Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital I&C Subcommittee Meeting

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Friday, November 16, 2012

Work Order No.: NRC-2019 Pages 1-292

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

1 UNITED STATES OF AMERICA

2 NUCLEAR REGULATORY COMMISSION

3 + + + + +

4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

5 (ACRS)

6 + + + + +

7 DIGITAL I&C SUBCOMMITTEE

8 + + + + +

9 FRIDAY

10 NOVEMBER 16, 2012

11 + + + + +

12 ROCKVILLE, MARYLAND

13 + + + + +

14 The Subcommittee met at the Nuclear

15 Regulatory Commission, Two White Flint North, Room T2B3,

16 11545 Rockville Pike, at 8:30 a.m., Charles H. Brown,

17 Chairman, presiding.

18 COMMITTEE MEMBERS:

19 CHARLES H. BROWN, JR., Chairman

20 DENNIS C. BLEY, Member

21 JOHN D. SIEBER, Member

22 JOHN W. STETKAR, Member

23

24

25

1 NRC STAFF PRESENT:

2 CHRISTINA ANTONESCU, Designated Federal

3 Official

4 SUSHIL BIRLA, RES/DE

5 MILTON CONCEPCION, NRO/DE/ICE

6 NORBERT CARTE, NRO/DE/ICE

7 EUGENE EAGLE, NRO/DE/ICE2

8 IAN JUNG, NRO/DE/ICE

9 PETER KANG, NRR/EEB

10 KHOI NGUYEN, NRO/DE/ICE2

11 PAUL PIERINGER, NRO/DCIP

12 DAN SANTOS, NRO/DE

13 MOHAMMED SHUAIBI, NRO/DE

14 JOELLE STAREFOS, NRO/DARR/SMR/LB1

15

16

17

18

19

20

21

22

23

24

25

1 ALSO PRESENT:
2 BRIAN ARNHOLDT, B&W
3 RUFINO AYALA, NuScale Power, LLC*
4 STEVE BLOMGREN, NuScale Power, LLC*
5 DERICK BOTHA, NuScale Power, LLC*
6 GREGG CLARKSON, NuScale Power, LLC*
7 JOHN CRAIG, NuScale Power, LLC*
8 PAREEZ GOLUB, EXCEL Services*
9 CHRIS GRAHAM, Safeware Engineering
10 PETER HASTINGS, B&W*
11 MARC HAYDEN, NuScale Power, LLC*
12 BOB HIRMANPOUR, Southern Nuclear*
13 GARY JONES, NuScale Power, LLC*
14 DON LEWIS, NuScale Power, LLC*
15 DENISE McNABB, NuScale Power, LLC*
16 STEVE MIRSKY, NuScale Power, LLC*
17 CHET POSLUSNY, B&W
18 DON STATILE, NuScale Power, LLC*
19
20 *Present via telephone
21
22
23
24
25

TABLE OF CONTENTS

Opening Remarks 5

DSRS Chapter 7 Introduction 7

Overview and Summary of DSRS Chapter 7 10

Break .....
87

DSRS 7.0 Introduction and Overview of Review
Process .....
87

DSRS 7.1, Fundamental Design Principles 95

Lunch Recess 149

DSRS 7.1, Fundamental Design Principles
(continued) .....
149

Appendix A, Evaluation of Hazard Analysis 181

Break .....
206

Appendix B, I&C System Architecture 206

Appendix C, Simplicity 213

DSRS 7.2, System Characteristics 230

Public Comment 282

Closing Remarks 288

1
2
3
4
5
6 P R O C E E D I N G S
7 (8:39 a.m.)
8 CHAIRMAN BROWN: The meeting will now come
9 to order. This is a meeting of the Digital
10 Instrumentation and Control Systems Subcommittee.
11 I'm Charles Brown, Chairman of the
12 Subcommittee. Advisory Committee members in
13 attendance are Dennis Bley, John Stetkar and Jack
14 Sieber. Christina Antonescu of the staff, ACRS staff,
15 is the Designated Federal Official for this meeting.
16 During this meeting the staff will discuss
17 the Design-Specific Review Standard, Chapter 7, as part
18 of a new Licensing Approach for Instrumentation and
19 Control systems for Babcock and Wilcox mPower. I guess
20 that's a small modular reactor design.
21 Also in preparation for the Digital I&C
22 Subcommittee meeting, we provided some suggestions on
23 the framework based on some earlier stuff five or six
24 months ago.
25 In addition to that, we are hoping that we

1 will have some information presented relative to the
2 following questions. In other words, an outline of the
3 schedule and intent of the entire effort, an explanation
4 of the mPower design information that the staff already
5 has and how that influenced the Design-Specific Review
6 Standard, what items from the present SRP NUREG-0800
7 were dropped and why, a description of the philosophy
8 behind the development of this standard, a comparison
9 of the level of detail in this standard relative to the
10 SRP topic by topic, chapter by chapter, issue by issue,
11 subject by subject, whatever the appropriate category
12 is, and somewhat of a mapping of how the items listed
13 in the Table 7.1 are addressed in Chapter 7.
14 The Subcommittee will gather information,
15 analyze relevant issues and facts and formulate proposed
16 positions and actions as appropriate for deliberation
17 by the full Committee.
18 The rules for participation in today's
19 meeting have been announced as part of the notice of
20 this meeting previously published in the Federal
21 Register in November of 2012.
22 We have received no written comments or
23 requests for time to make oral comments/statements from
24 members of the public regarding today's meeting.
25 Also, we have Bob Hirmanpour from Southern

1 Nuclear on - I believe these are on the phone bridge;
2 is that correct?
3 MS. ANTONESCU: Right.
4 CHAIRMAN BROWN: Southern Nuclear; Chet
5 Poslusny from B&W; Pareez Golub, EXCEL Services
6 Corporation and others from NuScale, LLC. There's 11
7 folks. I'm not going to - and please excuse me. I'm
8 not going to run through the entire list of 11. I don't
9 know who the leader is, but the first name on the list
10 is Don Lewis.
11 To preclude interruption of the meeting,
12 the phone line will be placed in a listen-only mode
13 during the discussions and presentations and Committee
14 discussions.
15 A transcript of the meeting is being kept
16 and will be made available as stated in the Federal
17 Register Notice.
18 Therefore, we request that participants in
19 this meeting use the microphones located throughout the
20 meeting room when addressing the Subcommittee.
21 The participants should first identify
22 themselves and speak with sufficient clarity and volume
23 so that they may be readily heard.
24 We will now proceed with the meeting and
25 I will call upon Mr. Mohammed Shuaibi, Deputy Director

1 of the Division of Engineering in the Office of Nuclear
2 Reactors to provide some introductory remarks.
3 Mo.
4 MR. SHUAIBI: Thank you, Mr. Brown, and good
5 morning, everyone.
6 I'm the Deputy Director of Division of
7 Engineering in Office of New Reactors. As you said,
8 I am acting Director as I am normally here for Tom Bergman
9 who is the Director of the Division. He is on rotation
10 to NRR. Otherwise, he would have been here to introduce
11 this topic. So, I just wanted to point that out.
12 I'm going to provide just a few short
13 opening remarks and then turn it over to the team that
14 worked hard to develop this Review Standard with
15 Milton's lead at the table. I'm very proud of their
16 work and their dedication to this project.
17 Let me start by saying that we appreciate
18 the opportunity to brief you on this project. I know
19 that Digital I&C has been, and continues to be, a very
20 important topic for the Committee and it's also very
21 important to us.
22 I have sat through several ACRS meetings
23 on Digital I&C and I'm glad that we have the opportunity
24 to brief you on this Review Standard prior to finalizing
25 it and prior to using it for the review of the mPower

1 design.

2 We last briefed you on this initiative in

3 February of this year, I believe. We have continued

4 to follow that same path that we briefed you on back

5 in February. So, I hope that you'll find what you hear

6 today consistent with that briefing and your

7 expectations from that briefing that we are here for.

8 We undertook this project to incorporate

9 lessons learned from our past new reactor reviews and

10 our interactions and feedback with the Committee.

11 We believe we have an opportunity here to

12 significantly enhance future reviews, and this effort

13 is intended to do that for the mPower design.

14 I will note that this Review Standard is

15 specific to mPower design at this point. So, what we're

16 reviewing here today is for the mPower design.

17 I do also want to note that cybersecurity

18 is not within the scope of this effort. We know and

19 understand that the Committee is very interested in the

20 topic of cybersecurity, but this effort and this Review

21 Standard were really not intended to cover that topic.

22 So, I want to bring that up front and I want to make

23 sure that we - I'll let you know what the scope of the

24 presentation is today.

25 So, with that, I'll turn it over to Milton

1 Concepcion unless you have any questions.

2 CHAIRMAN BROWN: I have one other comment.

3 Since you brought up the cybersecurity issue, you can

4 be rest assured that we have been thinking about

5 cybersecurity in terms of the development of the SRS

6 standard -

7 MR. SHUAIBI: Okay.

8 CHAIRMAN BROWN: - because the architecture

9 is so integrally a part of even having a structure that

10 can allow cybersecurity to be actively and accurately

11 and effectively countered and we've had that discussion

12 before.

13 MR. SHUAIBI: We have.

14 CHAIRMAN BROWN: I'm not going to discuss

15 it again now, but because you're not going to discuss

16 it doesn't mean it may not be considered. I just wanted

17 --

18 MR. SHUAIBI: I understand.

19 CHAIRMAN BROWN: - to pass that tidbit on

20 as part of the discussion, okay?

21 MR. SHUAIBI: I understand.

22 CHAIRMAN BROWN: Thank you very much.

23 MR. SHUAIBI: Thank you.

24 CHAIRMAN BROWN: Milt, if you would like to

25 go ahead?

1 MR. CONCEPCION: Sure. Good morning.

2 For those who don't know who I am, my name

3 is Milton Concepcion. I'm a senior digital I&C in the

4 Office of New Reactors, ICE Branch 2.

5 I'm really excited to be here and present

6 the status of this initiative to provide new guidance

7 for the review of instrumentation and controls and how

8 we will apply to the mPower design.

9 A little bit about myself. I have a

10 Bachelor's and Master's degree in electrical

11 engineering. Been with the NRC for about 10 years now.

12 I'm a qualified technical reviewer and

13 qualified vendor inspector. I have done many

14 inspections of I&C systems here for the NRC and recently

15 did some research and collaborated some research efforts

16 in the digital I&C area.

17 I recently came back from, like I said,

18 Research. Been with NRO since early this year and took

19 the lead for this project, and I'm really excited to

20 brief you on the status of it.

21 As stated on the slide, we'll provide an

22 update on our early commitment on the development of

23 the DSRS for Chapter 7. We've been working really hard

24 collecting information, identifying areas for

25 improvement and putting together the sections that end

1 up in this draft guidance that we're presenting today.
2 With me on my right side is Ian Jung, the
3 Chief of I&C, Branch 2. Dan Santos, Senior Technical
4 Advisor, NRO. And Dr. Sushil Birla from Senior
5 Technical Advisor in the Office of Research.
6 If we go to the next slide, like I said,
7 we're going to present the status of Chapter 7 DSRS and
8 how we intend to implement it to the mPower design.
9 We're very much interested in collecting
10 feedback from the Subcommittee, and we're also here to
11 answer any questions that you might have.
12 And since I have Dan Santos and Ian Jung
13 sitting around the table, I guess I can say being there's
14 an I&C briefing, we're triple redundant today.
15 MR. SANTOS: And diverse.
16 MR. CONCEPCION: Yes. Next slide.
17 (Laughter.)
18 (Discussion off the record.)
19 MR. CONCEPCION: So, as far as the agenda,
20 we have a full agenda for today. And if you will, the
21 topics are going to be broken down in two major areas.
22 The first couple of bullets will address
23 the background, the status and schedule of Chapter 7,
24 all the key activities that we did, provide some
25 background and philosophical approach to the

development of the DSRS.

And then the second half would get into the details of each section of the DSRS starting with 7.0 and going down through the fundamental design principles and those system characteristics that we identified from IEEE 603.

And then we get into the appendices that we developed to support the review of the fundamental design principles.

Now, I will turn it over to Joelle Starefos, which is on my left side. She will provide you an update on the overall DSRS schedule and how we fit - how Chapter 7 fits in the overall DSRS development.

Joelle.

MS. STAREFOS: Thank you, Milton.

Good morning. My name is Joelle Starefos. I'm the Senior Project Manager in the Office of New Reactors. I'm responsible for the mPower pre-application activities, including the DSRS development.

And I just wanted to take an opportunity to answer your first question, Mr. Brown, which was what kind of schedule do we have for this and how does it fit into the overall plan that we had?

As I'm sure you're aware, SECY-11024 was

1 a SECY that the Commission had asked us to address how
2 we could improve efficiency and include risk information
3 into the future reviews of the advanced reactors or small
4 modular reactors when they came into - for application.
5 We addressed this with the full Committee
6 back in March of 2011, and with the Subcommittee about
7 a month earlier with what our plans were for that. And
8 I think what we're going to share with you today is what
9 the implementation has resulted in.
10 So, I have a timeline here. This is our
11 approximate timeline for finalizing the mPower
12 Design-Specific Review Standard. This is the first
13 DSRS that we're issuing.
14 And in September 2012, we had put the draft
15 together and had issued several topics or sections prior
16 to that in draft manner for informal public comment.
17 Chapter 7 fell into one of those draft slide
18 packages or draft presentation packages that the public
19 had an opportunity to look at. So, we've actually had
20 some comments and opportunities to interact with B&W
21 and members of the public on this section.
22 In October, we were working through interim
23 concurrence and OGC/NLO being obtained. We're now in
24 November and we're still working through our
25 concurrences and OGC/NLO. We have it on numerous

1 sections, but we're working on some of the stragglers.
2 Just like with any project, you get to the
3 last month or so and you start to make sure that
4 everything is coming together.
5 And right now we do have a few challenges
6 that we're working through, but we anticipate that this
7 certainly will be issued no later than the end of the
8 year if we end up slipping our date.
9 CHAIRMAN BROWN: That's for public comment,
10 correct?
11 MS. STAREFOS: Yes.
12 CHAIRMAN BROWN: For official public
13 comment.
14 MS. STAREFOS: Exactly.
15 CHAIRMAN BROWN: Okay.
16 MS. STAREFOS: That's what we're calling
17 "for interim use and comment." And that will be the
18 opportunity for the public to comment via the Federal
19 Register Notice.
20 We had originally planned on 60 days. But
21 because of the holidays and other considerations, we
22 decided it's beneficial to give the public a little bit
23 more time. So, we're anticipating about a 90-day
24 comment period.
25 This is a very voluminous document, a lot

1 of changes, and we don't want anybody to be rushed
2 through their decisions on this.
3 So, our plan here is to issue it for public
4 comment. And at the same time, send a memo to the ACRS
5 inviting your thoughts and reviews. And if you'd like
6 to meet, we look forward to that as well.
7 We'll also send our notice to OMB for the
8 Congressional Review Act review. All of this should
9 happen, as I said, by the end of the year.
10 We anticipated public comment being
11 received by February. Again with the 90 days, that will
12 push maybe to March time frame.
13 And we'll start resolving public comments
14 and revising the document as appropriate with an eye
15 on getting the final mPower DSRS document issued no later
16 - well, sometime around the time when we're anticipating
17 their application to come in.
18 The concern that we had about getting the
19 first round issued and the comments resolved was to make
20 sure that we meet the requirements for the applicant
21 to review or consider the SRP, and address any
22 differences that they have from what the standard SRP
23 is. As you know, we have a rule that requires that in
24 Part 52.
25 So, we've talked with our general counsel

1 and this will suffice, this DSRS will suffice as being
2 their Specific Review Plan, or SRP, for the mPower
3 design.
4 CHAIRMAN BROWN: Well, you state that in the
5 document itself already.
6 MS. STAREFOS: We will.
7 CHAIRMAN BROWN: No, I think you already
8 have.
9 MS. STAREFOS: Yes, and we will state that
10 in the preface to the document that goes out with how
11 to use this DSRS, what it applies to and the specific
12 application of these aspects to mPower alone at this
13 point.
14 CHAIRMAN BROWN: Yes. Well, that was one
15 of the reasons we asked for, you know, what was in, what
16 was left out.
17 MS. STAREFOS: Right.
18 CHAIRMAN BROWN: So that we know what - is
19 there anything in what I would call - I don't want to
20 call it the collective opinion of importance that
21 reviewer guidance is not getting that they used to get.
22 I'm not worried about the IEEE 279
23 references and things like that. I'm talking about the
24 more substantive -
25 MS. STAREFOS: I understand.

1 CHAIRMAN BROWN: Using more substantive -

2 MS. STAREFOS: And I hope what you'll find

3 today is that they address that for I&C for you in this

4 presentation. We're certainly prepared to discuss

5 that.

6 As far as the other sections, we actually

7 have - just a little statistics for you. We have four

8 different categories of the Standard Review Plan that

9 we had considered.

10 We characterized them as either use as-is,

11 which meant that we were going to use the SRP as it is

12 to appropriate and applicable as it stands for the mPower

13 design. There's 87 sections that fall into that

14 category.

15 CHAIRMAN BROWN: 87 sections of the existing

16 NUREG-0800 SRP.

17 MS. STAREFOS: Existing SRP, correct.

18 There's 82 sections that we're going to

19 delete that includes all the original Chapter 7

20 sections. So, that actually gained about 30 of them

21 in there.

22 But a lot of those sections -

23 CHAIRMAN BROWN: Hold it. Retrace that

24 again. You deleted - you're not using any of the Chapter

25 7 stuff? That's the way I -

1 MS. STAREFOS: That's correct. We have
2 rewritten the entire Chapter 7 and now it is -
3 CHAIRMAN BROWN: So, you eviscerated
4 whatever previous - that's a nice word.
5 MS. STAREFOS: Well, I wouldn't say
6 eviscerated. I would look at it more like incorporated
7 it in an efficient way in the future guidance.
8 How is that?
9 CHAIRMAN BROWN: Well, I tried to look at
10 the old SRP and track it over to some of the stuff and
11 it was virtually impossible. I threw the towel in.
12 MS. STAREFOS: I know our guys have spent
13 a lot of time ensuring that all of those important and
14 required aspects are incorporated. And I hope that
15 you'll get that today in this presentation.
16 CHAIRMAN BROWN: Okay. Thank you.
17 MS. STAREFOS: We've also got modified -
18 we've modified 154 sections. And we have 13 new
19 sections, including the seven for the I&C.
20 Some of those are for new systems or new
21 ways that the systems or functions have been
22 characterized by the mPower design.
23 So, we've done a lot of work and we're
24 hopefully headed towards a very solid and good product.
25 And we hope to share that with you in the future.

1 CHAIRMAN BROWN: Okay, thank you.

2 MEMBER STETKAR: Joelle, or this is a heads
3 up to Milton, perhaps. As I read through this, it was
4 not clear to me how this was specifically tailored to
5 mPower.

6 So, if you could point out places where
7 there is specific - this is a Design-Specific Review
8 Guidance and I'd like to understand what features of
9 the mPower design were considered in this guidance.

10 I understand digital I&C compared to other
11 things in a very generic sense. But I'm thinking going
12 forward if this is the mPower-specific review, what
13 about, you know, the next one that comes down the line?

14 What differences, what changes might there
15 be from this guidance, because this is tailored to
16 something that is very specifically associated with this
17 particular design?

18 And if there are those, I'd like to know
19 where they are.

20 MEMBER BLEY: And if I could just expand this
21 just a tiny bit, it is, in fact, what John was just
22 talking about, an mPower-specific one, or is this the
23 first draft of what you see actually replacing the I&C
24 material and the Chapter 7 material in the SRP for the
25 future?

1 CHAIRMAN BROWN: You mean the general SRP.

2 MR. BLEY: Yes, I do.

3 MS. STAREFOS: Yes, actually I should have

4 mentioned that in my preface, and I apologize. That's

5 a great question because one of the challenges we had

6 when we were doing the DSRS, we had amazing

7 pre-application interaction with the mPower B&W

8 organization. They have been very open and very - I

9 guess they've given us a lot of pre-application

10 information.

11 I would probably say having been working

12 around new reactors for many, many years, probably more

13 so than we've done to date.

14 With that, though, this particular I&C

15 project was really an initiative. And I would say this

16 was kind of our - this was probably our pilot chapter

17 that you could argue based on even the information we

18 did have from B&W, we wanted to try to make something

19 that would give us a more efficient look, a more, I guess

20 - well, probably "efficient" is a good way to put it

21 for the pilot program.

22 A way to approach the I&C that did not cut

23 out too many of our general criteria for our review until

24 we actually had the application in. This is one of the

25 challenges we have with many of the sections.

1 Although B&W mPower has been so open with
2 their pre-application work, their design is not yet
3 complete. So, our reviewers face that challenge on
4 every section whether they had sufficient information
5 to make the decision to eliminate or change our Review
6 Standard, because we knew something was not going to
7 be there.
8 In some cases, it was very evident. The
9 system didn't even exist. This was a passive plant and
10 some of the information in the SRP could be a nonpassive
11 boiling water reactor-related concept that wasn't
12 applicable. So, it was easy to cut those out.
13 In other cases, it wasn't so easy. And so,
14 some of these sections, and you'll even see this in the
15 general DSRS, are more generic in nature. And we plan
16 to try to bring those down to a more specific mPower
17 focus when we have - if we have more additional
18 information before the application is received.
19 But if not, the reviewers are in a position
20 where they can make those determinations immediately
21 upon receipt of the application and seeing what the
22 presented material is.
23 So, we try to put the reviewers in a much
24 stronger position. And I think the benefit we've seen
25 out of it is that the issues that we normally would

1 identify in the first six months or year of a review
2 are coming up in pre-application. So, we feel like this
3 has been a very beneficial effort.
4 MR. SHUAIBI: Very quickly, and I do want
5 to turn it over to Milton. I think he'll probably try
6 to address some of those as we go through this
7 presentation.
8 I did, you know, we both mentioned, and all
9 of us will mention this is specific to mPower. We don't
10 mean that this is specific to the specifics of the design
11 that they're going to be proposing to us and Milton will
12 address that.
13 I wouldn't be surprised if we come here
14 sometime in the future and we have another small modular
15 design and say, well, with very minor tweaks, this is
16 basically the same guidance we'll use.
17 So, I don't want to mislead you to make you
18 think that this is so specific to mPower that it only
19 applies to the design that we're looking at for mPower.
20 So, it is a pilot. And if this works well
21 for us here, then don't be surprised if we use it again
22 for other designs that come in the new reactors area.
23 So, I'll just leave you with that. And
24 unless you have any other questions, I guess I'm sure
25 Milton can answer most of them as he goes through.

1 CHAIRMAN BROWN: That's what I thought.

2 MR. CONCEPCION: Just to add a little bit

3 to it, yes, I understand that the mPower DSRS is

4 specific. But in the area of I&C, you will know - you

5 will know in the presentation it will be capturing more

6 than 90, 95 percent of the guidance that's today in the

7 SRP.

8 So, and I'll get into it and I believe B&W

9 is in the audience today. They can talk about some of

10 their information that was shared with staff, but the

11 majority of the information today in the SRP is contained

12 in the DSRS.

13 It is modified in terms of structure, but

14 all of the information is in the SRP and there is no

15 loss of relevant guidance.

16 Okay. So, we set a couple of goals, a

17 handful of goals for the DSRS development. And one of

18 the main goals was to enhance the focus of the reviews

19 and provide clear guidance to the reviewers on how they

20 could resolve high-order issues such as redundancy,

21 independence, single failure and determinism and some

22 others.

23 And we also wanted to improve the efficiency

24 of reviews by incorporating some of the lessons learned

25 that have been discussed at length with this committee,

1 as well as internally in our I&C reviews.

2 We also see a benefit of us developing this

3 guidance and putting it in the public domain and have

4 the mPower and B&W applicant to understand the scope

5 and intent and level of review that we expect them to

6 - that they expect us to do in their design.

7 So, in general, what we expect is that they

8 understand what kind of review we're going to be doing

9 so they can provide the information we need to close

10 all of our safety issues and have a comprehensive review

11 that hopefully will enhance the efficiency compared with

12 what we do today and using the existing SRP.

13 We'll move to the next slide to provide some

14 background of where we are. We've gained significant

15 review experience, as I said, review I&C designs and

16 those lessons learned. We're doing our best to capture

17 it in the DSRS development.

18 As you know, some of those reviews have been

19 really challenging ranging from a lack of level of detail

20 in some areas, to an applicant's difficulty in trying

21 to - presenting a safety case and demonstrating safety

22 given a particular I&C architecture.

23 So, as you know, this has had some

24 significant impact in licensing certainty in terms of

25 both schedules and resources, which is of concern to

1 our management as well as the industry in general.
2 So, we took all of the lessons learned and
3 the material and developed a list of the lessons that
4 we have learned and try to implement them in Chapter
5 7.
6 Some of those lessons learned were - have
7 been discussed with the Subcommittee. And fundamental
8 design principles comes to mind as one of the key lessons
9 that we try to incorporate in the DSRS.
10 Continuing on the background, so we took
11 all of that information and we reorganized it. We took
12 the lessons learned and we put together the DSRS with
13 - using information from the existing SRP, using the
14 ISGs to the extent practical and developed this approach
15 using sound engineering principles such as
16 defense-in-depth, using simplicity as an attribute,
17 using integrated hazards, and also enhancing the
18 structure and providing some clarity in the way the
19 reviewers will address the information in the
20 application.
21 So, this slide provides a representation
22 of all of the - of the major lessons learned that we
23 captured in the last several years of reviewing I&C.
24 You probably recall that these were
25 discussed with you back in February of this year. And

1 what I'm going to do today is I'm going to go through
2 each of those colored blocks and provide some examples
3 of what we did to address each of those lessons learned
4 in the DSRS.
5 And as I said before, a key point is that
6 we took - we took the SRP and we took the ISGs to the
7 extent practical, and we manipulated the information
8 and we rearranged it and we made sure that no relevant
9 guidance was left behind with the exception of guidance
10 that clearly doesn't apply to the mPower design.
11 Yes, sir.
12 CHAIRMAN BROWN: Excuse me. There's two or
13 three ISGs. I can't remember the numbers. The one on
14 data independence, I think it was ISG-2 or Three, Four?
15 MS. ANTONESCU: Four.
16 MR. CONCEPCION: Communication
17 independence.
18 CHAIRMAN BROWN: Yes, and there was another
19 - what was ISG-5? I'm trying to remember what that one
20 was. That's human factors. And then there was a third
21 one.
22 MR. SANTOS: ISG-2, diversity.
23 CHAIRMAN BROWN: Two, diversity. Those
24 were specifically reviewed and we went through those.
25 You've been using them.

1 Are all - has all of that now been put in?

2 MR. CONCEPCION: Okay. ISG-2 was rolled

3 into BTP 7-19. And we took BTP 7-19 and incorporated

4 it into DSRS. So, that is captured.

5 CHAIRMAN BROWN: That's interesting.

6 Because in reading the DSRS, there's not - the BTP 7-19

7 is, what, 40 pages long or something like that, and D3

8 in the DSRS is about four and there's never any mention

9 of BTP 7-19. It's not even referenced in the guidance

10 documents.

11 At least I didn't find it going through that

12 list of reference reg guides, IEEE standards, rules and

13 everything else.

14 So, the ability to take 40 pages of

15 information without ever mentioning it and then crank

16 it into four pages, that's a pretty good consolidation.

17 MR. CONCEPCION: Well -

18 CHAIRMAN BROWN: And it's a little bit that

19 blows my mind.

20 MR. CONCEPCION: We took what's in 7-19 and

21 we - if you're looking at the review guidance section

22 of D3, you will see those four elements that are in the

23 SRM to the SECY paper.

24 We captured the major elements that are in

25 7-19 and put them in the D3 section. So, we made sure

1 that the guidance - we moved repetitive information that
2 isn't in BTP 7-19 in particular since we're talking about
3 it, but the essence of the information is in the D3
4 section.
5 CHAIRMAN BROWN: Well, but it's at this level
6 where if you look at BTP 7-19, the guidance, there was
7 some specific reviewer guidance that's in there that's
8 not over there.
9 The high-level thought process is, yes, I
10 agree they're stuck in there. But the details of giving
11 the reviewer guidance as to what he should look for,
12 it's like he's got to invent it again all by himself
13 in terms of some of the details.
14 There was a lot of time spent on 7-19 from
15 a D3 standpoint. So, I, you know, that's one of the
16 questions that at least I was going to ask later. So,
17 I'm asking it now instead. That seems to be a little
18 bit sparse.
19 And on top of that, 7-19 is not mentioned
20 anywhere even in the reference documents in the back,
21 because it's no - I guess because it's no longer a
22 technical position anymore other than -
23 MR. CONCEPCION: It is no longer applicable
24 and we should have captured all of the important elements
25 of BTP 7-19, as I said, and put it in D3.

1 CHAIRMAN BROWN: Well, top-level elements
2 I'm probably not going to argue with. But the positions
3 and everything else that was in it or however they
4 rephrased it did not seem to make it.
5 I mean, how do you go from 30 or 40 pages
6 to four or five and capture it adequately, I don't know.
7 And I didn't have the time to go through
8 and try to do a side-by-side comparison all the way
9 through.
10 MR. CONCEPCION: We have a side-by-side
11 comparison of how we captured the information. We're
12 more than happy to share it with you.
13 CHAIRMAN BROWN: Okay.
14 MR. CONCEPCION: It is not in the DSRS. We
15 have - I have my supplemental material with information
16 that shows how we took all of the information from all
17 of the BTPs and their relevant ISGs and how we captured
18 them in the DSRS.
19 MEMBER BLEY: That would be really helpful
20 for us to see.
21 MR. CONCEPCION: Yes, I could certainly -
22 MEMBER BLEY: It's a little - well, you
23 probably did a lot of work on that and it's hard for
24 us in our review to really track that and be comfortable
25 with it.

1 MR. JUNG: Okay. Ian Jung, Chief of the I&C.
2 The intent of DSRS is to capture sufficient
3 staff guidance to reach a safety finding on its own.
4 That's one of the reasons we are not referencing any
5 of the existing BTPs.
6 We wanted to incorporate so that the
7 reviewer would have sufficient information by itself
8 to review and make a decision so that the staff wouldn't
9 have to refer to many other documents. That was one
10 of the intent.
11 The intent is to make sure all the relevant
12 guidance that is important to make decision on D3 is
13 captured in diversity section.
14 So, we've done exercise, but it will - we'll
15 continue to look for any feedback from the B&W and the
16 public.
17 If we somehow missed it, then we will let
18 you know. The reason that the BTP 7-19 was a lot bigger
19 than DSRS is I remember ISG - the purpose of the BTP
20 7-19 was to incorporate ISG into the existing BTP 7-19
21 original version, but the ISG was not - incorporation
22 of ISG was sort of addition of more information.
23 That particular effort did not go back and
24 we evaluated what are the redundant information in the
25 existing BTP.

1 So, we went through that, we scrubbed it.
2 Our staff did a clause-by-clause comparison of all of
3 the BTP 7-19, Revision 6, and made a decision which ones
4 are repeated, which ones are relevant and we made a
5 decision.
6 It turns out that, you know, the information
7 we believe is just sufficient to do that. But if we
8 dropped any of the criteria or relevant guidance, we'll
9 let you know specifically.
10 So, we'll look for - we'll continue to look
11 at it. And B&W and others are looking at it. So, we'll
12 continue to look into that.
13 MR. SANTOS: Dan Santos here.
14 I just want to echo what Ian said and even
15 the current SRP doesn't contain all the guidance for
16 I&C.
17 There's many, many references. There's
18 many, many standards out there and it's impossible.
19 We have never incorporated all of that.
20 So, none of that is going away. None of
21 the BTPs, none of the IEEE standards. They're always
22 going to be available for the staff to do their review,
23 but we felt that some of the items can only come up if
24 they have a particular question that the design forces
25 them to go into those other reference. Then, they can

1 go do that, pick up those reference.

2 But what we wanted to capture on the DSRS

3 was the essence to answer the necessary safety question.

4 And if a particular complexity in the design forces

5 the reviewer to other reference, they'll always be

6 available. That's the case today with the current SRP.

7 Having said that, I would echo what Ian

8 said. If there's any things that members feel, no, you

9 cut too much, then that's a good feedback. And

10 hopefully when we get to the particular section, we can

11 discuss that and we're very open to get that type of

12 feedback and we appreciate it.

13 CHAIRMAN BROWN: Okay. I just went and

14 looked at BTP 7-19 again just to make sure I was accurate,

15 you know. 20 pages down to five, five-and-a-half, and

16 that just seems to be a lot of slicing and dicing in

17 terms of - I didn't realize there was that much

18 repetition in BTP 7-19 and redundant information.

19 It certainly didn't read that way when we

20 did the review of that for the incorporation of ISG-2

21 - was that ISG-2 at the time?

22 MR. JUNG: Charlie, I'm little bit

23 simplifying that. Not only the repetition, BTP 7-19

24 has a lot of background and explanation. It is not

25 really directly relevant to the staff guidance.

1 So, those documents will be available if
2 someone wants to be trained on the background of, you
3 know, current BTP 7-19 is an official Agency-broad
4 guidance that's out there.
5 If somebody, one of my staff wants to review
6 that background or history in the 1990s, it describes
7 a lot of what happened.
8 We want the staff to really focus on what
9 we are looking for, why diversity is there, you know,
10 what kind of approach is acceptable to the staff. So,
11 it's a lot of the discussions that are not relevant to
12 the staff review.
13 We are not putting that DSRS as repetition
14 to existing - the reference material that's in the BTP
15 7-19.
16 CHAIRMAN BROWN: Okay. Well, just to beat
17 this dead horse a little bit deader, okay? I understand
18 your point. But, yet, when you look at - if you look
19 at the existing thing in the DSRS, a basis, you know,
20 a regulatory basis for why is not - is really not there
21 in terms of the way it's discussed in BTP 7-19.
22 There's a more thorough discussion of, you
23 know, the regulatory basis and the various - both the
24 rules from the GDCs, as well as other guidance that's
25 put out there. And there's a number of points made with

1 then clarifying discussion on those.

2 In other words, I mean, the reviewer now

3 if he hasn't, if he doesn't have the background that

4 you have or Dan has and the rest of your talented team,

5 it's going to be difficult for them to try to invent

6 some of this stuff on their own.

7 And maybe they won't even know they can go

8 to this since it's not even listed anywhere in the DSRS

9 relative as to a former basis - document that establishes

10 a regulatory basis for it.

11 So, anyway, that's -

12 MR. CONCEPCION: We're taking the feedback,

13 you know. We're taking it. We're going to go back and

14 look at D3.

15 MR. SHUAIBI: Let me add something here.

16 You said we're beating a dead horse. Maybe I'll beat

17 it a little more.

18 CHAIRMAN BROWN: You're going to make me talk

19 again.

20 MR. SHUAIBI: We've got statistics, I think,

21 that we can share with you on, you know, how many pages

22 was the old guidance versus how many pages are in this

23 Review Standard.

24 And if we want to do that comparison,

25 actually the difference is pretty significant. We know

1 that we're coming in here with a much, much shorter
2 document than what we had before.
3 So, we believe we've captured what's
4 important. But, again, as Ian and Dan said if you
5 believe that there's something missing, I mean, that's
6 part of our interaction with you, that's part of our
7 interaction with the public and everybody else.
8 We'll take that back. We're happy to take
9 that back, think about it, discuss it further with you.
10 And, you know, if we need to put it in, we'll put it
11 in.
12 But if we're going to compare numbers of
13 pages, I think - I think what we're ready to share with
14 you right now, you know, what the reduction is in the
15 number of pages, that's not what our focus was -
16 CHAIRMAN BROWN: I don't disagree with that.
17 I'm not a page guy, okay? I'm interested in content.
18 MR. CONCEPCION: Yes.
19 CHAIRMAN BROWN: And what I tried to look
20 at when I did that one basic comparison was what was
21 the content of 7-19 and relative to what the content
22 was.
23 MR. CONCEPCION: Yes.
24 CHAIRMAN BROWN: And I agree that there's
25 some stuff that could be left out, but it just seemed

1 to be, you know, if I looked and said what's the reviewer
2 - if you look at what - where's the reviewer guidance,
3 it's not - there's not a whole lot in there.
4 So, anyway, that's - well, I'll pass on
5 that.
6 MR. CONCEPCION: Yes.
7 CHAIRMAN BROWN: Do you have any other
8 comments, Dennis, John, Jack?
9 MR. SANTOS: We'll get to that specific
10 section later today.
11 MR. CONCEPCION: Yes, we'll have a chance
12 to -
13 MR. SANTOS: We'll present our logic, and
14 then we can take it from there.
15 MR. CONCEPCION: Absolutely.
16 CHAIRMAN BROWN: Okay.
17 MR. CONCEPCION: Okay. So, moving on to the
18 next slide.
19 So, in the process of reviewing the SRP and
20 the relevant guidance, we used our I&C reviewers who
21 have done some of these I&C reviews in the past and we
22 also reached out to other staff members in NRO, to
23 reinforce those interactions and activities that we do
24 as part of our review of other systems that interact
25 with I&C. So, we attempted to strengthen those areas

1 where there's overlaps in our review guidance.

2 And there's a bunch of other regulatory

3 requirements that show up in the existing SRP for I&C.

4 So, we had lengthy discussions with staff to better

5 coordinate those reviews and clearly establish review

6 responsibilities and all of that.

7 As part of the feedback we received from

8 NRR, NRO, we had people reviewing the DSRS internally.

9 We had NRO provide some feedback. We had OGC providing

10 feedback. And also, external stakeholders provided

11 feedback.

12 So, let me touch briefly on what the status

13 of the DSRS is today and what led us to be here with

14 this second version of the DSRS.

15 Back in June we published 7.1, which is the

16 fundamental design principles. And we published

17 Appendix B, which is the I&C architecture, and Appendix

18 C, simplicity, along with the references for initial

19 review and comment to support a meeting with

20 stakeholders on June 21st.

21 And the feedback we received - oh, and there

22 was some feedback that we received from this committee

23 as well.

