priorities, as
10	well, and there's some miscommunications about
11	that, as I'll explain as we go forward.
12	The Commission also directed a steering
13	committee to be formed. We have formed the
14	steering committee and put together a charter. As
15	the Director of the Division of Engineering in NRR,
16	I'm the chair of the steering committee. Other
17	members of the committee include the Director of
18	the Division of Engineering and Research, which is
19	Ryan Thomas; Mike Mayfield, who is the Director of
20	Engineering, Infrastructure and Advanced Reactors
21	in NRO. And then we have ad hoc members as
22	division directors from NSIR to do the
23	cybersecurity issues and also from NMSS. While
24	this plan is focused on reactors, we believe it's
25	important to coordinate with NMSS because they're

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	190
1	dealing with similar type issues and we need to
2	make sure that coordination takes place.
3	So we did develop the steering
4	committee. It also required an integrated action
5	plan to be provided to the Commission within 90
6	days from the date of the SRM, so May 25th is the
7	date that the action plan is due back to the
8	Commission. And it did ask us to focus on
9	stakeholder interactions as we're going through the
10	development of the plan, as well as going through
11	the process for implementing the actions in the
12	plan.
13	So what I'll talk about next is some of
14	the key items. We listed these as near-term
15	priorities, and that's why I said we're struggling
16	a bit when we talk about priorities because, if you
17	look at all the items in the plan, they have
18	importance to them. They have a prioritization.
19	But in listening to where the stakeholders are
20	coming back, we had to prioritize from the
21	standpoint of our resource expenditures at this
22	point. We only have so many resources within the
23	NRC and outside the agency. When we talk to our
24	external stakeholders, NEI has led the development
25	of a digital I&C working group that also has a

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

191 steering committee, and they're trying to 1 focus 2 their efforts on their top priority items. 3 So if you look at the list here, the 4 industry, and we just had a public meeting with 5 them last Wednesday and they reiterated that they believe that the top two issues that are presenting 6 7 regulatory challenges at this point are common 8 cause failures and our guidance for common cause 9 failures and guidance on 50.59 upgrades. They 10 believe that if we cannot get past those two 11 challenges then everything else doesn't matter 12 because they'll look at digital upgrades as being a 13 failure if we cannot get by those two challenges in 14 forward of moving because the cost and the 15 efficiency in trying to move those forward. So 16 they're definitely high on the list. So with respect to that, on the common 17

18 cause failure, we're dealing with the SRM in 1993, 19 for SECY-93-087, and we're looking at re-evaluating 20 that criteria to determine if it's adequate, if it 21 needs to be changed, should it be a more graded 22 approach, what type of risk information should we 23 be including in that as we move forward, and what 24 are the clear differences when we're dealing with 25 digital systems versus analog systems and are we

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

	192
1	really focused on those differences?
2	Right now, the schedule shows, our
3	proposed schedule that we'd like to engage ACRS in
4	the summer with where we are from that standpoint.
5	And we're hoping to go to the Commission with a
6	paper by the end of the calendar year and
7	definitely, with respect to that paper, that would
8	be, because we're talking about a potential change
9	in common cause failures and how they're assessed,
10	we would definitely want to engage ACRS and get
11	your input on that.
12	Let me go to the next one on the list
13	here, review of cybersecurity design aspects. This
14	is an issue that we have engaged with ACRS, and the
15	issue is whether or not we look at those during the
16	licensing process or not. As you know, as part of
17	Diablo, we did not do a full cybersecurity design
18	review. We have gotten engagement from external
19	stakeholders, mostly in the new reactor area, where
20	they would like to see us evaluate those as part of
21	the licensing process to provide them additional
22	certainty.
23	So we plan to come back in, I have
24	April - May here. I think actually May is when a
25	draft SECY paper will be provided to ACRS for

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	193
1	review. And I'm looking at Christina. I want to
2	say the June time frame is
3	MS. ANTONESCU: Oh, May 17th.
4	MR. LUBINSKI: I'm sorry. May 17th,
5	we'll be having a meeting with ACRS to discuss
6	that. What it looks like now, as a preview of the
7	paper we talked last week, is what we would be
8	proposing is this would be voluntary on the part of
9	the licensees, that they could come in and decide
10	whether they wanted it done as part of their
11	licensing review, the cybersecurity aspects.
12	And in order to do that, though, it
13	would also mean we need to update guidance because,
14	if we're going to be doing reviews of cyber, we
15	need to have guidance. And we also felt it was
16	important that, if staff identified a concern along
17	the way, even though we're not doing a cyber review
18	but something that may have impact, then that
19	should be identified early to the licensees for
20	certainty, so we would want to improve the guidance
21	in that area, as well, even though it's not a cyber
22	design review but providing guidance to staff on
23	how to address those types of issues. So, again,
24	we're looking at coming back to ACRS in the April -
25	May time frame.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

there's quidance for 1 And then 50.59 2 This hits a lot of aspects. upgrades. There's 3 been concerns in the past with the guidance that's currently endorsed by NRC. It's NEI document 0101. 4 5 That has led to a lot of misinterpretation by NEI has a commitment to provide us a 6 licensees. 7 new document for our review and endorsement, and I 8 believe the current commitment is that we would 9 have that by COB today. So looking that it's after 10 five, it may be in our inbox right now. So we'll 11 be reviewing that.

12 They're really looking at the scope to 13 try to determine, from an industry standpoint, how 14 many upgrades can be done under 50.59 versus those 15 amendments? coming in for licensing This also 16 would play, depending on how this 50.59 guidance 17 plays out in the view of the industry, to the issue 18 Rich brought up earlier about when do do you 19 factory acceptance testing and from a certainty 20 standpoint? There are many in the industry, and, 21 again, it's an opinion and we haven't made anv 22 decisions on it yet, but we've had recommendations 23 from the industry that we should complete our 24 licensing review before the factory acceptance 25 testing, and then they have the risk of whether

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

	195
1	they need to come back in with license amendments
2	or, if the changes are small enough, they can do
3	them under 50.59, and that provides them more
4	certainty.
5	MEMBER BLEY: I'm just curious. Have
6	those discussions followed the alternative path
7	that Rich mentioned earlier about some kind of a
8	letter stating the status?
9	MR. LUBINSKI: That was the other
10	option is, when we heard that from a factory
11	acceptance testing, we were looking at, again, this
12	letter of assurance and whether
13	MEMBER BLEY: You really haven't chased
14	that with the
15	MR. LUBINSKI: We haven't chased the
16	final answer to that yet. I don't want to speak
17	too much for the industry, but I believe where the
18	industry is is they're looking at where the 50.59
19	guidance may play out and what we would approve as
20	far as that guidance, and then that would help to
21	lay the groundwork for how would we take the next
22	step. So that's where they're looking at these
23	three items as I'm sorry? Did you have a
24	MR. WATERS: I'm sorry. The document
25	came in at 4:59.

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

1 MR. LUBINSKI: Yes, I was just 2 informed, 4:59, that we did get the document from 3 AI at 4:59 today, so they made it under the close 4 of business today.

