

**Official Transcript of Proceedings**  
**NUCLEAR REGULATORY COMMISSION**

Title: Advisory Committee on Reactor Safeguards

Docket Number: (n/a)

Location: teleconference

Date: Friday, September 9, 2022

Work Order No.: NRC-2076

Pages 1-127

**NEAL R. GROSS AND CO., INC.**  
**Court Reporters and Transcribers**  
1716 14th Street, N.W.  
Washington, D.C. 20009  
(202) 234-4433

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S  
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

UNITED STATES OF AMERICA  
NUCLEAR REGULATORY COMMISSION

+ + + + +

698TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

FRIDAY

SEPTEMBER 9, 2022

+ + + + +

The Advisory Committee met via  
videoconference at 1:00 p.m., Joy L. Rempe, Chairman,  
presiding.

COMMITTEE MEMBERS:

- JOY L. REMPE, Chairman
- WALTER L. KIRCHNER, Vice Chairman
- DAVID A. PETTI, Member-at-Large
- RONALD G. BALLINGER, Member
- VICKI M. BIER, Member
- CHARLES H. BROWN, JR., Member
- VESNA B. DIMITRIJEVIC, Member
- GREGORY H. HALNON, Member
- JOSE A. MARCH-LEUBA, Member
- MATTHEW W. SUNSERI, Member

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

ACRS CONSULTANTS :

DENNIS BLEY

STEPHEN SCHULTZ

DESIGNATED FEDERAL OFFICIAL :

CHRISTOPHER BROWN

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

1:00 p.m.

CHAIRMAN REMPE: Okay, it's 1:00 p.m. on the East Coast, and we're back in session. And at this time, I'd like to ask Member Ballinger to lead us through the next topic.

MEMBER BALLINGER: Thank you, Madam Chairman. The topics this afternoon are from SHINE and the staff on cyber security, which is sprinkled throughout the documents and Chapter 14 on technical specifications. Let's see. The slides themselves, I don't see any slides that are closed --

CHAIRMAN REMPE: Ron, your mic is not on.

MEMBER BALLINGER: Rewinding, thank you, Madam Chair. And this afternoon we'll hear from SHINE and the staff on cyber security and Chapter 14 technical specifications.

The schedule calls for a closed session if needed. I don't see any slides from either the staff or SHINE that would be closed, so I suspect that unless we make some -- part of the discussion results in proprietary information being discussed, we will not need to have a closed -- closed session.

And let's see what else. I think that pretty much -- pretty much does it. I'll think we'll

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 do cyber security first, and it's up and the SHINE  
2 folks are here. So does the staff -- Josh, you want  
3 to make any statement?

4 MR. BORROMEO: Sure, my name is Josh  
5 Borromeo, I'm Chief of the NPUF Licensing Branch here  
6 at the NRC. So thank you, ACRS, for your continued  
7 review on this project. It's really important, and I  
8 feel like we're working well together moving things  
9 along.

10 So today you'll hear about cyber security.  
11 This is -- this is unique because it's the first time  
12 we're applying cyber security to an NPUF. So this is  
13 first time application of this.

14 You'll also hear about tech specs today as  
15 well. The interesting thing about this part of the  
16 review was we're merging the research test reactor  
17 ANSI standard tech specs with the power reactor tech  
18 specs. So you'll hear aspects of that.

19 And then the last thing that we're  
20 planning on -- well, SHINE is planning on discussing  
21 today is software life cycle development. We wanted  
22 to give you a head's up of where -- where that review  
23 was going.

24 The staff is still working on our safety  
25 evaluation for that. We're planning on presenting

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 that at the October Subcommittee meeting, but we just  
2 wanted to give you a head's up of a -- of a --

3 MEMBER BALLINGER: I think we have had  
4 brief discussions on that in the past, right?

5 MR. BORROMEO: Yeah, yeah, so at the  
6 Chapter 7 discussion, we touched on it. We'll touch  
7 on it again today, and that'll -- that'll come after  
8 the cyber discussion and the tech spec discussion.

9 MEMBER BALLINGER: And I just realized  
10 that we are lacking a key participant in this. Member  
11 Brown was here.

12 MS. ANTONESCU: I will try to get in touch  
13 with him, Ron.

14 MEMBER BALLINGER: Okay, thank you.

15 MR. BORROMEO: But that's all I have, and  
16 thank you for --

17 MEMBER BALLINGER: Thank you. So I think  
18 we should -- we should begin. And who's the presenter  
19 for SHINE?

20 MR. BARTELME: Good afternoon, this is  
21 Jeff Bartelme, I'll be -- I'll be presenting.

22 MEMBER BALLINGER: Oh, okay, all right,  
23 okay. Good enough. All right, I think we can  
24 proceed.

25 MR. BARTELME: Good afternoon again, this

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 is Jeff Bartelme, SHINE's Director of Licensing, and  
2 I'll be presenting on the cyber security plan.

3 Just going to go over the outline here.  
4 This afternoon we'll be discussion requirements  
5 related to the SHINE cyber security plan and SHINE's  
6 consideration of cyber security through the design of  
7 the SHINE facility. Provide an overview of the SHINE  
8 development plan.

9 We'll discuss SHINE's approach to defining  
10 consequences of concern. Discuss SHINE's process for  
11 identification of critical digital assets, or CDAs and  
12 determination of their associated cyber security  
13 controls. And then lastly we'll just touch on a  
14 number of -- a couple of additional programmatic  
15 considerations, which SHINE has incorporated into the  
16 cyber security plan.

17 In terms of requirements to develop plan,  
18 there's no regulatory requirement for a medical  
19 isotope production facility like SHINE to establish a  
20 CDA-specific cyber security plan, nor does the  
21 application guidance direct the development of such a  
22 plan. However, preventing or limiting unauthorized  
23 physical and electronic access to digital assets has  
24 been considered throughout the design of the SHINE  
25 facility.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1           Just to note a couple examples of these  
2           considerations that are described in the licensing  
3           basis. PICS, the process integrated control system,  
4           provides information to the facility data and  
5           communications system via a one-way data diode such  
6           that no inputs can be provides to the PICS from  
7           offsite sources, as we described in the FSAR.

8           MEMBER BROWN: This is Charlie Brown.  
9           Would you back up and repeat that for me again?

10          MR. BARTELME: Sure. PICS, or the process  
11          integrated control system, provides --

12          MEMBER BROWN: Let me ask my question  
13          maybe a little clearer. The architecture diagram that  
14          I looked at has the, you know, your TRPS systems and  
15          the other systems isolated with the HIPS system, and  
16          it sends data up to the PICS. Are those data  
17          communications also isolated from the operating  
18          systems?