24 So, we took that feedback and considered

25 the feedback and put it in the second version of the

1 DSRS, which is what you have in front of you today.
2 We published it again - I guess those three
3 sections were published and that we expanded and covered
4 hazard analysis and provided basically the full Chapter
5 7 without the section on quality and software
6 development. We published it back in September of this
7 year and that is the reason why we're here today.
8 We're still in the process of collecting
9 public comments and still in the process of developing
10 the guidance of quality and software development, which
11 will take us some time to finish.
12 Hopefully by sometime next year we will be
13 able to publish this section and then collect some
14 additional feedback on that.
15 Okay. So, now I'm going to get into the
16 specifics of how we incorporated the lessons learned.
17 And I have two examples associated with reorganization
18 of the review guidance and separating those fundamental
19 design principles from other system characteristics.
20 So, if you go to the next slide, I'm on Slide
21 11. We wanted to focus the review guidance on how the
22 applicant should address those fundamental design
23 principles of independence, redundancy, determinism and
24 all of the - in D3.
25 And we provided specific language to

1 address some of those activities so the reviewer
2 understands how to review those to assure that there
3 is regulatory compliance.
4 And this is an example that I'm going to
5 show here. In the case of independence, we centralized
6 the discussion about independence in 7.1.2 of the DSRS.
7 And we repeated that same approach for each fundamental
8 design principle that is in Section 7.1 of the DSRS.
9 So, in addition, we alluded to the level
10 of detail that we expect to receive in the application
11 that the reviewer - that the reviewer should use to
12 review the application.
13 We're getting to asking for logic diagrams
14 and architectural descriptions and signal directions
15 and inputs and outputs and all of that information so
16 that we get a complete picture of the I&C system and
17 how it - how the components interrelate and get that
18 perspective directly in the application so the reviewer
19 understands.
20 This is another example of how we
21 reorganized the information. Today, the SRP has a
22 system-by-system approach. And on top of Section 7.2
23 through 7.9 of the SRP, you have the branch technical
24 positions which provide a resolution of a particular
25 technical issue.

1 So, Section 7.2 contains all the regulatory
2 requirements applicable to RTS and there is repetition
3 of regulatory requirements as you go through each of
4 those sections. So, inherently, that structure lends
5 itself to be repetitive.
6 So, what we did was we segregated whatever
7 we considered important as part of the fundamental
8 design principles, put them in 7.1, we took all the
9 additional design and functional characteristics and
10 put them in 7.2 of the DSRS, and then considered all
11 of the BTPs and relevant ISGs and put them in those
12 sections of the DSRS.
13 So, we made sure that - again, this came
14 up already, but we tried to make sure that we didn't
15 lose relevant guidance associated with those concepts.
16 And I guess in the case of D3 we're going to go back,
17 but this is the structure we came up with.
18 And, again, we expect the applicant to
19 provide information and address those fundamental
20 design principles and system characteristics in a single
21 location rather than scattered in different sections
22 of the application.
23 CHAIRMAN BROWN: Okay. Before you go - back
24 up one slide. I just wanted to make one point.
25 MR. CONCEPCION: Yes.

1 CHAIRMAN BROWN: And I'm not speaking for
2 the - I'm speaking for myself right now, not necessarily
3 for the Subcommittee.
4 Personally, I like the setup of bringing
5 the various types from the independence standpoint,
6 bringing them into one section as opposed to having them
7 spread out through a number of different sections they
8 have to evaluate. So, that's a good idea in terms of
9 integrating it, putting it in one location.
10 However, to make a - just to make a point
11 under the communications independence, the first
12 sentence that leads off says that determination of
13 communications independence is self-evident,
14 self-evident, if one-way communication is used among
15 redundant channels or divisions and between safety and
16 nonsafety systems.
17 And I, I mean, I think my brain just about
18 exploded when I read that. I'm using very soft words.
19 Could have made it stronger.
20 One-way communications does not ensure
21 independence. That is so far from the truth. It's what
22 you send and the method of sending, the type of data,
23 the information and everything else that gets put in
24 with that.
25 So, if I was a reviewer and I was looking

1 for independence and a design came in and said, hey,
2 we're one way, I stop. I mean, his job is done from
3 a communications standpoint.
4 And that is so far from the truth that it's
5 just difficult for me to really integrate that and
6 understand that and even sign up to it.
7 And if you've participated in any of our
8 other design center meetings, we've spent multiple
9 meetings trying to make sure that point got across and
10 that we had ways to compromise - not compromise, excuse
11 me, accommodate or - I've forgotten what the right word
12 is now - recognize or, you know, to make sure that if
13 you were compromised on your independence, it didn't
14 compromise safety. It didn't compromise your ability
15 to trip a channel or to, you know, fail as-is or to
16 execute a safeguards function.
17 So, I mean, that's, you know, that's, you
18 know, you go through a whole bunch of other stuff after
19 that which is relevant to the discussion which blatantly
20 says, you know, the first statement is not true.
21 So, that's just a difficult - when you say
22 we've addressed it in one location, you're right. But
23 yet, you've made a blanket statement in terms of what
24 constitutes satisfactory communication independence,
25 which is really the lynchpin. It's one of the most

1 difficult areas of software-based I&C systems because
2 of sending digital type signal data from one division
3 to another division for voting purposes, or any other
4 purpose.
5 MR. SANTOS: We're taking the feedback - this
6 is Dan Santos. Charlie, good comment. We can probably
7 come up with a better word.
8 (Laughter.)
9 MR. SANTOS: What I want to say is that as
10 you know, communication independence is not the full
11 story. That the real story is independence, okay?
12 CHAIRMAN BROWN: Well, that's one of
13 multiple -
14 MR. SANTOS: Right.
15 CHAIRMAN BROWN: I agree with that.
16 MR. SANTOS: We have many attributes when
17 it comes to independence. I mean, it's the collection
18 and the systematic look at the system to ensure
19 independence.
20 Includes functional, sharing of parameters
21 -
22 CHAIRMAN BROWN: I agree with you, Dan.
23 MR. SANTOS: - basic -
24 CHAIRMAN BROWN: Stop for a minute. I
25 understand.

1 MR. SANTOS: Okay.

2 CHAIRMAN BROWN: The functional
3 independence and electrical independence are fairly
4 relatively - I'm saying it's relatively easier to grab
5 your hands around.

6 Communication independence and
7 software-based systems is very difficult to get your
8 hands around, because it's invisible. Little bits and
9 bytes running around on buses.

10 So, I mean, and how that communication is
11 done, I mean, relative even if you look at the base
12 diagram of the mPower design, all of their information
13 flows out from -- like the PTL level, I actually looked
14 at that gross top-level architecture out to a -
15 everything goes through one set of buses. It's all
16 conglomerated; ESF systems, control systems and reactor
17 protection systems.

18 Well, what part of independence do I not
19 understand when I look at that, okay? There's no -
20 there's physical independence, but there's certainly
21 not functional independence and there's certainly not
22 communication independence, or at least not based on
23 the level of detail in that particular diagram, which
24 admittedly is very high-level.

25 My point being I agree with you. But the

1 communication setup in this stuff and the independence,
2 the whole issue we've been dealing with the last four
3 years, is to make sure this independence issue is not
4 compromised.
5 If you don't have it, you don't have a safe
6 system, period, whether it's reactor trip systems or
7 whether it's safeguard systems.
8 MR. CONCEPCION: We understand the feedback
9 and we're going to go back and look at the section one
10 more time.
11 I believe we're getting into some -
12 CHAIRMAN BROWN: It was an example.
13 MR. CONCEPCION: - proprietary details
14 that I just don't -
15 CHAIRMAN BROWN: No, I didn't see it say
16 proprietary and I didn't even say what it looked like.
17 I just said it's -
18 MR. CONCEPCION: Okay.
19 CHAIRMAN BROWN: I have to go back and look
20 at what those levels are.
21 MR. SHUAIBI: Good comments and we'll take
22 that one back. We'll relook at that section.
23 CHAIRMAN BROWN: This is a critical part of
24 this DSRS.
25 MR. CONCEPCION: We understand and we're

1 going to go back and look at this section.

2 CHAIRMAN BROWN: Okay, thank you.

3 MR. CONCEPCION: Yes.

4 MEMBER BLEY: I think what follows is pretty

5 good though.

6 MR. CONCEPCION: Oh, yes.

7 MEMBER BLEY: This makes sense to me, the

8 last two slides you talked about. And it makes sense

9 to me given we've had all these discussions the last

10 four years.

11 I know you've been really busy. Have you

12 had a chance to run this draft past some of your people

13 who might be doing reviews in the future who aren't as

14 experienced, to see if this is - hangs together as well

15 for them as it appears to hang together for me, anyway?

16 MR. CONCEPCION: Well, part of this effort

17 includes a training activity once we are done with

18 developing the chapter. So, we intend to go and train

19 our staff on how to implement this DSRS.

20 And staff has been able to look at this draft

21 version today. So, this version is available. We

22 shared it with staff, but we intend to have training

23 once we're done with it.

24 And once we get the application, we will

25 involve staff members to make sure they understand how

1 to implement.

2 MEMBER BLEY: How to use it.

3 MR. CONCEPCION: This is a clear change in

4 the way we're doing reviews from the current SRP from

5 these fundamental principles. And we're sensitive to

6 that and we know that there is some training associated

7 with it.

8 MR. JUNG: Mr. Bley, just to add from my

9 branch who led this project, and our branch is assigned

10 to review this particular design, advance reactors

11 coming up, so development of DSRS is a branch-level

12 activity.

13 I think most of them were involved starting

14 from depending what kind of structure do we want? And

15 we divided many of the efforts between the junior

16 reviewers all the way up to senior reviewers.

17 So, in the audience, most of my staff, I

18 see their faces. Some of the junior engineers who's

19 been with NRC only a few years, all the way through,

20 you know, decades of experience. They were all part

21 of that. We've been addressing their suggestions and

22 comments along the way.

23 They are part of the ownership right now.

24 So, in a way, not to mention about the training, but

25 they are already getting trained on what it looks like,

1 what's needed. So, they've been providing their own
2 -
3 MEMBER BLEY: I'm glad to hear that.
4 Sometimes these things that look so good on the
5 conceptual level, don't quite work when you actually
6 try to use them. And I was hoping you had those folks
7 involved.
8 MR. CONCEPCION: We should be able to collect
9 some additional lessons learned once we start
10 implementing it.
11 MS. STAREFOS: Can I also comment on that,
12 Mr. Bley? Joelle Starefos, Project Manager.
13 It was really remarkable the number in
14 variety of experience in the room for the people that
15 were developing this. It was very impressive.
16 And it was interesting to see that across
17 Ian's, I guess to say, almost whole branch had been
18 involved at one point or another here.
19 So, I think that those aspects had been
20 incorporated and thought about during this as well.
21 So, I just wanted to share that.
22 MEMBER BLEY: It will be interesting to see
23 what happens.
24 CHAIRMAN BROWN: Another point relative to
25 this since you're using examples, was under the

1 redundancy part of the - I'm trying to find it now.
2 Yes, redundancy.
3 When you read through that, there is - the
4 only reference in terms of evaluating this from an
5 acceptance criteria was listed as single failure
6 criteria, which gives you to believe that that is the
7 sole basis for why we have redundancy.
8 And yet, if you look at that in a bigger
9 - on a bigger scale, the real point is there is other
10 operations that drive you to higher levels of
11 redundancy.
12 I mean, for instance, if only single failure
13 was a criteria, all I'd need was three channels.
14 But yet, if I have to allow myself to operate
15 when I'm in maintenance bypass and I've got to channel
16 down, it drives me to four.
17 So, there's no discussion - I see somebody
18 shaking their head up and down over there. So, I don't
19 know if you're all agreeing or disagreeing with me.
20 MR. CONCEPCION: Well, I agree with you.
21 CHAIRMAN BROWN: But the point being is that
22 that's, you know, when the reviewer has to address what
23 I'm looking for in terms of redundancy, what are the
24 factors that he looked at?
25 Is it just single failure, or are there

1 other modes of operation that drive you to different
2 levels of redundancy?
3 And it's not - and I don't know that's in
4 the rest of the old SRP or not, but it's certainly not
5 - it's certainly not listed or at least I didn't
6 recognize it in here.
7 So, that's just - I'm just trying to use
8 an example of something that appeared to be missing.
9 In other words, what does the reviewer use when he looks
10 at the acceptance criteria and when he looks at the -
11 what is it - the review procedures that he goes though?
12 So, all those factors that drive you in
13 certain areas somehow - and I don't mean pages of this
14 discussion, but what's the functional - what is the
15 specific design thing you look for relative to other
16 modes of operation whether they be maintenance or
17 whether they be testing or whatever they happen to be.
18 MR. SANTOS: That's a good comment. And,
19 actually, we have got a comment like that already and
20 we're going through. So, I thank you for that and that's
21 the type of feedback we're looking for to make sure we're
22 complete.
23 So, again, we already had a comment very
24 similar to that and we're going to be dispositioning.
25 So, thank you.

1 CHAIRMAN BROWN: Okay.

2 MR. JUNG: Yes, Charlie, generally the - our
3 redundancy guidance as we pull together our fundamental
4 design principles, redundancy was somewhat difficult.

5 The way the current guidance is structured,
6 the current guidance somewhat focus on a lot of
7 regulatory requirements and what to review.

8 So, redundancy was not specifically
9 identified as a relatively good section -

10 CHAIRMAN BROWN: In the old -

11 MR. JUNG: The existing SRP.

12 So, I think we made an improvement overall
13 from a redundancy. But maintenance bypass and
14 operating bypass, those are 603 requirements
15 specifically listed in 7.2 as well. There's even an
16 argument what drives a redundancy as a single failure
17 criterion or bypass. Those are very controversial kind
18 of topic.

19 Generally, I think it is well understood
20 that single failure criteria and 603 really drives
21 fundamentally what redundancy is required and some of
22 the bypass conditions are accepted, condition of the
23 tech specs, for example, that allows two out of three
24 instead of two out of four.

25 So, is that a redundancy or not? It could

1 be arguable, but regulation requires maintenance
2 bypass, operating bypasses are designed in a safe way
3 for all operating modes. So, we have another
4 requirement to handle that.
5 Whether we want to put that into redundancy
6 to have another redundant, a repetitive guidance, that's
7 a different aspect.
8 CHAIRMAN BROWN: Let me phrase it another
9 way. When I look in many of the sections you addressed
10 and refer to either IEEE 603-specific clauses and here
11 the only reference was to 379 -
12 MR. CONCEPCION: Yes.
13 CHAIRMAN BROWN: - but yet that does not
14 - to my knowledge, that does not go into that
15 information. It's been a while since I looked at 379.
16 So, the point being is if there's relevant
17 regulatory basis or rule basis for it, then I think you
18 could make an - it's just what does the reviewer look
19 at when he's - personally, I think the approach relative
20 to fundamental high-level principles of design that you
21 want to get across to people, a different approach to
22 looking at this not be reg guide or, you know, bottom-up.
23 You want to be top-down, and then you want these other
24 pieces to feed in as to how do you deal with each of
25 these fundamental principles.

1 And so that, I don't have any - I personally
2 don't have any disagreement with that. But yet, you
3 still have to give the reviewer when he's thinking about
4 the principles, what are the points that drive - or the
5 regulatory basis that drive those whether it be from
6 a reg guide, or whether it be GDC, or whether it be IEEE
7 603.
8 MR. CONCEPCION: Let me just add something
9 real quick here.
10 Like I said before, we're manipulating the
11 existing guidance in the SRP. And perhaps we might need
12 additional information to the reviewer to address this
13 particular aspect of redundancy.
14 Now, when you look at RTS in the existing
15 SRP, it points you to IEEE 603, Section 5.1, which calls
16 for IEEE 379. And that is endorsed in Reg Guide 1.53.
17 So, I understand the point, but we are using
18 existing information to populate the sections that are
19 in the DSRS today. And if we need additional guidance
20 for the reviewer to perform a review and determine what
21 is it that we need for them to establish that redundancy
22 is, in fact, implemented in the design, we can go back
23 and look and identify those and incorporate it in the
24 DSRS, but we're using the existing information.
25 We did not reduce guidance particularly for

1 redundancy in the DSRS. We've extracted what's in the
2 SRP and put it in there.
3 And we're taking the comment - this is
4 something that NRR brought up already and we're going
5 to address it, definitely.
6 CHAIRMAN BROWN: All right. Well, I'm
7 repetitive in my comment then. I didn't know that.
8 MR. CONCEPCION: That's okay. That's okay.
9 Okay.
10 CHAIRMAN BROWN: I will continue to be
11 repetitive if I have to.
12 MR. CONCEPCION: That's okay. No, that's
13 not a problem at all. We're addressing the comment as
14 we speak.
15 MR. SANTOS: Just to add real quick, sorry
16 to interrupt, you mentioned redundancy. But like we're
17 saying, we're taking a new approach with the four
18 fundamental principles and our current guidance wasn't
19 structured like that.
20 So, to go from this top-down approach
21 there's this translation that's going on, but we're all
22 for being complete. So, that's all I want to say.
23 MR. CONCEPCION: Okay. I think I covered
24 Slide 12 already. So, moving on to Slide 13. This is
25 another lesson learned that we're trying to incorporate

1 in the DSRS.

2 And moving on to the next slide, this is

3 the structure we came up with after we decided to

4 incorporate the fundamental design principles.

5 So, you have the introduction in 7.0, you

6 have directly addressing the fundamental design

7 principles in the middle column of that slide, and then

8 you have the system characteristics which are design

9 and functional characteristics are contained in IEEE

10 603-1991.

11 And what's missing in this particular slide

12 is the list of appendices that we expect to use in

13 conjunction with 7.1 and 7.2, but this is pretty much

14 the structure we're implementing in order to use that

15 lesson learned related to the fundamental design

16 principles and incorporate in the guidance.

17 That's the only point I'm trying to make

18 here with this slide.

19 CHAIRMAN BROWN: Plus the appendices.

20 MR. CONCEPCION: Plus the appendices, yes.

21 Plus the appendices. There's a better slide later on

22 that I will show everything in there.

23 Okay. So, I have two examples that show

24 how we remove redundant and nonapplicable information.

25 There is one that comes across really obviously, which

1 is IEEE 279 if we go to Slide 16. And, by the way, there
2 is a typo on that slide.
3 On the right-hand, the first bullet, it
4 should read "pre-1999 licenses." That is the
5 applicability of IEEE 279. I apologize for that.
6 So, like I said, we considered all the
7 guidance and tried to improve the efficiency of it by
8 modifying, incorporating information and removing the
9 stuff that we didn't find necessary to the reviewer as
10 we went through and identified what it was that we needed
11 for the DSRS.
12 And in the end once we removed, for example,
13 the 279 and the repetitive information and some other
14 sections, we end up with this document that has around
15 150 pages from 500 plus pages. But that includes BTPs
16 that we - that were applicable to I&C that we were able
17 to roll into the DSRS and some other information that
18 we didn't consider, because it was not applicable to
19 this particular project.
20 And I have to emphasize that we did not lose
21 relevant guidance. We took what we had and we put it
22 in the DSRS.
23 Perhaps we can improve in some areas, but
24 the net effect of the existing guidance and the
25 rearrangement gave us this result and this particular

format.

MEMBER BLEY: In the past, we feel that we've had a great number of unnecessary RAIs.

(Laughter.)

MR. CONCEPCION: You want to answer that?

MR. JUNG: Milton wasn't quite here. I have to be careful what I say.

MR. CONCEPCION: I would think so.

MR. JUNG: I think there could have been efficiency -

MEMBER BLEY: So, they were repetitive or -

MR. JUNG: - that could have obtained. Because in February meeting I mentioned to you about repetitiveness in different systems and different areas, right? Many of my folks are involved in one design center to be able to accommodate the review.

So, each person looking at 7.2 reactor trip system, it contains a lot of the redundant, repetitive review areas, including independence, all of the, you name it, digital systems. And somebody reviewing 7.9 on data communication system, you're looking at communication type of things.

MEMBER BLEY: So, we're really talking about repetitive RAIs that were asking the same issue, but

1 from slightly different point of view.

2 MR. JUNG: In some cases because it should

3 be the nature of the information, the applicant also

4 does make a mistake in providing some different

5 information, different level of detail, different

6 sections to address the same issue.

7 I remember there are cases that RAI could

8 have been combined into one single, very clear RAI that

9 you would have - it got repeated multiple times in some

10 cases to make sure what it was really meant by the

11 applicant, because it was not clear in two different

12 sections.

13 But I think overall we worked it out okay.

14 I think, you know, eventually as we write the SER, we

15 have to make a conclusion.

16 MEMBER BLEY: This side could get you in

17 trouble somewhere.

18 CHAIRMAN BROWN: Well, I would amplify your

19 comment relative to - I don't think it's necessarily

20 all driven by just having stuff in different places.

21 Because if anything stood out to me in some of the

22 earlier what I'd call design center reviews, was a lack

23 of either understanding or agreement by the design

24 agents relative to what NRC needed or wanted relative

25 to clarity and detail in the functional designs that

1 they presented.

2 And, I mean, I remember specifically

3 sitting in the first meeting I was in, in June or July

4 of 2008 where we were just told, no, we don't have to

5 give you the information.

6 It turned out that that didn't work out for

7 a couple of years and we eventually got it, but the point

8 being is that it's critical for the review standards

9 to be very clear relative - and I don't think they were

10 before from what I went and looked at when we were doing

11 that in terms of what level of detail do you want and

12 how do you specify how certain basic, for instance,

13 independence or diversity or what have you are actually

14 accomplished.

15 So, it's important to have enough detail

16 that people understand what you're looking for and what

17 is an acceptable approach to doing things.

18 So, I think that's what drove a lot of the

19 RAIs in trying to get that level of information. And

20 so, that's why we drive to try to have a little bit more

21 information. This is what the reviewer is going to be

22 looking for and that detail is there, and we go on from

23 there.

24 MR. JUNG: Thank you, Charlie. We fully

25 agree. I just want to add one aspect of it related to

1 complexity and simplistic design.

2 In some cases, the solution was not about

3 more details. It was about demonstration of safety

4 with, in some cases, a simpler design.

5 CHAIRMAN BROWN: Absolutely. I won't

6 disagree with that.

7 MR. JUNG: So, in those cases, simpler design

8 does not require more detail. It needs that decision

9 to be made up front.

10 CHAIRMAN BROWN: Well, if you get a design

11 submitted to you in functional diagram language which

12 is extremely complex looking, that immediately sends

13 the message that, you know, we're - that's going to be

14 a problem.

15 Whereas if it's emphasized - and that's why

16 it's important to emphasize the simplicity standpoint

17 even though it's not - there is no rulemaking relative

18 to simplicity.

19 MEMBER BLEY: Could you back up one slide?

20 MR. CONCEPCION: Yes, sir.

21 MEMBER BLEY: I think you might have a good

22 story for this, but there's a thing that worries many

23 people, me in particular, when you go from the existing

24 SRP when you do it at higher levels with some licensing

25 issues, to a design-specific and you get this idea of

1 what we have to do is remove the irrelevant parts from
2 the general guidance to our specific guidance.
3 Where do you cover looking very hard to make
4 sure that you add things that are necessary due to the
5 new design as well?
6 MR. CONCEPCION: Well, we added new
7 guidance. We added the guidance on HA. We added the
8 guidance on I&C architectural description. We added
9 guidance on simplicity.
10 And we had limited information and I don't
11 want to talk too much about this, because the information
12 we received is clearly proprietary and there are some
13 - there's some information in the DSRS today that alludes
14 to it in a subtle way, but we had those pre-application
15 interactions with B&W and we captured the essence of
16 some of those early design decisions and we try to tailor
17 the DSRS to capture those.
18 In the case of nonapplicable guidance where
19 clearly 279 is not applicable to the mPower design, that
20 is one -
21 MEMBER BLEY: No, nobody is going to argue
22 with you that -
23 MR. CONCEPCION: Right.
24 MEMBER BLEY: - there's reason to remove
25 inapplicable things. It was the other side. And at

1 least for me, the thing that helps - well, there are
2 two things that help. And the one is this focus on the
3 fundamental design principles that cover things that
4 maybe you weren't covering well before, and the
5 elimination of the use of DAC also kind of helps with
6 that as well.
7 So, I think you might have a story, but you
8 can get a sense of what we did was take away the stuff
9 that didn't matter rather than we really looked to make
10 sure we were being inclusive as well.
11 MR. CONCEPCION: The only major information
12 that we did not consider for this was 279. Everything
13 else was fair game and we considered it - we removed
14 the repetition.
15 Now, this exercise is uncovering certain
16 areas where we don't have strong guidance to the reviewer
17 and that's reflected in some of the sections.
18 So, we're taking that feedback back and make
19 sure that we provide what the reviewer needs to address
20 those areas, because we understand that the structure
21 provides a different approach that is - that will need
22 additional information to the reviewer to make sure that
23 all of the safety issues are resolved.
24 I guess Dan wants to - or Mo. I'm sorry.
25 MR. SHUAIBI: I'll just add one other comment

1 to that. A very relevant comment. And kind of it's
2 where we are today and where they are today as an
3 applicant.
4 So, let me just say that regardless of what
5 you see here today if we learn something in design space
6 in the future that we haven't considered, there is
7 nothing to stop us from going out and developing either
8 new guidance or new RAIs to deal with those issues.
9 So, they don't have a complete design right
10 now that we could basically tailor our review standard
11 very specific to that design. But as that gets closer
12 and as we learn more about their design if anything comes
13 up where we need new guidance, I'll be back sometime
14 in the future, and you can quote me on this, we will
15 address that design feature - those design features if
16 they come up.
17 So, I guess what I'm saying is right now
18 what you've got is based on the information that we have.
19 And the more information that we get, the more we'll
20 be looking at it to see if we need more guidance or if
21 something else needs to change.
22 MS. STAREFOS: I'd also like to add that our
23 overall philosophy for the DSRS was to have more
24 information rather than less, unless we were certain
25 that removing it was appropriate.

1 So, in some cases you might see things that
2 are more generic than you would imagine the design would
3 be, but we didn't have the certainty in where the design
4 was at that point to eliminate it as a review aspect.
5 So, we were - we tried to be very
6 conservative in that to allow the reviewer to make that
7 decision at application.
8 MR. SANTOS: I just want to offer that when
9 we get to the specific sections later today if there
10 is any particular area that you feel what happened to
11 this, we can explain to you our evaluation process that
12 resulted in inclusion or elimination.
13 And we have to be careful with the examples
14 so we don't get into proprietary information, but we'll
15 share that with you.
16 MR. CONCEPCION: Okay. I'm on Slide 17 now.
17 So, this is another example where we
18 identified an area where there was repetitive
19 information in both Chapter 7 and Chapter 18 of the
20 application.
21 And we had the luxury of having someone from
22 the human factors group doing a rotation to our branch
23 in the time that we were identifying these overlaps.
24 And he was quick to identify there were some areas that
25 had clear overlap.

1 And what we did was we strengthened the
2 coordination of human factors considerations which is
3 an IEEE 603 requirement that we need to address in I&C
4 systems.
5 And what we did was the stuff that's on the
6 left used to be in Chapter 7. What we did, we condensed
7 the information and put a direct pointer to Chapter 18
8 of the application, because that is an area where I&C
9 has to coordinate with human factors.
10 And this is something that we considered
11 an improvement, because we - this guidance was not -
12 was in Chapter 7. We were not doing an active review.
13 All right. So, where am I? DAC, okay.
14 Going to the next slide.
15 MEMBER BLEY: Just for me and is this really
16 a change at all? How do you coordinate the human factors
17 and the I&C? I mean, they're very closely correlated.
18 Do you have each other on the review teams
19 for each of those?
20 MR. CONCEPCION: Yes, I need a lifeline,
21 Paul.
22 MR. PIERINGER: Hi, I'm Paul Pieringer,
23 human factors technical reviewer.
24 The way we used to do it is pretty much we
25 would independently come to our conclusions and

1 sometimes we would talk and make sure our conclusions
2 were the same. Other times it would be caught in the
3 review process where we might have disconnect.
4 The plan going forward is that these kind
5 of references cause tech reviewers to come down and talk
6 with each other and to review the results of each chapter
7 before they become finalized.
8 There are certain areas we know that we have
9 to have a team orientation. One of them is the D3 manual
10 action review, because all that material comes to the
11 Chapter 7. And Chapter 18 people wouldn't see it unless
12 we go in and pull the Chapter 7 material. So, this
13 rewrite specifically directs that interface.
14 And the other, I would say, even more
15 important interface is around Reg Guide 1.97. And that
16 only - not only requires an interface between Chapter
17 18 and Chapter 7 people, but in the last design center
18 review we did, we actually had a team fielded with the
19 Chapter 15 people, the systems people, TRA people, HFE
20 and tech specs.
21 So, I can't give you a number, but it was
22 probably on the order of 10 to 12 people. And with that
23 interface, we were able to start from the design basis
24 material and understand what that required and work it
25 down through every step in the various system designs

1 and verify that the end product was that every control
2 display alarm needed to support - managing design basis
3 events had been properly characterized and cataloged
4 within the 1.97 structure.
5 We took that concept and we embedded it in
6 this rewrite. And what it does, it's centered in
7 Chapter 7. So, they've taken on the leadership
8 responsibility for that and is in the direction for the
9 reviewers of Chapter 7.
10 It says, contact the following people as
11 a minimum and it recommends establishing this team for
12 Reg Guide 1.97. That's the basics.
13 MR. CONCEPCION: Yes. Thanks, Paul.
14 MEMBER BLEY: Anything that drives us in this
15 direction is good.
16 (Laughter.)
17 MR. CONCEPCION: Thanks. Okay. So, I'm
18 back on Slide 19 and I'm trying to address the concept
19 of DAC and I want to be clear here.
20 We understand that DAC is policy and we
21 understand that it can be used in DSRS, but we're looking
22 for a level of detail that is sufficient for us to resolve
23 all safety issues without reliance on DAC.
24 Now, B&W is on board and they have been
25 forthcoming. They have been cooperative with the level

1 of information - they say they will provide the
2 information sufficient to address all safety issues.
3 So, we don't expect any particular issue regarding DAC.
4 Yes, sir.
5 CHAIRMAN BROWN: Okay, question. Where
6 does it say that in the DSRS?
7 MR. CONCEPCION: It does not mention it.
8 CHAIRMAN BROWN: That's my point.
9 MR. JUNG: Charlie, we don't discuss DAC -
10 CHAIRMAN BROWN: Hold on. There's no reason
11 why you shouldn't state in the fundamental start-off
12 of this thing that the level of information provided
13 to evaluate the design should be sufficient to establish
14 that whatever the overarching reactor safety, et cetera,
15 et cetera, you don't have to even use the words DAC.
16 I agree you don't - it would not be a good idea to kind
17 of cross-play that and get into a food fight.
18 But the point being is the purpose of a good
19 bit of the information that's provided in here is to
20 ensure that we get that information. Not just the
21 Advisory Committee. I mean, that's just so you all have
22 the ability to provide us with the information that we
23 can walk away knowing that on a licensing basis you now
24 have - you don't have to wait for something to happen
25 five years later.

1 You don't have to say that, but you've got
2 to be able to establish the firm licensing basis as part
3 of your, you know, final design certification or
4 whatever.
5 So, you say that, but you don't talk about
6 DAC. So -
7 MR. JUNG: Thank you, Charlie.
8 CHAIRMAN BROWN: - that will be - that will
9 probably be a comment. I just - I don't know whether
10 it will be a comment or not, because I've got 14 other
11 people to deal with.
12 From my viewpoint -
13 MR. JUNG: Thank you, Charlie. We accept
14 your comment and -
15 CHAIRMAN BROWN: I'm glad you accept it.
16 (Laughter.)
17 CHAIRMAN BROWN: Now, what are you going to
18 do with it?
19 MR. JUNG: We'll work with the applicant.
20 We are communicating what you're just saying with the
21 applicant and we'll see what we can do in the guidance
22 space.
23 CHAIRMAN BROWN: Well, this is - remember,
24 this is the Design-Specific Review Standard. The
25 applicant shouldn't - well, maybe I shouldn't say that.

1 I'm very blunt.

2 MR. CONCEPCION: We're working with the

3 applicant.

4 CHAIRMAN BROWN: This basis, I mean, quite

5 frankly, again, my opinion, not the Committee's opinion,

6 is that the higher level fundamentals plus this thing

7 really should be a better format for overall generic

8 design reviews or, you know, a Standard Review Plan for

9 staff.

10 It's a far more functional level of looking

11 at in terms of meeting basic safety goals. There are

12 a lot of details, but you start from the top down.

13 And fundamentally from that top-down

14 standpoint, you set the guidance for what is acceptable

15 for processing and say, yes, we accept this design.

16 You ought to just say it.

17 MR. CONCEPCION: We're taking steps to get

18 there and give the reviewer the tools so that he or she

19 understands what level of information is needed.

20 We're not mentioning DAC, but we're

21 alluding a lot to certain aspects of the design

22 description that should get us there without necessarily

23 having an applicant saying, okay, I'm just going to use

24 DAC.

25 CHAIRMAN BROWN: Well, up in the -

1 MR. CONCEPCION: Hopefully we're in the
2 right direction.
3 CHAIRMAN BROWN: - review of the review
4 process, all it takes is a small paragraph that says
5 that the purpose of this, you know, is to ensure during
6 the review that we have a satisfactory level of detailed,
7 functional instrumentation and control information to
8 establish that the licensing basis or safety basis is
9 met at this date and that we don't have to bet on - you
10 don't have to say - this is my extra words. You don't
11 have to say so we don't have to bet on something in the
12 future, but the point ought to be made up front without
13 saying that.
14 You can't say they can't use DAC. You can't
15 do that, because that's established policy.
16 MR. CONCEPCION: Understand. I appreciate
17 the feedback.
18 CHAIRMAN BROWN: Okay.
19 MR. CONCEPCION: Okay. Moving on, this is
20 another example -
21 CHAIRMAN BROWN: Know where I come from,
22 that's all.
23 MR. JUNG: Charlie, we're not ignoring it.
24 We are taking that into -
25 MR. CONCEPCION: No, absolutely.

1 Absolutely.

2 MR. JUNG: Good feedback.

3 MR. CONCEPCION: Moving on, this is another

4 area where we - that we identified as a lesson learned.

5 We're introducing the concept of simplicity

6 and hazard analysis in our guidance. And not mentioned

7 on this slide is also I&C architectural descriptions.

8 So, we have a User Need Request with the

9 Office of Research right now. And Dr. Sushil Birla is

10 here with us.

11 They are working on developing a technical

12 basis for the review of hazard analysis. And what we

13 did a couple of months ago, we took a portion of that

14 research effort and we developed this Appendix A that

15 is right now in the DSRS.

16 MEMBER STETKAR: Are you going to talk more

17 about this in detail later?

18 MR. CONCEPCION: Yes, I will. Yes, there

19 is a slide devoted to Appendix A and we can get into

20 the details of it.

21 MEMBER STETKAR: Okay, fine.

22 MR. CONCEPCION: Yes. In addition, we took

23 existing guidance, the very limited guidance on

24 simplicity, and we tried to develop these items that

25 is in the DSRS. And this is a running joke. This was

1 not a simple task, because there is very little on
2 simplicity.
3 And we looked at the common position from
4 the multinational design evaluation program. We looked
5 at the I&C safety guide from IAEA, as well as information
6 from IEEE 7-432, and tried to come up with something
7 that would make sense in the area of simplicity.
8 And we ended up bouncing it against the
9 fundamental design principles so that we could at least
10 give the reviewer some information that he would process
11 this as he goes through the review of these systems and
12 address how simplicity was factored in the design of
13 these I&C systems.
14 I see you're nodding your - you're shaking
15 your head.
16 CHAIRMAN BROWN: No, what did I say five
17 years ago? Okay. It was redundancy, independence,
18 determinism, D3 and an adjunct principle not rule-based
19 of simplicity.
20 Those are the key factors in trying to
21 determine that you've got, I mean, that's the only way
22 nondetailed design people can look at the basic system
23 like the Committee or other outside bodies and say, look,
24 they've looked at this from the high-level standpoint
25 and they've tried to make sure that the system is as

1 simple as possible because you've got less likelihood
2 of having things surprise you. Yet, you still have the
3 complexity necessary to meet the other requirements.
4 Not the nice stuff, but the nice, you know,
5 the necessary stuff only. And that seems to be personal
6 opinion again from looking at the other stuff we've seen
7 in the last four years on the new design.
8 There's a lot of, gee, we've got this big
9 computer that can do all kinds of stuff. So, we're going
10 to do all kinds of stuff whether it's needed or not.
11 And there's always a nice, oh boy, this is
12 nice because the operator can - but when it's really
13 useless, and I won't complete the rest of that phrase.
14 It's been heard before, and I'm -
15 MR. CONCEPCION: Okay. And not shown on
16 this slide is the concept of I&C architectural
17 description that we also captured in Appendix B of the
18 DSRS.
19 CHAIRMAN BROWN: You've got another slide
20 on that later?
21 MR. CONCEPCION: We have a slide that
22 addresses -
23 CHAIRMAN BROWN: A, B and C are covered by
24 roughly starting at Slide 35 or so.
25 MR. CONCEPCION: Yes, it's later in the

1 presentation. So, we can get into the details of it
2 if you guys are interested in it, and I believe you are.
3 (Laughter.)
4 MEMBER STETKAR: That would be a good belief.
5 MR. CONCEPCION: This is another lesson
6 learned. Again, we try to make sure that we covered
7 all of the regulatory requirements in the guidance and
8 the DSRS.
9 And if you go to Slide 23, I'm showing a
10 couple of regulatory requirements from 603 and GDC and
11 the location of the DSRS.
12 This is just an attempt to show an example
13 of how we do it, but there is a table, Table 7.1 in Section
14 7.0, that pretty much maps Table 7.1-T of the SRP today.
15 And I don't - I guess we can go maybe later
16 during the presentation, because I have a slide devoted
17 all on 7.0 alone and all the information on 7.0.
18 I can show you how we mapped all of those
19 regulatory requirements in the DSRS, how they're
20 captured. And even we put review responsibilities and
21 review scope for some areas where we have a clearer
22 coordination with plant systems, with containment
23 systems, electrical systems and all of those other areas
24 that interface with I&C.
25 CHAIRMAN BROWN: I'd like to make one

1 observation. I notice that throughout you did make
2 observations that this other group is responsible for
3 this, and this other group - you have the Chapter 15
4 guy and the Chapter 6 guy and the Chapter whatever folks
5 are responsible for this.
6 MR. CONCEPCION: Yes.
7 CHAIRMAN BROWN: And maybe it's because I
8 was an I&C guy and responsible for all this stuff for
9 35 years in another - in the Naval nuclear program and
10 I was never able to shuck responsibility, the key word,
11 responsibility, for ensuring that my systems addressed
12 all of the relevant requirements that everybody else,
13 all the, you know, whether it be a fluid system, whether
14 it be a trip system, whether it be a support system.
15 If I had to do that, I always looked at it
16 - well, let me put it this way: Admiral Rickover never
17 allowed me to not take responsibility or I would have
18 my, you know, I'd be skinned alive if I had ever said,
19 oh, no, that's somebody else's. I would depend on he
20 would have shot me and said, that wasn't a good idea.
21 MR. CONCEPCION: But we're not -
22 CHAIRMAN BROWN: But, I mean, when you read
23 this, just personal opinion again, it looks like, well,
24 gee, we're just an adjunct. These other guys are
25 responsible for making sure we meet - that we have

1 addressed their requirements.