So, again, that's where there's an interrelationship there. And where the industry would say to us at this point, if we were looking at making some of the changes, like the factory acceptance testing or the conditional letter that Rich talked about, is they'd want to see what kind of certainty there is in the 50.59 area first and bring that to closure, as well as the common cause failure.

14 believe the next items MP two are 15 important to list because this is what prompted the 16 reaction from the Commission the 603 was 17 rulemaking, lot of aspects of 603 and а the 18 rulemaking were centered also on IEEE 7432. So 19 what we've proposed right now in our action plan is 20 we will not, do no further action with respect to 21 603 2009 and, instead, we'll look towards the 2018 22 update and engage our external stakeholders, IEEE, 23 with respect to both of these activities from the 24 standpoint of the additional conditions that we had 25 proposed in the rulemaking and then the current

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

5

6

7

8

9

10

11

12

13

(202) 234-4433

direction we have back from the Commission to ensure that we're performance-based and technology neutral and try to work with those standard committees to determine how would they propose making any changes, if any, to 603 and 7432. And then we could make a decision, at that point, what we would need to do on the back-end of that from the standpoint of the 2018 version.

9 CHAIRMAN BROWN: I'm trying to 10 remember. There was a meeting or some public 11 meeting or some type of discussions where some of 12 items or the conditional items added to the 603 2009 to cover some of the technical issues that 13 14 people have been addressing weren't even going to 15 be considered for inclusion in the 2018 version. 16 That was just something I read from the, I don't know, public meetings --17

MEMBER BLEY: No, we had some discussion about that in one of our meetings some time ago, a couple of years ago.

21 CHAIRMAN BROWN: Okay. So maybe that's 22 what's ratcheting around. That seems -- I don't 23 have a problem with what you're saying. That's not 24 what I'm trying to, that's what I'm stumbling over 25 that, if you're qoinq here, except to issue

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

3

4

5

6

7

8

18

19

20

(202) 234-4433

	198
1	guidance for 10 CFR 50.59 upgrades in terms of how
2	the process is, you still have to have what you
3	want to accomplish as a fundamental basis for
4	making sure that the systems meet the fundamental
5	principles of, you know, independence, redundancy,
6	deterministic, diversity, defense-in-depth.
7	And from the cybersecurity standpoint,
8	cybersecurity gets mixed up. Fundamentally, that's
9	control of access, no matter how you slice it. If
10	you don't have access, you don't have a
11	cybersecurity issue externally. That doesn't mean
12	you can't have some guy come down and do something
13	funky.
14	So somehow, if those items get lost in
15	the process, there were a lot of very good
16	conditional items stuck in, not stuck in but
17	incorporated in 2009 because we've been fighting
18	about those during the new design reviews and other
19	types of reviews. Oh, it's not required;
20	therefore, we're not going to do it. If you lose
21	your independence, you're toast. It doesn't matter
22	what you do.
23	So to my mind, if you're going to do
24	something with I have no problem with looking at
25	the process, but you've got to have a strategy for

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	199
1	how do I ensure that these fundamentals are met
2	when these designs are accepted?
3	I agree there's a lot of piecemeal
4	stuff with all the various IEEE specs, the general
5	design criteria, and the various requirements in
6	other reg guides. There's a lot of little a piece
7	here and a piece there, and it gets very difficult
8	for the vendors and the licensees. Very difficult.
9	I totally understand their quandary.
10	Anyway, that's just
11	MR. LUBINSKI: Two points on that.
12	We're not going to lose those issues. We made it
13	very clear in our action plan with each of those
14	issues we plan to do a
15	CHAIRMAN BROWN: Oh, I read the whole
16	thing last night.
17	MR. LUBINSKI: we plan to do a final
18	disposition. Where we are right now is that, given
19	the new direction we got back from the Commission
20	in the SRM and to engage stakeholders, we felt it
21	was important first to go back to the owners of
22	those documents. We actually had a member of the
23	IEEE at the digital I&C commission meeting, as
24	well, and some of those issues weren't clearly
25	communicated as far as what their position was. So

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	200
1	we're really looking at trying to get a clear
2	position from the standards committee so that then
3	we can make our decisions on how to move forward.
4	One of the difficulties is the next
5	opportunity is going to be in July, and that will
6	be at NPEC. Ryan Thomas is our standards
7	executive, and he's going to try to set up a call
8	in the near term so that we can start to engage
9	IEEE from the standpoint of how they would address
10	these issues and what kind of communication and
11	interaction we would have.
12	With respect to how some of those
13	issues relate to common cause failure, 50.59, of
14	course we'll be evaluating those as we look at any
15	changes we would make in those areas.
16	CHAIRMAN BROWN: My concern is it's
17	just common cause failure is just not the only
18	major consideration that has to be factored in to
19	what do you want to accomplish at the end. I mean,
20	you say it's the biggest issue. Well, I could
21	probably argue it might not be the biggest issue
22	because there are other barriers you can put in
23	place that really help you.
24	The other point is a lot of these
25	standards or these requirements that were built,
	NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	201
1	they were built back in the analog days, and we're
2	struggling to try to apply those analog
3	requirements into the digital world with a
4	technology that's totally different in terms of its
5	execution and operation.
6	MEMBER BLEY: I have a couple of
7	questions. It's hard to have a problem with having
8	an overall plan, unless we spend two or three more
9	years finalizing the plan. Are you guys kind of
10	onboard with the two things the industry thought
11	were the highest priorities here? You have other
12	things up in your list that I saw recently.
13	MR. LUBINSKI: Sure. Well, with
14	respect to that, I would say really the top three
15	items that you see on this list because we've had
16	the most near-term interaction. If you take the
17	bottom two items, if we're looking more towards the
18	2018 standard and where we're going, that could be
19	a longer time frame. But given what we're hearing
20	from the industry, we're aligned because, number
21	one is we have identified instances where licensees
22	have misapplied 50.59, and we think it's important,
23	and we actually raised that to the industry a
24	couple of years ago and they had a commitment a
25	couple of years ago to start to upgrade the