19          MS. KOLB: This is Catherine Kolb. Your  
20          question is -- is it -- is the question are the TRPS  
21          and ESFAS systems separated from the PICS? Is that  
22          the --

23          MEMBER BROWN: Oh, no, I know they're  
24          separated. They hit -- the one-line diagrams of the  
25          architecture that you showed, which was just fine,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1       okay, shows data going from about six different parts  
2       of those systems, and with the little arrows that go  
3       into the -- a box that's called the PICS, you know,  
4       that's the process control stuff.

5                 And I just wondered if that was one-way  
6       communication also at that point, that going into the  
7       PICS general architecture, whatever it is. That was  
8       my first question.

9                 MS. KOLB:     Yes, this is Catherine.  
10       Without, you know, looking at the diagram  
11       specifically, there is communication from the TRPS and  
12       ESFAS to the PICS. There is some communication from  
13       the PICS back to TRPS and ESFAS, you know, for -- for  
14       different reasons.

15                So it does -- it doesn't necessarily  
16       communicate on the exact, you know, on the same -- on  
17       the same variable in both directions. But the --  
18       there is communication in both directions between  
19       those systems.

20                MEMBER BROWN: Okay, is that data, is that  
21       hardwired stuff like switches to activate, or is that  
22       literally instructions that are computer-driven?

23                MS. KOLB:     The PICS system, you know,  
24       without -- we're looking at the diagram that I think  
25       you're referring to right now. It is not just

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1       hardwired switches.

2                   MEMBER BROWN:   Okay.

3                   MS. KOLB:    If there was an actuation in  
4       the TRPS or ESFAS systems, the PICS would be used to  
5       send information, you know, from the operator  
6       interface in order to reset after an actuation.

7                   There is no mechanism for the TRPS or  
8       ESFAS to do that independently without X. You know,  
9       it -- I guess we, you know, we don't have all of the  
10      right people in the room to discuss the details --

11                   MEMBER BROWN:   Okay, I got it.

12                   MS. KOLB:    TRPS ESFAS communication,  
13      though.

14                   MR. GETCHIUS:   Charlie, this is Jamie  
15      Getchius, Senior Licensing Engineer.

16                   MEMBER BROWN:   Yeah.

17                   MR. GETCHIUS:   If you're looking at that  
18      diagram, the --

19                   MEMBER BROWN:   It's in my head right now,  
20      I don't have it.

21                   MR. GETCHIUS:   The lines that are shown in  
22      red depict unidirectional communication.

23                   MEMBER BROWN:   Oh, that was --

24                   MR. GETCHIUS:   What is shown on the --

25                   MEMBER BROWN:   Yeah, they come out of

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 what's called the M -- MICM or something like that.  
2 I've forgotten what, it's a communication module for  
3 the HIPS system. And those were -- used to be they  
4 were unidirectional back when we looked at it in  
5 another project, and that's why I was asking the  
6 question.

7 MR. GETCHIUS: And they are still  
8 unidirectional.

9 MEMBER BROWN: Okay, that's fine. The  
10 next question I had, I just wanted to hit this before  
11 you went on through the rest of it. In a previous  
12 conversation, the -- I asked about the PICS, because  
13 it wasn't really discussed in the previous meeting.  
14 You know, that's separate subcommittee meeting.

15 And it was mentioned that the PICS  
16 operates with an ethernet run throughout the PICS,  
17 overall PICS setup. And I guess my question there was  
18 is that ethernet system connected to the internet and,  
19 you know, exterior, or is it only feeds internal stuff  
20 and stuff within the PICS itself.

21 MS. RADEL: This is Tracy. The PICS is  
22 not connected to any kind of external networks or --

23 MEMBER BROWN: Well, the ethernet is --  
24 it's an internal network only and not connected  
25 external to the plant.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MS. RADEL: Correct.

2 MEMBER BROWN: Okay.

3 MEMBER BALLINGER: We have a separate  
4 subcommittee meeting on PICS.

5 MEMBER BROWN: I know that, but we're  
6 talking about cyber security. This is not cyber  
7 security, but it's how you communicate with the  
8 system. And therefore it embodies it if they connect,  
9 so I'm just trying to connect the dots to make sure I  
10 understand the picture of where you're flowing through  
11 with you, you know, with your presentation, that's  
12 all.

13 Go ahead, I'll -- you've calibrated me,  
14 and that's what I was looking for. Thank you.

15 MR. GETCHIUS: Okay. A couple other  
16 examples describe the licensing basis. Rack-mounted  
17 HIPS equipment is installed within locked cabinets.  
18 And access to TRPS and ESFAS safety-related control  
19 systems via the maintenance work station is password  
20 protected, as described in 74 -- Subsection 745 of the  
21 FSAR.

22 MEMBER BROWN: But that maintenance work  
23 station, from what I understand reading the other  
24 document was that's not connected out exterior either.  
25 That's a standalone operation that just connects back

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 into those systems. Is that correct, is that correct  
2 to understand?

3 MR. GETCHIUS: That's correct.

4 MEMBER BROWN: Okay, thank you.

5 MR. BARTELME: All right, lastly physical  
6 access to digital assets is controlled via the access  
7 control strategy just described in the SHINE physical  
8 security plan.

9 Following a regulatory audit of SHINE's  
10 administrative and design controls for preventing or  
11 limiting unauthorized physical and electronic access  
12 to digital assets at the SHINE facility, the NRC staff  
13 informed SHINE of the decision to impose via license  
14 condition a requirement for SHINE to develop a CDA-  
15 specific cyber security plan and provided SHINE a  
16 number of elements that the plan should consider,  
17 including the sampling of elements shown on the -- on  
18 the slide here.

19 The SHINE cyber security plan contains the  
20 commitment for SHINE to establish, implement, and  
21 maintain a cyber security program to detect, protect  
22 against, and respond to a cyber attack capable of  
23 causing a consequence of concern. Cyber security plan  
24 documents the various, administrative, programmatic  
25 controls to prevent or limit the unauthorized physical

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 and electronic access to CDAs.

2 As noted in this slide, SHINE defines a  
3 CDA, or critical digital asset, as a digital asset for  
4 which no alternate means has been identified to  
5 prevent the associated consequence of concern.

6 DR. BLEY: Can I interrupt you? It's  
7 Dennis Bley. When you folks did this, do you have an  
8 idea of how many critical digital assets you came up  
9 with and how burdensome was this analysis?

10 MR. BARTELME: The analysis is ongoing.  
11 We don't have that -- we're still working through the  
12 CDA identification process. Don't have a number yet,  
13 but burdensome, it's, you know, moderately burdensome.  
14 There's a number of digital assets that I'm working  
15 through the (audio interference) analysis. I think  
16 more timely than we expected, but not --

17 DR. BLEY: And the rules NRC set up for  
18 how you (audio interference) that's working pretty  
19 well for you?

20 MR. BARTELME: I think, yeah, utilizing  
21 the guidance, the draft guidance for fuel site  
22 facilities was helpful in, you know, in working  
23 through the process.