2 And I think it requires - personally, I

3 think you ought to have a little bit more stronger

4 ownership, myself, because this is the digital I&C -

5 this is the reactor trip safeguard systems and for all

6 the other support systems that feed in, auxiliary or

7 otherwise, that support that.

8 MR. CONCEPCION: Yes, we're trying to make

9 sure that the coordination is there, number one, but

10 we're not delegating responsibility.

11 CHAIRMAN BROWN: I don't disagree. But if

12 you read it, the way it reads is they have

13 responsibility.

14 MR. CONCEPCION: Okay.

15 CHAIRMAN BROWN: Okay. It's really being

16 I&C should be responsible to make sure that they do their

17 job and feed into you and coordinate with you.

18 You should be - the I&C folks should be

19 responsible for that. That's just kind of a generic

20 thought process I had when I was reading this.

21 MR. JUNG: Charlie, good comment. We will

22 take a look at that.

23 I just want to share one thought. One of

24 the lessons learned in some areas, I&C in some cases

25 have taken on someone else's - some other discipline's

1 work and spent a lot of time on as if we are the lead.
2 And there's some inefficiencies in terms of the, you
3 know, given the amount of time definitely we need to
4 take care of these fundamental design principles and
5 focus on what's really important, first. And then, also
6 coordinate with other branches.
7 This is a double-edged sword in terms of
8 how much we cover someone else's - I think it's a mutual
9 responsibility. We all have to have ownership,
10 understand the design.
11 A lot of the pre-application report of the
12 application interactions that's been going through, my
13 staff is attending, at least have a presence in
14 understanding the systems design and in fluid systems
15 and other areas.
16 So, how does I&C play a role in those things?
17 We are keeping on top of it. We understand your
18 comment. We'll take a look at that.
19 CHAIRMAN BROWN: Okay. I'm not - I wasn't
20 - I'm not trying to have you all take over the, you know,
21 what they're supposed to be.
22 The point being is that somebody, you, I
23 mean, if it comes up in the system as deficient later,
24 where is somebody going to go?
25 It's your system, Ian. Why, you know, how

1 did you guys let that one - all that means is you don't
2 - sure, you have to have a fundamental understanding
3 of the other systems. It doesn't have to be a detailed,
4 down in the, you know, what's the stress analysis for
5 the pipe and the flow velocities in the elbows and all
6 that. That's not what I'm talking about.
7 The point being is if you've got fundamental
8 functions that have to be accomplished, you have to make
9 sure in that coordination that they do them and give
10 it to you in a timely manner and that you understand
11 what they're giving you.
12 That's all I'm saying. I'm not advocating
13 that you do their work for them. That doesn't -
14 MR. JUNG: I think we understood the
15 feedback.
16 CHAIRMAN BROWN: And I just think you ought
17 to tweak the words a little bit to make it clear of
18 ownership and the necessary coordination.
19 So, instead of having, you know, these guys
20 are responsible, hey, you know, this is what we do and
21 we will make sure that all this other stuff comes in.
22 It's just a ways of phrasing it, that's all.
23 MR. JUNG: Yes, absolutely. Yes,
24 understand.
25 MEMBER STETKAR: To give you a specific

1 example that I kind of stumbled over in this area, you
2 say that, for example, you're not going to look at
3 separation of cables because people doing Chapter 8 does
4 that. So, we're not going to look at that.
5 That's okay. Last time I checked,
6 electricity got transmitted on copper wires. This
7 stuff gets transmitted on fiberoptic cables.
8 Who looks at separation of fiberoptic
9 cables? If you're not going to look at that, the
10 electrical guys aren't going to look at that. So,
11 nobody is going to look at it.
12 Okay. That's a little bit of what Charlie
13 is talking about in terms of this distributed -
14 CHAIRMAN BROWN: Yes, that's an obvious one
15 to -
16 MEMBER STETKAR: You and only you own
17 fiberoptic cables, but this says, no, we're not going
18 to look at the cable separation, because that's a Chapter
19 8 function.
20 Chapter 8 guys say, well, we looked at the
21 separation of our cables. We don't have to look at
22 those.
23 Okay. So, be careful about that.
24 MR. CONCEPCION: Yes, I understand that.
25 Okay. So, this is - I guess this is a better

1 representation of DSRS Chapter 7 on the right-hand side.
2 And we're putting it side-by-side with the existing
3 SRP. And I just want to make a couple of points here.
4 The information - and this alludes to how
5 we handle the information from the SRP and put it
6 somewhere in the DSRS or a higher level.
7 So, when you look at 7.0 and 7.1 of the
8 existing SRP, that information got transferred to
9 Section 7.0 of the DSRS. That's where you will see the
10 overall description of I&C, how we do the reviews, the
11 review scope and coordination and all of that
12 information that got transferred from those two sections
13 in the SRP.
14 Then you get into Section 7.2 all the way
15 down to the ISGs. That's how - we took all of that
16 information and we segregated it in 7.1, 7.2 and
17 Appendices A, B and C.
18 I just wanted to make those points and show
19 how we at a higher level, how we took the information
20 from the SRP and put it in the DSRS. And I guess we
21 will have a chance to get into the specific sections
22 right now with Section 7.0, which, like I said, talks
23 about the introduction and overview of the review
24 process.
25 MR. JUNG: Mr. Brown, I think it might be

1 a good time to take a break.

2 CHAIRMAN BROWN: Yes, I was just getting

3 flagged here. I was going to ask where -

4 MR. CONCEPCION: I was supposed to finish

5 this section and then get into the break, but we're -

6 it is 10:15 right now and I will not - I don't know if

7 I'm going to cover it in 15 minutes -

8 CHAIRMAN BROWN: Yes.

9 MR. CONCEPCION: - if you guys want to get

10 into the table.

11 CHAIRMAN BROWN: On the schedule, where are

12 we here?

13 MR. CONCEPCION: We are under Item Number

14 4 right now.

15 CHAIRMAN BROWN: We're just about to start

16 that?

17 MR. CONCEPCION: Yes, sir.

18 CHAIRMAN BROWN: Oh, so we're a half an hour

19 behind? I thought we were ahead.

20 MEMBER BLEY: I did, too.

21 (Laughter.)

22 CHAIRMAN BROWN: Blowing me away.

23 Did you think we were ahead?

24 PARTICIPANT: You're never behind as long

25 as there are 24 hours in a day.

1 CHAIRMAN BROWN: Well, we've gone through
2 24 slides out of 43. So, I mean, you know, I figured
3 we're halfway done.
4 PARTICIPANT: Charlie, stop talking.
5 MR. CONCEPCION: We're going to spend a lot
6 of time on those slides.
7 CHAIRMAN BROWN: I agree.
8 MR. CONCEPCION: I don't have a lot, but
9 there's a lot of discussion.
10 CHAIRMAN BROWN: That's excellent. I like
11 the suggestion. I'm glad everybody is pounding on me,
12 but I've got the hammer.
13 (Laughter.)
14 CHAIRMAN BROWN: So, we will take a break
15 and we will - what's the appropriate terminology here?
16 We pause the meeting?
17 MEMBER STETKAR: Recess.
18 CHAIRMAN BROWN: Recess, thank you. We will
19 recess the meeting for 15 minutes until 10:30.
20 (Whereupon, the proceedings went off the
21 record at 10:15 a.m. for a brief recess and went back
22 on the record at 10:44 a.m.)
23 CHAIRMAN BROWN: The meeting is now back in
24 session. Milt, fire away.
25 MR. CONCEPCION: Okay. Yes, okay.

1 So, we made it to Section 7.0 of the DSRS.
2 This is we established - like I said before the break,
3 we established the differences between the SRP and the
4 DSRS, including the level of scope, objectives, review
5 interfaces and the review process for I&C.
6 And one of the items that was mentioned at
7 the beginning of the meeting was to provide a mapping
8 of how those regulatory requirements in Table 7.1-T of
9 the SRP are addressed in the DSRS.
10 We developed DSRS Table 7-1 that provides
11 such a mapping. I have Section 7.0 here. I have the
12 table. If there is interest by any of the members to
13 go into the details of the table, we can answer questions
14 related to that. If not, I can continue to move on and
15 get into 7.1.
16 MEMBER STETKAR: Two questions.
17 MR. CONCEPCION: Yes, sir.
18 MEMBER STETKAR: Are you going to pull up
19 the whole table or -
20 MR. CONCEPCION: Yes, I can.
21 MEMBER STETKAR: Go to - it's not - I don't
22 know where you have page numbers. It's 5034F219. There
23 you go. It's the next up from the bottom on that slide.
24 MR. CONCEPCION: Displays and monitoring.
25 MEMBER STETKAR: Yes. You talk a lot about,

1 well, the EQ folks are going to take care of
2 environmental qualifications, instrumentation and the
3 digital I&C platforms and cabinets and all that kind
4 of stuff.
5 And that's good, except for the fact that
6 these instruments are supposed to apparently function
7 following core damage, which is far beyond the
8 environmental conditions that those folks look at.
9 So, who's going to look at the environmental
10 conditions for these instruments that have to function
11 in beyond design basis events?
12 MR. CONCEPCION: I don't know if I have an
13 answer to your question specifically, but we are - we're
14 trying to coordinate the reviews of Chapter 3 and
15 environmental qualification with our reviews in Chapter
16 7.
17 Specifically for Reg Guide 1.209 where the
18 process calls for the use of IEEE 323 for mild
19 environmental qualification of I&C equipment, we're
20 trying to strengthen that coordination with Chapter 3
21 folks.
22 And we can get into the details of your
23 question regarding how to address those components that
24 will have to perform beyond, I guess, after core damage
25 beyond design basis. We can get answers to that. I

1 don't have an answer to -

2 MEMBER STETKAR: You're telling me, wait

3 until we get to Chapter 3. So, I'll make a note.

4 CHAIRMAN BROWN: Well, it's not in Chapter

5 7.

6 MR. CONCEPCION: It's not in Chapter 7.

7 MEMBER STETKAR: Well, but this is another

8 issue if it's not in Chapter 7 and the Chapter 3 folks

9 know that they don't know that they need to worry about

10 beyond design basis environmental conditions, then it's

11 going to be no one.

12 MR. SHUAIBI: I don't want to get into a place

13 where we're telling you, see them, and they're tell you,

14 see us.

15 So, do you want us to take that question

16 back and try to get you back an answer -

17 MEMBER STETKAR: Yes.

18 MR. SHUAIBI: I would rather satisfy you

19 rather than -

20 MEMBER STETKAR: Yes, that would help.

21 MR. SHUAIBI: I remember those interactions,

22 and I don't think you appreciated that.

23 MEMBER BLEY: That's right.

24 (Discussion off the record.)

25 MR. CONCEPCION: We're definitely taking the

1 feedback back and then we'll give you a response.

2 MEMBER STETKAR: And if you drop down just

3 to - yes, that's the last one on this page. Failure

4 modes and effects analysis of the integrated control

5 system.

6 I went to 7.2.15, and I could not find a

7 - I could find the need to do a failure mode and effects

8 analysis of the integrated control system in the

9 introduction to that guidance, but I couldn't find any

10 other mention of reviews or what it might entail or -

11 and what I'm curious about is this smells like a post-TMI

12 issue.

13 And a specific function of the B&W plants

14 is they had something called an integrated control

15 system.

16 Now, we don't want to discuss details of

17 the mPower design or what they might call different bits

18 and pieces of their design, but is this specifically

19 focused on what the old B&W designs used to call the

20 integrated control system, or is this supposed to be

21 a failure modes and effects analysis of an integrated

22 protection and control system, which the mPower design

23 has one of?

24 MR. CONCEPCION: Right now the regulation

25 is very specific to B&W plants. And I -

1 MEMBER STETKAR: Old B&W plants.

2 MR. CONCEPCION: And I was going to say old

3 B&W plants. And we have not received any modification

4 from the applicant stating they will take exception to

5 this particular rule.

6 MEMBER STETKAR: My question -

7 MR. CONCEPCION: And I guess that is not your

8 question. Your question is whether the failure modes

9 and effects analysis needs to be applied to the

10 integrated control system.

11 MEMBER STETKAR: To the - I'll call it "Joe."

12 Joe being something that does protection and control

13 functions and exists in this particular design.

14 So, does a failure modes and effects

15 analysis need to be performed for Joe, to avoid specific

16 terminology?

17 And if so, where is the review of - guidance

18 for the review of that FMEA included in the SPRS?

19 MR. CONCEPCION: DSRS.

20 MEMBER STETKAR: Yes, whatever it is.

21 MR. CONCEPCION: First of all, GDC-23

22 addresses failure modes for - addresses failure modes

23 for - what is the terminology? Protection systems, yes.

24 Protection systems. I drew a blank for a second.

25 MEMBER STETKAR: No, Joe minus. It's a

1 subset of this thing.

2 MR. CONCEPCION: So, GDC-23 still applies.

3 Now, we've developed Appendix A which

4 provides the overall system hazard analysis that we

5 expect the applicant to address using whatever technique

6 hazards associated with the system and hopefully come

7 up with measures to prevent those hazards.

8 MEMBER STETKAR: Okay. Maybe we'll talk a

9 little bit more about that when we get to Appendix A.

10 I just want to make sure that the - my basic concern

11 is that because of the way things may or may not be

12 parsed, that people understand one part as being a

13 failure modes and effects analysis perhaps with only

14 the protection functions and they don't need to worry

15 about control functions.

16 This tends to point toward control

17 functions if I go away from the TMI era of B&W plant

18 design integrated control system. But they could say,

19 well, we don't have something that looks like that.

20 So, we don't need to do some FMEA of the control function.

21 As long as the hazard analysis scope in

22 Appendix A includes both protection and control

23 functions, anything that's tied together within that

24 - the scope of the Digital I&C system, then I'm happy.

25 Then people can take exception to this --

1 MR. SANTOS: This is Daniel --

2 MEMBER STETKAR: - all they want. But I'll

3 tell you if you want the guidance even with the

4 constraint of the what's called an integrated control

5 system here, if you want the guidance for your reviewers

6 to address that, it doesn't seem to - it just simply

7 mentions it as something that's thrown into that 7.2.15.

8 Everything else in 7.2.15 talks about other issues.

9 MR. CONCEPCION: We'll look into - it seems

10 to be an inaccurate point or two that the -

11 MEMBER STETKAR: Yes.

12 MR. CONCEPCION: But we'll look into that,

13 yes.

14 MEMBER STETKAR: It is mentioned in the

15 introduction to 7.2.15, but that's as far as it goes.

16 MR. CONCEPCION: Okay. Dan, do you want to

17 add something else, or Sushil?

18 MR. SANTOS: No, we'll wait for the Appendix

19 A discussion. It really covers everything.

20 MR. CONCEPCION: Okay. Anything else

21 regarding this section or the table 7-1?

22 MEMBER STETKAR: This is the only slide on

23 -

24 MR. CONCEPCION: Yes, this is the only slide

25 that addresses that particular section.

1 MEMBER STETKAR: Okay.

2 CHAIRMAN BROWN: This is actually out of the

3 DSRS. You called up the document, didn't you, to get

4 -

5 MR. CONCEPCION: Oh, I'm sorry. This is the

6 DSRS. This is DSRS Section 7.0.

7 CHAIRMAN BROWN: But this was not in your

8 slide or backup slides. This was in as part of the DSRS.

9 This is the table you just called up, right?

10 MR. CONCEPCION: Yes, that is correct.

11 CHAIRMAN BROWN: I have too many pieces of

12 paper here, as you can see. I don't have the one on

13 7.0. Do you want to hold on a second?

14 (Pause in the proceedings.)

15 CHAIRMAN BROWN: You can go on.

16 MR. CONCEPCION: Okay. So, I'm going to

17 switch the view here. Going to get back on the slide.

18 Okay. So, now we get into 7.1, which this

19 is the section on fundamental design principles. And

20 we're going to go into each of these subsections in more

21 detail.

22 So, we're going to talk about system design

23 basis. This is a direct regulatory requirement in

24 Section 4 of 603-1991. We're going to cover as part

25 of the review, the identification of safety functions

1 and corresponding protective actions, monitored
2 variables, minimum number and location of sensors, range
3 of transient and steady-state conditions.
4 And, again, these elements are part of
5 Section 4 of IEEE 603. And We're going to have
6 coordination with Chapter 15 as soon as we get those
7 functions from the accident analysis.
8 So, that is pretty much the essence of 7.1.1
9 and I don't have any more information. I can go and
10 pull 7.1 if we have to get into the specifics of it,
11 but this is pretty much in a nutshell what we're going
12 to be covering for 7.1.1, which is the safety system
13 design basis.
14 CHAIRMAN BROWN: This is kind of an adjunct
15 to a question that I had earlier, a statement I made
16 earlier.
17 You walk through all of the Section 4 items
18 and you do - there's a little paragraph or session in
19 each one of these.
20 The guidance is kind of general and I can't
21 cross this to the existing SRP. I don't know if there
22 just wasn't enough time to go and try to cross this over
23 to equivalent sections. I tried to find one or two and
24 it was very difficult for me to find those.
25 It says that reviewer should verify. I

1 picked one. Section 4.4, identification of variables
2 or monitor, et cetera, et cetera.
3 He should confirm adequate margin exists.
4 Well, what does that mean? I mean, how does he come
5 up with that type of a determination?
6 I don't object to the, I mean, I'm not
7 objecting to the general statement, because I think you
8 highlighted and you provided clarification of what the
9 Section 4 items mean. But what is the - if I looked
10 around, there's not, quote, a set of acceptance
11 criteria. I mean, that's earlier and that's a very
12 general statement.
13 It says there are no specific DSRS
14 acceptance criteria in this section.
15 MR. CONCEPCION: Okay.
16 CHAIRMAN BROWN: Let me finish, okay?
17 MR. CONCEPCION: I'm sorry.
18 CHAIRMAN BROWN: And it just seems like there
19 ought to be some level of guidance to the reviewer of
20 what is meant by acceptable.
21 And I'm not saying it's got to be the words
22 "acceptable," but what are the things you look for?
23 What are the little metrics or what have you?
24 And that seemed to be kind of the story
25 throughout a bunch of the Section 7.1. And it's not

1 just - this was one of them, but there's a number of
2 them. So, there are no - whatever the words were.
3 MR. CONCEPCION: No DSRS-specific
4 acceptance criteria.
5 CHAIRMAN BROWN: Exactly.
6 MR. CONCEPCION: Yes.
7 CHAIRMAN BROWN: And this one is - this is
8 pretty comprehensive relative to formulating in the
9 reviewer's mind what's the overall system design basis
10 that I have to think about and here's the metrics. What
11 does he look for, for each of these?
12 MR. CONCEPCION: Let me try to explain a
13 little bit in terms of the structure and what we adopted
14 as the structure of DSRS.
15 When you get into any particular section,
16 you have your errors of review and then you - I talk
17 about review interfaces and then you get into the
18 acceptance criteria.
19 The acceptance criteria is broken down in
20 two major elements. One of them is the regulatory
21 criteria or those requirements that are codified in our
22 regulations.
23 And then we get - we get this DSRS acceptance
24 criteria and that's where we identified NUREGs,
25 regulatory guides, generic communications, anything

1 that is - anything that surrounds the issue where we
2 have explicit information to capture an acceptable
3 method of satisfying those regulatory requirements.
4 In the case of system design basis in
5 Section 4 of IEEE 603, we don't have a reg guide to
6 address those elements. We clearly go back to the
7 standard and say, the applicant has to provide
8 information to address those 11 or 12 elements that are
9 in Section 4 of the standard.
10 So, the criteria for review is actually
11 contained in those 12 elements in Section 4. That is
12 what we have and that is reflected in the DSRS today.
13 I hear your comment that we can add
14 additional information to guide the reviewer in
15 addressing those 12 elements and we can certainly take
16 that back as feedback.
17 CHAIRMAN BROWN: Okay. I'll just pick
18 another one. Minimum number and location of sensors
19 for variables identified in Section 4.4, the one above,
20 should confirm that the application to analysis
21 demonstrates that the number and location of sensors
22 are adequate.
23 What does "adequate" mean? I mean, I just
24 - I don't disagree with that particular part of it.
25 But when you're a relatively - as you move through and

1 you move from a very senior level set of reviewers that
2 you've had in the past to bringing on - there's a lot
3 of built-in what is adequate and what's not that new
4 people that don't have.
5 And I don't know what's in the existing SRP
6 relative to this. It may be just as blank.
7 MR. CONCEPCION: It's the same information.
8 It is the same information. We did not modify with
9 the exception of some of these elements that were not
10 directly captured in the SRP, that we did add them in
11 this section. The information is a direct extraction
12 from the existing SRP into the DSRS.
13 CHAIRMAN BROWN: So, if I mucked around
14 enough in the existing SRP, I would find this section
15 on -
16 MR. CONCEPCION: I show you right now.
17 CHAIRMAN BROWN: - Section 4.4, Item 4,
18 that that paragraph would be a direct extraction from
19 the existing SRP.
20 MR. CONCEPCION: I can show you any one
21 example. I can show you right now. And, actually, we
22 have tables that show exactly where that information
23 is in the SRP and how we captured it.
24 I can show you any one example.
25 MR. SANTOS: I think it's good to know one,

1 Charlie.

2 CHAIRMAN BROWN: Well, I want to see one just

3 to see what it looks like or - I'd like to see one, if

4 you don't mind.

5 MR. CONCEPCION: Oh, yes. I have one here.

6 CHAIRMAN BROWN: I'd just like to see what

7 that means.

8 MR. SANTOS: Charlie, because we run into

9 this. We stumble a lot, you know, looking at a current

10 guidance and some of the issues with a current guidance.

11 MR. CONCEPCION: I wish I could project this

12 on the screen. I have the DSRS. I don't have the SRP

13 with me. And I have a single file with the entire SRP

14 electronically and I do - it didn't occur to me that

15 we were going to do this.

16 But on Page 7.1-C-4 of the existing SRP,

17 there's a section called System Safety Designation.

18 And it is what - it contains information. These two

19 pages contain pretty much the review guidance for -

20 CHAIRMAN BROWN: NUREG -

21 MR. CONCEPCION: This is 0800, Chapter 7.

22 CHAIRMAN BROWN: What part of Chapter 7?

23 I happen to have the NUREG.

24 MR. CONCEPCION: Okay, 7.1-C.

25 CHAIRMAN BROWN: That's in the introduction.

1 7.1, is that an appendix?

2 MR. CONCEPCION: It is an appendix, yes.

3 CHAIRMAN BROWN: All right.

4 MR. CONCEPCION: Yes, I'm sorry.

5 CHAIRMAN BROWN: Maybe you'll find something

6 else.

7 MR. CONCEPCION: Appendix 7.1-C.

8 CHAIRMAN BROWN: Yes, I've got it.

9 MR. CONCEPCION: In compliance with 603.

10 CHAIRMAN BROWN: Okay, there's 17 pages.

11 MR. CONCEPCION: So, page Number 4.

12 CHAIRMAN BROWN: Page 4. C-4, right?

13 MR. CONCEPCION: Yes. And I'm going to pull

14 the DSRS here so that we can make a direct comparison.

15 (Pause in the proceedings.)

16 (Discussion off the record.)

17 MR. CONCEPCION: Okay. Do you have it on your

18 screen?

19 CHAIRMAN BROWN: Yes, I happen to be looking

20 at part of it.

21 MR. CONCEPCION: Well, I have it here. I

22 can circulate these two pages if any member is

23 interested.

24 So, what you see on the screen is the

25 equivalent of these two pages in the SRP today. So,

1 we have the areas of review and pretty much this section
2 is - the format of 7.1-C is a little different, but -
3 MR. SHUAIBI: Could you give them the tables?
4 I think somebody may want to see the tables.
5 MR. CONCEPCION: They can pass them around
6 if you guys are interested in seeing it, yes.
7 MEMBER BLEY: I can look over Charlie's
8 shoulder.
9 CHAIRMAN BROWN: I'm looking at the Section
10 4 - I see what you're talking about. It looks like,
11 I mean, I'm not working every word for word. You
12 obviously had to change a couple of the words -
13 MR. CONCEPCION: Yes.
14 CHAIRMAN BROWN: - to be compatible with
15 the new document. But the final part says the reviewer
16 should confirm are adequate to ensure completion. And
17 where's the other part? Review adequate margin exists
18 between analytical limits and setpoints. And you've
19 added that it should include adequate margin.
20 So, that looks like that's an added part,
21 which is roughly you extracted and went. So, we're
22 good.
23 MR. CONCEPCION: Okay.
24 CHAIRMAN BROWN: I see what you did from that
25 standpoint and I'll take your word that you did that

1 on the rest of them.

2 MR. CONCEPCION: Thank you so much. It is

3 reflected in some of our documents that we put together.

4 CHAIRMAN BROWN: Okay.

5 MR. CONCEPCION: Okay. Member Stetkar, you

6 had a comment?

7 MEMBER STETKAR: Charlie, are you -

8 CHAIRMAN BROWN: I'm done. Stick a fork in

9 me.

10 MEMBER STETKAR: I had kind of a - well, don't

11 tempt me.

12 I had a broader -

13 CHAIRMAN BROWN: That's fine.

14 MEMBER STETKAR: - question. In the

15 introduction to 7.1, there's a statement that says

16 because the current state-of-the-art and available data

17 are insufficient to support risk-informed digital I&C

18 licensing actions at this time, for the digital I&C

19 guidance developed herein the staff will use a

20 traditional deterministic base review of the mPower IPWR

21 design.

22 And at one level, I understand that. And

23 certainly if I'm looking at the internal structure

24 components, functions internally how the digital I&C

25 system, however that's defined, works, I unfortunately

1 have to kind of agree with you.

2 However, and the reason I wanted you to keep

3 this page up on the screen, if you look at GDC-4 - I'm

4 sorry - GDC-16 and GDC-20, I see words that say,

5 containment design conditions important to safety. And

6 I see words that say, initiate the operation of systems

7 and components important to safety. Doesn't say

8 safety-related. It says important to safety.

9 Now, if this indeed will be a risk-informed

10 licensing submittal, and indeed there's already some

11 guidance being floated around about determination of

12 the SSCs that are important to safety using a

13 risk-informed process, then the interfaces between the

14 digital I&C system, both functional and signal

15 interfaces, are informed by the scope of that, perhaps,

16 not safety-related, but important to safety systems.

17 So, therefore, I'm a bit confused when I'm

18 a reviewer. How do I assure myself that indeed the scope

19 of the functions and signals and interfaces from the

20 digital I&C systems are appropriate for the whole scope

21 of those SSCs that are defined as important to safety

22 within the context of this particular licensing

23 submittal?

24 Are you following what I'm saying?

25 MR. CONCEPCION: Yes, I do.

1 MEMBER STETKAR: So that, you know, within
2 a little box that you can draw around something that's
3 got signals floating around in there and some software,
4 I understand why you have to look at that part of the
5 entire system from a deterministic review standpoint,
6 but I want to make sure that indeed the reviewers of
7 the I&C system are sensitive to the fact that the scope
8 of that system and its functions within the plant of
9 necessity will have some risk-informed basis.
10 MR. CONCEPCION: Okay. And let me try to
11 answer -
12 MEMBER STETKAR: And I didn't see that sense
13 anywhere.
14 MR. CONCEPCION: Yes, and let me try to
15 answer the question.
16 We're looking at essentially
17 safety-related systems and nonsafety-related systems.
18 So, from the Chapter 15 analysis that gets done and
19 those functions are identified and classified, we
20 receive those in Chapter 7 for review.
21 So, the safety-related aspects of this
22 platform will get reviewed against the guidance that
23 we have in 7.1 and 7.2 in the appendices.
24 MEMBER STETKAR: Let me -
25 MR. CONCEPCION: Independent of whether

1 those are - and I shouldn't say "independent." We're
2 looking at Chapter 7 using a deterministic approach,
3 but those functions, the allocation of those functions,
4 the classifications are contained in a different chapter
5 of, in this case, the DSRS.
6 MEMBER STETKAR: Let me ask you - let me try
7 this a different way.
8 You're using the terms safety-related and
9 nonsafety-related. I'm using the terms safety-related
10 important to safety, safety-related not important to
11 safety, nonsafety-related important to safety, and
12 nonsafety-related not important to safety. I'm using
13 those four terms.
14 I'm particularly concerned about things
15 that you're calling nonsafety-related, and I'm calling
16 them nonsafety-related important to safety.
17 Perhaps I'm wrong, but -
18 MR. CONCEPCION: Okay.
19 MEMBER STETKAR: - it was my understanding
20 that the risk-informed review guidance for mPower and
21 the small modular reactors in general, was going to adopt
22 that basic notion of perhaps something isn't
23 safety-related, but it is important to safety. And,
24 therefore, it perhaps would require more intense review
25 than a nonsafety-related not important to safety system,

1 SSC.

2 I believe that is the way I remember the

3 general review guidance being structured.

4 MR. CONCEPCION: But Chapter 7 -

5 MEMBER STETKAR: Not Chapter 7. I'm talking

6 about -

7 MR. CONCEPCION: Okay.

8 MEMBER STETKAR: - the entire review of the

9 design.

10 MR. CONCEPCION: Okay.

11 MEMBER STETKAR: Don't knock me into the

12 hole. I'm going to try to keep you out of the hole.

13 MR. CONCEPCION: Okay. Understand.

14 MEMBER STETKAR: So, my question is, if, for

15 example, and instead of using Joe again, I'll use Mary,

16 if, indeed, the risk-informed process determines that

17 there is a co-called nonsafety-related system called

18 "Mary" out there that is important to safety, and that

19 it's important that Mary gets actuated for control or

20 isolated or whatever to perform its important-to-safety

21 function, how does that relate to your review of the

22 signals that tell Mary to start or stop or isolate?

23 Because this says, initiate the operation of systems

24 and components important to safety.

25 Doesn't say safety-related. It doesn't

1 say the things that are only analyzed in the particular
2 deterministic design basis accidents in Chapter 15.
3 It says, important to safety.
4 MR. JUNG: Let me answer. There are two
5 parts I see. One, overall risk-informed approach that
6 was mentioned in this introduction, I don't want to go
7 into that particular approach because Chapter 7 - many
8 of the design aspects of our review, a particular
9 approach is not necessarily applicable. In Chapter 7,
10 we are making clear for that.
11 Now, John, I think, Mr. Stetkar, your
12 comments is more about how about the containment system?
13 Looking at it, they found some aspects of it that are
14 traditionally nonsafety-related, but maybe it's
15 important to safety.
16 I'm going to answer in two parts. One is
17 because the importance to safety - nonsafety-related,
18 but important to safety, has been a very important topic
19 to us.
20 So, currently from a Chapter 7 perspective,
21 there are, in fact, areas that are nonsafety-related,
22 important to safety. We are looking at that.
23 The backup system is one of them, and
24 annunciators, and there are other aspects. And in
25 addition, the current - as you know, the Chapter 19 PRA

1 requirements are there. So, actually, we worked with
2 the Chapter 19. I'm not sure you've seen Chapter 19.0.
3 It's been updated. It has extensive, actually,
4 discussion of coordination with the I&C, digital I&C
5 with some - understanding the basis and how Chapter 7
6 reviews are done along with the risk assessment and
7 quality of digital I&C systems extensively discussed.
8 I have a copy of it here.
9 But in terms of the other systems that are
10 being reviewed by other disciplines that - and those
11 situations has come up, I think it's a coordination
12 issue. We can take that back as something that we are
13 to highlight potentially.
14 Because right now there are - many, many
15 systems are out there. Especially nonsafety systems
16 are a lot more extensive. Especially for mPower designs
17 we expect that.
18 So, those systems that are being identified
19 as part of risk-informed approach that are being
20 discussed as part of the SECY response, those systems
21 that are being - I didn't apply those important to
22 safety, but other systems will have to coordinate with
23 them and need to somehow communicate with those
24 branches.
25 MEMBER STETKAR: Ian, that's exactly - I'm

1 glad you restated it that way. That's exactly my
2 concern, because I didn't see in the DSRS anywhere that
3 particular focus on coordination.
4 You know, whether it's in the table in 7.0
5 or in, you know, test guidance somewhere, that need for
6 looking at things that are perhaps outside the
7 traditional scope of the Chapter 15 analyses - there
8 are a lot of references to the Chapter 15 analyses and
9 the cross-talk there, but not the direction that we've
10 just been discussing in terms of -
11 MR. JUNG: Mr. Stetkar, I would go even
12 further. Those aspects that we are talking about, it
13 may not just be in the I&C. It could be other aspects.
14 So, it's a generic -
15 MEMBER STETKAR: Absolutely.
16 MR. JUNG: Right.
17 MEMBER STETKAR: That's one of the reasons
18 why I wanted to kind of back it out from just -
19 MR. JUNG: I understand.
20 MEMBER STETKAR: - the box of Chapter 7.
21 Because I'll agree with you that within however you
22 draw the lines around that box, you have no feasible
23 way of doing a risk-informed review of, you know, a
24 particular containment protection signal, how it's
25 processed within the digital I&C versus a, you know,

1 an injection actuation signal or something like that.
2 There's not enough basis for that within
3 the system itself.
4 MR. JUNG: Thank you for the comment. We'll
5 work with Joelle's group and see how it can improve as
6 a whole package.
7 CHAIRMAN BROWN: I'm sorry, go ahead,
8 Dennis.
9 MEMBER BLEY: I was just from where Mr.
10 Stetkar started out, was there an intent? And I think
11 this is what you said, and I think it's what I remember,
12 that these - this guidance you are preparing would
13 actually incorporate the ideas of 50.69 and without
14 having to refer to those externally. That's kind of
15 where you started.
16 MEMBER STETKAR: I believe at least on what
17 we've seen on the guidance for reviews of systems, that
18 that's the intent of the design-specific review.
19 MEMBER BLEY: And if that is the intent, this
20 idea Ian talked through of having - at least getting
21 the idea of the coordination across really important.
22 That's the only way it could work.
23 MEMBER STETKAR: That's right. I mean, I
24 think, I believe, I lose track of the guidance that we've
25 seen and what discussions we've had, but I seem to recall

1 that they were saying, well, from a risk-informed review
2 basis, a good starting point is to look at the hierarchy
3 of systems and organize the resources that will be
4 applied to the system on that risk-informed basis, you
5 know, without saying 50.69, basically.
6 But if you're going to do that, then it ought
7 to filter into the rest of the review.
8 MS. STAREFOS: Yes, I - thank you. Joelle
9 Starefos.
10 I would be hesitant to apply that 50.69.
11 We would try to weave that throughout this. In fact,
12 that's a big sensitivity we've had with some of our
13 stakeholders on whether or not that was the appearance.
14 Because as we talk about things, there's
15 only so many ways you can bin safety and nonsafety and
16 risk and nonrisk when you start breaking it down and
17 it looks a lot like 50.69, but it wasn't exactly -
18 MEMBER STETKAR: If it's not, then what do
19 these words mean right here?
20 MS. STAREFOS: Well, I think important to
21 safety - the important to safety, those are the GDC
22 words. Those have been part of our GDC for a long time,
23 and that has been something that's been a particular
24 challenge for us because of the interpretation of the
25 GDC -

1 MEMBER BLEY: The interpretation of that has
2 kind of evolved -
3 MS. STAREFOS: Yes.
4 MEMBER BLEY: And the most recent evolution
5 I kind of thought was 50.69 - no.
6 MS. STAREFOS: No, I don't think that's
7 exactly how we would interpret it.
8 MR. SHUAIBI: I think 50.69 defined its own
9 terms for how to bin things. Important to safety,
10 safety-related, nonsafety-related, those have been in
11 the books for a long, long time.
12 In fact, maybe what we could do is find you
13 memos that try to clarify to staff and the industry in
14 terms of what important to safety means, but you're
15 right. I don't think there's a definition in the books
16 that says here's what important to safety means, but
17 those have been there long before 50.69
18 MEMBER STETKAR: And you're going to have
19 to help me here. Isn't it true that within the whole
20 scope of the mPower review guidance, guidance, I think,
21 is being developed at least in the systems area to say
22 that you'll allocate resources, you know, the level of
23 detail and the depth of review that you perform will
24 be informed by - I don't know whether the words important
25 to safety or risk significance or what particular words

1 are used, but the notion is that there will be some type
2 of hierarchy.
3 MS. STAREFOS: Yes, that is correct.
4 MEMBER STETKAR: And I, for the lack of
5 knowing what those particular words are, let's call it
6 a hierarchy right now. And at some point, the reviews
7 will have less effort applied to them.
8 I don't want to imply that no, you know,
9 certainly the systems will be reviewed, but they'll
10 receive kind of a traditional nonsafety-related systems
11 review.
12 My only point is if that's indeed the
13 structure that's going to be used for the systems reviews
14 however that hierarchy is defined, if something falls
15 in the upper tier of that hierarchy for whatever reason,
16 then if that's important enough to merit a more detailed
17 review on that basis, it would seem that those systems,
18 those functions would be important enough to also merit
19 careful attention on how they interface with digital
20 I&C, electric power and, you know, you're right. It's
21 an overarching type of issue for the whole review, not
22 just within the context of individual systems.
23 MS. STAREFOS: I think these are some - and
24 don't let me overstep my I&C guys, but these are some
25 of the issues that I anticipated we would - we would

1 evolve as we started our first implementation of this.
2 In the sense of it being a pilot, these are
3 the important aspects that we're going to have to kind
4 of figure out depending upon what the answer is that
5 we get with the application. And the appropriate level
6 of review certainly if it's safety-related, it gets the
7 thorough level.
8 And I've always been under the
9 understanding that our I&C folks wrote this to a level
10 that all of our safety stuff is going to get this thorough
11 look.
12 Important to safety with the GDC, I would
13 imagine some of those pieces would slide up into that
14 safety and get that equivalent safety review.
15 And in very, you know, very rare cases, we
16 might find that the risk assessment of a system is
17 nonsafety. Maybe the risk significance of it didn't
18 rise to the level where we would give it that thorough
19 safety review. And that would be a one-by-one
20 evaluation done at that level and the decision would
21 be made in a case-by-case basis.
22 So, I think some of us will see, and I don't
23 want to push this forward and imply that, yes, we'll
24 have all the answers when we're doing the review, but
25 I think some of this will be more apparent at that point.