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

	202
1	guidance.
2	MEMBER BLEY: I'm personally not
3	familiar with NEI 0101. I don't know if we
4	actually have that. I've never seen it.
5	MR. LUBINSKI: What our understanding,
6	and we just got the document
7	MEMBER BLEY: Oh, is that
8	MR. LUBINSKI: at 4:59 today.
9	Actually, they're going a little different. We had
10	thought they were going to be a revision, and it
11	was NEI 0101, and what they were trying to do was
12	capture in that document kind of what we did in
13	ISG-06 of bring everything you need into that one
14	document, and it had all the technical evaluations
15	for how you would go through the 50.59 review. So
16	it was both regulatory and technical.
17	What they've decided to do now, they've
18	already got another document for 50.59, 9607 I
19	believe is the number, NEI 9607, and they said,
20	instead, we'll provide a new document that just
21	talks about the regulatory aspects of 50.59 and
22	make that Appendix D to 9607, and that will be a
23	full replacement for the NEI 01.
24	Now, the problem is many of these
25	technical issues, such as common cause failure, how
	NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	203
1	do you address those, you know, if you're just
2	staying at a high level? So we really can't
3	comment yet until we see the document.
4	MEMBER BLEY: It doesn't happen at high
5	levels.
6	MR. LUBINSKI: Right. Now, in
7	answering your question, I think, from a timing
8	standpoint, we believe with respect to all three of
9	these issues, by the end of this calendar year
10	we'll have made significant progress on identifying
11	do we believe we can accept, even with some
12	modifications to 50.59 guidance, we believe we'll
13	be engaging the Commission on the cybersecurity
14	probably through an info paper, and we'll be
15	engaging the Commission on the common cause
16	failure, as well.
17	So I think, as you said, without taking
18	a couple of years to sit back and put everything in
19	a plan, we think making progress on those top three
20	items within the first nine months of the plan is
21	going to tell us whether or not we're on the right
22	path, and then it would be a living plan to
23	readjust at that point.
24	MEMBER BLEY: I could buy that, yes.
25	MEMBER STETKAR: John, you haven't
	NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	204
1	gotten to the next slide, and I was going to wait
2	
3	MR. LUBINSKI: I can go to the next one
4	because I think we're done
5	MEMBER STETKAR: Okay. Flip over to
6	the next slide but remember this slide. And don't
7	go through these in detail. Just let me ask you
8	something. The last two items on the previous
9	slide, which were identified as being in the top
10	five but not as important as the top three, and the
11	second, third, and fifth items on this slide, to
12	me, are all the same thing. If you don't look at
13	it piecemeal, if you look at it as what is
14	regulatory guidance for NRC review of digital I&C
15	submittals, those are all part of the same thing.
16	They're all just bits and pieces of the same thing.
17	
18	So why perpetuate this notion of
19	parsing things up? Why do I need a separate item
20	for one IEEE standard compared to a different IEEE
21	standard compared to Lord knows, you know, 15
22	different reg guides. I bring up Samir's slide
23	here that is mind boggling in terms of this
24	paragraph of this revision of this reg guide that
25	refers to this chapter of that guidance in that

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	205
1	standard. Why aren't they all rolled into one? We
2	have an item to update regulatory guidance to make
3	it coherent and consistent. Not piecemeal,
4	coherent and
5	MR. LUBINSKI: Yes. And this is where
6	
7	MEMBER STETKAR: you can't do that
8	by the end of this calendar year probably. But you
9	might be able to do it by the end of next calendar
10	year if you set that as a goal. I don't need to
11	wait until 2018 for this particular change to this
12	particular standard or 2020 for this particular
13	change to this standard or to the next five-year
14	cycle for upgrading a particular reg guide or
15	something like that.
16	MR. LUBINSKI: Yes. So when I look at,
17	from the standpoint of updating the regulatory
18	guidance and the question was where do we see this,
19	and you asked are we talking five years away, and
20	Rich said, "I hope not," I'll agree with Rich.
21	We're not looking to go five years out on this.
22	What we believe, though, is with
23	respect to a couple of these issues, the 50.59 and
24	the CCF have some technical
25	MEMBER STETKAR: I got that. I wasn't

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

arguing with the first three bullets on your previous slide.

3 MR. LUBINSKI: No, I was just trying to explain though is I think, coming out of that, if 4 5 look at what prompted you to update the you regulatory guidance, so let me go that direction 6 7 instead is what prompted update me to the 8 regulatory guidance is, number one, the lessons 9 learned that Rich just talked about from the 10 review, and we have a clear set of those right now. 11 Some of those are pretty easy. Other ones are 12 going to be a little more difficult because, once 13 you start into the process, the letter process that 14 Rich talked about, there's going to be a lot of 15 engagement with the industry and we're sure the 16 industry is going to say, no, we stick to our 17 original recommendation of we want you to issue 18 this before the factory acceptance testing.

19 So what we want to be able to do is not 20 update the guidance piecemeal but try to identify, 21 at least up-front, what are the key issues that 22 we're going to put into guidance. So the one input is the lessons learned we just received. 23 The other 24 input, of course, is the first three on the other 25 We won't wait until the end of 2018 to page.

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

1

2

(202) 234-4433

	207
1	update the regulatory guidance. We'll know
2	up-front where we believe IEEE is going. Are they
3	even going to address these issues in the 2018
4	version? If they're not, how are we then going to
5	address those collectively in the guidance.
6	MEMBER STETKAR: John, you still
7	answered my question, though, in the context of the
8	existing framework, which is piecemeal. You said
9	we aren't going to wait until the end of 2018 to
10	update, you know, this little piece of this
11	regulatory guide and this little piece of this
12	regulatory guide. I'm saying wipe the slate clean.
13	You don't have any regulatory guidance. You have a
14	bunch of standards, you have a bunch of knowledge,
15	re-write SRP Chapter 7 and regulatory guidance.
16	MR. LUBINSKI: And we've looked at
17	that, as well. And that actually came up as a
18	comment we heard last week and some internal
19	stakeholders, and, among our working group that's
20	looking at this right now, we haven't fully
21	addressed that issue. The one concern with that is
22	wiping the slate clean and starting from square
23	one. That's not a one-year review process
24	MEMBER STETKAR: It isn't a one-year
25	review process; I'll give you that. It's not a

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

one-year review process. But the problem is, once 1 2 you start down this path of piecemeal updates to 3 things as you learn stuff, you just perpetuate this notion of somebody creating a slide that looks like 4 5 this, that I reviewed this paragraph of this 6 particular req guide which referred to this 7 paragraph and this sentence over here, which is 8 slightly different than this guidance over here. And it just keeps going. 9 10 MR. LUBINSKI: And here's where I'm 11 hesitating a bit. I'll use your words. It's a 12 subcommittee meeting where I can say what I want. 13 MEMBER STETKAR: It's a subcommittee; 14 that's right. I wouldn't say it in а full 15 committee meeting. 16 MR. LUBINSKI: So what I'll say is we 17 had our meeting with the industry last week on our 18 action plan and got a lot of comments back and 19 there were a lot of internal discussions after 20 that, as well. It was also with some internal 21 briefings. 22 So as I was going through and thinking 23 about this over the weekend, I had the same thought 24 you did. And, you know, maybe one of the items on 25 this action plan should be, once you hit this

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

integrated point to say what did I now learn, 1 how 2 do we set up what the framework looks like in the 3 future, right? In other words, the entire 4 framework. That's not going to be to say that you 5 fully implement it, but you develop over some short time period, at a key point, here's 6 what the 7 framework looks like, now I can work towards that 8 end vision, that end goal, and then take these 9 changes and put that in there. 10 Now, the reason I was hesitating that 11 is that's just something that's not been discussed 12 with our steering committee or our working vet 13 groups --14 MEMBER STETKAR: That's fine. And it's 15 revolutionary as wiping the slate clean not as 16 because I think that you have most of the building The problem 17 blocks there. is they're at the 18 probably fragmented Lego perspective, rather than, 19 you know --20 MR. LUBINSKI: And I think Rich's 21 comment, and I would agree with it, in the lessons 22 learned is, looking at ISG-06 and the way we pulled 23 information into it, yes, it would probably be 24 better iust doing references to these other 25 That way, as changes are made in the documents.