24 DR. BLEY: Okay, thanks.

25 MEMBER HALNON: This is Greg Halnon. Can

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 you explain just briefly how you came up with your  
2 consequence of concern scenarios? I don't want you to  
3 actually go into the consequence of concerns, but was  
4 it a team effort, or was it a single effort, was it  
5 the contractor, how did you that?

6 MR. BARTELME: We'll touch on that on the  
7 next slide.

8 MEMBER HALNON: Oh, okay.

9 MR. BARTELME: To touch on there, SHINE  
10 used the guidance of Draft Regulatory Guide DG-5062  
11 and associated rulemaking documentation related to  
12 cyber security at fuel site facilities to inform the  
13 development of the SHINE cyber security plan.

14 SHINE evaluated the fuel cycle facility-  
15 specific guidance and incorporated and put the  
16 guidance into the SHINE cyber security plan in order  
17 to satisfy the elements identified by the NRC staff as  
18 needing to be addressed.

19 Through the development of the SHINE cyber  
20 security plan, SHINE held clarification calls and  
21 public meetings with the NRC staff to ensure those  
22 programmatic elements SHINE are proposing, such as the  
23 SHINE-defined consequence of concern, planned audit  
24 periodicities, and planned event tracking and event  
25 reporting were adequately based on the guidance of DG-

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 5062 and met the intent of the planned license  
2 conditions to be imposed on SHINE.

3 MEMBER BROWN: This is the draft guide  
4 that's currently under -- that hasn't been turned into  
5 an official reg guide? Or you're talking about Reg  
6 Guide 5.71?

7 MR. BARTELME: It is not. We were using  
8 that June, June 20 -- or January 2017 draft.

9 MEMBER BROWN: Okay.

10 MR. BARTELME: Pre-decisional markings on  
11 that, yeah.

12 MEMBER BROWN: All right, so you all are  
13 at least focusing in on their levels of security, or  
14 I've forgotten what they call them, but the defense  
15 ring? You were using that as part of your planning?

16 MR. BARTELME: Not explicitly, though.  
17 They had discussions with the NRC staff on sort of,  
18 you know, the multilevel, you know, controls sets and  
19 defense-in-depth, but.

20 MEMBER BROWN: That's what I'm talking  
21 about.

22 MR. BARTELME: Okay.

23 MEMBER BROWN: All right, sounds like  
24 you're on that page anyway. All right, thank you.

25 MR. BARTELME: As shown in the slide here,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 SHINE-defined consequences of concern are adapted from  
2 the four types of consequences of concern for fuel  
3 site facilities identified in Table C-1 of DG-5062.

4 Consequences of concern have been adapted  
5 to the relative risk of the SHINE facility.  
6 Adaptations include modifying the active and latent  
7 safety consequences of concern to be relative to the  
8 SHINE safety criteria in lieu of the Part 70  
9 performance requirements considered in the DG-5062.

10 And SHINE removed the latent security  
11 consequence of concern from consideration as SHINE  
12 does not possess classified information in relation to  
13 the operation -- to the operation of the SHINE  
14 facility.

15 SHINE uses the SHINE safety analysis  
16 summary report to identify active and latent safety  
17 consequences of concern in assessing the vulnerability  
18 of the SHINE facility from the direct result of a  
19 cyber attack or the result of a cyber attack in  
20 conjunction with a secondary event.

21 The use of the SHINE safety criteria in  
22 assessing active and latent safety consequences of  
23 concern provides a consistent consequence threshold  
24 and an existing evaluation of facility response to  
25 known hazards.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 SHINE uses the physical security plan to  
2 identify latent safeguards consequences of concern  
3 providing an existing evaluation of site security  
4 strategies credited in the protecting of SNM of  
5 moderate strategic significance.

6 The SHINE process for identifying CDAs  
7 consisting of steps for a digital asset identification  
8 and performance of an alternate means analysis and  
9 ultimately the resulting determination of CDAs follows  
10 the guidance for vital digital asset identification in  
11 DG-5062.

12 This technical evaluation is led by  
13 SHINE's safety analysis organization and supplemented  
14 by responsible engineers of those systems containing  
15 digital assets associated consequences of concern.

16 As stated in the slide, the alternate  
17 means analysis performed -- alternate means analysis  
18 performed considers a function of the digital asset  
19 associated with the consequence of concern to  
20 determine whether -- determine when an alternate means  
21 exists to prevent the associated consequence of  
22 concern.

23 This alternate means (audio interference)  
24 various potential alternate means, including physical  
25 barriers, existing safety-related controls, other

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 critical digital assets, and manual actions as  
2 candidates for credited alternate means.

3 If an alternate means of protection is  
4 identified for a digital asset, a brief description of  
5 the alternate means is provided in the SHINE technical  
6 evaluation.

7 MEMBER MARCH-LEUBA: This is Jose, can I  
8 ask a question now? Hello, can you hear me?

9 MR. BARTELME: Yes.

10 MEMBER MARCH-LEUBA: Yeah, okay, will the  
11 cyber attack that will prevent production for the next  
12 three months because it disables -- it does not  
13 produce a consequence of concern, but prevents you to  
14 delivering products for the next three months. Would  
15 you consider that a critical digital asset? Did you  
16 consider it?

17 MR. BARTELME: Based on the definition of  
18 consequence of concern, that would not be defined as  
19 a critical digital asset.

20 MEMBER MARCH-LEUBA: But in my mind, it's  
21 not just a monetary consequence to the company, it's  
22 a serious safety consequence to the hospitals that  
23 rely on your product. So I'm thinking whether you  
24 would consider protection of the production of this  
25 very important isotope sufficient to protect.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 DR. BLEY: And this is Dennis Bley too, I  
2 want to chime in with Jose on this one. I suspect by  
3 orders of magnitude the possible health consequences  
4 to the public from an interruption of service could  
5 dwarf any radiological risk near the site. It seems  
6 to me we're being remiss in not looking at that.

7 MS. RADEL: So this is Tracy. You know,  
8 obviously, the -- meeting the patient needs is  
9 incredibly important to us, and we will be protecting,  
10 you know, protecting assets and our ability to meet  
11 those patients' needs.

12 But as far as, you know, the definition of  
13 critical digital assets and you know, protection of  
14 health and safety of the public, it's been a focus on  
15 those direct consequences from the facility versus  
16 downstream supply chain, you know, potential impacts.