1 And I think what I understood from my I&C
2 counterparts were - was that the intent here is to focus
3 on safety and do it all at this thorough level and bump
4 those pieces up into it as opposed to losing them and
5 doing a lesser review in this case.
6 Now, please, Ian, Milton, if I've
7 overstepped -
8 MR. JUNG: No, that's correct.
9 MS. STAREFOS: Okay.
10 MEMBER STETKAR: I think something that Ian
11 said sort of hit it, is I don't think we have all of
12 the answers and I think you're right that we need to
13 work through this process to really understand how it's
14 going to work.
15 My only concern, I think, that if this
16 guidance included those hooks, those references to other
17 disciplines that define that hierarchy, I'll call it
18 that, to alert the folks doing the digital I&C review
19 that they need to go out and look for those other things
20 that are perhaps in the gray area between the
21 deterministic Chapter 15 analysis strict safety-related
22 and the nonsafety stuff, would at least satisfy it at
23 this level.
24 Because as it stands right now, it says
25 safety-related, we're going to look at it very

carefully. Safety-related is determined by the Chapter 15 analyses. And we have to make sure that all of this is separated from all of that nasty nonsafety-related stuff.

MS. STAREFOS: Right.

MEMBER STETKAR: And we don't look at the nonsafety-related stuff in here.

MS. STAREFOS: There is another piece that -

MEMBER STETKAR: Except for those interface - except for the interfaces.

MS. STAREFOS: Yes, there is another piece that unfortunately hasn't been made public for consumption at this stage, but the introduction to the Standard Review Plan was rewritten with the intent of incorporating the SECY-11-024 guidance.

And we've been doing a lot of work to try to figure out what that looks like in incorporating these four pieces. And that's one of the reasons I said I'm hesitate to call it 50.69, because we've kind of written this other guidance.

Certainly, that's something that you're going to have an opportunity to take a look at and it really makes this picture complete. Because it tells the reviewer at the very beginning, you have two choices

1 here - or, well, not you have two choices, but there
2 are a couple of choices.
3 Part 1 of the introduction is a traditional
4 SRP review. Part 2 is this approach that we've taken
5 to develop the DSRSes and how that incorporation of risk
6 is going to be done fundamentally.
7 And those reviewers have been trying to
8 consider that as that guidance evolves while they're
9 developing these DSRSes.
10 The guidance generally talks about those
11 four categories that we've discussed, but it also gives
12 them a process path on how to move through and determine
13 whether or not something needs certain levels of review.
14 For example, programmatic types of items
15 the review would be different and we wouldn't
16 necessarily apply that risk information. We would
17 still want the thorough review from the program level
18 of the entire program.
19 So, that piece is unfortunately not on the
20 table for you to see. And I'm hoping that that will
21 clarify both this discussion, as well as some of our
22 external stakeholders' concerns or lack of
23 understanding of that aspect of it.
24 Right now - I'm sorry.
25 MEMBER BLEY: We saw a draft about a year

1 or so ago, I think.

2 CHAIRMAN BROWN: Chapter 1?

3 MEMBER BLEY: Yes.

4 MS. STAREFOS: Right.

5 MEMBER BLEY: So, it's evolved quite a bit

6 since then.

7 MS. STAREFOS: I think it's evolved a little

8 bit more than that.

9 MEMBER BLEY: Okay.

10 MS. STAREFOS: And, in fact, I think it's

11 with our -

12 MEMBER BLEY: That would help.

13 MS. STAREFOS: I think it's with our counsel.

14 We anticipated having it out later this year.

15 So, I'm not sure what schedule that's on.

16 That's not within the scope of what I'm working on,

17 but it's my understanding that they've been working very

18 hard and diligently to get that out especially because

19 we are, we would say, imminent on getting the DSRS out

20 for mPower.

21 It's a critical piece for that

22 understanding and evaluation.

23 (Discussion off the record.)

24 CHAIRMAN BROWN: Should we go on? Okay,

25 Milton.

1 MR. CONCEPCION: Yes.

2 CHAIRMAN BROWN: Slide 28? Were you

3 finished with 27?

4 MR. CONCEPCION: Let me get back to the

5 slides, because I don't know where I'm at.

6 CHAIRMAN BROWN: 27.

7 MR. CONCEPCION: Okay, yes.

8 So, any additional questions or feedback

9 regarding design basis at this point? If not, I'm going

10 to move on to 7.1.2, which is independence.

11 I'm on Slide 28 right now. So, this is

12 Section 5.6 of IEEE 603. The review will cover four

13 major areas. Namely, physical independence,

14 electrical independence, communications independence

15 and functional independence.

16 There was an earlier comment by Member

17 Stetkar regarding the review of physical and electrical

18 independence and the coordination with Chapter 8. We

19 captured that.

20 Okay. So, we are - this is Slide 29,

21 communication independence. This is where we have that

22 statement of one-way communication should be used among

23 redundant channels. We're going to look into that

24 sentence and see a way to reword it.

25 This is where we also discussed data flows

1 between redundant portions of the safety system. We
2 discussed whether the safety division should not depend
3 on information or resources originating from other
4 divisions to accomplish safety function.
5 Divisions should have their own sensors,
6 are dedicated to the division and that kind of guidance.
7 There is another slide that talks about
8 functional independence. On Slide 30, this is where
9 we verify isolation of a safety system function from
10 other safety systems, and verify that there's no
11 unwanted behavior from other system influencing,
12 basically, inner system interference.
13 So, any questions regarding 7.1.2?
14 CHAIRMAN BROWN: Just one observation. You
15 can do with this what you want. You walked about
16 repetitiveness and stuff you're trying to eliminate.
17 And if you walk through almost everything
18 after Section 7.0 when you talk about DSRS acceptance
19 criteria, there's a caveat statement in every one of
20 them; 7.1.1, .2, .3, .4, .5, 7.2.1, on and on and on.
21 MS. STAREFOS: Yes, sir.
22 CHAIRMAN BROWN: That one caveat would have
23 fit very well, which says you don't have to follow any
24 of the regulations or guidelines as long as you can
25 justify doing something that we don't like.

1 So, it would fit very well one time on Page
2 7.0-6 under DSRS Chapter 7, Acceptance Criteria and
3 Review Process.
4 So, do with that what you want to.
5 MS. STAREFOS: Yes, sir.
6 CHAIRMAN BROWN: It's just taking up space
7 and the rest of -
8 MEMBER BLEY: It's annoying after a while.
9 CHAIRMAN BROWN: Yes, very annoying to read
10 through that every time.
11 MR. CONCEPCION: This is the section on DSRS
12 acceptance criteria. That paragraph, right? That's
13 what you're talking about?
14 CHAIRMAN BROWN: Yes, it's the paragraph
15 right on Page 7.0-6. It covers - and that little
16 statement of exceptions and the fact that you don't have
17 to follow anything we say would fit - I have to say it
18 that way very pejoratively.
19 MS. STAREFOS: You know, I would venture to
20 say you're absolutely right. And the guys have been
21 on me for a long time about this.
22 The intent of the repetitive nature was to
23 ensure that if a reviewer picked up one section and was
24 assigned one subsection to do, they wouldn't need to
25 necessarily go back and try to find those kinds of

1 directions and pieces throughout.

2 And so, we've done this throughout the whole

3 DSRS and it's - trust me if I tell you just keeping that

4 coordinated in the right version and every place is a

5 lot of work for us.

6 The intent is to ensure that the reviewers

7 have everything they need in that one place if that's

8 all they're assigned to. So, I understand for someone

9 looking at it, it's very repetitive.

10 We can rethink that. But, again, it -

11 CHAIRMAN BROWN: 7.0, your introduction and

12 overview of review process, it's very pointed as to what

13 that is.

14 MS. STAREFOS: Yes, sir.

15 CHAIRMAN BROWN: And if somebody is good at

16 doing something else and haven't read that, then you

17 probably shouldn't have them reviewing the other

18 section. That's the point I'm talking about.

19 MS. STAREFOS: Thank you for the comment.

20 CHAIRMAN BROWN: It's just an observation.

21 MS. STAREFOS: No, it's a good comment.

22 Thank you.

23 CHAIRMAN BROWN: Excuse me for that small

24 departure.

25 (Discussion off the record.)

1 MEMBER STETKAR: Milton, can you just pull
2 up the section of the DSRS?
3 MR. CONCEPCION: Yes.
4 MEMBER STETKAR: And scroll down to, I guess,
5 what's Page 10. Keep going. There's a long list of
6 things under -
7 MR. CONCEPCION: Which section? 7.1.2?
8 MEMBER STETKAR: 7.1.2 under communications
9 independence.
10 MR. CONCEPCION: Yes, sir, here we are.
11 MEMBER STETKAR: There you go. Number 4.
12 Functions that are not necessary for safety even if
13 they enhance reliability, should be executed outside
14 the safety system.
15 What does that mean and what are you - what
16 is the notion of reliability in this particular context?
17 MR. CONCEPCION: What is the relationship
18 with reliability?
19 MEMBER STETKAR: Yes. I mean, this says -
20 I'm trying to understand what this means in practice.
21 MR. CONCEPCION: In practice, what it means
22 is that we're trying to have the divisions perform their
23 own safety functions without influence from any other
24 division.
25 MEMBER STETKAR: Yes.

1 MR. CONCEPCION: That is, in essence, what
2 we are trying to do with this particular element in this
3 section.
4 MEMBER STETKAR: I understand that basic
5 notion. What I'm not understanding is that something
6 if it's not necessary for safety, but it enhances
7 reliability, enhances reliability of what? Enhances
8 reliability of performing the safety function?
9 Enhances reliability of what?
10 MR. CONCEPCION: In this context - I'm going
11 to take a shot at it. In this context, it should enhance
12 the reliability of the system.
13 MEMBER STETKAR: Well, but if something
14 enhances the reliability of the system -
15 MR. CONCEPCION: Yes.
16 MEMBER STETKAR: - which because I'm a
17 numbers kind of guy, makes it 0.999 reliable instead
18 of 0.99, why isn't that a good thing to have and why
19 shouldn't it be within the context of my safety system?
20 MR. SANTOS: Dan Santos. We're not going
21 to argue with that reliability. It's not a good thing
22 to have.
23 The issue is that this is very subjective
24 area when it comes especially to software and digital
25 communication systems.

1 We feel that the tradeoff between increased
2 reliability versus the protection against unknown
3 errors and for variations of those errors, we want to
4 make the point towards the conservative part of
5 simplicity, okay. Because to date, no applicant has
6 been able to make a sound reliability improvement case.
7 It's the tradeoff of the claim of
8 reliability versus the ability to protect against
9 unknown -
10 MEMBER STETKAR: So, if I had a system that
11 had a knife switch that was operated by somebody who
12 didn't have any hands in one channel, and a - let's see.
13 I don't know. Something else. Some other type of
14 thing that's operated by an automatic system that has
15 a failure rate of 0.5. Because they are diverse and
16 they are completely separated, that is an adequate
17 design even though it's almost guaranteed to fail a fifth
18 of the time.
19 MEMBER SIEBER: Well, about a quarter of the
20 time.
21 MEMBER STETKAR: I mean, that's what I hear.
22 It's ludicrous, but that's what I hear you saying is
23 that you've ignored the concepts of reliability because
24 you need something that by definition, something that
25 is completely separated is adequate even though it's

1 not very reliable.

2 MR. JUNG: Mr. Stetkar, let's - I'll bring

3 up the safety system when design basis analysis and it's

4 performed to demonstrate what safety functions are

5 required to be performed and those SSCs that are relied

6 upon to perform those functions, many of the

7 regulations, because it's in the regulations, including

8 GDC-21 and some aspects that talks about reliability,

9 reliability of those systems that are relied upon has

10 to be, you know, highest quality, it is a very

11 safety-critical aspect.

12 So, safety system already are required to

13 demonstrate high-quality systems, right? So, what we

14 are - using the example we are talking about is, goes

15 in some experience have shown that certain vendors would

16 introduce a nonsafety system functionality that beyond

17 what's required for safety function are introduced with

18 the claim that it increases the reliability.

19 Because this feature would allow early

20 detection of something, the parameter changing because

21 the nonsafety system has other functionalities using

22 the data that's been coming from safety analyze and all

23 that.

24 In some cases, their basis for that

25 argument, that benefit of reliability versus the

1 potential hazards that are introduced by having the
2 connection from nonsafety/safety, that argument
3 couldn't be - the basis wasn't sufficient enough in most
4 of the cases because of the complex nature of the digital
5 systems.
6 So, we are generally discouraging that
7 argument to be used in those regards.
8 MR. SANTOS: This is a direct reflection from
9 the experience of reviews. But if it will avoid
10 confusion, we could delete even if they enhance
11 reliability and maintain the essence of the sentence,
12 which is functions that are not necessary for safety
13 should be executed.
14 MEMBER STETKAR: That would held me a lot.
15 MR. SANTOS: I understand.
16 MEMBER STETKAR: Because my fallback, I
17 think I know, you know, from experience, I know what
18 you're talking about ludicrous examples aside. But I
19 was also in terms of reliability, also think in terms
20 of reliability of the operators.
21 So, for example, information that might be
22 transmitted from the safety-related system to the
23 operators could also be part of the context of this sort
24 of generic sense of enhanced reliability.
25 MR. SANTOS: I understand.

1 MEMBER STETKAR: It's just that little
2 phrase left me very confused.
3 MR. SANTOS: Yes, we can delete that phrase
4 without losing what we really want. It was just an
5 explanation of the type of -
6 MR. JUNG: Experience we were having.
7 MEMBER BLEY: I think your point is you were
8 getting claims of reliability that you didn't believe
9 either because of uncertainty or because of unintended
10 consequences of this thing. And if you could somehow
11 get that sense in here, it would be good.
12 The language goes too far the other way to
13 ignore reliability, which of course you don't want to
14 do.
15 MEMBER STETKAR: Yes, that's true. That is
16 correct.
17 MR. JUNG: Thanks for comment. Only just
18 observation this particular criteria is exact quote from
19 the ISG-4. So, we just have to work with NRR to make
20 sure it is consistent.
21 (Discussion off the record.)
22 MR. CONCEPCION: I guess we have another
23 comment from staff.
24 MR. NGYUEN: This is Khoi Nguyen, I&C 2
25 branch.

1 I would like to share with you an example
2 on that particular sentence that in the past we have
3 seen some of the design that claim to enhance the
4 reliability for the data communication system.
5 They introduced the diagnostic test from
6 the nonsafety system. That's what we want to make a
7 point here. We don't want any design that claim to
8 enhance the reliability that interface with the safety
9 system from the nonsafety side.
10 That's what the point that we wanted to
11 make. That's all I -
12 MEMBER STETKAR: Yes, I know. I understand
13 that basic concept, certainly.
14 MR. CONCEPCION: I guess he took it through
15 a different level used with the word "enhanced
16 reliability." And that was never the intent of staff,
17 yes.
18 MEMBER STETKAR: Can we in the interest of
19 time, thanks, scroll up to Number 8?
20 CHAIRMAN BROWN: Don't worry. I'm going to
21 finish after you finish.
22 MEMBER STETKAR: I figured as long as I can
23 get my ranting in before you start, I'll do -
24 CHAIRMAN BROWN: Keep going before I start.
25 Thank you.

1 MEMBER STETKAR: I choose my words
2 carefully, actually.
3 It says, safety commands should have
4 highest priority and should override all other commands.
5 "All" is a big word.
6 Is the intent of this that safety commands
7 should override equipment protection signals?
8 MR. CONCEPCION: No.
9 MEMBER STETKAR: Ah.
10 MR. CONCEPCION: In the use of priority
11 modules, the intent is to make sure that those priority
12 modules prioritize those safety functions that need to
13 take place, and not focus on those other functions that
14 are not necessarily safety-related.
15 MEMBER STETKAR: That, I understand. But
16 should override all other commands implies -
17 MR. SANTOS: I think a better word would be
18 -
19 MEMBER STETKAR: For example, if I'm an
20 inexperienced reviewer without the benefit of the last
21 30 seconds and I see a design that comes in and it says,
22 oh, a pump trip signal because it has no cooling, will
23 block the pump from starting and that is not an
24 acceptable design because it doesn't meet this, I'm
25 going to ask a question about that.

1 MR. SANTOS: Better than safety commands
2 safe-state is what we're really looking for.
3 MEMBER STETKAR: It's just "all" is a big
4 word.
5 MR. SANTOS: Yes.
6 MR. CONCEPCION: No, we're going to look into
7 that. Appreciate it. Thank you.
8 MEMBER STETKAR: Thanks. Because I found
9 it in two or three other places also that has this notion
10 that -
11 MR. CONCEPCION: We're going to look into
12 that.
13 MEMBER STETKAR: I can start something to
14 discussion.
15 MR. CONCEPCION: We can use better words to
16 describe what we intent with that.
17 MEMBER STETKAR: Just trying to think about
18 it the way a reviewer might interpret this without the
19 benefit of the knowledge of -
20 MR. SANTOS: And we'll have to also
21 coordinate it with ISG-04, because a lot of this language
22 is already current guidance. So, comment taken.
23 MEMBER STETKAR: Okay, thanks. I'm done.
24 CHAIRMAN BROWN: Okay. Go back to Page 11.
25 Right there. Now, scroll up. Nope, scroll down. I'm

1 sorry. Stop. Let me see where this is.

2 Okay. The sentence that starts right at

3 the second paragraph, the reviewer shall also confirm

4 - this is data communications - conforms to the guidance,

5 to the separation and isolation of data processing

6 functions of interconnected contained in IEEE standard

7 7-4.3.2. Clause 5.6 as endorsed by Reg Guide 1.52.

8 Consider the following.

9 The problem that I - I guess I don't

10 understand this. Annex E is not endorsed in - at least

11 it was not at the time we did the revision to Reg Guide

12 1.152. Only Annex A was endorsed at that time. B

13 through F were not.

14 Annex E is used for - it defines - if you

15 go read 7-4, it shows here's what defines communication

16 independence, which is just a travesty. It's the worst

17 definition.

18 I mean, there are little pictures which are

19 barely comprehensible and are meaningless relative to

20 data communication. That's my own personal opinion.

21 Just meaningless. That's point one.

22 So, the statement that we've got to go back

23 and meet this thing as endorsed, I think that's - somehow

24 that's got to be fixed. That is incorrect right now.

25 MR. CONCEPCION: Okay. We will -

1 CHAIRMAN BROWN: I'm not quite finished.
2 Let me finish the last point, and then you can blow me
3 up - no, excuse me. You can tell me why I'm wrong in
4 a more, you know, polite manner than I use normally.
5 It also talks about barriers in 5.6.
6 MR. CONCEPCION: 5.6 of?
7 CHAIRMAN BROWN: 7-4.3.2.
8 MR. CONCEPCION: Yes, okay.
9 CHAIRMAN BROWN: Barrier requirements shall
10 be identified to provide adequate confidence that the
11 nonsafety functions cannot interfere with the
12 performance of safety functions.
13 The barrier shall be designed in accordance
14 with requirements of the standard, but nonsafety system
15 hardware is not required to meet the nonsafety system
16 - nonsafety software is not required to meet these
17 requirements.
18 And then it says, if barriers between safety
19 software and nonsafety software are not implemented,
20 the nonsafety software shall be developed in accordance
21 with requirements of this standard.
22 It's circular. I couldn't figure out where
23 you were going with this stuff.
24 MR. CONCEPCION: Yes.
25 CHAIRMAN BROWN: And then it goes on to say

1 guidance for established communication independence
2 provided in Annex E, which is not endorsed.
3 MR. CONCEPCION: Yes. Okay, I'll let you
4 finish.
5 CHAIRMAN BROWN: I'm finished.
6 MR. CONCEPCION: Okay. So, when you look
7 at that sentence, the sentence points you to 5.6 of
8 7-4.3.2, right?
9 So, the section on the standard has to be
10 used in accordance with the information in the Reg Guide
11 which endorse the standard.
12 So, off the bat, Appendix E does not apply.
13 CHAIRMAN BROWN: It does not -
14 MR. CONCEPCION: Let me finish.
15 When we look at the Reg Guide, the Reg Guide
16 says, Appendix E does not apply or it was not considered
17 for endorsement. Let me just say it that way.
18 CHAIRMAN BROWN: So, it's a downstream
19 disavowal -
20 MEMBER BLEY: As endorsed by -
21 CHAIRMAN BROWN: Okay, okay. I got that.
22 MR. CONCEPCION: Okay.
23 CHAIRMAN BROWN: Are you finished telling
24 me -
25 MR. CONCEPCION: Well, the information -

1 maybe I'm going to repeat myself, but what the sentence
2 says is basically 5.6 will be used. And you use the
3 Reg Guide to bound the information, because it is an
4 endorsed standard. So, Appendix E is not in the scope
5 of review.
6 There are elements associated with
7 communication independence in 5.6 that do apply and we
8 use those elements.
9 CHAIRMAN BROWN: Now, I will address that
10 comment.
11 In addition to the requirements of IEEE
12 Standard 603-1998, data communications between safety
13 channels or between safety and nonsafety shall not
14 inhibit the performance of the safety function.
15 That is a grandiose statement. I have no
16 doubt that is a very high-level and it provides
17 absolutely no enlightenment at all of what it means to
18 not inhibit the performance.
19 I just - I have not liked - if you haven't
20 gotten it yet, I haven't liked 7-4.3.2 since it was first
21 published in 1993.
22 MR. SANTOS: And that's why we expand it on
23 the DSRS.
24 CHAIRMAN BROWN: Yes, I agree with that, but
25 it says you should consider the following, okay. And

1 it's -

2 MR. CONCEPCION: That is our guidance. That

3 is what we tell -

4 CHAIRMAN BROWN: Okay, I'll go with that.

5 I'm just aggravated with looking at this thing, that's

6 all.

7 I'll make one other point, and then we can

8 go on. When you get down into Section 2.2, the safety

9 division shall not be dependent, if you'll scroll up

10 a little bit.

11 MR. CONCEPCION: Number 2?

12 CHAIRMAN BROWN: Yes, just scroll up so the

13 whole - A and B and C are shown. I don't have any problem

14 with this, except it addresses what appears to be reactor

15 trip-type functions.

16 Like in B it says, "and a reactor trip shall

17 result if everything locks up. An alarm should be -

18 an alarm should be initiated," which is fine.

19 But engineered safeguard systems also are

20 subject to the same problem of lockup. And there, you

21 fail as-is. If they lock up, they don't perform a

22 function. They don't do anything.

23 And yet, there's no - there's nothing that

24 clearly says that those functions, that particular

25 safety function should at least alert, provide an alarm.

1 And maybe I've misread it somewhere in here. It just
2 was - it didn't stand out to me that all those would
3 be communicated.
4 Only A led this and the emphasis on reactor
5 trip. For some reason to me, you ought to have
6 safeguards and functions at least highlighted somehow
7 in this discussion as to what happens since they are
8 fail as-is-type functions as opposed to trip functions.
9 That's the only point.
10 MR. CONCEPCION: It was to cover both, but
11 we're going to add additional language to make sure that
12 it is clearly reflected in that section.
13 CHAIRMAN BROWN: That's all. I mean, that's
14 just trying to make it clear.
15 MR. CONCEPCION: By the way, this is direct
16 feedback from this committee where we collected input.
17 You provided this feedback and we incorporated it into
18 this.
19 CHAIRMAN BROWN: Oh, no, I know you all -
20 I provided this information to you. You did quite well.
21 It's just that I'm not saying that I caught everything
22 at that time.
23 MR. CONCEPCION: Anything else you want to
24 add?
25 CHAIRMAN BROWN: Until I saw what you wrote,

1 it wasn't clear that, I mean, how you did it.

2 MR. CONCEPCION: Yes, we were trying to -

3 CHAIRMAN BROWN: You did a good job of taking

4 my thoughts and cranking them in. I'm not objecting

5 to that.

6 MR. SANTOS: We agree with that comment.

7 MR. CONCEPCION: Yes, absolutely. Okay.

8 Any additional comments or thoughts regarding

9 independence?

10 CHAIRMAN BROWN: I can go on and on, but I

11 won't.

12 MR. CONCEPCION: Okay, moving on.

13 Redundancy, okay. This is Section 5.1 of

14 IEEE 603. We talk about single failure, we talk about

15 removal from service of components or channels and how

16 that should not result in a loss of required minimum

17 redundancy.

18 We have guidance for reviewing channel

19 assignments to address redundancy and diversity

20 requirements. And it is all based on Reg Guide 1.53,

21 which endorses IEEE 379.

22 This section is a true reflection of what's

23 in the SRP today.

24 CHAIRMAN BROWN: I think I made an earlier

25 comment on that relative to single failure being the

1 only ones. I'm not going to be repetitive with that.
2 MR. CONCEPCION: Okay.
3 CHAIRMAN BROWN: I just think we need to
4 provide a little bit more flesh on that one.
5 MR. CONCEPCION: Yes.
6 CHAIRMAN BROWN: Okay?
7 MR. CONCEPCION: We've got that, yes.
8 Okay, determinism. I think this is the
9 only slide on determinism. We talk about system timing.
10 We talk about confirm deterministic performance of data
11 communications. And we intend to use Appendix B to
12 support the review of determinism.
13 CHAIRMAN BROWN: Two observations on this.
14 MR. CONCEPCION: Yes, sir.
15 CHAIRMAN BROWN: I've made the one about
16 there's no acceptance criteria. And you explained how
17 since there is not - you can only quote the rules.
18 MR. CONCEPCION: For determinism?
19 CHAIRMAN BROWN: Well, yes. It says right
20 here there are no specific DSRS acceptance criteria in
21 this section.
22 MR. CONCEPCION: Correct. Yes, correct.
23 There is no regulatory guidance or NUREGs or any other
24 surrounding document to support the review of
25 determinism aside from BTP 7-21, which was rolled into

1 this section as well.

2 CHAIRMAN BROWN: Yes. Again, you address

3 some of the stuff that should be considered as acceptance

4 criteria in Items 1 through 10 on the next page - on

5 the next two pages.

6 I guess my only point on this one because

7 there is not a, quote, regulatory basis or real-base

8 basis, however you phrase it, I probably didn't say that

9 right again, that almost makes it sound like these are

10 just - well, you ought to think about these, but they're

11 really not necessary to be complete.

12 And I don't know that I'm phrasing that

13 right or not. I mean, maybe if somebody wants to tell

14 me that I'm just so -

15 MR. CONCEPCION: This is the acceptance

16 criteria for determinism today. So, we have the

17 regulatory requirements in 603. We have this section,

18 Section 4.10, which talks about -

19 CHAIRMAN BROWN: I got that.

20 MR. CONCEPCION: - deterministic approach.

21 And then we get into the GDCs. So, this is an area

22 that is a regulatory requirement.

23 What we do not have is a, like I said, a

24 NUREG or a reg guide or an ISG. We do have the BTP 7-21

25 and we factored that into the guidance. We stayed with

1 the regulatory requirements. We put the guidance in.
2 CHAIRMAN BROWN: I guess what I was expecting
3 to see because of that and what I was thinking of after
4 I read A, I mean, it very clearly says you got to go
5 to completion, that's all going to completion. Just
6 says once you've established that you need to trip, it's
7 got to finish the action.
8 It just says realtime must ensure
9 completion of protection action within the critical
10 points of time. And then in 4.10 it identifies your
11 critical points of time, and I recognize that.
12 MR. CONCEPCION: Yes.
13 CHAIRMAN BROWN: It just seems if I had been
14 writing this myself, I would have said there are no
15 specific requirements, design acceptance requirements.
16 However, you know, Guidance 4 establishing appropriate
17 periods, et cetera, et cetera, are, you know, are used
18 in the next - just to highlight, hey, look, we're really
19 paying attention to what you're looking for.
20 MR. CONCEPCION: I see what you're saying,
21 okay.
22 CHAIRMAN BROWN: Between independence and
23 determinism of the processing, the sample times and
24 whether it's FPGAs or whether it's microprocessors even
25 though they're different technologies, they still have

1 their own little nuances within them.

2 For instance, interrupt-driven software is

3 not prohibited in terms of their review, because you

4 can't prohibit it.

5 MR. CONCEPCION: We're trying not to

6 encourage it either.

7 CHAIRMAN BROWN: Well, I wouldn't say you

8 haven't - you haven't really discouraged it as much as

9 it ought to be either.

10 Were you going to say something, Dan?

11 MR. SANTOS: I think we have the basis and

12 we run this through OGC. And I think we are - we're

13 on good grounds here to expect some of this to be provided

14 as part of the application.

15 CHAIRMAN BROWN: Okay. I just don't want

16 it to get lost. I mean, I sat through one design where,

17 you know, fighting about the interrupt-driven

18 microprocessor-base system was like sucking blood out

19 of rocks to get the information needed to try to make

20 sure it was okay and it just makes the whole design

21 difference and just trying to not lose opportunities

22 to make sure that the design agents that come forward

23 really know you mean business when it comes to, you know,

24 independence and deterministic behavior.

25 Everybody pays attention to diversity.

1 Beat the bejeebers out of them on that. I mean, they've
2 got diverse stuff and defense-in-depth coming out their
3 ears. But yet, this always seems - independence and
4 this seem to get short - I don't want to say short shrift,
5 but just it's harder to work your way through them.
6 MR. JUNG: Charlie, we - to that subject,
7 we are interfacing with the applicant in several
8 meetings there. They fully understand the - they
9 already are looking at the previous ACRS transcription.
10 (Laughter.)
11 MR. JUNG: We are also emphasizing through
12 this guidance what we are looking for. Applicant wanted
13 licensing, they certainly know which area has been
14 challenging. Determinism is one of them and they fully
15 understand.
16 I think we are very competent that -
17 CHAIRMAN BROWN: Okay. So, I can never
18 retire. Is that what you're telling me?
19 (Laughter.)
20 CHAIRMAN BROWN: Not going to work.
21 MR. JUNG: I just briefly, Charlie, you
22 mentioned that the - about, you know, there's no specific
23 regulatory basis or regulatory requirement speaking
24 about determinism. It is much broader than that.
25 The current regulation in Chapter 7 -

1 related to Chapter 7 never talks about software and some
2 other things.
3 CHAIRMAN BROWN: Yes, I know.
4 MR. JUNG: It's an evolving technology, you
5 know, from, you know, we are going decades back to now
6 that - but the fundamental hazards and the way the safety
7 questions came up, certain regulations still dictates
8 that it has to be - all the safety concerns and hazard
9 has to be addressed.
10 So, I think we don't want to overly
11 highlight this does not have regulatory basis
12 requirements. We want to -
13 CHAIRMAN BROWN: Oh, no, I understand your
14 point.
15 MR. JUNG: Yes, we want to just go over what
16 the current regulatory basis. In the future, we'll see
17 if there is a better way to establish better - clear
18 regulatory basis addressing digital technology.
19 That's something we've been thinking about.
20 CHAIRMAN BROWN: That digital, it's either
21 FPGA, combinational logic-type thought processes where
22 it's hard-wired type stuff or its software-based.
23 MR. JUNG: All of those -
24 CHAIRMAN BROWN: Are you going to do
25 something with our other discussion relative to sensor

1 input to safety actuation that we talked about in Item
2 9?
3 MR. CONCEPCION: Yes, we will.
4 CHAIRMAN BROWN: Okay.
5 MR. CONCEPCION: Yes, we will.
6 CHAIRMAN BROWN: Okay. We can move on then
7 if Dennis and John don't have anything else, or Jack.
8 Okay. I just like to rub it in for a little bit.
9 Next slide.
10 MR. CONCEPCION: I guess at this point it
11 is almost noon and we're supposed to have a break. We
12 either start the section on Diversity, which I have two
13 slides, or we can just break for lunch and then come
14 back and address it.
15 This is the last section of the DSRS before
16 we get into Appendix A.
17 CHAIRMAN BROWN: You said you had something.
18 MEMBER BLEY: We're going over to training.
19 CHAIRMAN BROWN: At noon precisely?
20 MEMBER BLEY: Yes.
21 CHAIRMAN BROWN: You want to go ahead and
22 break now and finish this up when we get back, or -
23 MEMBER BLEY: Be simpler.
24 CHAIRMAN BROWN: Okay. Why don't we -
25 PARTICIPANT: Are you going to lose

1 somebody?

2 CHAIRMAN BROWN: No, they have a commitment

3 to the members at noon for some training so we can do

4 one of the other reviews.

5 So, if we can go ahead and break here for

6 lunch, and we'll restart on Slide 33, and we will recess

7 until one o'clock.

8 (Whereupon, the proceedings went off the

9 record at 11:59 a.m. for a lunch recess and went back

10 on the record at 1:07 p.m.)

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 AFTERNOON SESSION

2 1:07 p.m.

3 CHAIRMAN BROWN: The meeting will come back

4 to order. And, Milt, I'll turn it back over to you to

5 start where we left off.

6 MR. CONCEPCION: Okay. So, we are on Slide

7 33 on diversity and defense-in-depth. We briefly

8 touched about this section earlier this morning when

9 we talked about a level of detail and the comparisons

10 of BTP 7-19 and what ended up in Section 7.1.5 of the

11 DSRS.

12 I'm going to go back and restate what we

13 put together under this section. We're using the SRM

14 to SECY-93-087. We're also referring to the guidance

15 in NUREG-6303 which is - has comprehensive information

16 on diversity and defense-in-depth.

17 And we also rolled BTP 7-19 into this

18 section to the extent that we found appropriate removing

19 the repetitions and all of that.

20 This section as mentioned earlier, has

21 coordination with human factors engineering to evaluate

22 the assessment that is done in accordance with D3. And

23 also touches on 50.62, the ATWS rule.

24 Now, on Slide 34 we get into the details

25 of what that assessment is about. And again, it's

1 consistent with the SECY and the SRM to the SECY paper.
2 In summary, what we do is we identify - or
3 the applicant has to identify vulnerabilities and
4 analyze the events in Chapter 15, provide automatic or
5 manual actions as diverse means, and displays and
6 controls, and prioritization between safety-related and
7 diverse actuation signals.
8 Again, this is all consistent with the BTP
9 and the SECY paper. I guess Ian has a comment.
10 MR. JUNG: Charlie, a couple of comments.
11 In terms of relationship, interface with
12 other disciplines, D3 analysis itself involves Chapter
13 15 folks as part of it. They actually have to analyze
14 the acceptability of the D3 analysis which allows the
15 use of the best estimate or realistic assumptions used
16 in analysis. So, we enhance the interface for Chapter
17 15.
18 Also, a little clarification, Charlie.
19 Earlier you mentioned about the current DSRS and the
20 number of pages for diversity. It's actually ten pages
21 right now.
22 CHAIRMAN BROWN: You all really beat me up
23 on that earlier. You had to bring it up in the
24 transcript, right?
25 (Laughter.)

1 MR. JUNG: If you subtract the references
2 out of BTP 7-19, which is about two, three pages -
3 actually, it's a two-to-one relationship, not the
4 five-to-one as you mentioned. I just want to clarify
5 that.
6 (Laughter.)
7 CHAIRMAN BROWN: Can I take my glasses off
8 so you can poke me in the eye?
9 I did have one other - now that you did that,
10 you're going to pay.
11 (Laughter.)
12 MR. JUNG: I expected it.
13 CHAIRMAN BROWN: Let me make sure I get this
14 right.
15 MEMBER STETKAR: Milton, while he's looking
16 -
17 MR. CONCEPCION: Yes, sir.
18 MEMBER STETKAR: - why don't you just pull
19 up that section of the DSRS.
20 MR. CONCEPCION: Absolutely.
21 MEMBER STETKAR: Because I'm going to have
22 some comments or questions.
23 CHAIRMAN BROWN: Can I go ahead?
24 MEMBER STETKAR: Yes.
25 CHAIRMAN BROWN: Mine's a small one. I

1 think on Page 7.1-26 under the Diverse System
2 Characteristics, there was an item - two items there.
3 It said that in the context, the diverse means should
4 be initiated from the control room.
5 MR. CONCEPCION: Yes.
6 CHAIRMAN BROWN: And my memory is failing
7 me in this case. I thought I remembered a couple of
8 circumstances where somebody had to leave - that we
9 reviewing, they actually had to leave the main control
10 room and go to a room somewhere else. Not far, but it
11 was like through a hall and into a door or something
12 like that.
13 I can't remember where that was or where
14 that was presented. And I didn't know whether that -
15 somebody has got to help me, because I very distinctly
16 remember that comment that it was not located in the
17 main control room itself. It was exterior.
18 MEMBER STETKAR: That's right. There was
19 one design I recall that was in a room adjacent to the
20 main control room.
21 CHAIRMAN BROWN: And it had some access
22 controls on it as well, but it was something else I
23 thought I remembered. But I - it's fuzzy.
24 MR. CONCEPCION: You want to answer that,
25 Paul?

1 MEMBER STETKAR: I think they did that for
2 control room habitability issues and things like that.
3 MR. PIERINGER: One applicant proposed
4 manual actions to isolate main steam.
5 MEMBER STETKAR: Yes, that was it.
6 MR. PIERINGER: And it was out of the control
7 room. And we submitted an RAI asking them to quantify
8 all the time delays that would entail.
9 And they decided that there were too many
10 time delays and they put in automatic isolation from
11 the - well, I won't say - from the -
12 MEMBER STETKAR: From the other panel.
13 MR. PIERINGER: - gas panel in the control
14 room.
15 MEMBER STETKAR: Okay, okay.
16 CHAIRMAN BROWN: So, they doubled up on the
17 automatic feature as opposed to -
18 MR. PIERINGER: We didn't put in an automatic
19 -
20 CHAIRMAN BROWN: You just said automatic.
21 MR. PIERINGER: Sorry. That was incorrect
22 then.
23 They put in a switch on the gas panel in
24 the control room so the operators could shut the main
25 steam isolation valves.

1 CHAIRMAN BROWN: Manually from -

2 MEMBER STETKAR: And you're right, Paul.

3 That was the function that I was recalling.

4 CHAIRMAN BROWN: All right. I don't

5 disagree with what you've said. It's just that I -

6 that's fine. That answers that one.