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

	210
1	future, we can just reference the documents. And
2	then if there's any conditions, they go right into
3	that guidance.
4	MEMBER STETKAR: Things always change.
5	MR. LUBINSKI: So I appreciate the
6	comment. I feel a little bit better about my
7	thoughts over the weekend.
8	MEMBER STETKAR: Good. So long as
9	weekends are good.
10	CHAIRMAN BROWN: Since we're sitting
11	here chitchatting, the SRM very clearly stated
12	you've got to look at this thing from a
13	performance-based standpoint, and I've yet to
14	figure out, I've been struggling with this ever
15	since I read it, how do I define independence via
16	performance-based performance? Am I going to have
17	to argue with somebody every time, or is
18	independence really independence, or is it sort of
19	independent but, if I do it on a performance base
20	and I can prove I've got some other way to make
21	sure it's independent but you don't miss it? How
22	in the world do you come up with a
23	performance-based approach, other than being able
24	to drop a barrier between the things and there's no
25	communication? That's prescriptive if you say

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	211
1	don't communicate.
2	MR. LUBINSKI: Right. Now, at a high
3	level, we had this discussion last week, as well,
4	and we believe the guidance from the Commission, if
5	you read on the SRM, is it's performance-based
6	requirements, okay?
7	CHAIRMAN BROWN: But how do you make
8	independence a performance-based requirement?
9	MR. LUBINSKI: If I could go on, then
10	the question is, listening to the Commission from
11	the standpoint of the Commission meeting, as well
12	as reading into their vote sheets on this issue, as
13	you then implement and you look forward, of course
14	the technology is going to continue to change, and
15	there could be other ways to just say don't have
16	communication for independence. Do I know what
17	they all are at this point? No. But to be able to
18	develop that in guidance space rather than in
19	regulatory space is where I believe the Commission
20	really had their direction.
21	So in guidance space, and this was
22	another discussion we had last week, it is
23	sometimes very simple to say, yes, if you have no
24	communications, that's independence, you meet it.
25	Okay. We know that. But that doesn't mean that's

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	212
1	the only way.
2	CHAIRMAN BROWN: Sure it does.
3	MR. LUBINSKI: For some people.
4	CHAIRMAN BROWN: No.
5	MR. LUBINSKI: So that's
6	CHAIRMAN BROWN: It worked that way in
7	the analog world. You didn't talk from one channel
8	to the other, period. It didn't, it's technology
9	neutral.
10	MR. LUBINSKI: And the reason I'm
11	saying that is, if you look at the conditions that
12	we had in the 603, it talked about that you could
13	have those communications if there was a safety
14	benefit.
15	CHAIRMAN BROWN: I'm sorry, but we
16	argued about that and we were ignored. Not
17	ignored. Our recommendations were not accepted.
18	Let me put it in a nice, polite framework. Voting
19	units are one thing, but we proposed you have to
20	vote somewhere, and, if you vote digitally, then
21	you have to do something else to get guarantee, and
22	you can do that. And that's why you have to watch
23	the log timers on the voting units if you're
24	dealing with microprocessors. And we phrased that
25	in technology-neutral language. It was not

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	213
1	specific. You had to monitor it with non-software
2	based equipment that if something happened then you
3	got a trip out of that channel. But my point being
4	is there are, from a fundamental standpoint, there
5	are prescriptive fundamentals that you have to
6	implement in a manner that's a barrier. You can't
7	be quasi-independent. I've got, I mean, I started
8	doing this 37 years ago. In 22 years, we delivered
9	stuff for submarines, aircraft carriers. And
10	believe me, you could have taken a steel plate and
11	driven it down between the channels and you
12	wouldn't hit any wires. And all the voting today
13	is done analog-wise with bistables.
14	MR. LUBINSKI: Right. Well, I'm not
15	going to talk about the full review but
16	CHAIRMAN BROWN: My point being is that
17	you've got, in terms of John's thought process,
18	you've got to start mapping and you've got to start
19	thinking outside of the box a little bit. What do
20	you want to accomplish? How do you maintain the
21	ability for these systems to maintain their
22	performance and shut down the plant or initiate
23	safeguards when they need to? That's the
24	overarching requirement. Some people start fuzzing
25	it up with these funny base words of

NEAL R. GROSSCOURT REPORTERS AND TRANSCRIBERS1323 RHODE ISLAND AVE., N.W.(202) 234-4433WASHINGTON, D.C. 20005-3701

	214
1	performance-based this and that and think no
2	prescriptive stuff is ever required.
3	Technology-neutral sounds good, and you can do that
4	the way you phrase it. But independence is not
5	independence if somebody figures out another way to
6	be independent.
7	MR. LUBINSKI: And that's an issue.
8	Today, we're talking about our plans for moving
9	forward, but, from the standpoint of how we address
10	those issues, we'll definitely be back with you
11	guys and talk about that.
12	So from a communications standpoint,
13	one of the things that also was good feedback last
14	week from the industry and in a meeting and we'll
15	continue to look at is even the wording on these
16	two slides, and I mentioned the word priorities, we
17	call this near-term priorities, and then we talked
18	about the other actions. We really need to look at
19	how do we integrate those into an integrated plan
20	so there's not a thought process? Because it's not
21	our communication to say, yes, these things are
22	hanging out there, and if we get to them in the
23	next five years that will be fine. That's not our
24	intent. We still want to address these issues, but
25	how do we integrate that from the standpoint of

NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433
	215							
1	what resources we have today and what the industry							
2	has in addressing those issues?							
3	Stakeholder interactions, just talk							
4	about a couple of things what we've had so far and							
5	where we're moving forward is we did have a meeting							
6	on the first version of the action plan with the							
7	public in January, had a RIC session. The 21st of							
8	March, we had a public meeting talking about CCF, a							
9	lot of good input on the scoping of that project							
10	and where that's going. We did release the plan on							
11	the 24th, had a public meeting on the 30th, just							
12	last week. So you can see a lot of things are							
13	moving quickly here.							
14	We have a meeting scheduled on the							
15	26th, our second meeting on CCF that's in our plan.							
16	And then on the 28th, we have a public meeting to							
17	talk about the NEI guidance that we just received							
18	today, and, again, on May 25th is when we'll							
19	provide the SECY to the Commission with our action							
20	plan for moving forward.							
21	I was remiss in noting as one of the							
22	other items that was in the SRM was to provide the							
23	Commission any policy issues that we believed were							
24	right for consideration at this time, and we don't							
25	expect any policy issues to be provided in the							

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	216
1	paper at this time. Given the time frame, we're
2	looking at just the planning at this point. The
3	policy issues will be identified to the Commission
4	as we go through each of the items in the plan, and
5	that will be when we engage the Commission on those
6	items.
7	I already talked a bit about the
8	interactions with ACRS. Of course, May 17th, as
9	Christina reminded me, is when the draft SECY to
10	ACRS for review and discussion. This summer, we'll
11	be back with ACRS to talk about our CCF working
12	group activities and then in the fall to talk about
13	50.59 and where we're going there.
14	Of course, any other issues, such as if
15	we were to go through a rulemaking or a major
16	guidance development, we will be putting
17	interactions into the plan and work with Christina
18	on when the best time frame is for interacting with
19	ACRS.
20	CHAIRMAN BROWN: Okay. I mean, I can't
21	speak for the committee. I mean, we're here just
22	discussing this stuff, which we very much
23	appreciate the candid discussion. I think it's
24	always useful to do that. Yes, we saw the planned
25	interactions, and I presume that, if the committee

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

so decides, that they may ask for some additional interactions based on specific subjects based on what we see.