17 We certainly do consider those aspects in  
18 how we -- how we design the facility for reliability  
19 and meeting our customer needs and the patient needs.

20 DR. BLEY: I want to speak maybe to the  
21 staff rather than you. You're following the rules  
22 exactly as you see them, but I want to take the staff  
23 back to the 1960s, when NRC considered no  
24 environmental hazards and ended up in a court case  
25 where NRC was essentially directed to include that in

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 the future.

2 This strikes me as of the same nature, and  
3 I think the staff, and maybe the staff in consultation  
4 with the Commission, ought to perhaps reconsider how  
5 they're thinking about that in this case.

6 MEMBER MARCH-LEUBA: I mean, in defense of  
7 SHINE, I'm pretty sure they're going to protect all  
8 the equipment from cyber attack. I mean, even if you  
9 have an office, a shipping office somewhere in the  
10 middle of Washington, you protect your computers.

11 I'm concerned that these guys that are  
12 attacking you are very smart and they'll always find  
13 the weak link. And this is one that is obvious.  
14 Anyway, we put it on the record.

15 MR. BARTELME: Continue, lastly, if no  
16 alternate means of protection is identified for a  
17 digital asset associated with the a consequence of  
18 concern, the digital asset is determined to be a CDA  
19 and appropriate cyber security controls are identified  
20 for protection of the CDA.

21 MEMBER BALLINGER: Let me make sure that  
22 I understand what Dennis is saying. What -- we're  
23 talking basically about two consequences of concern  
24 definitions, one related to the rules as they're  
25 written, the other related to the consequences of the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 cessation of the product on the customer. But that's  
2 a -- that's a very different thing, right?

3 DR. BLEY: It's very different, but to me,  
4 the analogy with environmental harm is a pretty good  
5 one. And you know, the Commission and the staff might  
6 say they have no justification in law for this. I  
7 think they need to look at that, I'm not a lawyer.

8 But of -- when you look at potential  
9 consequences of this facility, that strikes me as  
10 maybe the biggest consequence that can accrue. And  
11 the Committee advises the Commission, not just checks  
12 to see that all the rules are being carried out.

13 MEMBER HALNON: Dennis, this is Greg. The  
14 other analogy that bring more clear is the power-  
15 producing portion of the nuclear power plants were put  
16 under cyber controls because of the critical nature of  
17 maintaining base load power, especially during  
18 emergency situations.

19 So sort of the same thing, is it going to  
20 reduce the ability to make power. That's going to  
21 affect the public in a certain adverse way,  
22 henceforth, it deserves some level of protection.

23 DR. BLEY: Yeah, I almost brought that one  
24 up, Greg, I agree with you completely. But I think  
25 these two examples kind of clearly show that if we're

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 thinking about consequences, there are other ones  
2 besides direct radiological consequences that are of  
3 great concern to the public, society, the government.

4 MEMBER BALLINGER: But to pull that string  
5 a little further with respect to the -- to a power  
6 plant output, the grid is --

7 PARTICIPANT: Point, because --

8 MEMBER BALLINGER: So that what you're  
9 saying is, is that if this were the only facility that  
10 can supply the product in a timely manner, that's one  
11 thing. And I don't know that that's the case or not.

12 DR. BLEY: Well, Ron, the grid's  
13 resilient, but despite that, over the last 40 years,  
14 there have been some very significant ties together  
15 taking parts of the grid down that have had massive  
16 consequences.

17 MEMBER HALNON: Right, but you're making  
18 the point, is that there are other power plants that  
19 could compensate for a loss of a single nuclear power  
20 plant, but there's no other isotope facilities that  
21 can make up for the loss of this isotope.

22 MEMBER MARCH-LEUBA: There will be.  
23 They're building some in the Netherlands.

24 CHAIRMAN REMPE: Well, okay, let's pull  
25 the string another way. We used to get, in more

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 recent years, we used to get the moly-99 up from  
2 Canada or some place, right.

3 But there -- at one point, weren't we ever  
4 getting it from a place in the U.S., and we get other  
5 isotopes. I know at HER they have used it for isotope  
6 production.

7 Are we going to start, you know, saying  
8 that all isotopes for medical use are so important  
9 that all of the facilities need to be considered and  
10 have special requirements?

11 MEMBER MARCH-LEUBA: Well, if you have to  
12 -- if you get -- if you get a cancer and you're  
13 waiting for your CAT scan for -- or the PET scan, you  
14 consider it very important.

15 CHAIRMAN REMPE: Yeah, I just am thinking  
16 that, you know, I don't know. I --

17 MEMBER MARCH-LEUBA: In a sense, SHINE is  
18 a victim of their own success. I mean, they're so  
19 good.

20 CHAIRMAN REMPE: But what, okay, what  
21 about maintenance? If it takes it out, it's not a  
22 cyber security attack, what if they can't do their  
23 maintenance in a timely fashion?

24 MEMBER MARCH-LEUBA: Let me give you an  
25 example, okay. So they have some filtering beds for

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 -- to clean up the tritium so the accelerator can work  
2 properly. If I -- and that's not a safety concern.  
3 If I gain control to that, access to that controller,  
4 I can mess up their beds so the tritium cannot be  
5 cleaned up.

6 So it has no, absolutely no millirem  
7 exposure whatsoever, but the plant is down.

8 CHAIRMAN REMPE: There may be other  
9 reasons we don't know yet that the plants go offline  
10 for three months because of something or other that  
11 didn't quite work as expected. So I'm not sure --  
12 this is a can of worms.

13 MEMBER HALNON: Well, it's a can of worms,  
14 but it's not a can of worms for SHINE. It's whether  
15 or not we want to lay another regulatory requirement  
16 on top of it. And the NRC has decided not to or staff  
17 had decided not to.

18 MEMBER MARCH-LEUBA: I think, I mean, my  
19 -- in the letter, we should recommend to the staff  
20 that they need to look at it. I mean, we're raising  
21 it as a question, we don't have a solution. But this  
22 is a function of society, producing moly-99 of such  
23 importance that keeping it up and running is important  
24 to society.

25 CHAIRMAN REMPE: Maybe the NSA should run

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 a couple of these facilities, it might be cheaper.

2 MEMBER BALLINGER: They are funding.

3 CHAIRMAN REMPE: Then we should put a  
4 regulation in just because another one might come  
5 online and it's not so important.

6 MEMBER BALLINGER: We have discovered it's  
7 another reason why I would -- why I like to be on this  
8 committee, learn something every day.

9 MEMBER KIRCHNER: I mean, one could take  
10 this argument for a nuclear power plant. This is not  
11 just for cable-ized grid, but for averted admissions.  
12 But there has to be a line somewhere, I mean, and I  
13 think the line here, it's a good point. Obviously a  
14 very important societal benefit to this operating.  
15 But at some point, you have to draw --

16 MEMBER HALNON: Well, I would say however,  
17 we're in that situation right today. Right, because  
18 they're not producing.