7 I can't remember - I've got another question

8 here. Go ahead and do yours, John, and let me -

9 MEMBER STETKAR: Okay.

10 CHAIRMAN BROWN: - come back after I figure

11 out what I was - what I wrote.

12 MEMBER STETKAR: Can you scroll down, I don't

13 know, three pages or so from where you are? Page 29.

14 One more. Number 2. There we go.

15 Talking about software common cause failure

16 under Number 2. And the words, credible postulated

17 spurious actuations or credible spurious actuations are

18 used under here. What's a credible spurious actuation

19 as opposed to an incredible spurious actuation?

20 The reason I bring this up is that people

21 have used that term in traditional analyses to say, well,

22 this is not considered credible. Therefore, we will

23 not evaluate it. And whenever asked what that means

24 in a quantitative sense, they fell open.

25 So, I'm curious what a credible event is

1 within this context.

2 MR. CONCEPCION: Yes, you want to tackle

3 that, Ian? Yes, we're getting into the details of D3

4 and BTP 7-19.

5 MR. JUNG: Okay. Let me tackle that.

6 The current SRP in 7.1, as well as, I think,

7 in this BTP 7-19, the word "credible" shows up. The

8 way the conversation took place with the industry is

9 not the interpretation we had in a quantitative

10 argument, because that's the one that we talked about

11 earlier, digital system PRA. Quantification of digital

12 system in PRA has been proven to be very challenging

13 and nobody so far that I know other than UK, some folks

14 I was told they took 10, 15 years to use quantitative

15 PRA in digital systems in the practical sense at the

16 site as well.

17 The credible - there was the term used.

18 It was - of course the burden is on the applicant to

19 say whether it is credible or not, but typically it was

20 about the basis. The staff went after the what do you

21 mean by credible? Can this happen, or not? Is there

22 any proof of data that shows that it hasn't happened

23 or it happened?

24 But most of the - many of the cases, those

25 arguments are made either to take credit for - as part

1 of the, you know, design basis prevention or mitigation.
2 It was very difficult to demonstrate that and come up
3 with failure in general when complex system is used in
4 protection systems.
5 The incredibility of the - the possibility
6 of common cause failure nobody was able to demonstrate
7 is not credible. That's one.
8 In terms of spurious actuation, we are
9 getting to an area of, again, judgments that, you know,
10 in those cases where there is spurious actuation needs
11 to be evaluated, staff has been asking the question of
12 the credible nature of it.
13 And on a case-by-case, we are evaluating
14 what everyone needs.
15 MEMBER STETKAR: I guess I hear what you're
16 saying, but I'm not sure that I understand how it's going
17 to play out in practice, because I always say that the
18 way I would like to die is to be flying in an airplane
19 that's hit by a meteorite. It's very fast, and I think
20 just the irony would just be too much.
21 To me, that's a credible event. It can
22 happen. I can actually calculate the frequency of that
23 happening. There might be uncertainty about it, but
24 it is a - it is not an impossible event. And to me,
25 credibility is something that I can actually put my hands

on.

Is it something that I worry about every time I climb on an airplane? Absolutely not. I don't.

But if you leave it at this area, what I hear you saying is that I, as an applicant, will come in and say I've evaluated X, Y and Z because I believe they are credible, and I have not evaluated A, B and C, because I believe that they're not credible.

And you say, well, I believe that A, B and C are credible. So, now all you're doing is arguing about belief systems.

Is there not a better way to provide some guidance about what your intent is here?

MR. JUNG: If you look at -

MEMBER STETKAR: I mean, if you mean all possible spurious actuations, that's pretty broad. All possible common cause failures. That's pretty comprehensive. It's not clear anybody could do that, but it's pretty comprehensive.

If you mean something else, I'm not sure what credible means.

MR. JUNG: To some degree that's the reality of it, because there's going to be some line drawn. Because when you start talking about multiple spurious actuation, which always - it's a possible.

1 So, while we are - the guidance which was
2 improved through the ISG-2 and incorporation of ISG-2
3 through the input from ACRS is to clarify the language
4 in such a way that possibility of spurious actuation
5 is evaluated to show.
6 It is bounded by what's already required
7 by the Plan Safety Analysis which already evaluates the
8 spurious actuation.
9 It's different types of spurious actuation
10 if you are using the software that the burden has to
11 be still in the applicant. We have to look at it.
12 It's a difficult area. And the degree of
13 concern to the staff on this area has been - it's very
14 - it is hard to determine exactly what it is. If we
15 had a lot more data, we could provide a better guidance.
16 Right now it's from, oh, I've never seen
17 that to, oh, yes, it's possible. And some of the
18 consequences that could come - in some cases, gets down
19 to actually coding of software themselves. How you code
20 it, the quality of software, they are all intertwined.
21 It's a simple digital system, you know,
22 logics that are being employed in some of the newer
23 designs and may be possible to better demonstrate that.
24 So, in some cases, some applicant has
25 demonstrated actual analysis of potential for multiple

1 spurious actuation, but it's one of those areas how far
2 the guidance would go on, you know, if you go down to
3 application-specific software development if you start
4 putting in quality and all of that, it could be somewhat
5 challenging.
6 MEMBER STETKAR: See, what I'm concerned
7 about here, quite honestly, is that the staff reviewers
8 will use this guidance for their review.
9 And if you have a staff reviewer like me
10 who believes that a meteorite hitting an airplane is
11 a credible event, I, as a reviewer, am going to be
12 pressing the applicant to provide me confidence down
13 to that level of detail, because my belief system is
14 that that's a credible event.
15 That's my concern with using that word
16 "credible." And perhaps Charlie is a different
17 reviewer who might have a different belief system about
18 what he believes is a credible event. And, therefore,
19 you don't have necessarily consistency in the review
20 in terms of demands, RAIs and so forth on an applicant
21 to demonstrate assurance to your reviewers of adequate
22 coverage of credibility.
23 MR. CONCEPCION: I think we understand what
24 the concern is and we will look into it and we'll get
25 back to you, because this is coming from the existing

1 guidance, the BTP 7-19.

2 So, we want to make sure that we have

3 expanded information in NUREG 6303 to cover this. Or

4 if we don't, we probably have to enhance this particular

5 section.

6 MEMBER STETKAR: Thanks.

7 MR. CONCEPCION: Anything else on -

8 CHAIRMAN BROWN: Yes. Go ahead, Dennis.

9 MEMBER BLEY: Yes, I had a couple. Back

10 about two pages higher up where you had the list of things

11 for manual actions - that's it.

12 On several of these, two of them are minor.

13 In the first one - oh, I'm sorry. Where it had the

14 numbered list up at the top of the page. Must have been

15 the page before.

16 I saw it up there when I looked at - there

17 you go. Whoa. You just passed it. There you are, yes.

18 Yes, and we'll have to go a couple lines lower.

19 MR. CONCEPCION: That's okay.

20 MEMBER BLEY: The first one, if the

21 assessment indicates its safety-related manual

22 initiation would be subject to the same potential common

23 cause, we'll probably never be able to show it would

24 be. We can show it could be, perhaps. Since we don't

25 know quite what the common cause failures are inside

1 these systems, that's really minor.

2 MR. CONCEPCION: Yes.

3 MEMBER BLEY: The next one is less minor in

4 Number 2.

5 MR. CONCEPCION: I need to make sure that

6 we capture this elsewhere, but, yes.

7 MEMBER BLEY: Number 2 kind of bothers me

8 especially looking at your picture. If the

9 safety-related system or division required - it's

10 sufficiently diverse, the second manual means would not

11 be necessary.

12 Well, you still have that common cause thing

13 laying in your picture. What's "sufficiently diverse"

14 mean? How do you get around - does sufficiently diverse

15 mean that it really can't have the same common cause?

16 I don't know what that means.

17 Is that what it means? Is that what it

18 meant to you guys? If it's sufficiently diverse such

19 that no common cause exists between the two, then I kind

20 of buy into it.

21 But, you know, sufficiently diverse as a

22 reviewer, to me, might mean this looks different from

23 this one without digging into what underlies all that.

24 MR. JUNG: I think that's the current intent.

25 Sometimes we don't want to - I'm still hesitating to

1 some degree where is the absolute. Even for hardware
2 systems there is certain nature of common cause failures
3 possibility, for example, environmental conditions.
4 MEMBER BLEY: Exactly, which can be there.
5 MR. JUNG: So -
6 MEMBER BLEY: That's a real tough one to buy
7 into unless we know a little more what sufficiently
8 diverse means.
9 MR. JUNG: The NUREG-6303 has extensive
10 guidelines on different types of diversity. You
11 probably remember Mike Motorman's wheel chart and all
12 that.
13 MEMBER BLEY: Yes.
14 MR. JUNG: Which generated the NUREG-7007.
15 There are set of guidance that's out there to allow
16 the staff to make some judgment on it, but -
17 MEMBER BLEY: Well, since this is
18 self-contained, do we refer to that guidance?
19 MR. CONCEPTION: We don't have NUREG-7007
20 referenced in this particular version of the DSRS, but
21 we have 6303.
22 Doesn't mean that 7007 don't apply -
23 MEMBER BLEY: Well, think on it. If you're
24 convinced this takes care of it, then we're probably
25 all right.

1 The next one I've commented on back on both
2 of the ISGs that deal with this one here. Number 4 still
3 bothers me.
4 Difference between time available and time
5 required for operator action is a measure of safety
6 margin. Yes, it is.
7 The next sentence is the one that bothers
8 me. As the difference decreases, uncertainty should
9 be appropriately considered.
10 Uncertainty should be appropriately
11 considered, period. I don't care if you've got 30
12 minutes if the time available is pretty close to the
13 time required, or if there are complexities in the
14 situation where you'd be doing it that increase the
15 uncertainties. Things that sound like you got a lot
16 of room, don't have so much room.
17 So, if you don't always think about that
18 uncertainty - now, how carefully do you do the
19 uncertainty analysis, that can of course vary. But
20 there's no easy cut here that says, gee, you have to
21 be done within ten minutes of each other or two minutes
22 of each other before uncertainty matters. It's just
23 not true.
24 Think about some of the scenarios on a
25 boiler where you got to open a vent. Now, we're not

1 talking about a boiler with a vent, because you're
2 design-specific, but there's probably something in here
3 that gets you into a spot where the complexity or the
4 operational considerations involved in carrying out an
5 action gives you enough uncertainty that even if there
6 is - looks like substantial time, it matters.
7 So, there's no easy way around this other
8 than saying you should consider the uncertainty as
9 necessary for the case at hand or something like that.
10 That's all.
11 MR. JUNG: And just to - I appreciate the
12 comment. This particular paragraph, ACRS letter on ISG-2
13 and conversion into Revision 6 of BTP 7-19 came. We
14 had couple of reiterations.
15 MEMBER BLEY: It's getting closer to what
16 I like, but I still am not happy.
17 (Laughter.)
18 MR. CONCEPCION: It's a good sign we're
19 getting there.
20 MR. JUNG: We worked with the reactor systems
21 and the human factors and it was excruciating efforts
22 to get to this language. And these particular elements
23 are - even though it's here, it is being referred - this
24 particular one is also being referred by, you know,
25 Chapter 18.

1 MEMBER BLEY: I know, and ISG-5 covers it
2 as well, but it's a concept that's not quite right and
3 it still bothers me. So, I'll keep telling you that
4 it still bothers me.
5 (Discussion off the record.)
6 MR. CONCEPCION: A staff member is coming
7 up to the podium.
8 MEMBER BLEY: Oh, okay, from the hinterlands
9 of the room.
10 MR. EAGLE: Gene Eagle, I&C.
11 I just want to point out an additional word
12 that it went through a very complex review, all these
13 different groups and everything. And I'd just like to
14 point out right there in the last sentence where it says
15 this is for complex situations and for the actions with
16 limited margin.
17 In other words, you mentioned that the
18 complex situation -
19 MEMBER BLEY: I did, and limited margins.
20 MR. EAGLE: That got added. I thought you
21 might be interested in that.
22 MEMBER BLEY: But you had to throw in the
23 lousy 30-minute thing.
24 (Laughter.)
25 MEMBER BLEY: If you had left that out, I

1 would have been happier.

2 MR. EAGLE: Well, we want to keep that

3 specifically, because that carries over from -

4 MEMBER BLEY: I know it carries over, but

5 it's a concept that's not quite right.

6 MR. EAGLE: Well, we just said, you know,

7 if it falls below 30 minutes, that particularly you're

8 going to pay a lot of attention to it.

9 There are not many manual actions that would

10 require more than 30 minutes -

11 MEMBER BLEY: It's true.

12 MR. EAGLE: - that are going to be - and,

13 remember, we are replacing and, remember, these cases

14 -

15 MEMBER BLEY: It's getting better.

16 MR. EAGLE: We are replacing automatic

17 functions.

18 MEMBER BLEY: That's true.

19 MR. EAGLE: That's one of the key things.

20 MR. CONCEPCION: Good. Thanks, Gene. I

21 appreciate it.

22 CHAIRMAN BROWN: Okay - oh, I'm sorry. Go

23 ahead.

24 MEMBER STETKAR: Let me follow up a little

25 bit on Dennis. If you go down to testability on Page

1 30 or so - are you done?

2 MEMBER BLEY: Yes, I'm sorry.

3 MEMBER STETKAR: Bottom of Page 30, top of

4 Page 31. It says - and if you can bring up all of -

5 just scroll up a little bit more so we can see that

6 paragraph on the bottom of - first paragraph on 31 also.

7 There you go.

8 This says - again, I'm trying to think of

9 this as a reviewer. It says, if a system is sufficiently

10 simple such that every possible combination of inputs

11 and every possible sequence of device states are tested

12 and all outputs are verified for every case, then CCF

13 within the system can be considered to be appropriately

14 addressed without further action. If a portion of a

15 component or a component of a system can be fully tested,

16 then it can be considered to have no - not to have a

17 potential for software-based CCF.

18 What's the basis for that assertion? I

19 test pumps all the time - or I think I test pumps. I

20 have test procedures and I test the pumps. And I have

21 documented tests that I've tested these pumps for years.

22 Then a common cause failure happens and I

23 find that, oh, gee, I wasn't really testing for that

24 particular failure mode. I didn't really design my test

25 to test for that. And lo and behold I'll test for that

1 in the future, because I had one.

2 So, why now do I have confidence that what

3 you're calling a hundred percent testability says that

4 common cause failures are impossible?

5 Because, again, I'm a reviewer. Somebody

6 comes and says, okay, I have 100 percent testability.

7 You say, fine. I don't need to think about common cause

8 failure. You are now given a free card. You don't need

9 to consider that in any of your assessments.

10 That's the way I understand this.

11 MR. CONCEPCION: Gene, are you going to

12 tackle that?

13 MR. EAGLE: Yes. This definition when you

14 use the exact definition that came out of ISG-04 and

15 this is out of the key ideas, if you got this, we're

16 dealing of course with software, particularly digital,

17 and we look at the idea of being able to describe and

18 you have a digital input that has a component that has

19 a certain number of inputs, certain number of outputs

20 and perhaps some states inside.

21 And if you can go through every possible

22 combination in there of inputs and every possible

23 combination and you look at the outputs, then that's

24 pretty thorough testing. That's a hundred percent

25 testing of all states.

1 This is the basic definition that came
2 directly out of ISG-04 that was developed with a suitable
3 amount of stakeholders and everything trying to describe
4 it.
5 MEMBER STETKAR: It does that if it's every
6 possible combination.
7 MEMBER BLEY: Well, but it doesn't look at
8 the environment, it doesn't look at failures internal
9 to the chips that aren't just software. I mean, it's
10 software running on hardware, on firmware on hardware.
11 You can't test all of that.
12 CHAIRMAN BROWN: I'll give you an example.
13 And you're a hundred percent right. I totally agree.
14 How about that?
15 But, I mean, I've actually experienced a
16 circumstance where -
17 MEMBER BLEY: I'm going to go home and die,
18 Charlie.
19 CHAIRMAN BROWN: - there was a generator,
20 a turbine generator overspeed trip system required to
21 have, you know, separation, independence, all kinds of
22 good stuff between the controls function and the
23 overspeed trip function.
24 Had separate sensors. Had separate wires.
25 They were electrically isolated. They had optics.

1 It was an analog system on top of that. No software.
2 And in the process of operating the plant,
3 the crew found, gee, they were always - seemed like TG
4 set was always trying to move off of its nominal value.
5 And the - they started troubleshooting, as
6 you would imagine. They went through all their normal
7 checks. Checked all the operational parts. It seemed
8 to come out okay.
9 Then they decided, okay, well, let's go
10 remove the power supply. Turns out both of those
11 functions were supplied by the same two auctioneered
12 power supplies.
13 Well, they pulled out the wrong power
14 supply. They pulled out the one that turned out to be
15 the problem. And as soon as they did that, they pulled
16 out the good one.
17 The TG set immediately tried to overspeed.
18 They caught it at 149 percent overspeed manually.
19 That's how fast it went.
20 Now, this was an unloaded TG set.
21 Obviously, they weren't troubleshooting. The problem
22 as it turned out to be was noise coming out of that,
23 that told the control system to increase speed. Told
24 the overspeed trip system, don't pay any attention to
25 it simultaneously.

1 Now, that's not a testable situation you
2 would ever think of doing. And, I mean, to say that
3 you can test all possible, as you say, combination of
4 inputs and outputs, your environmental question or other
5 functioning question is an issue.
6 It's an interesting thought process that
7 you can test everything, but there are a lot of other
8 circumstances that can interfere.
9 That can happen software-wise. It can
10 happen analog-wise. And that's the only reason I bring
11 up an analog version of that.
12 I'd just be cautious with the use of a
13 hundred percent testability.
14 MEMBER STETKAR: Part of this, by the way,
15 I know Dan wants to say something, but part of this
16 actually dovetails back into my previous comment about
17 what is a credible common cause failure.
18 Certainly if you can test every possible
19 combination of inputs and assure that every possible
20 combination of outputs still remains within your
21 operating constraints, that gives you some confidence
22 about the range of possible common cause failures that
23 could occur.
24 It doesn't ensure that no common cause
25 failures can occur, but it gives you higher confidence

1 that indeed you have a system that is at least less
2 resistant to common cause failures than a system where
3 you could not do at least that level of testing.
4 But just to say that if it's a hundred
5 percent testable, it's not prone to common cause failure
6 is - that bothers me.
7 MR. SANTOS: I just want to say I agree with
8 the comment and maybe there's something there we can
9 improve.
10 We never implied to cover all common cause
11 failures here. Clearly, you can have requirements
12 adverse testing, you test the requirements most of the
13 time.
14 So, even the example that Charlie was saying
15 that you may have some environmental conditions that
16 put you outside your design space, there's many ways
17 you can get to common cause failures. So, we were trying
18 to just simply address one small aspect through testing
19 of existing requirements due to software.
20 Maybe there's a better way that we can take
21 a look back to make that point more clear that we are
22 not implying that we are taking care of all common cause
23 failure even if we use the words over it, you know.
24 I brought more clear guidance to the staff on that.
25 MEMBER BLEY: Maybe the way you've said it

1 is literally true, because you did say software-based
2 common cause failure.
3 MR. SANTOS: Right.
4 MEMBER BLEY: But the software, like I said,
5 firmware and on hardware.
6 MR. SANTOS: Yes.
7 MEMBER BLEY: And I think you're right.
8 Software doesn't break like a bearing can break or
9 something. So, if you've tested all those and the
10 software is okay until something is running on - makes
11 it not work the way -
12 MR. SANTOS: Correct. That's what we meant,
13 but clearly it still creates confusion. So, we'll take
14 it back to see if we can add more clarification.
15 DR. BIRLA: Even for software, I would not
16 accept that premise.
17 CHAIRMAN BROWN: Yes, you're probably right.
18 Thank you, Sushil. I agree with you.
19 One other observation. There was two parts
20 to that of which I did not state the second part.
21 You'll note that I said they were completely
22 independent, and then I went on to say there were two
23 power supplies that fed both.
24 In other words, independently, they were
25 not really independent. They were not really

1 independent. And that issue actually came up working
2 on another project and I had told people, look,
3 independence means independence.
4 If you wonder why I'm hard over on
5 independence, you know, for the reactor trips and all
6 the safeguard systems, that's an example of what
7 independence really means independence.
8 It doesn't mean, wow, I've got two power
9 supplies that both feed and go someplace. And it's,
10 you know, prove to us, show us a circumstance when I
11 told them, hey, you really ought to have a separate pair
12 of power supplies for each of - it's on a new project
13 - for each of those functions.
14 Said, no, no, no, they're not independent
15 if you don't. Oh, no. Tell us this is not a problem.
16 We never ever had that problem occur before.
17 Sure enough about six months later is when
18 this occurred and all of a sudden now there's a
19 multimillion dollar redesign.
20 MEMBER BLEY: You've even seen some where
21 if the hot side is independent, they're running on a
22 common ground, that suddenly they get -
23 CHAIRMAN BROWN: Exactly right.
24 MEMBER BLEY: Something happens and the
25 ground is not as good and suddenly you have different

1 -

2 CHAIRMAN BROWN: That's happened because the

3 ground wires that they had common between a bunch of

4 things were too small and you end up building common

5 mode voltages across the system that tore everything

6 up once you got an imbalance.

7 MEMBER BLEY: And those have happened.

8 CHAIRMAN BROWN: I just, you know,

9 independence is independence. And if you want safety,

10 you better be independent everywhere. I had to say

11 that.

12 Now, I'll go on and I'll ask my one other

13 question - two other questions on D&D.

14 MR. CONCEPCION: Yes.

15 CHAIRMAN BROWN: On Page 26, and again this

16 is a suggestion, this is not - I'm not trying to point

17 out - right where it says - right above Use of Automation

18 as a Diverse Means where it says that when a diverse

19 means is needed to be available, on and on and on. And

20 the last sentence says, the preferred diverse means is

21 normally an automated system.

22 The last, absolutely last word in all the

23 discussion of characteristics, the preferred system is

24 automated. And that's the - you wait until the end.

25 You really ought to have that paragraph at

1 the beginning of the diverse system characteristics
2 before you go into things that could cause problems.
3 In other words, it could be manual, it could
4 be automatic, but we prefer automatic and then go into
5 the rest of the - just a suggestion, okay, in a matter
6 of setting the tone so people know what's considered
7 to be important. That's number one.
8 The second one, and we may have dealt with
9 this earlier, but on Page 29, Item 1(b) and - first,
10 1(b).
11 MR. CONCEPCION: Yes, we discussed it when
12 we talked about priority modules, I believe.
13 CHAIRMAN BROWN: Okay. Well, let me go -
14 safety-related commands - we did - that direct a
15 component to a safe state should always have the highest
16 priority and must override all other commands.
17 So, if I have a reactor trip system that
18 locks up, it should lock up in a safe state and override
19 all - I'm not sure between that and the engineered
20 safeguards system which - that just gets confusing.
21 I just think it's a little bit ambiguous from the thought
22 process. I'm not proposing a solution. Just pointing
23 it out.
24 And then the one in C where it says, commands
25 that can be - let's see how did they - commands that

1 originate in a safety-related channel, but only cancel
2 or enable cancellation, should have a lower priority
3 and my be overridden by the - that tends, to me, you're
4 right on the margins about what should the
5 safety-related channel commands mean and what should
6 they not mean.
7 You've automatically assigned a priority
8 based on two specific circumstances; cancellation, or
9 enabling cancellation of something, as opposed to a more
10 thoughtful process. That's the only point.
11 It's just confusing to me when I read it.
12 And how would that be evaluated? And that could be
13 subject to a lot of different reviewers' thoughts.
14 MR. CONCEPCION: Yes, we're going to look
15 into that.
16 CHAIRMAN BROWN: The last one, and you're
17 glad to hear this probably from me, anyway, Page 7-31
18 7.1-31, and it's on conformance with 10 CFR 50.62. And
19 I'm like Dennis on this one. I have gone over this time
20 and again.
21 The last sentence in that paragraph, not
22 the A, B or C, is you can put every function within one
23 controller.
24 Come on, guys. Just submit it to me and
25 I'll evaluate all this stuff and hope it comes true.

1 I mean, having all your safety functions in one single
2 controller or CPU, you're just kind of inviting it.
3 That's one of my - raises the fur on the back of my neck.
4 It's just instead of saying we really don't
5 like this, but if you really insist, we'll give it an
6 evaluation just to set the tone.
7 I don't know how you - the preferred thing
8 is to - you ought to at least say the preferred way to
9 do this, have separate things. But if you really
10 insist, then we'll beat you to death on there other
11 points.
12 MEMBER BLEY: Maybe another reason to have
13 that general disclaimer up front once and for all that
14 if you do something that's not here, we'll look at it.
15 CHAIRMAN BROWN: Yes. Anyway, I just - I'm
16 just giving you a heads up.
17 MR. SANTOS: We accept your comments,
18 Charlie, and the clarifications. And, again, we've
19 said it many times that some of these were direct -
20 CHAIRMAN BROWN: Well, this is right out -
21 this is out of 1.152, I believe.
22 MR. SANTOS: Yes, direct copy of -
23 CHAIRMAN BROWN: We had the discussion on
24 1.15. I didn't like it then. It's clear that I don't
25 like it now because of the context.

1 MR. CONCEPCION: And it is today in BTP 7-19.
2 CHAIRMAN BROWN: It probably is.
3 MR. CONCEPCION: I'm pretty sure it is.
4 MR. SANTOS: We'll capture an action item
5 to see how we -
6 MR. CONCEPCION: Yes, absolutely. We'll
7 look into it. We'll look into it.
8 CHAIRMAN BROWN: This is again one of those
9 ones where the preferred means should be multiple
10 controllers for multiple safety functions. And then
11 you should have the however, if you really want to resort
12 to his, we'll tear your throat out with the rest of these
13 reviews.
14 I like those words, to put it bluntly.
15 MR. CONCEPCION: No, we got it. We got it.
16 We understand.
17 CHAIRMAN BROWN: Okay, I'm done. Thank you.
18 For this section.
19 MR. CONCEPCION: Diversity and
20 defense-in-depth.
21 CHAIRMAN BROWN: Where are we now?
22 MR. CONCEPCION: If there are no more
23 comments, we're getting into Appendix A, Hazard
24 Analysis.
25 So, this is the guidance that provides an

1 approach to review hazards analysis. The focus of this
2 section is on evaluating whether the applicant
3 identified and evaluated each loss of impairment or of
4 safety function and developed the necessary
5 compensatory measures in the form of architectural
6 constraints in the system.
7 This section provides a set of evaluation
8 topics that the reviewer will go through to make sure
9 that all of the hazards were identified and
10 compensatory measures were incorporated in the design.
11 And also, there are two examples on a
12 section related to ITAAC for implementation activities,
13 because we believe that - or we consider HA to be an
14 iterative process that will be executed in every phase
15 of the system life cycle.
16 One point I want to mention is that Appendix
17 A does not provide guidance to do an HA. It provides
18 review guidance to assess whether hazard have been
19 identified and corrected in the system.
20 MEMBER STETKAR: Milton.
21 MR. CONCEPTION: Yes, sir.
22 MEMBER STETKAR: Does the staff or does
23 anybody have an example of what a hazard analysis might
24 be?
25 MR. CONCEPCION: Dan or Sushil.

1 DR. BIRLA: This is Sushil Birla from
2 Research, senior technical advisor here in support of
3 NRO to answer questions pertaining to the technical
4 basis that Research has provided them.
5 I presume your question is in the context
6 of I&C systems, or in general? If it was in general,
7 you know that the NRC has a seismic hazard analysis
8 report that is world renown.
9 MEMBER STETKAR: That's a seismic hazard
10 analysis.
11 DR. BIRLA: Right.
12 MEMBER STETKAR: I'm trying to think of what
13 does - I'd like to see - let me not talk about seismic
14 events then, because this is I&C.
15 What do we really mean by hazard analysis
16 in the context of a digital I&C system? The reason I'm
17 asking that is there is a statement in the DSRS that
18 says, current hazard analysis technique such as fault
19 tree analysis and failure modes and effects analysis
20 by themselves, do not assure discovery of or the absence
21 of system internal hazards rooted in system development
22 activities.
23 By implication, whatever this thing is does
24 assure completeness of that. So, I'm really curious
25 about what this is, because I'd like to learn what it

is. Because I've never used one of these things and I'd like to learn how people do use it. Because if this is complete, that's great.

MEMBER BLEY: I read that statement differently, but I'm more interested in the answer.

(Discussion off the record.)

MEMBER STETKAR: This is apparently a new method.

DR. BIRLA: So, this is not advocating a particular method, but it is recognizing that people who have used the traditional methods of FTA, ETA, FMEA resulting in thousands of pages of analysis reports, have heated systems that eventually failed and you could not trace the failure to any revelation from those analyses.

MEMBER STETKAR: Is that because of the fault trees, FMEAs and event trees, or is that because the people using those little tools didn't really think carefully enough?

DR. BIRLA: Well, when it comes to the root cause being rooted somewhere in the engineering process that meets an engineering effect, the system has been so complex that the space is so large that you cannot possibly do an exhaustive FMEA on components of that sort. This is what it's amounting to.

1 MEMBER STETKAR: That's fine.

2 DR. BIRLA: Individual software unit-wise
3 if it's small enough, perhaps you could, but scale it
4 up to a representative system of today, nobody is able
5 to.

6 MEMBER STETKAR: That's fine.

7 DR. BIRLA: Secondly, what do you do the FMEA
8 or FTA on? You do it on some design given to you.

9 Unfortunately, the propagation paths are
10 not reflected in the design the way they are in an
11 electrical circuit and we haven't overcome the problem.

12 We don't have explicit, verifiable,
13 architectural design constraints that assure us that
14 these four properties perhaps will not exist.

15 MEMBER BLEY: The design might not give you
16 those, but the analyst might be - must understand them
17 to be able to be able to do hazard analysis.

18 DR. BIRLA: What information does the
19 analyst analyze? All the analyst can analyze is the
20 design given to the analyst.

21 Now, we can suspect that the design isn't
22 showing you everything and what do you do with that
23 suspicion?

24 So, you seek evidence in some other way.
25 That's what this is getting at.

1 MEMBER BLEY: Which is the way you ought to
2 do fault tree analysis and event tree analysis anyway.
3 You ought to look at the history of failure and
4 understand that and apply that to your model.
5 But the way I read this wasn't that they
6 were saying they have a new hazard analysis, but that
7 the tools of hazard analysis don't guarantee it will
8 be okay. That's all I thought you were saying.
9 DR. BIRLA: That's exactly right, yes.
10 MEMBER BLEY: So, we read it very
11 differently.
12 CHAIRMAN BROWN: No, I read it like John did,
13 because I read it like the FMEA and FTA -
14 MEMBER BLEY: Since I didn't see the answer,
15 I figured that's all they were telling me was that you
16 need to do it, but it's not perfect.
17 DR. BIRLA: So, let's take your observation
18 on will the analyst should look at the history. Well,
19 in this business the history isn't adequate.
20 What do you look at the history on?
21 Something that is repeating? Something that is
22 consistent? Something that is the same like a family
23 of motors that's been used in industry and we've got
24 an extensive record? We don't have such a thing.
25 In the whole history of NRC's event reports,

1 we have less than 450 incidents.

2 MEMBER BLEY: But there's more than that in

3 the common cause database that NRC had one of your labs

4 put together that identified failure modes in this kind

5 of equipment.

6 Now, they didn't get down - unfortunately,

7 they didn't chase it to the failure modes. They chased

8 it to card level kind of things, which don't let you

9 do the analysis in any -

10 DR. BIRLA: That's exactly right. You can

11 identify failure modes for simple electronic

12 components. But when it comes to complex systems, we

13 had the discussion in the last review meeting that you

14 just don't have complete enough set along which you can

15 start collecting operating history and develop a

16 statistically significant amount of findings to base

17 any analysis on.

18 MEMBER BLEY: We've been pounding Research

19 to really chase these failure modes. And the folks who

20 make these things not just for the nuclear business,

21 but for other business, there's lots and lots of these

22 out there, must have collected a lot of information on

23 just what's gone wrong in these systems.

24 DR. BIRLA: Well, the most renowned

25 organization and its capabilities is JPL. We went to

1 JPL to get their records. We have about 10,000 - we
2 call them anomalies in their database and extract
3 information from them.
4 There isn't anything that you can organize
5 along the lines of suggesting classic failure modes with
6 why would you condemn and start accumulating data, but
7 - and let's us come to the same conclusion.
8 So, what they are doing and what we would
9 like to do is take a lessons learned approach, meaning
10 from each one of those incidents' anomalies, what do
11 you learn.
12 MEMBER BLEY: That's certainly the place to
13 start. I agree with you there.
14 DR. BIRLA: Right, right. And then go into
15 the preventative direction. What is it in the design
16 or the process that allow such a thing to happen that
17 we should allow?
18 So, the leading organizations are taking
19 more a preventative approach and checking whether the
20 means are adequately specified or not. And secondly,
21 whether they are implemented adequately or not.
22 So, if you look at what's happening in
23 Europe right now where even though some organizations
24 talk about reliability of I&C systems or
25 software-reliant systems, the reliability part for the

1 hardware is classic. Because when it comes to software,
2 they begin using a term called "development assurance."
3 MEMBER BLEY: So, we're leaning toward
4 continuing the same kind of hazard analysis we've always
5 done, because it has some value, but we're just saying
6 that we know that can't cover other things.
7 Is that where you guys stand or have I
8 oversimplified it far too much?
9 DR. BIRLA: Well, we will continue to do the
10 same kind of hazard analysis that we have been doing.
11 Well, if you look at the submittals in I&C systems,
12 we have not had anything other than FMEAs.
13 Our licensing officers report that they
14 have not seen a single good hazard analysis in their
15 career in this field.
16 MEMBER BLEY: In the I&C field?
17 DR. BIRLA: Yes, yes.
18 And to give you a couple of examples, what
19 you call the program manual, software program manual,
20 where it came to the section for software hazard
21 analysis, the applicant's answer was we don't do
22 software hazard analysis, because we do it at the system
23 level.
24 So, then you go to the system level and the
25 applicant's response there is, we have no hazards in

1 our system, because it's well proven in the field.

2 MR. SANTOS: In another case, applicant

3 stated if you use our systems the way we told you so,

4 you would be free from hazards.

5 (Laughter.)

6 DR. BIRLA: So, the point is we would not

7 want those kinds of hazard analysis submitted again.

8 MEMBER BLEY: So, what does Appendix A tell

9 us to do or look for?

10 DR. BIRLA: Can you pull up Appendix A?

11 MEMBER STETKAR: What I was going to ask

12 while he's pulling it up, I wanted to kind of understand

13 it. I think I'm getting a better appreciation of this

14 right there.

15 The third paragraph says, the application

16 should contain hazard analysis information sufficient

17 to ensure that the applicant has identified the hazards

18 of concern.

19 From what I heard you saying is that there

20 is - does that mean that there has been a comprehensive

21 compilation of everything that's ever happened in

22 software failures and that they've provided assurance

23 why their design won't do that?

24 Because you're saying, well, you know, JPL

25 has thousands and thousands of incidents and you can

1 learn from those things. Is that the intent of that,
2 identify the hazards of concern?
3 DR. BIRLA: No, that would be too limiting.
4 MEMBER STETKAR: Okay.
5 DR. BIRLA: The operating experience in the
6 whole world collected together isn't enough to cover
7 all the possible ways in which we can get this wrong.
8 MEMBER STETKAR: Okay.
9 MR. SANTOS: The intent is for them to take
10 a systematic approach, okay, of the whole I&C design
11 and understand the ways their identified safety
12 functions can be lost or impaired.
13 And in that context, okay, postulate what
14 are things that could lead to that scenario.
15 MEMBER BLEY: Okay. Now, since nobody has
16 ever submitted one that your field people have said has
17 been worth a nickel, this is guidance for the reviewer,
18 but what are we giving the people who have to submit
19 something to review such that they won't give you
20 something that's not useful in the future?
21 How is this moving forward, or are we just
22 saying nobody is ever going to pass this step and what
23 are we going to do about it?
24 Are we going to say it's okay, or it's not
25 okay? I don't know where we're headed with this.

1 DR. BIRLA: So, what you see here is the first
2 draft, about five pages, sent out into the public domain
3 to start the dialog.
4 The technical basis that it draws from is
5 a research document, Research Information Letter that's
6 also going to be -
7 MEMBER BLEY: That's not out yet?
8 DR. BIRLA: That's not out.
9 MEMBER BLEY: Okay. So, we haven't seen
10 that.
11 CHAIRMAN BROWN: What document did you say?
12 MEMBER BLEY: The Research Information
13 Letter.
14 DR. BIRLA: That we would like to develop
15 to a point that we can also release that into the public
16 domain, invite some comment, engage in dialog.
17 As you recognize that in an area where this
18 has not been done well enough by anyone in industry,
19 there is going to be a learning curve both on the industry
20 side and on the review side. And this is the beginning.
21 MEMBER BLEY: Okay, but we have approved
22 designs. I'm just - now, you've had - as you've built
23 this work we're looking at today, you've had a lot of
24 interactions with the mPower people at least and maybe
25 some of the others. I can't speak for them, but I assume

they're getting the idea of where you're headed with this and what they're going to have to do.

I don't know if they've actually tried to accomplish something in this new direction or not.

MR. CONCEPCION: We have had interactions with them, but this is the first time they see the draft. And we receive preliminary comments on the draft, including the section on HA, but we don't know - we don't know what has been done by the applicant in this area. We do not know.

MEMBER BLEY: As I read it, it wasn't - I didn't quite get what I'm understanding now, and maybe that's my fault in the way I read it.

I was left with the idea of, well, you just do the best you can with the event trees and fault trees and tell us a story wit it. But what you're saying is really to get at the root of what's going on and address that in a qualitative -

MR. SANTOS: Right. And if you look at the structure around evaluation topics, that basically drives to the areas that from our current reviews, have been issues that resulted in long RAIs and long issues.

MEMBER BLEY: To get at these very things.