1

2

3

I did see the action, I did read the 4 5 action plan last night, and it's, you know, got a lot of stuff in it, some of which some of us may be 6 7 concerned about or not, as we've voiced. But it's 8 a challenge, and my biggest concern is that we are 9 losing, we may lose sight of the top-level strategy 10 on what we're trying to accomplish by putting in 11 what Ι call policy thought processes that don't 12 deliver -- I may phrase that wrong, but that aren't 13 based on what we're trying to accomplish with these 14 I mean, they have a very large and very systems. 15 critical safety component them, their to and 16 performance should not be diluted, D-I-L-U-T-E-D, 17 diluted, just D-E-L-U-D-E -- a little play on words 18 there -- in terms of their ability to accomplish 19 those functions so that we get a mishmash of stuff 20 is justifying, you where everybody know, some 21 unusual or different things because, oh, gee, well, 22 I can show you I can make this work. And if you 23 think your work is difficult now, it will be even 24 harder if you don't have а clear set of 25 requirements that can be envisioned as to how they

> NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

217

	218							
1	can be done that the licensees and vendors have to							
2	work with.							
3	MR. LUBINSKI: Appreciate that. And,							
4	yes, we would, you know, on your first point of							
5	additional engagement on any of the subjects, yes,							
6	without a doubt, we would, as we're going through							
7	the processes and plans							
8	CHAIRMAN BROWN: And we appreciate							
9	that.							
10	MR. LUBINSKI: we do that. And, of							
11	course, if there's any comments right now about							
12	where you would want some additional interactions,							
13	we would definitely put that in.							
14	We are a little bit different, and I							
15	should have said this earlier, we put this document							
16	out for comment, but, unlike a rulemaking where we							
17	put it out for 30 days and we sit back and wait for							
18	comments, we're continuing to modify the plan and							
19	have engagement along the way just because of the							
20	short time frame. So every week, the document							
21	continues to be updated based on the comments we're							
22	getting, so I appreciate the comments today so that							
23	we can incorporate those, as well.							
24	CHAIRMAN BROWN: Okay.							
25	MR. LUBINSKI: So thanks for the							
	NEAL R. GROSS							

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

	219							
1	opportunity to allow us to give an overview.							
2	CHAIRMAN BROWN: Any other comments							
3	right now? Anybody in the audience care to make							
4	comments on the presentation or the content of the							
5	meeting? Is the line open? Can somebody on the							
6	phone line say something just to let me know that							
7	it is open?							
8	MR. CLEFTON: Yes, this is Gordon							
9	Clefton, a member of the public. I'd like to							
10	compliment Ross and John and Rich Stattel for their							
11	good representation of the interface we've had with							
12	the NRC and NEI and look forward to continued							
13	interface in the near weeks.							
14	MR. LUBINSKI: If I could add, Mr.							
15	Clefton introduced himself as a member of the							
16	public. He has worked with us through NEI on these							
17	issues up until his retirement from NEI a couple of							
18	weeks ago.							
19	CHAIRMAN BROWN: Oh, okay. Oh, thank							
20	you. Didn't realize that.							
21	MEMBER STETKAR: Congratulations,							
22	Gordon.							
23	MR. CLEFTON: Thank you very much.							
24	It's been a long time coming.							
25	CHAIRMAN BROWN: Is there anyone else							
	NEAL R. GROSS COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. (202) 234-4433 WASHINGTON, D.C. 20005-3701 (202) 234-4433							

	220							
1	on the line that would like to make a comment?							
2	Hearing none, could you go make sure it's closed?							
3	One last round here. John?							
4	MEMBER STETKAR: I don't have anything							
5	more. As far as the Diablo Canyon application and							
6	the SER, I really appreciate the briefing. I							
7	thought it covered a lot of ground, and I don't							
8	have anything more to add. Thank you.							
9	MEMBER BLEY: Nothing more from me.							
10	Thank you.							
11	CHAIRMAN BROWN: Joy?							
12	MEMBER REMPE: Nothing more. Thanks.							
13	CHAIRMAN BROWN: Myron? Okay. I do							
14	want to thank the staff. I thought this was a very							
15	good meeting today. We did try to cram quite a bit							
16	into a very short period of time, and I think there							
17	was a lot of very good discussion along the way							
18	that was useful and I thought the staff did an							
19	excellent job of presenting it and answering the							
20	questions. And I look forward to having the full							
21	committee meeting in May. Richard, you'll							
22	obviously have to spiff up the slides a little bit.							
23	John, did you have some other comment?							
24	Other than that, I want to thank							
25	everybody, and we'll close the meeting.							

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS 1323 RHODE ISLAND AVE., N.W. WASHINGTON, D.C. 20005-3701

(202) 234-4433

							221
1		(Whereupon,	the	abov	ve-refer	red	to
2	matter	went	c off	the	record	at	5 : 38
3	p.m.)						
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
				~			

DIABLO CANYON POWER PLANT PROCESS PROTECTION SYSTEM REPLACEMENT ACRS Digital Instrumentation and Control Systems Subcommittee Meeting April 4, 2016



Ken Schrader Principal Engineer PG&E kjse@pge.com 805-545-4328

Kate Williams Senior Project Manager PG&E <u>k2w8@pge.com</u> 805-545-6615

Scott Patterson Consultant



- NRC Interim Staff Guidance 6 (ISG-06), Licensing Process for Digital I&C System Modifications, Pilot Application
- Process Protection System (PPS) Replacement Design
- PG&E ISG 6 Lessons Learned

ISG 6 Pilot Application

- Diablo Canyon is pilot plant for use of ISG 6
 PG&E participated in ISG 6 working group
- PG&E submitted pilot application 10/26/11 and supplement 04/30/13
- Process Protection System replacement
 - Invensys Tricon Version 10
 (PLC based, triple redundancy)
 - Westinghouse Advanced Logic System
 - (FPGA based, redundancy and diversity)



Project Scope



 Process Protection System Replacement Architecture



- PPS Replacement design is simple to improve safety
 - No use of cross channel communications
 - No two-way safety communications from nonsafety components to safety-related components
 - No signal voting of channels
- The PPS Replacement design eliminates the need to perform Manual Operator Actions to cope with a software CCF within the PPS

PPS Current Eagle 21 Design







PPS Current Eagle 21 Design





PPS Replacement Design Tricon Function Allocation



PPS Replacement Design Tricon Function Allocation



PPS Replacement Design ALS Function Allocation



PPS Replacement Design ALS Function Allocation



- Only one design change resulting from NRC review
- Original design shared 1 non-safety maintenance workstation computer for both Tricon and ALS subsystems in each division
- NRC questions were on testing plan and software requirements following software updates
- PG&E voluntarily changed design to use separate computer for each subsystem in each division
 - Simplifies testing requirements and eliminates potential vendor software interaction issues