19 MEMBER BALLINGER: Remember, when Congress  
20 considered the rule, the law supporting this, that  
21 argument was made.

22 MEMBER HALNON: Yeah, but what I'm saying  
23 is that loss of the grid is an emergency. And if loss  
24 of moly-99 is an emergency from the SHINE facility,  
25 we're in one right now. So, and we're surviving. So

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 there is an alternate means available. Therefore, it  
2 wouldn't even --

3 MEMBER MARCH-LEUBA: Once SHINE come into  
4 the operation, they're going to displace the other  
5 sources because they'll be more efficient. So those  
6 other conveyances are going to disappear.

7 Anyway, I'm sorry I brought it up, but  
8 it's important that we protect everything, not just  
9 the two or three that come up for this analysis. And  
10 I'm sure SHINE will protect everything.

11 MEMBER BALLINGER: Josh, I don't think you  
12 expected this line of question.

13 MR. BORROMEO: No, this took off in a  
14 different direction than what I was thinking, but it  
15 is a Friday afternoon. No, but I mean, this seems  
16 like a broader concern, right, and we certainly  
17 understand it.

18 MEMBER BALLINGER: Okay, can we continue?

19 MR. BARTELME: Yep. As stated on the  
20 previous slide, no alternate means of protection is  
21 identified for a digital asset associated with a  
22 consequence of concern. Appropriate cyber security  
23 controls are identified for protection of the CDA.

24 Utilizing the framework for control is  
25 offered NIST's special publication 853. CDAs are

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 analyzed and multilayered cyber security control sets  
2 are tailored to each CDA.

3 Implementing procedures, identify and  
4 document the cyber security controls applicable to the  
5 identified CDAs. Implementing procedures document in  
6 part the configuration and operating environment for  
7 the CDAs. Measures taken to address the performance  
8 specifications associated with the identified cyber  
9 security controls and the verification process for  
10 cyber security controls.

11 MEMBER HALNON: And Jeff, this is Greg  
12 again. Was there any or is it in your process that  
13 you come across a digital asset that you just don't  
14 want to make a CDA that you would put an alternate  
15 means in relative to either a procedure or some other  
16 means of either monitoring or controlling?

17 MR. BARTELME: The approach for assessing  
18 alternate means is more, I think more of a top-down  
19 approach. We assess if the digital asset is  
20 associated with a consequence of concern, is there an  
21 alternate means of protecting that digital asset.

22 Less so of, you know, this is a critical  
23 digital that we don't want to protect, let's determine  
24 an alternate means. We haven't really sort of gone  
25 more that thought of approach it.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1                   MEMBER HALNON:   Okay, so you haven't --  
2   you haven't, for lack of better terms, downgraded any  
3   CDAs to just asset, digital assets based on putting  
4   new or a different design or alternate means of place  
5   yet. I mean, is that on the table, though, to do that  
6   if down the road you see something that you're not  
7   sure you want to make a CDA?

8                   MR. BARTELME:   Yeah, per the, you know,  
9   the programmatic guides, if, you know, SHINE could  
10  establish a not yet existing alternate means for a CDA  
11  and then the technical evaluation would be -- would be  
12  updated to reflect that, just what new alternate means  
13  is or that developed alternate means for that -- what  
14  had previously been a CDA.

15                  MEMBER HALNON:   Okay, and one last  
16  question. In taking credit for operator actions, at  
17  the end, will you be doing an aggregate analysis to  
18  ensure that the operators are not overloaded with too  
19  many required actions as an -- as a potential cyber  
20  attack?

21                  MR. BARTELME:   We've not, you know, not  
22  got to that point of sort of cataloging or sort of,  
23  you know, looking in the aggregate of the alternate  
24  means. I don't know that we have any manual -- manual  
25  actions identified at this point right now. You know,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 right now my understanding we have not identified any  
2 manual actions that are being credited as alternate  
3 means.

4 MEMBER HALNON: Okay, I would encourage at  
5 the end of this to do some kind of aggregate analysis  
6 to make sure that, given a cyber attack, you're not  
7 overloading one control system, one, you know,  
8 expectations of something, or especially the operators  
9 that respond to the.

10 MR. BARTELME: Thank you. Lastly, the  
11 SHINE cyber security plan also provides for these  
12 additional programmatic controls offering temporary  
13 compensatory measures. Temporary compensatory  
14 measures are implemented.

15 It is determined that a cyber security  
16 controls -- or determined that cyber security controls  
17 are not meeting their defined performance  
18 specifications while new controls are developed,  
19 tested, and implemented.

20 Documentation is created for each  
21 compensatory measure that describes how the measure  
22 will effectively address the performance  
23 specifications of the cyber security control.

24 For configuration management, SHINE  
25 implements a facility-wide configuration management

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 program, which includes cyber security considerations.  
2 Specific cyber security considerations and approval or  
3 disapproval of conclusions will be included in the  
4 documentation related to changes to a CDA.

5 Periodic review. Periodic review of the  
6 cyber security plan occurs at least every 36 months.  
7 The review includes an audit of the effectiveness and  
8 adequacy of the cyber security program, including, you  
9 know, roles, responsibilities, requirements, and  
10 management commitments to the program.

11 Changes made to implementing procedures.  
12 Use of alternate means in defense of our protection  
13 for digital assets. SHINE cyber security incident  
14 response capability. And configuration management.

15 Define these deficiencies and remediation  
16 actions resulting from the periodic review are tracked  
17 via SHINE's corrective action program.

18 In terms of event reporting, SHINE informs  
19 the NRC Operations Center at the time of making an  
20 event-based notification, as prescribed in Sections  
21 5(A)(2) and 5(A)(3) of the technical specifications  
22 that the event is the result of a cyber attack.

23 If it's later discovered that a previously  
24 reportable event was a result of a cyber attack, SHINE  
25 notifies the NRC Operations Center within one hour of

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 discovery that the previously reported event was the  
2 result of a cyber attack.

3 MEMBER BALLINGER: Okay, this is Ron  
4 Ballinger. In looking through all of the documents  
5 related to this and actually discussing, we've had --  
6 we had discussions with something along these lines  
7 when we had our visit recently.

8 I may be a little paranoid, but I think  
9 that we're almost in never-never land when it comes to  
10 cyber security and that a periodic review every 36  
11 months just doesn't seem -- that's a -- that's a long  
12 time for cyber.

13 And I'm wondering whether or not somebody  
14 maybe should consider kind of an ongoing, maybe you're  
15 doing it, kind of an ongoing, I'm not sure what you  
16 would call it, evaluation, if you will.