MR. SANTOS: And our lesson learned from that was, gee, if the applicant from the beginning was taking

1 more of a systematic look at their distributed system,
2 we could have altogether come to a place we all
3 understand instead of where we did the reviews that were
4 so, you know, component by component and we were missing
5 kind of the forest view.
6 So, we're trying to do that with this
7 approach.
8 MEMBER BLEY: Is there anything going on in
9 your organization or in research along the lines of
10 digging into this information you received from JPL or
11 other sources to try to do this, look at the hazards
12 across the business of it to get some kind of reference
13 document out there for people to use?
14 DR. BIRLA: Let me answer that in two parts.
15 The specific question that you asked seemed to be about,
16 again, the lessons learned, learnable from the history
17 that's known.
18 MEMBER BLEY: Yes.
19 DR. BIRLA: There are a couple of papers from
20 NASA that have done very limited analysis of that data.
21 It is not adequate.
22 We undertook it as internally here to do
23 a more comprehensive lessons learned exercise on it in
24 collaboration with NASA. NASA has a small activity to
25 go on their headquarters website on lessons learned

1 database.

2 We're trying to link with that and join

3 forces, combined resources. We are at the very early

4 stage in that activity.

5 So, first to exercise the process so that

6 we can indeed have lessons learned from -

7 MEMBER BLEY: I mean, it seems that that

8 would be real helpful to an applicant if - because every

9 applicant is not going to go out and do that kind of

10 research.

11 DR. BIRLA: That's right. So, we recognize

12 that. We just haven't been able to scale up the

13 resources to that level, but that's a target on the

14 books. It's part of the research plan.

15 MEMBER BLEY: I don't remember - well, that's

16 your -

17 DR. BIRLA: That's part of the research, yes.

18 MEMBER BLEY: So, that's in the -

19 DR. BIRLA: In the research plan, yes.

20 MEMBER BLEY: Okay. I don't remember that.

21 I'll have to go back and look.

22 DR. BIRLA: So, there's a section in the

23 research plan with the title, operating experience.

24 It's in that section.

25 We subsequently after publishing the

1 research plan, have an official project with the DCM
2 on it, but just haven't scaled up the activity date.
3 But let me also give you two other parts
4 to the answer even though your focus was not on both
5 parts. But the more general part of your question was,
6 is there anything being published out there?
7 The Electric Power Research Institute
8 research team had a project on their books called failure
9 analysis.
10 A couple of years ago the project was
11 started based on - with industry request, that means
12 at the customer's request, from an observation that you
13 do all these FMEAs that are running thousands of pages
14 long, and yet things go wrong and we lose a lot of money.
15 Why? Again, in the context of I&C systems. So, that's
16 how the project was started. And the EPRI researchers
17 are converging to a conclusion that I just mentioned
18 to you that the traditional techniques are not good
19 enough.
20 So, they have now systematically run
21 through a test exercise or you might say case study,
22 about half a dozen different techniques. And are
23 putting together a report that compares the techniques.
24 Some techniques were able to discover
25 issues that other techniques were not able to. I do

1 not want to steal their thunder. Within a few months
2 you should hear from the field itself.
3 We have been as part of an understanding
4 and the memorandum of understanding research and EPRI
5 researchers been exposed to the work in progress. And
6 we believe that they are understanding the issue and
7 are directionally headed in the right plan of action.
8 MEMBER BLEY: We heard from them a couple
9 years ago probably the beginnings of this work.
10 DR. BIRLA: But this exercise was run in the
11 last four months.
12 MEMBER BLEY: Oh, okay.
13 DR. BIRLA: Yes, quite, you might say, a
14 90-degree turn in direction of what you might have seen
15 a couple of years ago.
16 MEMBER BLEY: And not just information from
17 the nuclear industry?
18 DR. BIRLA: Well, actually the exercise is
19 on a dual heat removal system in the nuclear industry.
20 MEMBER BLEY: Oh, okay. It's aimed at one
21 specific -
22 DR. BIRLA: Yes, yes. Something on which
23 they have already done - or some plants have already
24 done FMEAs. So, we have some baseline and an
25 understanding.

1 And internally, you might also be aware that
2 the NRC gave a research grant to MIT about a year ago.
3 And the work under that research grant examined a small
4 part of an EPR submittal to exercise one method and have
5 NROs, technical staff, understand what the issues are
6 in performing a hazard analysis. What difficulties you
7 run into, what are the gotchas, what are the right
8 questions to look for.
9 That report is in the review stage right
10 now. We hope that in a month to six weeks the NRC review
11 would become featured and MIT would be in a position
12 to publish that report.
13 Based on that report, MIT will be making
14 a presentation, publishing a paper in risk analysis.
15 And they are making a presentation in the next meeting.
16 MEMBER BLEY: Did they access information
17 that we haven't been looking at previously, or just
18 trying some new techniques?
19 DR. BIRLA: Whatever was on the docket is
20 basically what they had interaction with the NRC
21 technical staff to get an understanding of the immensely
22 complex documents.
23 MEMBER BLEY: Okay.
24 MS. STAREFOS: May I also add that there are
25 opportunities in our process to talk publicly with any

1 stakeholders that are uncertain about any of the
2 information that's been published in the DSRS?
3 And because we don't have a parallel reg
4 guide that talks about our minimum application content
5 like the large lightwaters do, we anticipate that we'll
6 be looking closely at these documents, the DSRS
7 sections, to give them some insights on what their
8 application needs to contain.
9 And we certainly have no intention of
10 leaving them out there alone to try to decipher that.
11 We plan to have a series of public meetings once the
12 comments are returned. And if necessary, we'll go
13 through and make additional changes to these documents.
14 I won't promise necessarily this section,
15 but I expect there will be sections that might have
16 additional information that need to be either included
17 or clarified, because there is a variety of stakeholder
18 interest in that clarification.
19 So, our process allows for that to be done
20 in the springtime.
21 MR. SANTOS: And, again, I want to repeat
22 one of the improvements I think we can get through both
23 the efficiency and the safety focus is going through
24 this systematic look - is going through some of these
25 topics.

1 If you look at the most contentious issues,
2 the RAIs, I think that took the longest. You can trace
3 it to some of these topics.
4 So, we do believe an approach like this will
5 early on - identify the issues early on, will save a
6 lot of time for both NRC and the applicant through the
7 process.
8 MR. JUNG: Ian Jung. Just to add, there's
9 a reason why this - some topics are in the appendix at
10 this point.
11 These are the type of sort of tools that
12 staff wants to use to enhance the efficiency and
13 effectiveness of our reviews.
14 Hazard analysis by itself does not have a
15 regulatory requirement that they have to do it here.
16 So, it is supposed to be - or what we envision is to
17 use this, have an integrated hazard analysis approach
18 as part of the, essentially, 7.1 and 7.2.
19 So, 7.1 and 7.2 regulatory requirements and
20 staff guidance is already - they already designed to
21 deal with set of hazards instead of the concerns that
22 we have.
23 Without this hazard section, what we will
24 see is those hazards are being discussed and even within
25 DSRS in those sections.

1 What this could do is validate the
2 comprehensiveness of all the hazards of concern that
3 we've challenged and should be - especially for new
4 designs like mPower, we are interested in those hazards
5 that are not just I&C initiated, but hazard that could
6 come from outside I&C.
7 So, we want to use this opportunity to
8 enhance and that's our review process. Even without
9 it, I think there's a possibility without full use of
10 this, the individual section, we could still cover the
11 regulatory basis for making a safety finding using
12 individual sections. But this particular process could
13 increase the efficiency of our reviews.
14 MEMBER BLEY: In truth, your section on scope
15 reads a lot like a section on a HAZOP for a chemical
16 plant. So, same words to figure out -
17 DR. BIRLA: Exactly. If you look at both
18 bullets, you could treat them as HAZOP question set.
19 MEMBER BLEY: Yes.
20 DR. BIRLA: Or you could treat them as
21 failure modes at a very high level. Functional overall
22 comprehensive level.
23 But systematically asking each question and
24 answering it appropriately takes care of a lot of those
25 issues.

1 MR. SANTOS: And although I don't know how
2 the applicant is going to recite to present their
3 information, we're not looking or repetition, meaning
4 compliance with Section 7.1 and then repeat on the
5 hazard.
6 I mean, if the applicant can demonstrate
7 their compliance to their regulatory requirements
8 through their hazard analysis, we'll definitely take
9 a look at that.
10 MEMBER BLEY: We don't have anybody from the
11 industry talking today.
12 CHAIRMAN BROWN: Well, there will be some
13 comments, public comments at the end.
14 Just relative to this one question, does
15 this - I just did a word search and could find no place
16 where FMEAs were required other than a statement in
17 testing - capability of testing calibration where it
18 referred to 10 CFR 50.34 F2xxii.
19 MR. SANTOS: That is a TMI action item, yes.
20 CHAIRMAN BROWN: Okay. And so, it seemed
21 like you all were just discounting it completely. And
22 the only thing people were doing and it says for
23 integrated control system for the effects of input and
24 output signals, but not the system itself.
25 So, it looks like not only had you said it

1 hasn't revealed much, we're really not encouraging
2 anybody to do it. And my question is, have people
3 submitted those in the past? Is there a requirement
4 for an FMEA or an FTA to be submitted as part of the
5 design?
6 MEMBER BLEY: The DAC was for ITAAC, was some
7 other design.
8 CHAIRMAN BROWN: Don't say that.
9 MEMBER BLEY: They were.
10 CHAIRMAN BROWN: That was the only place I
11 could find the failure mode -
12 MR. CONCEPCION: We have GDC-23 that talks
13 about failure modes for the protection system.
14 DR. BIRLA: He is right and -
15 CHAIRMAN BROWN: Who is right?
16 DR. BIRLA: The -
17 CHAIRMAN BROWN: I'm not right, again?
18 MR. CONCEPCION: Go ahead, Sushil.
19 DR. BIRLA: This is Sushil Birla from
20 research again.
21 It's not that the NRC is discounting failure
22 mode inspection analysis altogether. There is hardware
23 in the system and there is single failure criterion.
24 It's a well-used, well-proved,
25 well-established tool to satisfy the single failure

1 criterion.

2 CHAIRMAN BROWN: The FMEA is.

3 DR. BIRLA: Yes.

4 CHAIRMAN BROWN: So, you expect to get

5 something like that relative to an assessment of a single

6 failure criterion, okay.

7 DR. BIRLA: Yes.

8 CHAIRMAN BROWN: I just - I didn't see any

9 reference to it other than its more generic input to

10 output.

11 MR. SANTOS: Actually, as part of Section

12 2.1 on the hazard analysis, portions of it may be

13 supported by FMEA.

14 CHAIRMAN BROWN: 7.21?

15 MS. SANTOS: No, part of Section 2.1 of the

16 hazard analysis.

17 CHAIRMAN BROWN: Oh, okay.

18 MR. SANTOS: An applicant may support

19 portions of that with an FMEA.

20 DR. BIRLA: Yes, a system is always going

21 to have hardware in it.

22 CHAIRMAN BROWN: Okay. I just wanted to ask

23 you that and I think you've answered my little fallout

24 question.

25 MR. JUNG: Charlie, also not within the DSRS,

1 but in the standards that we endorse I think it goes
2 into one of the ways to handle some of the hazards or
3 FMEAs. And those are mentioned in that space.
4 CHAIRMAN BROWN: Okay. All right.
5 Anymore, John? Jack? Dennis?
6 MR. CONCEPCION: Okay. Well, it is 2:15 and
7 I'm about to start Appendix B, I&C System Architecture.
8 I don't know how long it's going to take,
9 but I'm going to take a stab at it. If we have to take
10 a break at 2:30, we're going to take a break, okay?
11 CHAIRMAN BROWN: There may be reasons to take
12 a break.
13 MEMBER BLEY: Even before then.
14 CHAIRMAN BROWN: Oh, would you like a break?
15 We're starting a new section.
16 MEMBER BLEY: Okay.
17 CHAIRMAN BROWN: Why don't we go ahead and
18 take a 15-minute break so we don't have to break in the
19 middle of the discussion. We'll recess for 15 minutes
20 until 2:32.
21 (Whereupon, the proceedings went off the
22 record at 2:18 p.m. for a short recess and went back
23 on the record at 2:39 p.m.)
24 CHAIRMAN BROWN: Okay. The meeting is back
25 in session.

1 MR. CONCEPCION: Okay. So, this is Appendix
2 B, I&C System Architecture. As we said earlier in the
3 presentation, this is new guidance, new material that
4 staff believes is useful to do our I&C system reviews.
5 We provided guidance to assess how those
6 I&C architectures are going to be described. And we
7 expect the applicant to address all of the I&C functions
8 in this I&C architecture along with interfaces between
9 I&C systems, signal flows and descriptions, simplify
10 functional diagrams and that kind of information.
11 And like I said, this is new guidance and
12 we hope to see a description, sufficient detail to
13 support the reviews in 7.1 and 7.2 of the DSRS.
14 CHAIRMAN BROWN: Okay. I'm not disagreeing
15 with anything you've got in here, except with one
16 exception for expansion.
17 Where you're talking about diagrams of the
18 overall architecture, that's a very generic and
19 high-level statement of what that means or what that
20 - of architecture.
21 And to me, what you need to do is have -
22 and I don't know where you get examples. But if you
23 go back to what we ended up having developed for some
24 of the projects that we were dealing with, they showed
25 functional block diagram, which is not mentioned

1 directly.

2 Where it shows process of the signal from

3 sensor through the data - through signal conditioning,

4 through a data processing unit which says trip or don't

5 trip, and then to the voting units, and then out to the

6 actuation, whatever form it is, and what has been missing

7 has been the hardware timer - for software-based systems

8 and probably FPGAs also depending on the design, the

9 hardware nonsoftware-based thing that says, hey, look,

10 if you lock up any particular thing as you all talk about

11 up in Section 7.1.1. I think it's 7.1.1.

12 So, that level of functional block diagrams

13 are what you really need. I mean, logic diagrams

14 doesn't cut it.

15 That's like saying I got temperature, I got

16 pressure, I got flow, I got power and I want to put all

17 these things into some algorithm and that's a logic

18 diagram, but I'm talking about a functional

19 signal-crossing diagram that goes from start to the end.

20 MR. SANTOS: Does Item D -

21 MS. ANTONESCU: Yes.

22 CHAIRMAN BROWN: It says, key blocks.

23 MR. SANTOS: Can we expand?

24 CHAIRMAN BROWN: It doesn't say beginning

25 to end. It just says functional key blocks.

1 MR. SANTOS: Okay.

2 CHAIRMAN BROWN: So, I don't want somebody

3 just giving me a block where I have to take a block here.

4 Here's the carburetor, here's the tire. Over here I

5 got a steering wheel. How do I put those together?

6 MEMBER SIEBER: So, there's a block in the

7 middle.

8 MR. CONCEPCION: We can expand the

9 description.

10 CHAIRMAN BROWN: That's all I'm -

11 MR. SANTOS: It's a good comment. We'll

12 take C that talked about end-to-end, and D, and reword

13 it.

14 CHAIRMAN BROWN: The end-to-end signal

15 flows, again, is a little bit more -

16 MR. SANTOS: Got it.

17 CHAIRMAN BROWN: - ambiguous. What do you

18 mean?

19 MR. SANTOS: I got it.

20 CHAIRMAN BROWN: Here's a piece of data.

21 It goes to here, it goes to there. That just doesn't

22 cut it. You really -

23 MR. SANTOS: We have the example from the

24 -

25 CHAIRMAN BROWN: There are several examples

1 and I'd quote the projects, but I don't want to in this
2 particular meeting. And the words I prefer, it's nice
3 to have examples with pictures, but I admit you have
4 to have words in here to say what we want.
5 MEMBER SIEBER: And what you want is
6 functional blocks as opposed to hardware blocks.
7 CHAIRMAN BROWN: Yes, I'm not looking, you
8 know, yes, it's a functional block. And where you have
9 to break down a block into a couple of pieces for
10 instance, there might be a platform that has its
11 processing unit and it has a little hardware timer, you
12 know, backup timer there to trip the thing off.
13 It might be on the same platform, but it's
14 independent. I mean, it's a separate set of circuits
15 on - in that little package. And it's independent of
16 software.
17 That's - there are times when you need to
18 break that down and show why does that do what it's
19 supposed to do when it's supposed to do it type thing.
20 And we've made that comment in the meetings also.
21 So, I'm just looking for whether you expand
22 C or D or 3 or however you do it. I think that the concept
23 of functional block diagrams, not a piece.
24 And that's where I had a problem with the
25 key functional part, because I thought, you know,

1 somebody will show me a carburetor and somebody else
2 a tire and, you know, have a crankshaft somewhere and
3 then, okay, now that's a car. Do you realize it? No,
4 I don't' know that's a car.
5 And that's the only comment I had. And it's
6 really kind of a sensor input - sensor, not input, but
7 the sensor to the other thing and to show - and those
8 diagrams ought to show the independence. It ought to
9 show that there is no communication and what the nature
10 of that communication is and all that type of stuff.
11 MR. CONCEPCION: Yes, the intent is to use
12 this appendix along with 7.1 and 7.2. So, this is kind
13 of like an additional aid to the reviewer to confirm
14 those fundamental principles. I understand your
15 comment.
16 CHAIRMAN BROWN: Those words might be in 7.1.
17 MR. CONCEPCION: Those words are -
18 CHAIRMAN BROWN: No, 7.1.1 or 7.1.2. I'm
19 not sure.
20 MR. CONCEPCION: Yes, those words are at the
21 bottom. And let me just pull this section.
22 CHAIRMAN BROWN: I know there's some of that
23 in 7 - whatever. You don't need to go through that.
24 Just that's the point wherever you get it from that
25 I think you need it here because this is, quote,

1 architecture.

2 MR. CONCEPCION: There is a paragraph that

3 talks about that in -

4 CHAIRMAN BROWN: Where?

5 MR. CONCEPCION: At the bottom of the

6 section.

7 CHAIRMAN BROWN: The architecture section?

8 MR. CONCEPCION: Yes, sir. Yes, sir.

9 There's a paragraph there.

10 CHAIRMAN BROWN: I missed that. Obviously,

11 I did this late at night.

12 MR. CONCEPCION: Okay, at the bottom - I have

13 it on the screen. The reviewer should consider the I&C

14 overall architecture in concert with the sections

15 relating to the fundamental design principles.

16 MS. ANTONESCU: Which page?

17 MEMBER SIEBER: Yes, but what you're saying

18 is you want to see it on a diagram.

19 CHAIRMAN BROWN: Yes. You should consider,

20 I mean, it doesn't say anything about functional block

21 diagrams and I don't see the word like that. Other

22 sections, you should evaluate other sections for

23 consistency.

24 MR. CONCEPCION: Your point is taken.

25 CHAIRMAN BROWN: Thank you. I didn't think

1 I seen that.

2 MR. CONCEPCION: We'll look into it.

3 CHAIRMAN BROWN: I know I'm old, really old,

4 but that's beside the point. Okay. That's all I had

5 on architecture, unless anybody else got something.

6 John? Dennis?

7 MR. SANTOS: I just want to point out that

8 while this section is very short, it's very powerful.

9 CHAIRMAN BROWN: I agree with that.

10 MR. SANTOS: There are some designs that have

11 been three years in the review and we still are asking

12 for this type of information.

13 CHAIRMAN BROWN: I'm well aware of that also.

14 Still waiting for one of them to come back on it.

15 MR. SANTOS: Having this type of information

16 from the beginning is very powerful and we consider this

17 even though short, a significant improvement to the way

18 we've been doing reviews.

19 MEMBER SIEBER: That's going to be the basis

20 of your review.

21 MR. SANTOS: Yes.

22 MR. CONCEPCION: Okay. Moving right along

23 to Slide 37, this is the section on simplicity. This

24 is another area where we provided new guidance to enhance

25 the reviews in I&C.

1 We're looking at how simplicity was
2 considered by the applicant in the design of the system.
3 This is a section that will also be used in conjunction
4 with 7.1 and 7.2 of the DSRS.
5 And what we did was, we wrote this section
6 based on those fundamental principles and what we
7 believe shows simplicity for those principles in the
8 way the system is designed.
9 So, we talk about signal flows, separation
10 and segregation among functions, simplify
11 communications and all of that good stuff under the
12 section of simplicity.
13 So, is there any feedback or comments you
14 might have on this section?
15 MEMBER STETKAR: You don't need to open it.
16 There are a couple places in here that say that one
17 of the characteristics is no unnecessary communications
18 between a safety and nonsafety system, unless the safety
19 system is out of service.
20 I was trying to think what that meant. I
21 mean, it implies that - if you want to open it up, it's
22 on Page C-3. It's the last sub thing under Item 3.
23 MR. CONCEPCION: It's a good one, John.
24 C-3?
25 MEMBER STETKAR: It's D(iii). Right there.

1 MR. CONCEPCION: Yes.

2 MEMBER STETKAR: And I don't know what that
3 means. It implies that unnecessary communications are
4 okay when the safety system is out of service, which
5 leads me to think about what might those unnecessary
6 communications do to the safety system when it's put
7 back in service.

8 We have examples of people making changes
9 while - to software updates that have unintended
10 consequences that weren't discovered until, you know,
11 sometime later. So, I was curious what this meant.

12 MEMBER BLEY: Because of things left in the
13 system.

14 MEMBER STETKAR: Because things left -

15 MEMBER BLEY: Because, to me, it bothered
16 me because if the capability is there to communicate
17 when the safety system is down, unless you've got
18 interlocks that remove that when you start up the system,
19 how do you make sure it's never there when it's
20 operating?

21 MR. SANTOS: First of all, I think the
22 comment - I feel the first thing we need to do to be
23 consistent is to maybe make a comment to better clarify
24 this sentence. And I will strike "unless the safety
25 system is out of service."

1 MEMBER STETKAR: That would sure help me.

2 MR. SANTOS: Seriously. So, I got the

3 comment.

4 MEMBER STETKAR: I think it may appear in

5 a couple of different places.

6 MR. SANTOS: Yes.

7 MEMBER STETKAR: This was the first place

8 that I flagged it, but you may want to look. I was trying

9 to understand what - anyway.

10 CHAIRMAN BROWN: Well, there are no

11 necessary inter-channel communications at some point

12 through some part of it. That's another way of phrasing

13 it.

14 MEMBER STETKAR: And the other one that I

15 had was if you go way down to the end of the section

16 under - it's on the last page, C and D.

17 C, features added to cope with particular

18 types of hazards that could negatively impact other

19 safety design features.

20 And here's where I was struggling to

21 understand what that means, or perhaps you might have

22 some specific examples of things that you've seen in

23 the past where somebody has done this.

24 I'm assuming that both C and D are things

25 that you found in the past.

1 MR. CONCEPCION: Yes, I believe this is
2 direct experience with the reviews in the past.
3 MEMBER STETKAR: Okay.
4 MR. CONCEPCION: So, that's why we
5 incorporated them.
6 MEMBER STETKAR: Without jeopardizing
7 proprietary information, do you have an example of C?
8 Sort of a generic example of C?
9 I sort of understand D, I think. But if
10 you had an example of C, something that somebody did
11 that was intended, I guess, to specifically cope with
12 one type of problem that introduced other problems
13 elsewhere, is that -
14 MR. CONCEPCION: I don't recall. Do you
15 recall what - well, we can't get into specifics, but
16 we'll look into it.
17 MEMBER STETKAR: Yes.
18 MR. CONCEPCION: We will look into it and
19 we will provide something.
20 MEMBER STETKAR: I'd appreciate something
21 if you had an example.
22 MR. CONCEPCION: Meaning to the actual
23 section.
24 CHAIRMAN BROWN: I can actually give you an
25 example.

1 MEMBER STETKAR: Sure.

2 CHAIRMAN BROWN: It wasn't a reactor safety
3 system, but it was a turbine generator control system
4 with a voltage regulator where we wanted - we did not
5 - we had dual regulators. And we wanted to be able to
6 handle a failure of one regulator and have it
7 automatically transfer to the other one within five
8 milliseconds so that it would not lose the load. And
9 it was very important in the particular context of the
10 systems we were using.

11 And when you think about five milliseconds
12 when you're at a high load and you want to transfer,
13 that means you have to have some fairly complicated
14 thought processes, plus the heartbeat between the two
15 that are saying, okay, is the other one still following
16 you directly?

17 And in the process of doing that, you can
18 potentially put yourself into a case where you lose
19 excitation or drive it in the wrong way and can create
20 some problems.

21 So, my point being is that that's a
22 circumstance - that's a complex circumstance that's not
23 a reactor trip circumstance, but it's a control system
24 circumstance.

25 The same thing goes with governor controls.

1 If you want to switch those without losing a load, it
2 requires an even more complex type of - and ability to
3 transfer fast.
4 And so, that capability to know the other
5 one is in service is not going to take you in the wrong
6 way because it's got something else going on with it
7 you haven't -
8 MEMBER STETKAR: Well, but I guess in the
9 context of this, is the solution to say, well, because
10 that's so complicated, we'll take the trip because we
11 don't want to transfer -
12 CHAIRMAN BROWN: Yes, you might do that.
13 MEMBER STETKAR: - because it's the only
14 way to deal with -
15 CHAIRMAN BROWN: You might do that. I don't
16 know.
17 (Simultaneous speaking.)
18 CHAIRMAN BROWN: Which has its own
19 implications internally.
20 MEMBER STETKAR: Exactly. You had to think
21 about it was the only point I'm saying. Am I willing
22 to accept that and what do you do and, et cetera.
23 MEMBER BLEY: And that's kind of covered here
24 with the negative impact.
25 CHAIRMAN BROWN: I think it's a good -

1 MEMBER BLEY: It's a tradeoff.

2 CHAIRMAN BROWN: It's just difficult.

3 MEMBER BLEY: Now that you've raised it, I'd
4 like to make sure I understand D, and I did. Now, in
5 hardware you might limit the testing because of
6 wear-out. Here, the problem is just the availability
7 of the system to do its normal function if you're
8 diagnosing too much?

9 MR. CONCEPCION: Not just the availability.
10 Also potential interference with the safety function
11 because of those self-diagnostics running at the same
12 time.

13 MEMBER BLEY: At the same time.

14 CHAIRMAN BROWN: Well, there's another
15 circumstance where you can have self-diagnostics that
16 are running and I say, gee, I've got a problem. So,
17 what does it do? It resets everything. And now, your
18 entire channel is being reset, rebooted right when you
19 don't want it to be rebooted and that's a problem.

20 And if you look at the way the platforms
21 that people are using so far, these things take forever
22 to reboot. They're not blink of an eyelash rebooting.

23 MEMBER BLEY: And that's what I was thinking.
24 That's an availability problem. It's not there when
25 you want it.

1 CHAIRMAN BROWN: Exactly.

2 MEMBER BLEY: You also raise the

3 interference problem that while it's actually an action,

4 this thing could start and interfere with the action.

5 It's not blocked somehow.

6 Do they have ways to block the - I'm sure

7 you could block the self-diagnostic if -

8 MR. CONCEPCION: You could have a feature

9 to, I guess, prevent the self-testing or self-diagnostic

10 to -

11 MEMBER BLEY: If the system is in some other

12 state, yes.

13 MR. SANTOS: So, to clarify, we are an action

14 item here from the members on these two items, or are

15 we just commenting?

16 MEMBER BLEY: What I captured was 7C and 7D

17 perhaps we may have an example using generic statements

18 that could perhaps clarify those two provisions in

19 there.

20 MEMBER STETKAR: I mean, for me personally

21 I'm happy with what I heard here. I just wanted to make

22 sure that indeed there were some examples that you had

23 seen of these types of issues.

24 MR. CONCEPCION: Yes, these are two examples

25 from previous experience and reviews.

1 MEMBER STETKAR: I tend to agree with Dennis
2 that there is a tradeoff. That taken literally, C says
3 if there is something installed to combat Hazard A that
4 could impact negatively - or a hazard for Safety Function
5 A that could potentially have a negative impact on Safety
6 Function B, that ought not to be there. And I'm not
7 necessarily convinced that that's always true.
8 CHAIRMAN BROWN: It doesn't say they're not
9 - you can't do it. I mean, I didn't read it that way.
10 MEMBER STETKAR: Well, it says -
11 MR. CONCEPTION: Carefully considered.
12 CHAIRMAN BROWN: Yes.
13 MEMBER STETKAR: Carefully considered is -
14 MR. CONCEPTION: In the context of
15 complexity.
16 CHAIRMAN BROWN: Unless you do a tradeoff
17 kind of analysis if you need to.
18 MEMBER STETKAR: Yes, then I'm done.
19 MR. CONCEPCION: Okay. So -
20 CHAIRMAN BROWN: I'd like to ask one relative
21 question relative to staff reviews. This is just one
22 I forgot to ask in other places.
23 Always had a problem with self-diagnostics.
24 And then when somebody detects a problem, there's
25 normally a default status that has to be done.

1 And I do remember and this is back in the
2 early days when we were first doing this, that
3 unbeknownst to us and it was not a system thing, an
4 internal self-diagnostic default put something to a,
5 oh, well, it's not working exactly right, we got a little
6 twidget over here.
7 Everything else was working fine and it was
8 not related to the direct path of the signal, but some
9 other feature of that run-through was giving them
10 heartburn and they defaulted to zero and ended up with
11 a reactor scram.
12 We found that out the wrong way. So,
13 self-diagnostics are always interesting and the
14 defaults.
15 And do you all look - do you all have
16 somebody assess what default circumstances are already
17 a part of your all's review process for all the
18 self-diagnostics?
19 I'm not saying you've got to list it in here.
20 I'm just asking if you do that.
21 MR. JUNG: I think we typically do go into
22 - and some designs definitely take more credit for
23 self-diagnostic features. Some others don't, you know,
24 sometimes they try to take credit for tech specs or
25 meeting certain 603 requirements.

1 In those cases, we delve into a little more
2 detail.
3 CHAIRMAN BROWN: Otherwise, you don't
4 necessarily - if they put in a default that somehow
5 screws them up sometime, it's just life in the big city
6 as long as it's not a safety function type thing.
7 MR. JUNG: And then in addition to that,
8 those features would eventually have a - the
9 requirements through the testing and other things come
10 along. So, they need to demonstrate that.
11 CHAIRMAN BROWN: Hopefully.
12 MR. SANTOS: Including strategies for
13 testing the tester.
14 CHAIRMAN BROWN: Okay, that's all.
15 MEMBER SIEBER: I take it all the software
16 is read-only memory software.
17 CHAIRMAN BROWN: Well, that's a good
18 question. We haven't addressed that before.
19 MEMBER SIEBER: Otherwise, you can't recover
20 it.
21 CHAIRMAN BROWN: The way the program, the
22 application program and the stuff is in there, is that
23 in programmable read-only memory-type thing or do you
24 know?
25 I mean, do you have any requirements on that

where you have to physically change out a chip to change the software, or can they come in and put a clip over the processor and do it with a laptop and download and offload software?

MEMBER BLEY: It's in the security sense.

CHAIRMAN BROWN: No, this is for you can change - that's not a security issue. This is just a matter of whether -

MEMBER SIEBER: It can be.

CHAIRMAN BROWN: Oh, yes, it can be an access control. It could be a configuration control issue.

MEMBER SIEBER: Right. It can be a security issue, too.

CHAIRMAN BROWN: Yes, I agree with that.

MR. JUNG: And those designs are very specific designs and those get - and some designs actually take the card out, put it in the temporary safety delay.

CHAIRMAN BROWN: Reprogram it?

MR. JUNG: They reprogram, replace it, fully test it, and actually put it back in with that particular channel.

That's very safe and we've seen that, but some other cases more complex and we delve into more details and how to mitigate any potential hazards.

1 CHAIRMAN BROWN: Do you deal with that under
2 configuration control management?
3 MR. JUNG: Oh, yes, they have to have an admin
4 control specific, but we also looking at the design
5 itself. How are - what are the design features that
6 you're going to utilize to perform the test?
7 Is that a separate cabinet? Is it online
8 you're going to do it? Are you pulling the card out
9 online? And you ask all the questions to make sure,
10 you know.
11 We've seen experience of those things
12 causing hazards.
13 MS. SANTOS: And what are the features for
14 integrity checks and CRC checks and everything else that
15 they have to check integrity of changes.
16 MEMBER SIEBER: Well, my question is if
17 there's an instantaneous loss of power and recovery,
18 is there any reloading of software that has to occur?
19 CHAIRMAN BROWN: I think the answer is yes.
20 MEMBER SIEBER: Or is it ready to run -
21 CHAIRMAN BROWN: On the platforms we've seen
22 to date, I'm saying that only for the ones that we've
23 looked at -
24 MEMBER SIEBER: The ones that I've seen,
25 they're ready to run.

1 CHAIRMAN BROWN: Not the ones in the
2 projects. I don't think so. They've got to reload the
3 software.
4 That's like a five-minute or six-minute -
5 they said a boot-up can be anywhere from three to ten
6 minutes for one of the particular platforms depending
7 on -
8 MEMBER SIEBER: That's a problem.
9 MR. CONCEPCION: But you have to consider
10 full loss of power for that to happen. And, you know,
11 we're talking about platforms that have backup systems
12 and have batteries and all of that.
13 So, I don't want to get into more detail
14 about that.
15 PATICIPANT: Almost hardly ever happens.
16 CHAIRMAN BROWN: Hardly ever.
17 (Simultaneous speaking.)
18 MEMBER SIEBER: All you have to do is have
19 a noisy cluster that has circuit breakers on it and
20 pulses you can get messed up like I have.
21 CHAIRMAN BROWN: Well, that was one of the
22 problems, Jack, when we were looking at one of the
23 designs where the hardware backup timer actually reset
24 the entire system and they said, well, okay, it's being
25 reset, it will be okay.

1 But if you go look at the manual itself or
2 the platform itself, it took anywhere from five to ten
3 minutes to reboot. Well, by that time you've melted
4 the plant.
5 MEMBER SIEBER: You might want to think about
6 that.
7 CHAIRMAN BROWN: Well, they've got multiple
8 other channels depending on how it goes about it.
9 MEMBER SIEBER: It depends on -
10 CHAIRMAN BROWN: Poor choice of words.
11 MEMBER SIEBER: If the same thing happens
12 on all the channels, you're -
13 CHAIRMAN BROWN: Well, I made that point and
14 nobody liked it.
15 MEMBER SIEBER: Okay.
16 CHAIRMAN BROWN: It could scram
17 automatically if you've locked them all up and they're
18 all resetting.
19 MEMBER SIEBER: Yes, well -
20 CHAIRMAN BROWN: If you read the tech manual,
21 it looked like nothing was going to happen until they've
22 gone through another resource like -
23 MEMBER SIEBER: Well, I read someplace where
24 mPower has endless -
25 MR. CONCEPCION: I think we've included

provisions through DSRS for that.

PARTICIPANT: I'm not sure if that's the best answer.

CHAIRMAN BROWN: What, scramming? Well, if they're all locked up and not operating, it probably is because you're not getting anything. Your meters cannot be in one place.

MEMBER STETKAR: I will give you the example of the Zion nuclear generating station that is no longer operating. So, I can tell you that when we had insufficient component cooling water, our tech specs required us to immediately shut down both units, which put us in a situation where we really needed that component cooling water more than we did during normal power operations.

Sometimes shutting down isn't necessarily the best thing to do.

MEMBER SIEBER: But sooner or later you're going to do it.

CHAIRMAN BROWN: All your safety systems, reactor trip systems are -

MEMBER STETKAR: Standby systems will start because -

(Simultaneous speaking.)

CHAIRMAN BROWN: All right. We're

1 digressing here for a few minutes. So, are we finished
2 with this one?
3 MR. CONCEPCION: If there is no more
4 questions, I think we can -
5 CHAIRMAN BROWN: You're going to get a lot
6 of discussion, I'm sure, on the simplicity thing.
7 MR. CONCEPCION: We sure hope so.
8 CHAIRMAN BROWN: Be interesting to see what
9 the feedback is. I like, I mean, I like the idea of
10 trying to get the point across.
11 MEMBER BLEY: I think the - as you guys said
12 early on, it's real hard to define "simplicity."
13 MR. CONCEPCION: It's not a simple task.
14 MEMBER BLEY: But against the design
15 principles, simplicity is say, here, it has to be clear
16 that you meet the design principles.
17 If it is clear, it's probably simple enough.
18 MEMBER SIEBER: Yes, but simplicity is like
19 handsome.
20 PARTICIPANT: It what? I'm sorry.
21 MEMBER SIEBER: It's all in the eye of the
22 beholder.
23 CHAIRMAN BROWN: That only applies to some
24 of us, Jack.
25 MEMBER SIEBER: Some of us, right. Not

1 many.

2 CHAIRMAN BROWN: Okay.

3 MR. CONCEPCION: All right. Moving along,

4 now we got into 7.2, which is system characteristics.

5 These characteristics come directly out of IEEE 603.

6 And what we did was we segregated or was

7 like we discussed, we segregated the fundamental design

8 principles and now we're talking about those design and

9 functional requirements are contained in 603 and the

10 way we expect applicants to address them.

11 If you notice, this is pretty much a slide

12 that covers all of the 15 sections of 7.2. And I did

13 not intend to get into the details of all of them, but

14 two that are on the slides.

15 If you have any particular questions about

16 any section regarding 7.2 aside from 7.2.1 and 7.2.2,

17 we can get into the details now or maybe after I go

18 through the next two slides.

19 CHAIRMAN BROWN: What's wrong with 7.2.2?

20 That one is all written. We got to look at that one,

21 didn't we?

22 MR. CONCEPCION: No, I just -

23 MEMBER BLEY: He says he's going to talk

24 about it.

25 CHAIRMAN BROWN: Oh, when you get there.

1 So, what are you going to do first?

2 MR. CONCEPCION: I'm going to talk about

3 7.2.1 right now.

4 CHAIRMAN BROWN: Oh, okay. Everything went

5 blank in the document.

6 MR. CONCEPCION: This is directly related

7 to BTP 7-14, which is software development. What we're

8 doing is we're evaluating the review responsibilities

9 and the role of I&C in this programmatic area and we're

10 trying to come up with a better way to address the

11 software and system development and leverage the folks

12 in Chapter 17 for this activity.

13 This is still a work in progress. I'm

14 personally working on this section. We're trying to

15 expand BTP 7-14 and address development at the system

16 level considering hardware and software and their

17 integration as part of the system.

18 So, that is pretty much what I have to say

19 regarding this section. I sure hope to be done with

20 it before the end of the year and circulate it internally

21 so that we can share it with the public or, I guess,

22 share with ODC first, and then publish it for review

23 and comment.

24 Any questions or comments about it?

25 CHAIRMAN BROWN: Yes, one comment.

1 MR. CONCEPCION: Yes.

2 CHAIRMAN BROWN: This is a suggestion. My

3 own personal suggestion.