Conclusion

- The PPS Replacement design provides significant improvements in safety, reliability, and human factors
 - Designed using latest NRC guidance (ISG-04 and ISG-06)
 - Utilizes current state-of-the-art NRC-approved PLC and FPGA technology with built-in internal redundancy and selfchecking diagnostics
 - Eliminates the need for operators to perform manual actions to cope with a software CCF within the PPS
 - Lessons learned from recent plant digital upgrades have been incorporated



Protecting People and the Environment

Diablo Canyon Process Protection System License Amendment Request Informational Briefing

ACRS I&C Subcommittee Meeting

Presented by: NRR / EICB

Maryjane Ross-Lee Mike Waters Rich Stattel Rossnyev Alvarado Samir Darbali Deputy Director DE Branch Chief EICB Technical Reviewer EICB Technical Reviewer EICB Technical Reviewer EICB



Protecting People and the Environment

- Introduction
- Evaluation Topics
 - Diversity and Defense in Depth (D3)
 - System Time Response / Deterministic Performance
 - Communication Independence
 - Control of Access
- Lessons Learned on the Digital I&C Licensing Process (ISG-06)



Introduction Diablo Canyon PPS Replacement LAR

Protecting People and the Environment

- Diablo Canyon License Amendment Request Submitted (October 26, 2011)
 - LAR is to replace the existing Eagle 21 Process Protection System with a new more modern digital system.
 - The Diablo Canyon Digital Process Protection System (PPS) is based on both the Microprocessor based Invensys Tricon and the FPGA based Westinghouse ALS Platforms.
- License Amendment Accepted for review (January 13, 2012)
- Safety Evaluation Complete (March 23, 2016)
 - Open Item: Confirmation of Seismic Local Environment Qualification

PROCESS PROTECTION SYSTEM REPLACEMENT ACRS Digital Instrumentation and Control Systems Subcommittee Meeting April 4, 2016



Ken Schrader Principal Engineer PG&E kjse@pge.com 805-545-4328

Kate Williams Senior Project Manager PG&E <u>k2w8@pge.com</u> 805-545-6615

Scott Patterson Consultant

Agenda

- NRC Interim Staff Guidance 6 (ISG-06), *Licensing Process for Digital I&C System Modifications*, Pilot Application
- Process Protection System (PPS) Replacement Design
- PG&E ISG 6 Lessons Learned

ISG 6 Pilot Application

- Diablo Canyon is pilot plant for use of ISG 6
 PG&E participated in ISG 6 working group
- PG&E submitted pilot application 10/26/11 and supplement 04/30/13
- Process Protection System replacement
 - Invensys Tricon Version 10
 (PLC based, triple redundancy)



- Westinghouse Advanced Logic System
 - (FPGA based, redundancy and diversity)



Project Scope



Process Protection System Replacement
 <u>Architecture</u>



- PPS Replacement design is simple to improve safety
 - No use of cross channel communications
 - No two-way safety communications from nonsafety components to safety-related components
 - No signal voting of channels
- The PPS Replacement design eliminates the need to perform Manual Operator Actions to cope with a software CCF within the PPS

PPS Current Eagle 21 Design






PPS Current Eagle 21 Design



PPS Replacement Design



2 of 3

Aux Feedwater Initiation

PPS Replacement Design Tricon Function Allocation



PPS Replacement Design Tricon Function Allocation



PPS Replacement Design ALS Function Allocation



PPS Replacement Design ALS Function Allocation



PPS Replacement Design

- Only one design change resulting from NRC review
- Original design shared 1 non-safety maintenance workstation computer for both Tricon and ALS subsystems in each division
- NRC questions were on testing plan and software requirements following software updates
- PG&E voluntarily changed design to use separate computer for each subsystem in each division
 - Simplifies testing requirements and eliminates potential vendor software interaction issues

Conclusion

- The PPS Replacement design provides significant improvements in safety, reliability, and human factors
 - Designed using latest NRC guidance (ISG-04 and ISG-06)
 - Utilizes current state-of-the-art NRC-approved PLC and FPGA technology with built-in internal redundancy and self-checking diagnostics
 - Eliminates the need for operators to perform manual actions to cope with a software CCF within the PPS
 - Lessons learned from recent plant digital upgrades have been incorporated



Diversity and Defense in Depth (D3) Guidance

Protecting People and the Environment

- Guidance for Diversity Assessment
 - SRM to SECY-93-087 Item II.Q Establishes NRC policy for Diversity and Defense in Depth
 - NUREG/CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems
 - Branch Technical Position (BTP) 7-19 Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems
 - Interim Staff Guide (DI&C-ISG-02) Diversity and Defense-in-Depth Issues



Diversity and Defense in Depth (D3) Analysis Preformed by Licensee

Eagle 21 (1993)

Assumed CCF of PPS resulting in loss of all PPS safety functions

Replacement PPS System (2011)

Assumed loss of all Functions performed by the Tricon Subsystem.

- Update to previous analysis tables
- All plant accidents and AOO's are included in the analysis
- Identifies three parameters for which there is no existing automatic diverse backup function.
 - Pressurizer Pressure
 - Containment Pressure
 - RCS Flow
- Describes ALS diversity and postulates CCF of ALS. This CCF does not result in loss of ALS assigned safety functions



Diversity and Defense in Depth Diablo Canyon PPS Diversity

Protecting People and the Environment





Diversity and Defense in Depth Diablo Canyon PPS Diversity

Protecting People and the Environment





Diversity and Defense in Depth Diablo Canyon PPS Diversity



* OR function is accomplished by DO contacts in series for De-energize To Trip (DTT) or in parallel for Energize To Trip (ETT) function.



Diversity and Defense in Depth Diablo Canyon PPS Diversity



* OR function is accomplished by DO contacts in series for De-energize To Trip (DTT) or in parallel for Energize To Trip (ETT) function.



Diversity and Defense in Depth Diablo Canyon PPS Diversity

Protection Set 3 Protection Set 1 Protection Set 2 Protection Set 4 (\times) (\times) \bigotimes $(\times$ Core Core Core Core Logic B Logic A Logic B Logic B Logic A Logic B Logic A Logic A SSPS Coincidence Voting Safety Component Actuation

* OR function is accomplished by DO contacts in series for De-energize To Trip (DTT) or in parallel for Energize To Trip (ETT) function.



Diversity and Defense in Depth Anticipated Transient Without Scram (ATWS)





Diversity and Defense in Depth Manual Operator Action

- The new Diablo Canyon Digital Process Protection System eliminates the need to perform Manual Operator Actions as a means of coping with a software CCF within the PPS.
- The modification does not however affect the ability of operators to perform manual actuations of safety functions.
 - Manual Initiation signals are provided directly to the SSPS system which is not being modified.
 - Previously credited Manual Operator Action controls will still be available to the operators.
 - Existing component and division level actuation capability at the main control boards will be retained



PPS System Time Response / Deterministic Performance

- The NRC staff determined that there is adequate diversity within the plant design that the plant responses to design basis events concurrent with potential software CCF of the PPS system meet the acceptance criteria specified in BTP 7-19.
- The NRC staff determined that the ALS and Tricon subsystems of the PPS are sufficiently independent and diverse from each other such that any failure of either subsystem will not result in a condition that is not accounted for in the plants accident analysis.
- The DCPP PPS design includes diverse means of providing required safety functions in the event of a PPS software CCF.