17 MEMBER MARCH-LEUBA: I kind of disagree  
18 with you. I mean, they're talking about plan, not the  
19 --

20 MEMBER BALLINGER: Oh, the plan, okay.

21 MEMBER MARCH-LEUBA: Not the cyber -- I  
22 mean, obviously they're going to be -- there's going  
23 to be somebody in the plan that is cognizant of this  
24 topic, and they're going to implement on the patches  
25 and all the good stuff to make sure they stay on. So

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 I think the plan doesn't need to change more than  
2 every three years.

3 MEMBER BALLINGER: Okay, so there is a  
4 mechanism by which there's an ongoing --

5 MEMBER MARCH-LEUBA: There better be.

6 MEMBER BALLINGER: Yeah, yeah.

7 MEMBER MARCH-LEUBA: You have your  
8 antivirus, it continuously monitor.

9 MR. BARTELME: Yeah, and, you know, broad  
10 responsibility within SHINE. But you know, we've got  
11 our IT team and others that are constantly saying --  
12 staying aware of the threat environment and, you know,  
13 making any changes to implementing procedures or plan  
14 documents as need by.

15 The 36-month required is just sort of  
16 that, you know, really not to exceed timeframe, and  
17 the expectation is that we will be auditing the  
18 effectiveness of the plan at a more frequent basis  
19 than that.

20 MEMBER BALLINGER: Okay, I'm just, I'm  
21 kind of a layman here in that every time I start my  
22 cellphone up in the morning, there's a notification  
23 that there's like ten apps that need upgrading.

24 MR. BARTELME: There's always plenty of  
25 fixes.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1                   MEMBER MARCH-LEUBA: And that -- and that  
2 won't happen in the plan because it's not connected to  
3 internet.

4                   MEMBER BALLINGER: Okay. All right, all  
5 right.

6                   MEMBER MARCH-LEUBA: It has to be done.  
7 Let me -- well, we're on tangents, we all think cyber  
8 security has been an internet attack, because I can do  
9 it from the comfort of my kitchen in Bulgaria, but  
10 there are many other vectors to use for cyber security  
11 attacks.

12                   The obvious one is USB drives. But you  
13 have pulse -- like the famous hard drive that is  
14 manufactured in a foreign country and it comes with a  
15 flaw in firmware. Does the plan include all those  
16 unusual controls, non-internet controls?

17                   MR. BARTELME: Yeah, without, you know,  
18 having not identified the specific cyber security  
19 controls, you know, for each CDA, you know, the  
20 technical evaluation doesn't have that level of detail  
21 right now.

22                   But you know, with the NIST, you know,  
23 NIST -- NIST guidance and in discussions we've had  
24 internally, there will be -- where -- where portable  
25 media is required to be brought into the -- brought

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 into the facility for any software updates or whatnot  
2 for a digital asset, you know, there are -- there  
3 would be considerations for -- for checking that in  
4 the chain of custody thereafter to ensure we don't  
5 introduce a vulnerability.

6 MEMBER MARCH-LEUBA: Yeah, my experience  
7 is with UF-6 enrichment facilities. And you get shot  
8 on site if they see with you two things: a bucket that  
9 can contain water and produce a criticality event, or  
10 a USB drive. Literally, they -- that thing cannot be  
11 seen within five miles of the -- of the fence.

12 Your cyber security plan should include  
13 non-standard attack vectors. You have to think about  
14 the possible scenarios that bad guy can attack you.  
15 And don't go paranoid, but be cognizant of all those  
16 ways that they can get you. Thank you.

17 MEMBER BALLINGER: That NIST document has  
18 a lot of.

19 MR. BARTELME: And then lastly, event  
20 tracking. Within 24 hours of the discovery, SHINE  
21 records and tracks to resolution any failure,  
22 compromise, discovered vulnerability or degradation  
23 that results in a decrease in effectiveness of a cyber  
24 security control or a cyber attack that compromises  
25 the CDA associated with a consequence of concern.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1           That's the end of the presentation. Any  
2 additional questions on the cyber security plan?

3           MEMBER KIRCHNER: Jeff, this is Walt  
4 Kirchner. This is kind of -- kind of a clear field or  
5 blank sheet of paper thinking. Thank you for the  
6 visit, or your colleagues for the visit to your  
7 facility last month. I was impressed with the  
8 facility.

9           And given the importance of your product,  
10 which we talked about earlier in this discussion, and  
11 guaranteeing, you know, the reliability of the  
12 facility to meet the demand, is there a way to just  
13 put an air gap on this facility?

14           What I mean by an air gap is just do not  
15 run anything in, and anything that goes out is  
16 unidirectional diode-protected. Do you really need to  
17 bring the internet into this facility? Or certainly  
18 within the -- well, both.

19           I'm trying to think where the line is for  
20 seismic and other external threat production. But is  
21 it feasible to air gap the facility and then things  
22 like Jose just mentioned are then where you spend your  
23 effort? To isolate this, make it an island unto  
24 itself?

25           MS. KOLB: Yeah, this is Catherine Kolb.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 The equipment, the systems that, you know, directly  
2 control plant equipment do have those unidirectional  
3 capabilities, right. So that then they're an axis  
4 from the outside if we're, you know, transmitting  
5 things to servers for data retention and things.

6 But you know, as to completely air gapping  
7 the facility, I mean, our document control system in,  
8 you know, company-wide. Some people at headquarters  
9 need to be able to use it as well as the people in the  
10 facility. So you know, email for internal  
11 communications.

12 So it's not practical for us to air gap,  
13 you know, some of the business software that we have,  
14 you know, for day-to-day email communication and data  
15 control.

16 MEMBER KIRCHNER: But that's what I worry  
17 about. Those become the vulnerabilities. I'm trying  
18 to think about it in a way that limits your effort in  
19 cataloging all the CDAs by trying to isolate the  
20 facility as much as possible.

21 Do you, you know, does corporate a couple  
22 of blocks away, where we had lunch, do they really  
23 need to be having any input into the plant? They can  
24 get the data coming out. But I'm just thinking about  
25 it philosophically in a way that makes you, well.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MS. KOLB: No, we --

2 MEMBER KIRCHNER: As possible to resist  
3 cyber events.

4 MS. KOLB: No, as Jeff talked about, you  
5 know, we've considered, we're considering, you know,  
6 different aspects of this and your point is well-  
7 taken. But.

8 MEMBER KIRCHNER: Email is a convenience.  
9 Email is also a distraction. Email is -- it's useful  
10 for exchanging information, maybe.