4 There has to be a fundamental principle in

5 which the assumption you look at software is relative

6 to the safety systems. And a fundamental assumption

7 in my own mind, at least what I used for three-and-a-half

8 decades - two-and-a-half decades, was that there is no

9 - software will always fail on you.

10 It will always have characteristics -

11 something will happen which will be unexpected and you

12 should design your systems, overall system, to assume

13 that software will fail. Doesn't mean it all has to

14 fail in every channel simultaneously, just it will fail.

15 And that's one of the reasons not

16 necessarily for diversity, but for multiple,

17 independent divisions of anything or channels of

18 anything you are particularly interested in.

19 So, it's a thought process that from the

20 quality of the review you should test it, because you

21 all cannot do that. You will not be setting up a

22 full-scale set of the instrumentation for any particular

23 plant.

24 The vendor won't be doing that. He'll be

25 doing little partial pieces and they will not run tests

1 that are totally prototypic. I can almost - maybe I'm
2 speaking out of school here, but I bet you that's going
3 to be the case.
4 You'll never see a full suite of equipment
5 set up with a massive computer modeling the plant that
6 they had feeding everything in through emulators and
7 running it through every possible mode and operation.
8 I don't think - that's extremely expensive.
9 There is a program that does that, but it won't be this
10 one commercially.
11 So, anyway that's - I just say you all are
12 encumbered by not being able to do line-by-line and other
13 types of code validations and verifications. So, you
14 ought to - my suggestion is to make sure you have a
15 process that allows you through the design, an
16 architecture in the way the systems are designed to
17 ensure that, yes, software - we'll do the best we can,
18 but we've got to make sure the software doesn't kill
19 us and we put other protections in place. That's just
20 a suggestion.
21 MR. SANTOS: Yes, we understand that.
22 CHAIRMAN BROWN: And I didn't see that stated
23 anywhere.
24 MR. SANTOS: Yes, we will work on it, but
25 basically high-quality software development process is

1 not sufficient to claim that the software will be free
2 from defects.
3 CHAIRMAN BROWN: That's right.
4 MR. SANTOS: So, we understand that. And
5 when we do that, we can -
6 MR. CONCEPCION: Yes, absolutely. We're
7 still - this section has not been published. It's still
8 in the works.
9 CHAIRMAN BROWN: Just bear in mind that
10 people were irradiated by the Therac-25 and died. You
11 can't talk to them right now. And it was all a matter
12 of keystrokes and a few other things in terms of the
13 way the computing system, the software interpreted
14 keystrokes and the timing and everything else.
15 There were a number of factors, but that
16 was one.
17 MR. CONCEPCION: It did what its designers
18 wanted it to do.
19 CHAIRMAN BROWN: Exactly right.
20 MR. CONCEPCION: The operator didn't know
21 how it was programmed yet.
22 CHAIRMAN BROWN: That's right. So, no
23 matter how smart, they know it was simple compared to
24 this stuff. We had to tell it to do two things. Here's
25 how much, and here's how long.

1 MR. CONCEPCION: So, like I said, this is
2 an area where we're trying to improve the guidance in
3 BTP 7-14. So, from that perspective we're trying to
4 expand it to address system development and come up with
5 something that we can use for licensing reviews.
6 We're considering industry standards in
7 this area as well. So, more to come. That's what I
8 have to say.
9 Anything else?
10 CHAIRMAN BROWN: Not on this one.
11 MR. CONCEPCION: Okay. Equipment
12 qualification. We wrote this section and this is an
13 area that is also addressed in IEEE 603. Talks about
14 seismic and environmental qualification.
15 And what we're trying to do is do the
16 coordination with Chapter 3 and leverage the expertise
17 and qualification that is in the NRC today.
18 We're going to be doing confirmations that
19 the equipment, the I&C equipment located in mild
20 environments is qualified in accordance with the
21 requirements that are established for those systems.
22 And we're trying to improve in this area,
23 because in the past we had - we took over some of these
24 activities where we clearly didn't have the right
25 expertise. So, this is an area where we're trying to

1 improve the coordination.

2 The seismic aspect has been always handled

3 in Chapter 3. What we're trying to do is better

4 coordinate with Section 3.11 of the DSRS, have better

5 coordination.

6 We're still retaining some of the

7 responsibilities associated with instrument sensing

8 lines and EMI/RFI, but the aspect of qualification and

9 the qualification program that will be used to qualify

10 and see equipment is going to be handled by the folks

11 in Chapter 3.

12 MEMBER STETKAR: And we made the note this

13 morning about that instrumentation that specifically

14 intended to operate beyond design - under beyond design

15 basis conditions. We have to close that loop.

16 MR. CONCEPCION: Yes, we captured that.

17 Yes.

18 CHAIRMAN BROWN: This one is - did you just

19 use the words that the Chapter 3 people are responsible

20 for making sure your stuff is qualified to the equipment

21 qualification process?

22 I thought that's what you just said, I

23 thought.

24 MR. CONCEPCION: We're going to be

25 leveraging the expertise of -

1 CHAIRMAN BROWN: You've changed -

2 MR. CONCEPCION: - Chapter 3 people.

3 CHAIRMAN BROWN: - the words.

4 (Laughter.)

5 MR. CONCEPCION: For the review of

6 environmental qualification of I&C equipment located

7 in mild environment.

8 CHAIRMAN BROWN: If your stuff is supposed

9 to work from five degrees, I'll just pick some number,

10 five degree C to 50 degree C and it doesn't work, who's

11 responsible for making sure it does work? You, or

12 Chapter 3 people?

13 They don't know squat about your equipment.

14 All they know is it's supposed to work over that range.

15 You're responsible for making sure it works over that

16 range.

17 MR. CONCEPCION: And that should be

18 confirmed through the environmental qualification

19 program.

20 MR. JUNG: Charlie, let's explain. The DSRS

21 Chapter 7 that we are doing -

22 CHAIRMAN BROWN: The what?

23 MR. JUNG: The main purpose of Chapter 7,

24 we are talking about chapters. That's important

25 distinction.

1 If you go to Chapter 3, seismic
2 qualification is led by mechanical engineering branch
3 discipline. And electrical qualification,
4 environmental qualification, EQ, is led by electrical
5 engineering branch. And I&C branch is the supporting
6 branch.
7 So, when we say Chapter 3, who's going to
8 do that work as agency is going to put in the right
9 resources? We're going to work with electrical branch
10 and their expert is in EQ and seismic qualification.
11 And I&C is supporting branch. So, we'll work with them
12 to make sure the right expertise are applied.
13 From the perspective of DSRS, what we wanted
14 to clear is Chapter 7 had a lot of descriptions on EQ
15 that's already covered in Chapter 3. So, what we are
16 doing is Chapter 3 has a fully - Chapter 3 fully describes
17 the necessary guidance for the Agency staff.
18 CHAIRMAN BROWN: I don't have a problem with
19 nonduplicating, you know, repeating this stuff. I
20 mean, I'm sitting here thinking, okay, it goes off and
21 the seismic requirements are defined. And then, but
22 who's responsible for making sure that the seismic -
23 that it actually performs to those requirements?
24 I mean, if they go run a seismic test on
25 a cabinet, is that you all that have to agree that it

1 worked okay, or is it the seismic guys that have to agree
2 that it worked okay?
3 MR. JUNG: I think it worked okay from the
4 mechanical structure guys, the seismic -
5 CHAIRMAN BROWN: But it's not always
6 structure.
7 MR. JUNG: Yes, I understand. Structure is
8 typically seismic characteristics are transferred to
9 structures. Structures are transferred to mechanical
10 devices and electrical I&C. We understand the
11 framework.
12 So, a lot of the - we did a lot of
13 confirmation working with those people to make sure the
14 qualification requirements in Chapter 3 in fact covers
15 I&C.
16 CHAIRMAN BROWN: What if you get
17 intermittent making and breaking of pins when you plug
18 the card in that it makes and breaks and ends up with,
19 you know, signals that are undesirable or cause
20 unintended consequences?
21 MR. JUNG: During the operation or -
22 CHAIRMAN BROWN: Yes, during the seismic
23 test.
24 MR. JUNG: Those -
25 MR. CONCEPCION: That should be part of the

1 qualification program for those pieces of equipment.

2 MR. JUNG: There's an ITAAC associated with

3 that if that becomes an issue. The applicant and

4 licensee has to address that issue.

5 CHAIRMAN BROWN: Yes.

6 MR. JUNG: Inspection goes out and finds

7 those will verify their corrective action program is

8 appropriate. If mechanical engineering branch helping

9 Region 2 constructions with the inspection program

10 identifies the need for I&C expertise to be involved,

11 we will be involved.

12 CHAIRMAN BROWN: I guess this is not clear

13 for -

14 MEMBER BLEY: Well, what's not completely

15 clear, I think, is how that interaction works. Going

16 back some years ago, most of the seismic qualification

17 work was done by structural and mechanical guys even

18 for electrical - electronic equipment.

19 And electrical, I mean, the mechanical guys

20 didn't really understand how the equipment was built

21 internally. So, and some of the SQUG stuff had this

22 in it.

23 So, when they'd do a test for seeing if you

24 had contact chatter, relay chatter, they didn't realize

25 that if the device is energized, those contacts are

1 really locked shut and aren't going to vibrate. And
2 if it's not energized, they will.
3 So, they didn't have the right testing.
4 And they didn't come to the electricals, because they
5 didn't understand how the equipment worked.
6 So, the electrical electronics people, I&C
7 people, need to be involved in making sure that the tests
8 are set up to test the parts of the equipment you care
9 about.
10 So, if you're relying on the seismic folks
11 to come to you when they need to, that might not be good
12 enough, because they don't know they need to come to
13 you if they don't understand how your things can fail.
14 And, you know, Charlie's pin thing is one
15 of the ways these can fail.
16 CHAIRMAN BROWN: Contact bounce on switches,
17 also.
18 MEMBER BLEY: That's all we're trying to get
19 at. If it's relying on them to come to you, maybe that's
20 not good enough. Maybe you need to be in on the review
21 of the test to make sure the equipment you care about
22 is being tested in a way that meets your needs.
23 MR. JUNG: You know, for a design and
24 certification perspective, some of these obviously
25 detail design and qualification testing, of course I&C

1 is going to be later after the design certification.
2 So, during the licensing review, you know,
3 certification of the design like mPower, the description
4 of their EQ is going to be more programmatic. And
5 they'll identify types of equipment for a lot of the
6 I&C equipments are tested at the cabinet level.
7 Peter Kang is here. So, Peter can explain
8 more from electrical engineering branch, NRR. So,
9 there's a limitation of how much we can look at it, but
10 Peter's branch has been on the same floor until recently
11 became part of NRR.
12 So, I'll leave it up to Peter if you can
13 add anything you want.
14 MR. KANG: My name is Peter Kang from
15 electrical engineering from NRR. And basically EQ
16 50.49, equipment qualification of electrical equipment,
17 I&C equipment and a digital portion of it is - we are
18 coordinating between I&C, as well as electrical, as well
19 as mechanical aspect of it.
20 So, when we write the safety evaluations,
21 we do take all the input from three guys and electrical
22 engineering group is taking all combined together.
23 But on the other hand, there is three
24 important to safety, which is safety-related equipment,
25 as well as nonsafety-related equipment, which failure

1 equipment factor safety-related functions. And also
2 the PAM equipment, I&C equipment is also listed. Those
3 are classified as important to safety and monitoring
4 equipment.
5 So, when applicants, they are supposed to
6 go out, test or they should have what they call this
7 EQ DP, equipment - environmental qualification data
8 package, which they tested all this equipment.
9 And based on IEEE or 323 or whatever, we
10 use 1974 version, but I&C portion is like lately later
11 ones. Like most of our computer systems is mild
12 environment. For that, we have IEEE 323 later version,
13 2003 version is used.
14 So, based on that that we're supposed to
15 test. And supposed to record all the results of the
16 findings and make a summary of environmental
17 qualifications.
18 Also, we have ITAAC system. ITAAC, we
19 supposed to verify all the equipment, I&C equipment.
20 CHAIRMAN BROWN: Well, the ITAAC is done when
21 you're in place. That's largely at the plant, isn't
22 it, after it's installed?
23 So, that's not really a -
24 MR. KANG: Are you talking about the special
25 inspections?

1 CHAIRMAN BROWN: Well, that's -

2 MEMBER SIEBER: Acceptance -

3 MR. KANG: ITAAC.

4 MEMBER SIEBER: - of installed equipment

5 at the plant.

6 CHAIRMAN BROWN: Yes, that's what I'm

7 saying. You bring it in, you plug it into the plant.

8 That's not a qualification test. That's just that you

9 hook it up right.

10 MR. KANG: Yes.

11 CHAIRMAN BROWN: That's an operational test,

12 effectively.

13 MR. KANG: 14.2, yes. Initial testing

14 programs and that those once they install, that they

15 are testing, yes.

16 CHAIRMAN BROWN: No, I understand that.

17 MR. KANG: Yes.

18 CHAIRMAN BROWN: I thought I understood that

19 part. I'm only looking on the qualification side.

20 MR. KANG: Right.

21 CHAIRMAN BROWN: I mean, for example, and

22 agreed I haven't read all the versions of 323. I'll

23 guarantee that.

24 But are they tested in an operational state,

25 a normal operational mode and such that they're - let's

1 go to a real actuator or whatever they're supposed to
2 control?
3 MR. CONCEPCION: Yes. I guess the important
4 aspect about 323 is that it is not influenced by I&C.
5 CHAIRMAN BROWN: I understand that.
6 MR. CONCEPCION: I'm struggling with the
7 concept of what is it that is really unique to I&C that
8 needs to be factored in the 323 qualification -
9 CHAIRMAN BROWN: Failure design. That's
10 what I'm used to. So, that's why I asked the question,
11 okay. I had cradle and grave. And so, that's what I'm
12 used to and that's why I'm asking the question trying
13 to make sure I understand.
14 Here, it's not cradle to grave, from what
15 I understand. There's disparate groups that have
16 pieces -
17 MR. CONCEPCION: We're still coordinating
18 with them.
19 CHAIRMAN BROWN: Pardon?
20 MR. CONCEPCION: We're still coordinating
21 with Chapter 3 people, but we don't have the expertise
22 to review EQ programs though. We do not.
23 CHAIRMAN BROWN: All right.
24 MR. CONCEPCION: Those 323 programs, we
25 don't have the expertise.

1 MR. KANG: Basically, the applicants is
2 supposed to test it and have data files in order to form.
3 So, under 50.49, always make it available to staff go
4 down and inspect it.
5 CHAIRMAN BROWN: Somebody review the actual
6 test procedure that they -
7 MR. KANG: Yes, there is a test. DCIP has
8 a test and -
9 CHAIRMAN BROWN: Who?
10 MR. KANG: DCIP, Division of -
11 MR. CONCEPCION: Inspection and -
12 construction inspection and operational programs.
13 CHAIRMAN BROWN: Okay. So, somebody who has
14 no knowledge of I&C is reviewing the test procedure.
15 MR. CONCEPCION: They're doing it with our
16 support in I&C. At least in NRO, yes.
17 CHAIRMAN BROWN: All right. I'm stop
18 beating this horse for a minute. Let's go on. Let's
19 go ahead and roll into the next one.
20 MR. SANTOS: I just want to -
21 CHAIRMAN BROWN: I'm not sure what to do with
22 this, Dan.
23 MR. SANTOS: The theme has been consistent
24 regarding all interactions and interfaces of Chapter
25 7 with any chapter.

1 So, you can come up with similar question
2 for any other interaction with other staff.
3 CHAIRMAN BROWN: I understand.
4 MR. SANTOS: So, we understand the comment.
5 CHAIRMAN BROWN: I gave you my viewpoint
6 earlier relative to what I thought and I'm just a little
7 bit concerned about the left hand, the middle hand, the
8 next to the middle hand, the right hand and a piece of
9 foot over here that are all not knowing who's doing what
10 or coordinating what.
11 Okay. Where is the brain that puts it
12 altogether? And I don't see a brain that's putting it
13 altogether based on the discussions. I just see that
14 he's responsible, he's responsible and they may talk
15 to us or they may not, depending on what they see.
16 I'm not trying to be disparaging on it.
17 I'm just - it's just what it appeared to be relative
18 to my experience. And that's, you know, that's fine
19 - well, it's not necessarily fine, but that's the way
20 it is.
21 MR. JUNG: We understand and we are very
22 cognizant about the full coverage using expertise by
23 the Agency.
24 And Chapter 3, you know, the overall topic
25 belongs to Chapter 3. Chapter 3, we'll coordinate with

1 the Chapter 3 folks. Maybe there could be additional
2 language to highlight the role of I&C much clearer.
3 MEMBER BLEY: I like what I'm hearing on
4 coordination, but you guys need to understand in the
5 last three or four designs we've sat through, the Chapter
6 3 people come and say, no, you'll get that in Chapter
7 7. The Chapter 7 people come and say, no, you'll get
8 that somewhere else. Those people come and it didn't
9 seem to be working the way we're talking about it here.
10 If it is in the future, I think that's great.
11 We'll be happy.
12 MEMBER STETKAR: How long has it - you guys
13 belabored this long enough. There's something, and I'm
14 not sure whether it's relevant or not, but in the
15 environmental qualifications under environmental
16 control systems, it says the design basis in
17 environmental control systems may rely upon monitoring
18 environmental conditions and take credit for
19 appropriate action to ensure that environmental
20 conditions are maintained within predetermined limits
21 within which system or component damage will not occur
22 during the period until the environmental control
23 systems are returned to normal operation.
24 That's a long sentence. Down below in that
25 area it says, well, part of that assurance is that, for

1 example, temperature sensors are separate from the
2 environmental control system.
3 Now, well, that's okay. The environmental
4 control people look at that and they say, okay, we've
5 got a cooling system for this room and we've got
6 temperature sensors that are not part of that cooling
7 system. So, everything is okay.
8 The I&C people, maybe you need to restore
9 that cooling within, oh, 27 seconds before a particular
10 failure mode presents itself.
11 The environmental control people don't know
12 that. They don't' know anything about that. All
13 they're looking at is a cooling system and a temperature
14 sensor, right?
15 So, how does that kind of loop get closed
16 that the design is adequate? Is that within your
17 purview that adequate time is available for people to,
18 I don't know, open up doors and put in portable fans
19 or do what?
20 MR. KANG: Dr. Stetkar, I think you're sort
21 of a little bit - we're talking two different things.
22 MEMBER STETKAR: That's the problem.
23 MR. KANG: Equipment qualification versus
24 environmental qualifications. So, you are actually in
25 space of equipment qualification area, right? That's

1 what you're talking about.

2 Is that going to be able to - but

3 environmental qualification is slightly different.

4 This is within accident atmosphere contained within

5 equipment mostly inside of a containment or the accident

6 LOCA conditions or large-break LOCA conditions is that

7 equipment going to be survived.

8 MEMBER STETKAR: Okay. Yes, yes, I think

9 I was confusing that. That's the first - that's

10 addressed in the first paragraph your notion of

11 equipment qualification.

12 This is the second paragraph about

13 environmental control systems and it sounds as though

14 that's totally under your - in your house.

15 MR. CONCEPCION: Yes. Yes, it is.

16 MEMBER STETKAR: Okay. I'm sorry. I

17 misinterpreted that. Thank you. That helps. Thank

18 you.

19 MR. CONCEPCION: I shouldn't say that I'm

20 confused wit this and your feedback, but I will, but

21 I move on. I really don't understand what is it that

22 is -

23 CHAIRMAN BROWN: I'm not sure we have any

24 -

25 MR. CONCEPCION: - confusing in 7.2.2.

1 CHAIRMAN BROWN: I don't think we have a
2 specific piece of feedback for you right now on the
3 discussion. I don't. I can't speak for my peers.
4 MR. CONCEPCION: Okay.
5 CHAIRMAN BROWN: Just leave this as a
6 diaphanous, amorphous discussion.
7 MEMBER STETKAR: It's one of the reasons we
8 have subcommittee meetings.
9 MR. CONCEPCION: Okay. I'm going to go back
10 real quick to this slide and -
11 MEMBER STETKAR: I had one more.
12 MR. CONCEPCION: Yes, sir.
13 MEMBER STETKAR: On 7.2.3.
14 MR. CONCEPCION: Let me just pull that
15 section up.
16 MEMBER STETKAR: Yes, if you could, it will
17 help. And this is - I don't think it's a big deal.
18 I just need some help.
19 MR. CONCEPCION: 7.2.3?
20 MEMBER STETKAR: 7.2.3, correct. And it's
21 the -
22 MR. CONCEPCION: Reliability, integrity and
23 completion of protective action.
24 MEMBER STETKAR: And it's on Page 7.2-9.
25 I think it's the next page. Right there. It says the

1 DSRS acceptance criteria are as follows. And Number
2 2, it says the components and system should conform to
3 the reliability guidance in NUREG/CR-6101.
4 I'm not familiar with that NUREG. I didn't
5 have enough time to download it and read through it.
6 I did note that it's dated 1993. So, it's 20 years
7 old.
8 I also noted that nothing under the Review
9 Procedures makes any reference whatsoever to that NUREG.
10 They do refer to 7-4.3.2. So, I curious
11 - I don't know - I was curious why it's listed here as
12 one of the requirements for the acceptance criteria
13 given the fact that it's 20 years out of date.
14 Now, it might be wonderful. As I said, I
15 have not read it, but one suspects that we've learned
16 a lot more in the last 20 years about these things and
17 the fact that it's not cited anywhere from a reviewer's
18 perspective, just raises a question in my mind.
19 MR. SANTOS: Well, I think it's a great
20 catch.
21 MR. CONCEPCION: Well, I have to say that
22 usually going back to why we have the guidance the way
23 we have it is because it is existing guidance in the
24 SRP.
25 That is not a justification, but I'm using

1 what I have and put it in the context of the sections
2 that were put together as part of 7.2.
3 MR. SANTOS: It's a good catch.
4 MR. CONCEPCION: The adequacy of 6101 is
5 something that we have to consider and I believe it is
6 a good catch.
7 MR. SANTOS: Yes, and I'll take the action
8 item to take it out, basically.
9 MEMBER STETKAR: Is it worthwhile looking
10 at that? I was going to download - I just didn't get
11 a chance to look at it.
12 MR. SANTOS: When I say that, you know -
13 MEMBER STETKAR: No, okay. Thanks.
14 MEMBER SIEBER: There may be something
15 newer.
16 MEMBER STETKAR: I have enough other things
17 to read.
18 MR. SANTOS: We have looked at it already.
19 It should not belong in there.
20 MEMBER STETKAR: Thank you.
21 MR. SANTOS: We will take the action item
22 to evaluate it accordingly, go through the process.
23 CHAIRMAN BROWN: You're looking up something
24 for somebody, or are you just -
25 MR. CONCEPCION: I am, but I'm not - if

1 there's no more questions, I will -

2 CHAIRMAN BROWN: I wanted to ask kind of a

3 related - unrelated, but 7.2.2 and three. And it might

4 show up somewhere else, but I stopped looking after that.

5 In the DSRS acceptance criteria for 7.2.2

6 and 7.2.3 -

7 MR. CONCEPCION: Yes.

8 CHAIRMAN BROWN: - there is no reference

9 under the specific acceptance criteria for DSRS for

10 reliability or completion. There's no reference there,

11 or in the 7.2.2 to IEEE 603.

12 Yet, the lead-in paragraph in both of them

13 refer to Section 5.4 for equipment qualification. And

14 the lead-in under requirements refers to IEEE under

15 integrity, completion of protective action refers to

16 IEEE 603.

17 And if you'll look at IEEE 603, it has words

18 and criteria relative to completion of protective

19 action, et cetera.

20 MR. CONCEPCION: Yes.

21 CHAIRMAN BROWN: So, they were - it was

22 missing. There was no reference. Instead, we

23 referenced 7-4.3.2 which is not as complete. And I

24 guess the disconnect for me was why was it missing?

25 The other interesting thing was 603 also

1 calls out under equipment qualification IEEE Standard
2 627. I don't know what that is, but I just notice it
3 was missing from all the equipment qualification.
4 I don't think I saw that. Either that, or
5 my brain fried at that time. So, I just - that was a
6 leave-out relative to the - we keep going to 7-4.3.2,
7 which is somewhat less definitive if I go off and look
8 at that again.
9 MR. CONCEPCION: Peter, do you recall
10 whether IEEE 627 is endorsed for equipment
11 qualification? I don't think it is, right?
12 CHAIRMAN BROWN: Well, it is in 603.
13 MR. CONCEPCION: Yes, but that is not an
14 endorsed standard though.
15 CHAIRMAN BROWN: Well, it's in the rule.
16 MR. CONCEPCION: It is in the rule, yes.
17 MR. CORTE: Can I add something?
18 MR. CONCEPCION: But it is not an endorsed
19 standard in our framework.
20 Yes, sir.
21 MR. CORTE: Norbert Corte, I&C.
22 If you look at the statements of
23 consideration for 603, it basically said something to
24 the effect it's a matter of law that all standards
25 referenced in 603 are not incorporated by reference

1 unless they're explicitly done so.

2 So, basically every time you say it shall

3 do this per this standard in 603, that's not a regulatory

4 requirement. And that's stated in the statements of

5 consideration.

6 So, basically any standard that's

7 referenced in 603, you basically ignore unless it is

8 separately referenced - incorporated by reference or

9 endorsed by a Reg Guide.

10 MR. CONCEPCION: Yes, if it is within our

11 framework, then it has to be addressed.

12 CHAIRMAN BROWN: Yes, but a Reg Guide,

13 somebody doesn't - that's a guide. Nobody has to follow

14 that if it's a guide.

15 MEMBER SIEBER: You have to follow -

16 CHAIRMAN BROWN: So, why does - 323 does not

17 come into play even for equipment qualification if

18 that's the case.

19 MR. CORTE: It's just the legal legalities

20 associated with it incorporated by reference. It's

21 only 603, and nothing that's referenced by 603 that's

22 incorporated.

23 CHAIRMAN BROWN: Right.

24 MR. CORTE: That specific license -

25 regulatory action. And that's why some of those

1 standards are not endorsed by any Reg Guide and are not
2 spoken to at all.
3 MEMBER SIEBER: There's a lot of reg guides
4 out there.
5 MR. CONCEPCION: I can come up with another
6 example in 603 where there is no, I mean, probability
7 assessments under single failure have pointers to two
8 IEEE standards that are not part of our framework. So,
9 that's another example of where we don't consider those
10 as part of the review guidance.
11 CHAIRMAN BROWN: All right. Well, put 627
12 aside.
13 MR. CONCEPCION: Yes, and do you have another
14 question? I couldn't understand.
15 CHAIRMAN BROWN: Well, no. 603 is not
16 included under the acceptance criteria in -
17 MR. CONCEPCION: Under which section?
18 CHAIRMAN BROWN: Either 7.2.2. or 7.2.3.
19 MR. CONCEPCION: Okay, I have 7.2.3.
20 CHAIRMAN BROWN: It's under the general
21 acceptance, but it's not under the DSRS acceptance
22 criteria. It's excluded.
23 MR. CONCEPCION: This is 7.2.3 up on the
24 screen. And as per the requirements within the
25 acceptance criteria, the requirements point to the

1 sections on reliability, system integrity and
2 completion of protective actions as called in IEEE 603.
3 And there's a typo there. It says 1191, but -
4 CHAIRMAN BROWN: I got that. Yes, yes, I'm
5 not worried about that.
6 MR. CONCEPCION: Yes, but -
7 CHAIRMAN BROWN: But when I get over under
8 the specific DSRS acceptance criteria for are as
9 follows, that almost sounds like those supercede what
10 was under the other thing.
11 We say, well, okay, if they conform to this,
12 we're happy.
13 MR. CONCEPCION: But that is not the intent.
14 CHAIRMAN BROWN: That's why I've got a
15 disconnect between what's over in the, quote, the
16 general requirements part and then the DSRS acceptance
17 criteria.
18 Sometimes you say there are none, and then
19 I refer back here and sometimes you say there are some,
20 and they don't list the ones that are over here.
21 MS. STAREFOS: Mr. Brown, we wrote those as
22 cumulative. The way we should read these is that's the
23 requirement.
24 And in addition, the specific DSRS criteria
25 will be considered for acceptance in this case.

1 CHAIRMAN BROWN: Oh, okay. I didn't realize
2 that.
3 MS. STAREFOS: That's -
4 MR. CONCEPCION: Is that explained in
5 Chapter 1 of - or will it be explained in Chapter 1?
6 MS. STAREFOS: Well, I think this is
7 consistent with the way our SRP is set up as per the
8 SRP requirements.
9 CHAIRMAN BROWN: I suggest you put that up
10 in 7.0.
11 MS. STAREFOS: Okay.
12 CHAIRMAN BROWN: Make it clearer.
13 MS. STAREFOS: We'll take that as - thank
14 you. That's a great point.
15 MR. CONCEPCION: We'll take it as an action
16 item.
17 CHAIRMAN BROWN: Something actually worked.
18 Under 7.2.9, which is another one on your list, and
19 maybe I'm missing something here, but there were no -
20 this is control of access, identification and repair.
21 MR. CONCEPCION: Right.
22 CHAIRMAN BROWN: And there's some general
23 - again, the general requirements. And then under the
24 DSRS acceptance criteria you covered two of them. One
25 for identification, and one for - I'm not sure what this

1 one is - oh, both of them are identification.

2 MR. CONCEPCION: Yes.

3 CHAIRMAN BROWN: And there was no control

4 of access criteria.

5 MR. CONCEPCION: Or no guidance for repair,

6 because there is no reg guide or additional guidance

7 associated with those two topics beyond what's in 603.

8 CHAIRMAN BROWN: Other than what's in 603,

9 okay. All right. Thank you. That's consistent now

10 with what you said that these are cumulative.

11 MR. CONCEPCION: Right.

12 CHAIRMAN BROWN: That would be helpful if

13 that was added.

14 MS. STAREFOS: We will make that clearer.

15 Thank you for that.

16 CHAIRMAN BROWN: Okay.

17 MR. CONCEPCION: And I'm going to make

18 another relationship between IEEE 603 and 7-4.3.2. You

19 have those complimentary standards because you have the

20 requirements in 603. But if you use computer systems,

21 you have to refer to 7-4.3.2.

22 So, that shows up in those areas where there

23 is specific guidance associated with certain topics in

24 7-4.3.2 as additional or cumulative.

25 CHAIRMAN BROWN: I didn't look at them that

1 way. Now, I - as long as I understand the process, the
2 metric, that works. You've eliminated a bunch of other
3 notes that I had throughout here.
4 MS. STAREFOS: And we'll add that to our
5 clarification in the -
6 CHAIRMAN BROWN: 7.0 or whatever or
7 someplace.
8 MS. STAREFOS: Yes, we intend to actually
9 have a preface or introduction to the table that talks
10 about how we're going to use this, what the point was
11 and how we developed it.
12 CHAIRMAN BROWN: This is like Chapter 1 or
13 something?
14 MS. STAREFOS: Kind of like a preface to
15 Chapter 1 of the DSRS. And it will explain all of this.
16 And that's the perfect place for that.
17 And perhaps even the standard details that
18 you had pointed out that earlier that repeat throughout.
19 CHAIRMAN BROWN: Okay.
20 MS. STAREFOS: Thank you.
21 CHAIRMAN BROWN: All right. So, when we see
22 this the next time, all that other stuff is going to
23 disappear and we're not going to know where it went.
24 The black hole, right?
25 MS. STAREFOS: I can't make those promises

on -

CHAIRMAN BROWN: Because we haven't seen Chapter 1 yet.

MS. STAREFOS: - the record, but I will do my best.

CHAIRMAN BROWN: Okay. Onwards and upwards. I don't have anymore now that you've - that eliminated some of my other comments then.

MR. CONCEPCION: Great.

CHAIRMAN BROWN: So, we can go on to whatever the next slide is, which is the summary, I guess.

MR. CONCEPCION: I have a blank slide. I don't know if it is relevant at all, but -

MR. SANTOS: I think it's important because some of the feedbacks we've gotten is to add additional content in some areas.

CHAIRMAN BROWN: Add additional what?

MR. SANTOS: Additional context regarding some topics.

CHAIRMAN BROWN: You mean the references?

MR. SANTOS: No, no. What I'm trying to say is we could add references to help address some of those comments.

CHAIRMAN BROWN: Oh, all you're saying is you could add more to what you've already done.

1 MR. SANTOS: Yes.

2 CHAIRMAN BROWN: I mean, there's a list of

3 references right now.

4 MR. SANTOS: So, that could be our -

5 CHAIRMAN BROWN: But remember in the - excuse

6 me. I'm going to use this word again. In the context

7 of what you're trying to do in terms of putting stuff

8 in places where they'll see it and not have to refer

9 off, there probably is some subset of information in

10 the reference that you want to put in while you would

11 then say - and then either hit the reference for the

12 Reg Guide or whatever the other reference is if that's

13 necessary.

14 But you need to flag it somehow as opposed

15 to just let it be going around in the cloud.

16 MR. SANTOS: I agree.

17 CHAIRMAN BROWN: I said that on purpose.

18 MR. CONCEPCION: Okay. So, this is my

19 summary slide. We understand that we're breaking

20 ground with this new approach. There are some things

21 that we still have to improve in the content of the DSRS,

22 some areas that need to be expanded, some clarifications

23 that we need to consider, but that's why we're here.

24 I believe we've accomplished what we

25 intended to do. This document is still in the process

1 of being evaluated or considered by the public. We're
2 still in the process of collecting that feedback,
3 processing that feedback and also factor that into the
4 content of a document to make it better.
5 And hopefully by the next time that we
6 publish this document, it's in a better shape to be ready
7 to be used and implemented by some of us who will be
8 around to implement it.
9 (Laughter.)
10 CHAIRMAN BROWN: Are you implying you're
11 going to be gone, or are you waiting for me to be gone?
12 MR. CONCEPCION: I don't know.
13 We will continue - we will hope to continue
14 interactions with ACRS. Like I said, we will maintain
15 that - the same level of interactions we have had with
16 B&W and look forward to additional interactions with
17 this committee, and also with members of the public.
18 CHAIRMAN BROWN: Okay, question. We've
19 gone through and there have been a number of - you've
20 taken some action items, notes, whatever you want to
21 consider them to be that you will consider.
22 And before we - you asked if you could
23 address those, and we'll be happy to have you run through
24 those.
25 And after you do that, it would be - we would

1 appreciate it if you would send a copy to Christina of
2 that written down so that she can send them to us and
3 we'll at least have our memory - old memories calibrated
4 on what you're thinking about.
5 And I guess my next question after that is
6 if you're going to be doing something, you're going to
7 be then issuing this for final - in final for comment
8 to the public and I'm thinking back to the schedule.
9 This is November the 16th. So, what's the
10 time frame for trying to take into consideration these
11 astute observations that we've made during the meeting
12 and getting them into this before they go back out for
13 comment, or would they be subject to incorporation after
14 you get public comments back?
15 Don't shake your head up and down yet.
16 You're not supposed to telegraph what was said.
17 MS. STAREFOS: I would say it depends, but
18 I think right now we're pretty close to the end of having
19 gone through our concurrences by our high levels of
20 management and our Office of General Counsel.
21 In order to do this, reiterate or
22 reevaluate, we would have to revisit that again through
23 concurrence and OGC.
24 So, it would probably work out better for
25 us if we could delay and incorporate that at the point

1 where we were incorporating all of the comments from
2 the members of the public as well, and then revisit that
3 with you at that stage.
4 Would that be acceptable?
5 CHAIRMAN BROWN: Well, no, I think that would
6 - I think that's reasonable.
7 MS. STAREFOS: Okay.
8 CHAIRMAN BROWN: And the thing I would like
9 to have before we have our December 6th meeting, full
10 committee meeting, at least to have a copy of the notes
11 or -
12 MS. STAREFOS: Absolutely.
13 CHAIRMAN BROWN: - action items, if you
14 want to call it, so that we just have something in hand
15 not completed, just what you agree to at least think
16 about subsequently.
17 MS. STAREFOS: Yes, we'll commit to that.
18 You will absolutely have that.
19 CHAIRMAN BROWN: That's about three weeks
20 away.
21 MS. STAREFOS: That's not a problem.
22 CHAIRMAN BROWN: Again, I'm not asking for
23 how you intend to resolve them or whatever, but just
24 that you're cognizant of them.
25 MS. STAREFOS: You have quite a list. I'm

1 not sure you'd understand my henscratch here.

2 CHAIRMAN BROWN: Milt said he's going to run

3 through some.

4 MS. STAREFOS: I know that we need to kind

5 of work together to get a collective list. So, we'll

6 do that and get it to Christina.

7 CHAIRMAN BROWN: And if you want to collect

8 your stuff afterwards and add stuff to it, but you wanted

9 to go through something now, or did you want to do it

10 later? What did you want to do?

11 MR. CONCEPCION: Whatever works for you.

12 CHAIRMAN BROWN: We've got some time if you

13 want 15, 20 minutes to walk through a list. You could

14 run through it briefly.

15 MR. CONCEPCION: Yes, sure. Absolutely.

16 MEMBER SIEBER: I think you have more that

17 went on during this meeting than you would produce in

18 the list. On the other hand, I think maybe staff can

19 figure out what they agree to and not agree to -- you're

20 going to need the transcript.

21 CHAIRMAN BROWN: Okay. So, that's a good

22 idea. So, you all want to go ahead and think about this

23 after the meeting and -

24 MS. STAREFOS: That would be best for us.

25 CHAIRMAN BROWN: - put together this stuff?

1 MS. STAREFOS: Yes, sir.

2 MEMBER SIEBER: That brings up another

3 question. If you're going to use the transcript as the

4 basis for our comments to you for updating after public

5 comments, you probably won't need a letter for the

6 December meeting, right?

7 CHAIRMAN BROWN: Yes, it's a question of what

8 you all expect to see. I mean, we can wait until after

9 public comments if you so desire to get a letter.

10 MS. STAREFOS: Can we discuss that in -

11 MEMBER STETKAR: The Committee decides

12 whether we issue a letter.

13 CHAIRMAN BROWN: Well, I guess that's true.

14 MS. STAREFOS: Yes.

15 CHAIRMAN BROWN: Whether you want one or not,

16 we may decide to issue one.