System Time Response / Deterministic Performance

- Deterministic performance characteristics for each platform were evaluated and accepted by the NRC as part of the associated platform safety evaluation.
 - Each SE considered the following system characteristics;
 - Input and Output Signal Processing
 - Data Transfer Methods / Techniques
 - Software or Logic Implementation Structure
 - System Diagnostic functions
 - The NRC also evaluated Application Specific Characteristics of the PPS including:
 - System loading
 - Application architecture



ALS System Time Response / Deterministic Performance

- No Embedded Microprocessor Cores
- FPGA Design Does not use Interrupts
- Deterministic sequence of performing logic operations:
 - 1. Acquire Inputs
 - 2. Perform Logic Operations
 - 3. Generate Outputs



ALS System Time Response / Deterministic Performance

Access Time: The board access time is the fixed interval allocated to exchange data with an individual board using the Reliable ALS Bus (RAB) protocol.

Frame Time: The frame time is the interval between accessing each specific board so information will have been read once from all application input boards and written once to all application output boards.



Tricon System Time Response / Deterministic Performance

- The Tricon application program (calculational cycle) cannot be interrupted by any of the lower priority tasks during the program execution cycle.
- Actual processing time is established during program development.
- Once application program development is complete, the cycle time does not vary as a function of calculational loading of the system.



Tricon System Time Response / Deterministic Performance

				Accident Analysis Time Response
			Specified PPS Response	
		Program Scan Time	Time Allocation	
	Calculated Response Time			
Time				>



System Time Response / Deterministic Performance





PPS System Time Response / Deterministic Performance

"The NRC staff concludes that the DCPP PPS system's realtime performance is deterministic and known, as documented by the system performance requirements and tests performed for validation of these requirements. The NRC staff determined that the DCPP PPS system meets the criteria for deterministic and predictable performance."



Independence Guidance

- Guidance for Communication
 - IEEE 603 1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
 - IEEE 7-4.3.2 2003, "Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Station"
 - DI&C-ISG-04, "Highly Integrated Control Roomscommunication Issues"



Independence

Protecting People and the Environment

Architecture







Independence

Protecting People and the Environment

ALS Communication Architecture





Independence

Protecting People and the Environment

Tricon Communication Architecture





Independence

Port Aggregator Tap





10/100 Port Aggregator Tap

Product Diagrams







Independence Conclusion

The staff evaluated the Tricon and ALS system communication for the Diablo Canyon PPS and found they met the guidance provided in ISG-04



Control of Access

Review Guidance

- IEEE 603-1991, Clause 5.9 "Control of Access"
 - The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.
- RG 1.152, Rev. 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
 - Contains guidance for establishing a Secure Development and Operational Environment (SDOE)
- SRP BTP 7-14, and RG 1.169, Rev. 1, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
 - Contains guidance related to Configuration Management plans and activities
- SRP Chapter 7, Appendix 7.1-C, section 5.9 "Control of Access"
 - Provides acceptance criteria for IEEE 603-1991, Clause 5.9.



Control of Access PPS Replacement Design Features

SRP Chapter 7, Appendix 7.1-C, section 5.9 "Control of Access"

- Paragraph 1: Administrative control is acceptable to assure that the access to the means for bypassing safety system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access.
- Access to the PPS replacement is administratively controlled by control room personnel.
- Paragraph 2: The review of access control should confirm that design features provide the means to control physical access to safety system equipment, including access to test points and means for changing setpoints.
- ✓ Design features provide physical access controls to the PPS.
 - The system will be located in plant vital area
 - The PPS cabinets are locked
 - > Tricon keyswitch position (other than RUN) will result in an alarm
 - Connection of the Test ALS Bus will result in an alarm



Control of Access PPS Replacement Design Features

SRP Chapter 7, Appendix 7.1-C, section 5.9 "Control of Access"

- Paragraph 3: Review of digital computer-based systems should consider controls over electronic access to safety system software and data. Controls should address access via network connections, and via maintenance equipment.
- ✓ The PPS replacement design does not allow for remote electronic access to the Tricon or ALS platforms.
 - There is one Tricon MWS and one ALS MWS per protection set which only communicate with the safety-related controllers in that protection set.
 - Access to the MWSs is controlled.
 - Two-way communication is only allowed between the Tricon Communication Module and the Tricon MWS by means of the port aggregator network tap device.
 - Two-way communication is only allowed between the ALS and the ALS MWS through the use of the Test ALS Bus (not connected to the ALS during normal operation, and used only in test or maintenance mode).



Control of Access Review Areas

✓ SDOE and Configuration Management

- Evaluated during the Topical Report reviews and found to be acceptable
- The same measures were maintained for the PPS replacement application

✓ Secure Development and Operational Environment

Vulnerability Assessments → Security Control Requirements → Access Controls

✓ Configuration Management

- Identification of configuration items
- Access controls based on work responsibilities
- Change review, approval and verification process
- Error reporting and corrective actions program

✓ Unintended/Unauthorized Changes

• Vendors' V&V groups performed code reviews



Control of Access Conclusion

The NRC staff concludes that the DCPP PPS replacement design incorporates features to administratively, physically and logically control access to the system, both during development and operation. These features meet the guidance for Secure Development and Operational Environment, and Configuration Management.

The NRC staff determined that the DCPP PPS system meets the criteria for control of access.


Lessons Learned on the Digital I&C Licensing Process (ISG-06)

- Establish a graded approach to performing Digital I&C safety Evaluations. (Tier 1, 2, and 3)
- Provide clear guidance to identify supporting document submittal requirements. (Annex B)
- Provide an evaluation process which can be performed in parallel with the system / software development processes for these systems. (Phases of review)
- Streamline the licensing process by consolidating guidance from multiple sources into a single reference that will be easy to use.



Lessons Learned on the Digital I&C Licensing Process (ISG-06)

- Minimum Information (Documentation):
 - Assumes Entire Safety System Replacement
 - No provision for reducing based on scope
 - Provides a forum for determining what documentation from Enclosure B should be submitted with the LAR





Lessons Learned on the Digital I&C Licensing Process (ISG-06)

Protecting People and the Environment

- PG&E had several Phase 0 meetings with NRC to explain the design approach (defense-in-depth & diversity, variances from guidance, unique or complex aspects, etc.) for the PPS LAR
- All documentation needed to support the LAR was agreed to during these meetings

Lessons Learned

- 1) Interaction with the staff early and often in the pre-submittal phase was effective in preparing the licensee and staff for this license application.
- 2) Licensees and Vendors should request a Phase 0 meeting at least 6 months (one year is even better) prior to LTR submittal to go through Enclosure B and agree upon what documentation is required for the LAR or Topical Report submittal.



Lessons Learned on the Digital I&C Licensing Process (ISG-06)





Lessons Learned on the Digital I&C Licensing Process (ISG-06)

Protecting People and the Environment

- NRC Staff performed acceptance review in accordance with NRR Office Instruction, LIC-109
- Several items were identified that needed further clarification
- The staff used a Phase 1 documentation matrix to identify which documentation would be provided per enclosure B.