11 So I'm just saying that to the extent that  
12 you can eliminate things coming via internet in  
13 particular, as well as control access, then it makes  
14 the robustness of your cyber security plan not just  
15 with paper but the actual physical protections --

16 MEMBER MARCH-LEUBA: I think that what  
17 they're doing, they're creating an island protection  
18 system. And it's -- and their unidirectional diode is  
19 really good. Trying to isolate the business part, I  
20 mean, you have to be able to track the UPS truck that  
21 brings you there.

22 MEMBER KIRCHNER: Yeah.

23 MEMBER MARCH-LEUBA: You have to be able  
24 to order lunch from the restaurant next door. So --

25 MEMBER KIRCHNER: Do you? Do you?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MS. KOLB: Our engineering team is located  
2 in Headquarters, which is not inside the fence. So we  
3 -- I think we do need to be -- because people in the  
4 plant do need to be able to communicate with people  
5 that are in the Headquarters building.

6 MEMBER MARCH-LEUBA: Yeah, my concern is  
7 eventually you need to have one guy that is paranoid  
8 and is in charge of this. And everybody thinks of the  
9 internet because that's what we think about.

10 But I'm worrying about an instrument  
11 technician that has to go calibrating stuff and  
12 carries an iPod with him. And that iPod is connected  
13 to everything inside to do the calibration. You've  
14 got to make sure that iPod is sanitized before it goes  
15 anywhere.

16 USB drives, we all know about them now,  
17 but there are other portable media. You have to worry  
18 about everything. Okay.

19 MEMBER BIER: Just one example. I was in  
20 a classified meeting a couple of weeks ago where I was  
21 told that anybody wearing a Bluetooth hearing aid  
22 would need to remove it before entering the classified  
23 space. So.

24 CHAIRMAN REMPE: Sign language?

25 MEMBER BIER: I don't know. Fortunately

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 I think it didn't come up in that case.

2 MEMBER MARCH-LEUBA: In classified, we  
3 spend the money and we -- and we really -- you know,  
4 all of the cables, yeah, that might get classified how  
5 you do it. But everything is regarded, absolutely.

6 MEMBER BALLINGER: This whole topic is  
7 fascinating and almost depressing sometimes. But  
8 okay, are there other questions from the members on  
9 this presentation?

10 Okay, so we need to shift to the staff's  
11 presentation. And would you like to go away for 15  
12 minutes and then redo your presentation in light of  
13 the previous questions, or would you like to just keep  
14 on going?

15 MR. BORROMEO: We'll just keep on going,  
16 we'll do our best.

17 MEMBER BALLINGER: Okay.

18 MR. WARNER: All right, then I guess it's  
19 my turn. Good afternoon, my name is Dan Warner, I'm  
20 in the Cyber security Branch in the Division of  
21 Physical and Cyber security Policy in the Office of  
22 Nuclear Security Incident Response. And I have been  
23 responsible for the review of cyber security for  
24 SHINE. Next slide, please.

25 So kind of going back to where we came

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 from. In September 2019, the Commission issued Staff  
2 Requirements Memorandum SRM-18-0063 for non-power  
3 production in the utilization facilities intending to  
4 possess or use a Category II quantity of special  
5 nuclear material for production of moly-99.

6 In the SRM, the Commission approved the  
7 staff's approach for addressing cyber security at  
8 these facilities through development of appropriate  
9 license conditions based on the facility's operating  
10 license application. SHINE is the first applicant to  
11 submit a license application that is subject to the  
12 requirements of this SRM.

13 So as far as how we went about developing.  
14 So staff reviewed the proposed rulemaking on cyber  
15 security for fuel cycle facilities and developed a  
16 similar for use of SHINE and similar facilities.

17 And just as a note, just for  
18 clarification, I think there might have been a little  
19 bit of confusion earlier. The draft guide that Jeff  
20 was discussing, DG-5062, is actually the draft guide  
21 for nuclear fuel facilities that goes along with the  
22 fuel cycle facility rulemaking. And that is what we  
23 were presenting as references that they could use when  
24 developing their cyber security plan.

25 Staff provided SHINE feedback to consider

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 when identifying applicable consequences of concern,  
2 which are events that occur as a result of the  
3 compromise of a critical digital asset that have the  
4 potential to adversely impact public health and safety  
5 or common defense and security.

6 Staff reviewed the SHINE application,  
7 determined if there was adequate protections for CDAs  
8 that could result in a consequence of concern.

9 During our review, staff reviewed the  
10 final safety analysis report for discussions of cyber  
11 security with a focus on safety systems. Several  
12 sections discussed protections for the highly  
13 integrated protection system platform for safety  
14 systems.

15 FSAR Chapter 7, Section 7422 identifies  
16 protections with design criteria that target solution  
17 vessel reactivity protection system, and Section 7522  
18 as similar design criteria for the engineered safety  
19 feature actuation system.

20 Both of these sections include criterion  
21 three that identifies the TRPS and ESFAS systems will  
22 incorporate design or administrative controls to  
23 prevent and limit unauthorized physical and electronic  
24 access to critical digital assets.

25 Also in the FSAR, FSAR Section 74532,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 title Cyber security Design Features, includes the  
2 information on a defensive system architecture, which  
3 includes features such as one-way isolated  
4 communication, outside safety systems, maintenance  
5 work station access only when a module is out of  
6 service, and no capability for remote access to the  
7 safety system.

8 In FSAR Section 74533, Access Control, it  
9 identifies several features that are used to restrict  
10 access, including physical keys to prevent  
11 unauthorized use, locked cabinets for rack matter  
12 equipment with administrative key control,  
13 modification or replacement of the field programmable  
14 gate arrays are restricted when installed in the HIPS  
15 chassis. And the FPGA modules only allow  
16 modifications of set points and tunable parameters  
17 that may require periodic modification.

18 We also reviewed as part of the  
19 application review process the physical security plan.  
20 We reviewed it to see if there's any information  
21 related to cyber security for the security systems.  
22 And then we performed a cyber security audit.

23 Staff conducted a regularly -- regulatory  
24 audit with SHINE to gather more information regarding  
25 cyber security. SHINE identified CDA access controls

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 and protected features from the FSAR, but indicated  
2 there was no specific cyber security program at SHINE.  
3 For cyber security of physical security assets, SHINE  
4 only identified access of controls.

5 After the audit, we decided to issue a set  
6 of requests for additional information to SHINE based  
7 on the feedback received at the audit. We looking for  
8 information regarding the design, administrative, and  
9 programmatic controls that the SHINE cyber security  
10 plan will provide.

11 And also included how consequences of  
12 concern will be identified, how CDAs will be  
13 determined, how cyber security controls will be  
14 applied, and other programmatic controls to ensure the  
15 cyber security program is documented and maintained.