17 MEMBER STETKAR: Okay.

18 CHAIRMAN BROWN: Well, I mean, I'm sorry.

19 I'm learning how the process works here. That's why

20 I keep getting corrected all the time.

21 We won't make a decision on that, but go

22 ahead and do that and you could at least just get us

23 the list -

24 MS. STAREFOS: Absolutely.

25 CHAIRMAN BROWN: - of what you think is

1 there to work on or not work on. We'll then wait to
2 try to see what's done after the public comment period
3 and you're ready for the next step.
4 We'll figure out what we're going to do in
5 the interim period relative to letters or no letters.
6 MS. STAREFOS: Okay.
7 MR. SANTOS: This is Dan -
8 CHAIRMAN BROWN: Hold on. Jack.
9 MEMBER SIEBER: Just keep in mind that you're
10 going to have to prepare the letter before you make the
11 decision as to whether -
12 CHAIRMAN BROWN: Yes, I know. I always have
13 to do stuff when I'm sleeping. I'll figure out a way
14 to do that and then we can accept or reject the
15 suggestions as we go. That's my job.
16 MR. SANTOS: This is Dan here -
17 CHAIRMAN BROWN: Hold it, Dan.
18 MS. ANTONESCU: We have a short meeting or
19 presentation scheduled for the full committee meeting
20 on December 6.
21 CHAIRMAN BROWN: Yes. I mean, if they
22 wanted to address some of our comments then, they can.
23 If they're not ready to and they want to do it after
24 public comment, they can do that also. I just want to
25 make sure we get what we've gone through.

1 MS. ANTONESCU: It's kind of a short time
2 for them to prepare.
3 CHAIRMAN BROWN: One other point is for the
4 full committee meeting, we obviously have to shorten
5 this up a little bit. Hadn't really thought about where
6 to shorten, but that's always the issue.
7 MR. CONCEPCION: And I don't have the
8 strategy of how to do it.
9 CHAIRMAN BROWN: Do one. One, two.
10 MEMBER SIEBER: Could you make a day only
11 an hour long?
12 CHAIRMAN BROWN: I would focus on the - well,
13 a schedule. You've got to get a schedule. We've got
14 to have a schedule presented, okay, as part of the full
15 committee meeting. That's easy. You got one.
16 And I guess I would focus on 7.0, 7.1, 7.2.
17 In other words, the independence, you know, in other
18 words, the four principles.
19 MEMBER BLEY: Principles, and I'd get
20 something in on the hazard analysis.
21 CHAIRMAN BROWN: Yes, that was the other one.
22 MEMBER BLEY: Something short that says
23 where you want people to head. Not what you don't want
24 them to do, but what you want them to do.
25 CHAIRMAN BROWN: And in 7.1.2, you - in that

7.1.1 through 7.4.5, you can cover architecture as well. I wouldn't do that one separate.

The simplicity one, I think you ought to have a slide on the concept of incorporating simplicity as a thought process as something to be considered doing the design.

So, those are the pieces. I guess that's where I would focus the full committee meeting on. Any disagreements, Jack, Dennis, John?

MEMBER BLEY: No, no, I think that's right.

MR. CONCEPCION: Let me see if I understand correctly what you just stated. You want us to present in addition to a schedule which we already have, you want us to present 7.0, 7.1, 7.2 and the three appendices.

CHAIRMAN BROWN: Only something if - okay, let's start back.

We're only going to cover what we talked about today. You don't have to -

MEMBER SIEBER: A subset of that, yes.

CHAIRMAN BROWN: It will be a subset of that. And the subset should be part of the overall, the lead-in to 7.1 - or 7.0, 7.1, however the - and then 7.1.1, two, three, four, five.

MR. CONCEPCION: The principles.

1 CHAIRMAN BROWN: The principles. And then
2 a little bit on - talk about the hazards, Appendix A,
3 and something on simplicity since that's a new - that's
4 kind of new concept that we ought to throw that out at
5 least, get the members' reaction.
6 MEMBER BLEY: But that's probably a slide.
7 CHAIRMAN BROWN: That's 7.1.1 or two.
8 MEMBER STETKAR: I think the message is 7.2
9 in its entirety doesn't need to be discussed.
10 CHAIRMAN BROWN: Exactly. Thank you.
11 MR. CONCEPCION: I got it.
12 MEMBER SIEBER: I think it's okay to mention
13 simplicity that is qualitative rather than
14 quantitative.
15 CHAIRMAN BROWN: Yes, well, that's the whole
16 point.
17 MEMBER SIEBER: The philosophy as opposed
18 to something you could measure.
19 CHAIRMAN BROWN: Well, that's very clear
20 from reading Appendix C.
21 MEMBER SIEBER: That's right.
22 MR. SANTOS: Mr. Chairman, this is Dan here.
23 CHAIRMAN BROWN: Go ahead.
24 MR. SANTOS: Going back to the question of
25 the letter, clearly we will coordinate through our

1 project office. I'm just going to offer from the
2 technical staff perspective only for consideration is
3 that even the significance of this work, it is our
4 opinion from the technical staff that getting some sort
5 of high-level letter that provides some feedback on the
6 general direction of the effort would be very valuable
7 to the staff. And we'll coordinate the projects.
8 CHAIRMAN BROWN: Yes, that's fine. I
9 understand your point. I'm not going to commit the
10 Committee to anything right now.
11 MEMBER BLEY: Because you can't.
12 (Laughter.)
13 CHAIRMAN BROWN: I'd like to walk out of the
14 full committee meeting still on two feet.
15 MEMBER STETKAR: Voice of experience.
16 CHAIRMAN BROWN: Well, I've learned that.
17 It's been hard.
18 MR. CONCEPCION: How much time do we have
19 on December 6, you said?
20 CHAIRMAN BROWN: You probably have, what?
21 An hour and a half.
22 MEMBER SIEBER: An hour and a half or less.
23 MS. ANTONESCU: And hour and 25 minutes.
24 CHAIRMAN BROWN: No, you're going to make
25 sure we get an hour and a half - no, an hour and 25.

1 Why is it only - oh, it's at 8:35 to 10:00.

2 MS. ANTONESCU: Antonio's schedule.

3 MEMBER BLEY: You can go to P&P, Charlie.

4 CHAIRMAN BROWN: No.

5 MEMBER SIEBER: The Chair has to give his

6 introductory remarks.

7 CHAIRMAN BROWN: Okay. We've covered the

8 comments, what you all do with those. We'll wait until

9 after public comment to get resolution. We discussed

10 what to do in full committee. We've got a picture of

11 what that is.

12 If you've got questions, just contact

13 Christina and she'll fire it off and we'll think about

14 it if you need anything else.

15 And I guess next on the agenda if we're -

16 MS. ANTONESCU: Open the lines.

17 CHAIRMAN BROWN: Well, keep the line closed

18 right now.

19 MS. ANTONESCU: Okay.

20 MR. CONCEPCION: We have two individuals

21 from the public that wanted to -

22 CHAIRMAN BROWN: I understand that. I was

23 going to call right now to see if there's any folks out

24 here that would like to make a public comment. We have

25 a microphone.

1 Go ahead and announce who you are and where
2 you're from.
3 (Pause in the proceedings.)
4 (Discussion off the record.)
5 DR. BIRLA: Just to give you a few tidbits
6 that I missed in answering Dennis' question earlier,
7 when you were talking about NUREG/CR-6101-1993 so old
8 -
9 MEMBER BLEY: Well, that was my copy.
10 DR. BIRLA: Right. But in that same spirit,
11 there is another old NUREG, software hazard analysis,
12 that I would like to mention because in a NASA safety
13 systems handbooks, that NUREG has been cited as an
14 excellent piece of work. But, again, that NASA handbook
15 is also very old.
16 So, recognize that at that time, those
17 pieces of work were considered very highly. But also
18 as you pointed out earlier today, so much has happened,
19 technology changes and the new knowledge, that we have
20 to revisit that.
21 MEMBER STETKAR: Yes, I think that's the
22 basic concern. So much has transpired in the last 20
23 years.
24 DR. BIRLA: That's why NRO issued the UNR,
25 user need request, to research to undertake this work.

1 On the EPRI side, I forgot to mention a
2 couple of other events that they planned. I mentioned
3 a research activity in progress on which in a few months
4 we expect a report out.
5 Following that report, we have plans to
6 conduct the workshop. Again, this whole idea of how
7 do you get the learning curve and a training package.
8 So, in the training package right now from
9 the Office of Research at the NRC and the research team
10 in EPRI, we are exploring how we can synergize.
11 MEMBER STETKAR: I was going to ask you that.
12 I know you've mentioned that it's under the MOU that
13 you've been informed of this, but were you actually
14 working more closely together than just keeping abreast
15 of what they're doing?
16 DR. BIRLA: First of all, remember four years
17 ago we were on diametrically opposed viewpoints, if you
18 remember. We have made a significant turn. We are on
19 the same wavelength. That's a great accomplishment.
20 And now we have to move forward in synergy without
21 commingling resources. You understand these.
22 MEMBER STETKAR: Sure, sure.
23 DR. BIRLA: And my director of engineering
24 at the Office of Research is very supportive of this
25 kind of collaboration.

1 So, we are watching our Ps and Qs. We hope
2 to get there in the training program.
3 MEMBER STETKAR: Is there any notion of
4 issuing a joint NUREG as has been done for other issues,
5 you know? A NUREG/EPRI report or -
6 DR. BIRLA: I would not like to do that.
7 MEMBER STETKAR: Okay.
8 DR. BIRLA: I would like - let me tell you
9 what my vision is. My vision is that in this particular
10 matter, industry takes the lead. And just as in the
11 seismic hazard analysis. And say, hey, we have a better
12 way and this is what we like the NRC to take home.
13 So, they need some independence in that
14 respect rather than get associated with the regulator.
15 MEMBER STETKAR: Okay.
16 DR. BIRLA: But in terms of sharing knowledge
17 and exercising synergy, yes, that's going on.
18 MEMBER STETKAR: At least you know you're
19 not diametrically opposed anymore.
20 DR. BIRLA: That's right.
21 MEMBER STETKAR: That's important.
22 DR. BIRLA: That's right. Just a matter of
23 how do you synergize watching the Ps and Qs.
24 MR. SANTOS: And we in the licensing office
25 are being invited by research. So, we have been

1 observing some of these interactions realtime. So,
2 it's not like research is out on their own. We are very
3 connected too.
4 DR. BIRLA: So, just to give you an idea on
5 that research information letter on review guidance for
6 hazard analysis that research is working on, in the
7 beginning of October Research gave a presentation under
8 the MOU to the EPRI research team and a couple of their
9 advisors from industry.
10 And the reaction of one person from a
11 utility company who's got 30 years of experience was,
12 this is good guidance. Why does it have to be limited
13 to safety systems? If I have this - the freedom, I would
14 apply to every I&C system on the planet.
15 There was another individual on the EPRI
16 research team, contract support team who's also got more
17 than 30 years of experience. His reaction was, this
18 piece of work is so comprehensive. I've never seen all
19 this put together in one place.
20 So, those are a couple of examples or
21 getting on the same wavelength.
22 MEMBER BLEY: We look forward to seeing that.
23 That sounds interesting.
24 CHAIRMAN BROWN: You all finished now?
25 MEMBER BLEY: Yes.

1 CHAIRMAN BROWN: We'll proceed on with the
2 public comments, I believe. What order do you want to
3 go in?
4 Peter Hastings, are you on the line? Just
5 say something.
6 MEMBER STETKAR: For confirmation if anyone
7 is out there, just say something, please. We really
8 don't know whether the line is actually open.
9 CHAIRMAN BROWN: Well, something clicked off
10 while they were talking. It sounded like somebody -
11 MEMBER SIEBER: I heard a beep.
12 CHAIRMAN BROWN: I head a beep.
13 MEMBER SIEBER: I don't know what that means.
14 (Discussion off the record.)
15 MEMBER STETKAR: Thank you very much. We
16 now know the line is open.
17 CHAIRMAN BROWN: Who was that? NuScale,
18 okay. Thank you. So, the line is open.
19 MEMBER BLEY: Mr. Hastings, have we got -
20 CHAIRMAN BROWN: Is Peter Hastings there?
21 (Discussion off the record.)
22 MR. ARNHOLDT: My name is Brian Arnholdt.
23 I'm with B&W. I'm the manager for I&C design and
24 simulation and just appreciate the opportunity to come
25 here today and hear the interaction with the ACRS staff

1 and the NRC staff.

2 We've been working with the NRC staff, oh,

3 for the better part of this year on the DSRS effort for

4 the entire program.

5 We've provided several comments back to

6 about 25 sections of 40 that have been issued for the

7 entire program.

8 I'll jump right into the Chapter 7 issue,

9 because that's my area of purview. We had a meeting

10 with the staff back in June, looked at Section 7.1, one

11 of the appendices in 7.0, provided them comments back.

12 Actually had a really good public meeting

13 with them. I think the staff has been very receptive

14 to our feedback and other feedback.

15 Some specifics as far as how we see this

16 DSRS effort affecting us in our application with respect

17 to Chapter 7, I think it gives us a clearer line of sight

18 to an application submittal.

19 There was a lot of dialog about the level

20 of detail that we need and we're vetting that internally.

21 We've given that comment back to the staff.

22 I think as we work through, we're actually

23 generating content right now based on the framework

24 internally, reviewing it internally. Hope to share

25 that with the staff soon so we can start getting a dialog,

1 hey, this is the right level of detail, but we need more
2 here.
3 A couple comments about the hazards
4 analysis. We have the exact same comment back to the
5 staff as what are you looking for in a hazards analysis?
6 There's a lot of good practices out there
7 and a lot of different industries. I heard HAZOPS for
8 chemical industry.
9 We've got some thoughts internally about
10 what we want to do that I won't share publicly, but I
11 think - I agree working with the staff. I think if we
12 come up with a method and actually demonstrate from an
13 integrated system standpoint, we can make our case more
14 clear instead of focusing at the component level how
15 a card fails, how a channel fails.
16 If you look at it integrated across the
17 system and its interaction with the plant, I think the
18 approach is sound.
19 Just a couple of things. The way the DSRS
20 is structured, it was actually fairly coincidental.
21 It actually lines up quite well with the systematic
22 engineering approach we've applied to our I&C design
23 and architecture.
24 So, when we met with the staff and we've
25 given them updates and shared a lot of information with

1 them, they shared information with us on the framework
2 that they were planning for the DSRS and they actually
3 lined up quite nicely.
4 And right now as we speak, we are making
5 some design changes based on content that the staff has
6 put into the DSRS. So, that helps us put material in
7 front of the staff that hopefully will facilitate a more
8 efficient, effective review. So, that's - I think it
9 remains to be seen, but I think we're on a clear path
10 for that.
11 And then lastly, the thought fundamental
12 design principles, that really has - we spent a lot of
13 time in the last couple of months focusing on how do
14 high-level architecture elements meet those fundamental
15 design principles?
16 We shared a series of information with the
17 staff and we're going to continue to build that into
18 our design, but I think that gives us a way to more
19 straightforwardly focus our application material to
20 facilitate a more focused review.
21 So, that concludes my comments. Thank you.
22 CHAIRMAN BROWN: Okay.
23 (Discussion off the record.)
24 CHAIRMAN BROWN: Okay. Is there anybody
25 else in the audience that would like to make a comment?

1 MR. GRAHAM: Good day. Chris Graham with
2 Safeware Engineering. And we're going to be working
3 on the RAL 1101.
4 Today, my comments are more from me as a
5 citizen. I was an NRR reviewer back about ten years
6 ago here at NRC. And I see - what I've seen today of
7 how the SRP is being repackaged and condensed, one of
8 the things that concerns me is there still doesn't seem
9 to be a system level approach to making sure that these
10 interactions that need to occur between the Chapter 7
11 and things such as human factors.
12 I know when I was a reviewer, there's things
13 that I need to review in human factors, and there are
14 things that the human factors folks need to review.
15 The human factors folks can tell you where
16 switches need to go, what color the light needs to be,
17 alarm prioritizations. But me as the I&C reviewer,
18 needs to verify that those requirements are instantiated
19 and largely now they'll be instantiated in software.
20 And so, moving those requirements just to another
21 section may not cause that interrelation.
22 Ten years ago there was no one forcing me
23 as a reviewer to make sure I interacted with the
24 electrical folks doing Chapter 8.
25 The electrical folks now have to deal with

software in their breaker control such as undervoltage, overcurrent. Those are going to be oftentimes software setpoints.

So, I get the impression today that there's going to be a forcing function to require these interrelations. So, my suggestion is that we have a system - that you consider at least a system level approach to ensure that these interactions - I&C is not in a vacuum. It goes in a specific system, goes on a specific skid, goes into specific housing. And to fob off those requirements like environmental qualification, some of those we in the I&C world, some of those the other folks did.

I'm talking a little bit too much here. Sorry. I'm just trying to - I just didn't see a forcing function that's going to require these interrelations to occur. And this is a great opportunity for the NRC to for me as a reviewer back ten years ago, try to sort out to make sure that I go talk to the human factors folks, I go talk to electrical.

That's my comment. Thanks very much.

CHAIRMAN BROWN: Anyone else from the audience.

MEMBER BLEY: Or on the phone.

CHAIRMAN BROWN: Hearing none, is there

1 anybody on the phone that would like to make a comment?
2 (No response.)
3 CHAIRMAN BROWN: Now, no people are still
4 on the phone; is that correct? Somebody answer just
5 to make sure you're still - I heard a pop. Are you all
6 still there?
7 PARTICIPANT: Yes, NuScale is still here,
8 yes.
9 CHAIRMAN BROWN: Okay.
10 PARTICIPANT: Thanks for letting us listen
11 in. We appreciate it.
12 CHAIRMAN BROWN: Okay. Thank you very much.
13 Hearing nobody on the phone line that wants to make
14 any additional public comments, I guess I'll close the
15 meeting - oh, no, I'm sorry. I forgot the important
16 part. The members.
17 MEMBER STETKAR: You just don't have enough
18 subcommittee meetings, Charlie.
19 (Laughter.)
20 (Discussion off the record.)
21 MEMBER STETKAR: No, I don't have anymore.
22 I'd like to thank the staff. I think you've covered
23 a lot of material in the time, clarified a lot of
24 information. And look forward to seeing what it looks
25 like after the public comment period.

1 CHAIRMAN BROWN: Dennis.

2 MEMBER BLEY: I liked what I've read. I
3 liked what I heard today. Primarily, I think it all
4 hangs together pretty well. I think they're well on
5 their way for a pilot that will maybe evolve into
6 something even better.

7 On the last commenter, I like what I hear
8 about these interactions and I'd like to see something
9 that really ensured that. And right now I think it's
10 happening, but it comes and goes over time.

11 CHAIRMAN BROWN: jack.

12 MEMBER SIEBER: Well, I'd like to thank the
13 staff also. I think that this subject is very complex.
14 It's got a lot of little pieces. And to try to pull
15 it altogether in a framework that's manageable, I think,
16 is an accomplishment. And I think you're well on your
17 way to doing that.

18 And so, I don't see any fatal flaws in the
19 direction that you're taking. And I think there may
20 be a little difference between my idea of what the detail
21 is and others mainly because I like detail and it's
22 easier for me to understand what's going on when I see
23 it.

24 Your reviewers, I'm sure, have seen these
25 things over and over again and can make decisions based

1 on more functional documentation.

2 But overall, I think this was a very

3 productive meeting. I think the staff has done well

4 in this project and I wish them great success.

5 CHAIRMAN BROWN: Okay. As the chairman, I

6 would like to echo what everybody else said. I'm not

7 going to repeat it ad nauseum here, but this was a

8 substantial effort.

9 And in my view since I've come here, this

10 is a substantial - I don't want to say reorientation

11 in terms of how you approach a complex design with the

12 new software-based systems and how you come to a

13 conclusion in a rational, well-documented basis that

14 it will meet the fundamental principles and deliver,

15 you know, the safety actions that you need for these

16 plans.

17 I thought the organization was put together

18 pretty well. It was readable, which was in English.

19 That's what I meant by that. You could actually

20 understand it, which was very useful.

21 And I think you all did a very good job of

22 putting this together and obviously there's some ways

23 to go. And I'm sure you'll get some more very

24 enthusiastic comments from the public when this is

25 issued.

1 And there's a lot of players that are going
2 to want to dabble with this and I fundamentally think
3 that this is pretty significant and that it sets the
4 boundaries for consideration of how to expand this
5 concept to a general thought process and a standard
6 review plan as well in the long run.
7 So, I wanted to thank you all. I think you
8 all did a good job. Those were good conversations.
9 A lot of interaction. You were very straightforward
10 and were not hesitant to give us answers that we may
11 or may not have wanted to hear.
12 And since I've messed up already, I'll mess
13 up again and I'll pass it - I'll ask Mohammed if he would
14 like to say anything else here.
15 MR. SHUAIBI: I do. I just want to thank
16 the committee. We appreciate all of your comments.
17 It's obvious that you're going through the material in
18 detail. We do appreciate that. We're taking back your
19 comments. We take them seriously. We are going to go
20 back and try to incorporate those.
21 And at some point in time we'll come back
22 to you and share with you this is what we've taken, this
23 is what we'll put in, this is the logic for the ones
24 - if we decide not to take any, this is the logic for
25 why that didn't go in.

1 So, I'm sure we'll have that dialog in the
2 future. I want to make sure that you get a sense of
3 how seriously we take those comments and will come back
4 and share that with you.
5 So, again, thank you for your time and for
6 your efforts in working through our guidance documents.
7 CHAIRMAN BROWN: Okay. One last point. I
8 hope you will get at least the notes to us before the
9 meeting. No answers necessary, but at least so that
10 we'll have them to jigger our thoughts when we get there,
11 okay?
12 With that, am I missing something? We'll
13 close the meeting. Thank you.
14 (Whereupon, at 4:15 p.m. the meeting was
15 adjourned.)
16
17
18
19
20
21
22
23
24
25

1
2
3
4
5
6
7
8

An Update on the Initiative for the Licensing Review of Instrumentation and Controls (I&C) for the mPower™ Small Modular Reactor Design

Milton Concepcion, Sr. Digital I&C Engineer
Division of Engineering
Office of New Reactors

Ian Jung, Chief
Instrumentation and Controls Branch
Division of Engineering
Office of New Reactors

Dan Santos, Senior Technical Advisor
Division of Engineering
Office of New Reactors

November 16, 2012

Objectives

- Provide a briefing on the draft mPower™ Chapter 7 Design Specific Review Standard (DSRS)
- Receive feedback from the Committee

Agenda

- DSRS Status and Schedule
- DSRS Chapter 7 Goals
- DSRS Key activities
- Background
- DSRS Development Process
- Section 7.0, “Introduction & Overview of Review Process”
- Section 7.1, “Fundamental Design Principles”
- Appendix A, “Evaluation of Hazard Analysis”
- Appendix B, “I&C System Architecture”
- Appendix C, “Simplicity”
- Section 7.2, “System Characteristics”
- Appendix D, “References”

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

DSRS Status and Schedule

Approximate Timeline for Finalizing the mPower Design Specific Review Standard (DSRS)

September 2012~	Draft mPower DSRS is completed and labeled *For Interim Use and Comment*
October 2012~	Internal Concurrence; OGC NLO obtained
November 2012~	Federal Register Notice FRN is prepared and mPower DSRS is issued for public comment • Document and Memo sent to **ACRS** • Document and Memo sent to CRGR • Notice sent to OMB for Congressional Review Act review
February 2013~	Public Comment Period Ends
March -August 2013~	Resolve Public Comments revise document as appropriate Prepare Final mPower DSRS Document
May 2013~	SRP Updates Finalized to Support mPower DC Review *(coincides with APOB schedule)*
September 2013~	Internal Concurrence; OGC NLO obtained **ACRS** letter received
November 2013~	Prepare FRN and issue final *mPower DSRS* • Document and Memo sent to **ACRS** • Document and Memo sent to CRGR

Top DSRS Goals

By applying lessons learned in a timely manner

1. Enhance safety focus of staff reviews
2. Improve review efficiency

Background

- Licensing reviews of I&C have been a significant challenge from the perspective of both safety demonstration and schedule/resources for all design centers for new large light water reactors
- Industry has consistently expressed licensing certainty of I&C to be one of their highest priorities for new reactors
- The staff examined lessons and identified areas that can support the goals

Background (continued)

- The core of the DSRS Chapter 7 approach is based on the concept of applying proven system engineering principles (under the current regulatory framework):
  - Defense-in-depth
  - Design principles
  - Simplicity attribute
  - Integrated hazards
  - Technology neutrality
- The approach is further aided by structural changes in guidance for clarity and efficiency

DSRS Development Process

- Reorganize review guidance to separate design principles from specific system requirements
- Provide guidance on Fundamental Design Principles at system level
- Remove redundant and non-applicable information
- Eliminate the use of DAC
- Introduce Simplicity and Hazard Analysis
- Ensure adequate coverage of regulatory requirements and applicable guidance

Review process

- Reviewers who have used the existing SRP provided the horsepower to accomplish these actions.
- Reviewers from other disciplines were enlisted to help eliminate overlapping review responsibilities.

DSRS Development Process

Reorganize review guidance to separate design principles from specific system requirements

Provide guidance on Fundamental Design Principles at system level

Remove redundant and non-applicable information

Eliminate the use of DAC

Introduce Simplicity and Hazard Analysis

Ensure adequate coverage of regulatory requirements and applicable guidance

DSRS Results

Improve the safety focus of the staff reviews by ensuring the licensing application has sufficient detail to clearly demonstrate that the applicable regulations are met and key design principles are addressed.

SRP Chapter 7

- The "Independence" design principle is addressed in 23 of the 36 distinct pieces of the SRP.
- Information needed to perform review of the application is not explicitly stated.

DSRS Chapter 7

- The "Independence" design principle is addressed in one location.
- Review of design information, including functional block diagrams, descriptions of operation, and architectural descriptions.

DSRS Results

Organize the review material so that it aligns well with integrated I&C designs.

SRP Chapter 7

- Review guidance was presented on a system basis. As systems evolved, Branch Technical Positions were issued to document additional guidance. Limited cross referencing was provided.

DSRS Chapter 7

- Fundamental design principles segregated to Section 7.1.
- System Characteristics segregated to Section 7.2.
- All BTPs have been incorporated in the guidance.

DSRS Development Process

Reorganize review guidance to separate design principles from specific system requirements

Provide guidance on Fundamental Design Principles at system level

Remove redundant and non-applicable information

Eliminate the use of DAC

Introduce Simplicity and Hazard Analysis

Ensure adequate coverage of regulatory requirements and applicable guidance

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

DSRS Chapter 7 Structure

Areas Of Review	7.0 – Introduction and Overview	7.1 – Fundamental Design Principles	7.2 – System Characteristics
	• Review objectives • Review interfaces • Review process • Mapping of regulatory requirement to DSRS location	• Safety system design basis • Independence • Redundancy • Determinism • Diversity / Defense-in-Depth	• Quality • Equipment qualification • Reliability, Integrity , and completion of protective action • Operating and maint. bypasses • Interlocks • Derivation of system inputs • Setpoints • Auxiliary features • Control of access, identification, and repair • Interaction between sense and command features and other systems • Multi-unit stations • Automatic and manual control • Displays and monitoring • Human factors considerations • Test and calibration

DSRS Development Process

Reorganize review guidance to separate design principles from specific system requirements

Provide guidance on Fundamental Design Principles at system level

Remove redundant and non-applicable information

Eliminate the use of DAC

Introduce Simplicity and Hazard Analysis

Ensure adequate coverage of regulatory requirements and applicable guidance

DSRS Results

Improve the efficiency of reviews by eliminating unnecessary information from being docketed and reviewed, and by improving guidance to avoid unnecessary RAIs.

SRP Chapter 7	DSRS Chapter 7
• Included IEEE Std. 279.	• Removed reference to IEEE Std. 279 since it only pertained to pre-1995 licenses.
• 500+ pages (SRP & ISGs) of material including a considerable amount of background information and repetition.	• ~150 pages containing specific instructions to the reviewer.

Redundancy Examples

Examples of redundant review requirements between the SRP Chapters.

SRP Chapter 7	DSRS Chapter 7
"Human factors engineering principles and criteria should be applied to the selection and design of the displays and controls. Human-performance requirements should be described and related to the plant safety criteria. Recognized human-factors standards and design techniques should be employed to support the described human-performance requirements." (BTP 7-19 acceptance criteria)	This instruction was deleted after verification that it is included in Chapter 18.

DSRS Development Process

Reorganize review guidance to separate design principles from specific system requirements

Provide guidance on Fundamental Design Principles at system level

Remove redundant and non-applicable information

Eliminate the use of DAC

Introduce Simplicity and Hazard Analysis

Ensure adequate coverage of regulatory requirements and applicable guidance

DSRS Results

Eliminate the use of DAC

Chapter 7 information should be sufficient for NRC staff to address all safety questions at Design Certification stage without the use of DAC [design acceptance criteria] by the applicant.

DSRS Development Process

Reorganize review guidance to separate design principles from specific system requirements

Provide guidance on Fundamental Design Principles at system level

Remove redundant and non-applicable information

Eliminate the use of DAC

Introduce Simplicity and Hazard Analysis

Ensure adequate coverage of regulatory requirements and applicable guidance

DSRS Results

Provide guidance on new areas of review

The application of Hazard Analysis is described in Appendix A of DSRS Chapter 7.

The application of the “Simplicity” design principle is described in Appendix C of DSRS Chapter 7.

DSRS Development Process

Reorganize review guidance to separate design principles from specific system requirements

Provide guidance on Fundamental Design Principles at system level

Remove redundant and non-applicable information

Eliminate the use of DAC

Introduce Simplicity and Hazard Analysis

Ensure adequate coverage of regulatory requirements and applicable guidance

DSRS Chapter 7 Mapping Examples

Regulations	Location in DSRS
IEEE 603-1991*, Section 4, Safety System Designation	7.1.1 Safety System Design Basis 7.1.4 Determinism
IEEE 603-1991*, Section 5.1, Single-Failure Criterion	7.1.3 Redundancy 7.1.5 Diversity and Defense-in-Depth
IEEE 603-1991*, Section 5.2, Completion of Protective Action	7.2.3 Reliability, Integrity, and Completion of Protective Action
IEEE 603-1991*, Section 5.4, Equipment Qualification	7.2.2 Equipment Qualification
GDC 10, “Reactor design”	Coordinated with Chapter 4 of the DSRS
GDC 13, “Instrumentation and control”	7.1 and 7.2 of the DSRS

* 10 CFR 50.55a(h) approves use of IEEE 603-1991

Review Guidance Structure

- Existing Guidance
  - 7.0 Overall Review Process
  - 7.1 Introduction
  - 7.2 Reactor Trip System
  - 7.3 ESF Systems
  - 7.4 Safe Shutdown Systems
  - 7.5 Information Systems
  - 7.6 Interlock Systems
  - 7.7 Control Systems
  - 7.8 Diverse Systems
  - 7.9 Data Communication Systems
  - BTPs (7-1 to 7-21 & 8-5)
  - ISGs

- DSRS Chapter 7
  - 7.0 Overview of Review Process
  - 7.1 Fundamental Design Principles
    - Design Basis
    - Independence
    - Redundancy
    - Determinism
    - Defense-in-Depth and Diversity
  - 7.2 System Characteristics
  - Appendix A, Hazards Analysis
  - Appendix B, I&C System Architecture
  - Appendix C, Simplicity
  - Appendix D, References

mPower™ DSRS

7.0 Introduction & Overview of Review Process

- Establishes differences between SRP and DSRS
- Provides DSRS Review Scope, Objectives, Review Interfaces, and Review Process for I&C
- DSRS Table 7-1 provides mapping of regulatory requirements and guidance with review responsibilities

7.1 Fundamental Design Principles

- 7.1.1 Safety System Design Basis
- 7.1.2 Independence
- 7.1.3 Redundancy
- 7.1.4 Determinism
- 7.1.5 Diversity and Defense in Depth

mPower™ DSRS

DSRS 7.1

7.1.1 Safety System Design Basis

- Section 4 of IEEE Std. 603-1991
- Areas of review include:
  - Identification of the I&C systems' safety functions and corresponding protective actions
  - All monitored variables used to control each protective action
  - Minimum number and location of sensors required for protective purposes
  - Range of transient and steady-state conditions throughout which the safety systems shall perform
  - System performance
- Coordination with Chapter 15

7.1.2 Independence *(slide 1 of 3)*

- Section 5.6 of IEEE Std. 603-1991
- Review addresses the concepts of:
  - Physical independence
    - Physical separation and physical barriers
  - Electrical independence
    - Electrical isolation of safety system circuits and electrical equipment

7.1.2 Independence *(slide 2 of 3)*

- Section 5.6 of IEEE Std. 603-1991
- Review addresses the concepts of:
  - Communications independence
    - One-way communication should be used among redundant channels or divisions and between safety and non-safety systems.
    - Data flows between redundant portions of safety systems should be limited to those required for coincidence logic voting for actuation and interlocks used for the performance of safety functions.
    - A safety division should not be dependent upon any information or resource originating or residing outside its own division to accomplish its safety function.
    - Each safety division should receive plant data only from sensors dedicated to that division and that data should not be shared among divisions.
    - Review criteria for designs that implement sharing of data between trip processing units and voting unit processors, or among voting unit processors.

7.1.2 Independence *(slide 3 of 3)*

- Section 5.6 of IEEE Std. 603-1991
- Review addresses the concepts of:
  - Functional independence
    - Verify isolation of a safety system from other safety systems.
    - Successful completion of the system's safety functions should not be dependent upon any behavior (including failures and normal operation) of another system, or upon any signals, data, or information derived from the other system.

7.1.3 Redundancy

- Section 5.1 of IEEE Std. 603-1991
- Level of redundancy used to assure that:
  - No single failure results in loss of the protection function.
  - Removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.
- Review covers:
  - Single-failure criterion – RG 1.53.
  - Guidance for reviewing channel assignments to address redundancy and diversity requirements.

7.1.4 Determinism

- Evaluate real-time performance of the proposed digital I&C platform and data communications systems:
  - Verify that system timing derived from DBEs has been allocated to the digital I&C system architecture.
  - Confirm deterministic performance of data communications.
- Appendix B (I&C System Architecture) supports the review of determinism.

7.1.5 Diversity and Defense-in-Depth (D3) *(slide 1 of 2)*

- Acceptance Criteria used for D3 review:
  - SRM to SECY-93-087, Item 18.II.Q
  - NUREG/CR-6303
  - BTP 7-19
- Coordination with Human Factors and Reactor Systems branches to evaluate D3 assessment.
- This section also covers 10 CFR 50.62, the ATWS rule, which requires, in part, automatic initiation of ATWS mitigation systems and equipment that is diverse and independent from the reactor trip system.

7.1.5 Diversity and Defense-in-Depth (D3) *(slide 2 of 2)*

- Applicant shall provide a D3 assessment for the proposed I&C system that demonstrates that vulnerabilities to CCF [common cause failure] have been adequately addressed.
- Review of the D3 assessment addresses:
  - Identification of any vulnerabilities to CCF in the I&C system.
  - Analysis for each event that is evaluated in Chapter 15 with a postulated CCF using best-estimate methods.
  - Information to demonstrate that adequate diversity is provided.
  - Automatic and/or manual actions used as a diverse means.
  - Display and controls used for D3.
  - Prioritization between safety-related and diverse actuation signals.

mPower™ DSRS

App. A

Appendix A – Hazard Analysis

- New guidance provides an approach to review Hazard Analysis.
- Focus on verifying whether the applicant:
  - Identified and evaluated each loss or impairment of safety function.
  - Developed necessary hazard restrictions and controls in the form of architectural constraints.
- Provides a set of evaluation topics.
- Discusses ITAAC [inspections, tests, analyses, and acceptance criteria] for implementation activities.

Appendix B – I&C System Architecture

- Architecture description will support review of fundamental design principles.
- Review areas:
  - Description of all I&C functions that are part of the design basis.
  - Interfaces between I&C safety systems.
  - Safety to nonsafety interfaces.
  - Signal flows and descriptions.
  - Simplified/functional logic diagrams.

mPower™ DSRS

App. C

Appendix C – Simplicity

- Evaluate whether simplicity has been considered in the design of the digital I&C systems.
- Review concurrent with each fundamental design principles.
- Key factors for simplicity:
  - Logical, modular description of interactions, signal flows, definition of interfaces.
  - Separation or segregation among I&C functions.
  - Safety systems designed for only the minimal required functions.
  - Simplified communications and system integration.

mPower™ DSRS

DSRS 7.2

7.2 System Characteristics

- 7.2.1 Quality*
- 7.2.2 Equipment Qualification
- 7.2.3 Reliability, Integrity, completion of protective action
- 7.2.4 Operating and maintenance bypasses
- 7.2.5 Interlocks
- 7.2.6 Derivation of system inputs
- 7.2.7 Setpoints
- 7.2.8 Auxiliary features
- 7.2.9 Control of access, identification, and repair
- 7.2.10 Interaction between sense and command features
- 7.2.11 Multi unit stations
- 7.2.12 Automatic and manual control
- 7.2.13 Displays and controls
- 7.2.14 Human Factors consideration
- 7.2.15 Capability for test and calibration
- Hyperlink to DSRS 7.2

* Under Development

mPower™ DSRS

7.2.1 Quality (work in progress)

- Scope will address system engineering as well as software engineering – technical and quality requirements.
- Program description will address system/software engineering activities instead of reviewing project-specific plans.
- Leverage reviews conducted in Chapter 17, "Quality Assurance."

mPower™ DSRS

7.2.2 Equipment Qualification

- Scope addresses seismic and environmental qualification.
- I&C review of equipment qualification is limited to confirmation that I&C equipment (including isolation devices) subject to seismic and environmental qualification requirements has been selected and identified in the application.
- Review of Environmental Control Systems.
- Electromagnetic and Radio-Frequency Interference (EMI/RFI) – RG 1.180.
- Coordination with Chapter 3, equipment qualification sections.

Appendix D – References

Summary

- The staff has implemented lessons learned and restructured existing guidance in the development of the mPower™ DSRS Chapter 7 to:
  - Ensure clear line-of-sight from regulatory requirements to review guidance.
  - Enhance staff review focus.
  - Improve review efficiency.
  - Leverage NRC staff cross-organizational expertise.

Next Steps

- Issue draft DSRS for formal public comments.
- Continue ACRS interactions.
- Collect and resolve public comments.
- Continue pre-application interactions with B&W and other stakeholders.
- Issue final DSRS Chapter 7 to support the mPower™ application review.