Lessons Learned

- 1) The documentation tabulation of Enclosure B was effective in identifying information needed by the staff to start its technical review of the LAR.
- 2) Use of a Phase 1 documentation Compliance Matrix facilitated an efficient LAR acceptance review.



Lessons Learned on the Digital I&C Licensing Process (ISG-06)

Digital I&C Licensing Process Flow Chart Preliminary OK Vehicle (Letter/ RAI/ETC...) 2 Phase Supplement Phase 2 Questions **Resolve Audit** Issue RAIs EQ; HF; Change Conduct Audit Audit Open Items? Resolved? Items Control;; Startup Testing Plan То Phase 3



Lessons Learned on the Digital I&C Licensing Process (ISG-06)

Protecting People and the Environment

- No documentation guidance for Platform License Topical Report (LTR) reviews
- Sharepoint Access to documents gave NRC staff insight to development processes
- Some Phase 2 documents could not be submitted in the timeframes prescribed in ISG-06

Lessons Learned

- 1) ISG-06, Enclosure B should be enhanced to provide guidance on required information for a platform LTR submittal.
- 2) ISG-06 should be enhanced to promote remote, electronic websites/reading rooms for use to the extent practical to determine what proprietary information should be submitted on the docket.
- 3) Phase 2 document lists should be enhanced to acknowledge unavailability of certain documents until late stages of development.

April 4, 2016

Diablo Canyon License Amendment



Lessons Learned on the Digital I&C Licensing Process (ISG-06)





Lessons Learned on the Digital I&C Licensing Process (ISG-06)





Lessons Learned on the Digital I&C Licensing Process (ISG-06)

Protecting People and the Environment

Useful Principles of ISG-06

- Enclosure B Tables / ISG-06 Matrix –Cross Reference to body of ISG
- Open Item List
 - -RAI coordination
 - -Facilitation of Conference Calls



Lessons Learned on the Digital I&C Licensing Process (ISG-06)

Protecting People and the Environment

Living Document Concept

Some documents associated with software development are expected to be revised as system development activities progress. These are sometimes referred to as "living documents." Such documents should be classified as volatile. For such documents; a decision of what version of the document should be submitted and when (i.e. what phase) the document is to be submitted should be made during the acceptance review. It is not necessary for applicants to submit multiple versions of volatile documents to support the safety evaluation, however; the submitted volatile document should be sufficient to demonstrate conformance to all applicable regulatory requirements. In some cases it may also be necessary to provide accessibility to current versions of a volatile document for audit during a safety evaluation. Additional document specific guidance on document volatility is provided within Section D.



Improvements Being Considered

Protecting People and the Environment

<u>Phase 2a</u>

The initial Phase 2 document concept was that design output documents which might not be available for submittal at the time of LAR could be submitted at a later time as the system design was completed.

We have observed that some of these documents such as Summary Test Reports (D.4.4.2.4) are confirmatory in nature and can be distinguished from those which require detailed evaluation and assessment. Such confirmatory reports would not be subjected to the early submittal requirements of other Phase 2 documents.



Lessons Learned on the Digital I&C Licensing Process (ISG-06)

Protecting People and the Environment

Conditional Letter of Regulatory Compliance

- We have received feedback from industry on several occasions that the SE should be completed using design information and should be independent of the factory test processes. FAT testing could then be verified by the staff on a confirmatory inspection basis.
- The NRC has resisted this idea for the following reasons:
 - Safety Evaluation conclusions cannot legally contain conditional requirements.
 - Experience has shown; significant design changes are often initiated as a result of test performance of the systems. Such changes have the potential of invalidating safety conclusions.
 - In absence of system test results or conditional requirements it is difficult to reach and provide basis for reasonable assurance safety findings .



Conditional Letter of Regulatory Compliance

- Add a letter of regulatory compliance to the review process similar to what is currently being done in the Acceptance Reviews for License Amendments.
 - No Safety Conclusions or approval of license amendment
 - Provides Status of safety evaluation activities at completion of design
 - Provides Pre-decisional Regulatory Compliance statement.
- Would such a letter provide the level of confidence the industry is looking for to minimize Risk factors prior to expenditure of resources?



Summary

- ISG-06 has significantly improved the licensing process for digital I&C systems.
- Further Improvements are being pursued as a result of lessons we have learned during the Diablo Canyon Pilot Project.



Diablo Canyon PPS Licensing Activity Milestones

- Three Phase 0 meetings were held with the licensee
- License Amendment Request Submittal October 26, 2011
- Requests for Additional Information (75)
- ACRS Meetings -
 - I&C Subcommittee February 18, 2014
 - Full Committee March 6, 2014
- Vendor Audits Performed (4)
- Full Committee ACRS Meeting May 5-7, 2016
- Summary of the Seismic Calculation Results June 30, 2016
- Technical Evaluation of the Open Item (Seismic) July 15, 2016
- NRC Technical Staff Finalizes Safety Evaluation July 29, 2016
- Issue the License Amendment September 30, 2016



Digital I&C Integrated Action Plan for the Modernization of NRC Regulatory Infrastructure

ACRS Meeting April 4, 2016

John Lubinski, Director, Division of Engineering Office of Nuclear Reactor Regulation





Informational Briefing

• Overview of current Action Plan

• Discuss future interactions with ACRS





- SECY-15-0106 and Commission Direction
- January 20, 2015 meeting on draft Digital Action Instrumentation and Controls (I&C) Plan
- Steering Committee Formation
- Integrated Action Plan on Digital I&C
- Focus on stakeholder interaction



Working Group Action Plans (Near Term Priorities)

- Assess Potential Common Cause Failures (CCF)
 ACRS engagement summer 2016
- Review of Cyber Security Design Aspects
 ACRS engagement May/June 2016
- Guidance for 10 CFR 50.59 Upgrades
 - ACRS engagement fall 2016
- Incorporation by Reference of IEEE Standard 603 into 10 CFR 50.55a
- IEEE Standard 7-4.3.2 Regulatory Guidance Plan





- Embedded Digital Devices (RIS in April 2016)
- Regulatory Document Infrastructure Improvements
- Guidance for Evaluation of Proposed Alternatives to Regulatory Guides and Endorsed Standards
- Digital I&C Licensing Process
- Improved Guidance for Evaluation of Highly-Integrated Digital Technologies
- Improvement in Regulatory Consistency from Licensing to Inspection
- Digital I&C Topical Report Evaluation and Update Process



Stakeholder Interactions

- January 20, 2016 public meeting for action plan
- March 10, 2016 RIC panel discussion
- March 21, 2016 CCF public meeting
- March 24, 2016 Integrated Action Plan released to the public
- March 30, 2016 public meeting on integrated action plan
- April 28, 2016 public meeting on 50.59 guidance
- May 25, 2016 SECY to Commission



ACRS Interactions

- April 4, 2016 Subcommittee meeting- overview of integrated action plan
- May 3, 2016 Cyber Security draft Information SECY to ACRS for review and discussion
- Summer 2016 CCF Working Group Engagement with ACRS
- Fall 2016 10 CFR 50.59 Working Group Engagement with ACRS