16 Staff reviewed the SHINE application and  
17 then held the regulatory audit, followed by issuing a  
18 set of RAIs to gather sufficient information to make  
19 a determination. Staff determined additional program  
20 elements were required to ensure adequate protection  
21 at the SHINE facility and developed a list of  
22 important cyber security program elements applicable  
23 to SHINE.

24 Staff developed the license condition to  
25 address these additional program elements and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 determined the issuance of a SHINE operating license  
2 as conditioned in part by the license condition will  
3 not be inimicable to common defense and security or to  
4 the health and safety of the public. And therefore,  
5 meets the requirements of 10 CFR 5057, A(6).

6 So for the license condition, the licensee  
7 must have a CSP that describes how the facility's  
8 cyber security program provides reasonable assurance  
9 that digital computer and communication systems and  
10 networks are adequately protected against cyber  
11 attacks. This is similar to the approach followed in  
12 10 CFR 7354.

13 The licensee may make a change to the CSP  
14 provided that the cyber security program elements in  
15 the license condition and the performance objection of  
16 the CSP remain met.

17 And then just one last note, the intent is  
18 to review the cyber security plan as part of the  
19 inspection process once a -- once a facility is doing  
20 the pre-operational inspections and then afterwards.

21 CHAIRMAN REMPE: So this is Joy, and I had  
22 a question. And again, maybe this is what's normally  
23 done, but I was stumbling over the beginning of the  
24 last paragraph of the draft SE where you had, The  
25 licensee may not make a change that would decrease the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 effectiveness of the CSP without a prior approval of  
2 the Commission.

3 The beginning of your slides, when you  
4 Commission, you're talking about the five  
5 Commissioners, are you talking about the five or  
6 however many Commissioners are on the Commission at  
7 the time, have to approve any changes, or is it the  
8 staff?

9 MR. WARNER: It is the staff, but that is  
10 the standard wording that is used when we are  
11 incorporating those. However, that wording has been  
12 removed after consultation with OGC, so that now it  
13 basically is just they may make a change as long as it  
14 doesn't -- as long as the performance objectives of  
15 the plan remain met.

16 CHAIRMAN REMPE: Oh, okay. So the version  
17 that we reviewed for this meeting, unless I grabbed  
18 the wrong one, is no longer the version that exists  
19 that we're supposed to be reviewing? Because I  
20 thought it got it from the website not too long ago.

21 MEMBER BALLINGER: We have a new FSAR.

22 CHAIRMAN REMPE: But this is the SE.

23 MR. BORROMEO: So we transmitted the small  
24 tweak from OGC, oh, a little bit ago, a week, couple  
25 weeks ago, so.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 CHAIRMAN REMPE: Okay, I -- barely -- I  
2 may have grabbed a version that's not what Chris told  
3 me to review, and I don't know how that happened. But  
4 it's happened before.

5 MR. BORROMEO: Yeah, we'll make sure you  
6 get the correct version. I mean, the -- that was one  
7 change that we made, and there were some other small  
8 tweaks based off OGC feedback after that.

9 MEMBER BIER: Another question, this is  
10 Vicki Bier. You had said that you plan to review the  
11 cyber security program again at the time of  
12 operational commissioning, or whatever the term is.  
13 Is that a commitment that staff will review at that  
14 time, or is it one of a long list of things that staff  
15 might review at that time?

16 MR. BALAZIK: This is Mike Balazik,  
17 Project Manager for SHINE at the NRC. That's a --  
18 it's an inspection module that we've identified that  
19 we will review for the pre-operational readiness.  
20 We've identified I'd say about a dozen modules, and  
21 cyber security is one of them.

22 So there's no, I guess there's no might in  
23 it. That is our inspection plan to look at cyber  
24 security in the implementation of the program.

25 MEMBER BIER: Thank you.

1                   MEMBER BALLINGER: We just, apparently  
2 there's a bit of confusion of the version of the SE  
3 that we have, and we're trying to sort that out. We  
4 may have the current, not the current-current.

5                   CHAIRMAN REMPE: Well, maybe I grabbed the  
6 right one and it changed.

7                   MR. BORROMEO: Yeah, this is Josh  
8 Borromeo, Chief of the NPUF Licensing Branch. We --  
9 OGC -- we're continuing to work with OGC to get a  
10 dialogue on these. OGC provided some feedback on it.  
11 We made some small tweaks, so we'll get you the right  
12 version. But there was a substantive changes to the  
13 one that you have versus the on that you'll see.

14                   CHAIRMAN REMPE: But my concern that I  
15 tripped over has gone away is the other answer to my  
16 question. Thank you.

17                   MEMBER MARCH-LEUBA: And this morning we  
18 were chastising one of our members for putting  
19 revision numbers on the documents.

20                   MEMBER KIRCHNER: Ron, may I ask kind of  
21 a generic question. Dan, this is Walt Kirchner. I've  
22 -- so this guidance that the applicant's following,  
23 SHINE is following, basically derives the first order  
24 from what you apply with the -- to the fuel cycle  
25 facility.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1           So looking at the SHINE facility from what  
2 you know, how many -- you know, they have a lot of  
3 plumbing, a lot of actuators and so on. Much of this  
4 is obviously going to be modern, so it's going to be  
5 digital in one way or other.

6           How many critical digital assets do you  
7 think they'll have? Or do you put them into families?

8           MR. WARNER: At this point, I can't answer  
9 that question. Part of the reason we did it this way  
10 is we wanted to ensure that a solid program was being  
11 set up that would then be used to address the CDAs.  
12 As far as how many are going to be included, I can't  
13 say at this point.

14           MEMBER KIRCHNER: How many do you  
15 typically have in a fuel cycle facility?

16           MR. WARNER: I'm not sure, I haven't  
17 worked on a fuel cycle review. And actually, there  
18 hasn't been a review of that since the proposed  
19 rulemaking. It's still before the Commission.

20           MEMBER KIRCHNER: It just seems to me that  
21 there are a lot of digital-actuated valves,  
22 controllers, motors, pumps.

23           MEMBER BROWN: Might have a revision on  
24 what you're looking at. There's a lot of (audio  
25 interference).

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MEMBER KIRCHNER: Yeah.

2 MEMBER BROWN: So I'm just saying if the  
3 plant and what they're doing and you look at the --  
4 you know, the actions it has to take, the actuations,  
5 it wouldn't surprise me that every one of those  
6 probably has some type of a computer-based system. It  
7 just, particularly it depends on which system, if  
8 they've got an ethernet system that's set up.

9 I haven't even been able to figure out how  
10 they control those. Were they controlling them via  
11 the ethernet coming out whatever it is. It wasn't --  
12 wasn't real clear. But I suspect that's a computer-  
13 based actuation. Because it's -- that's just my  
14 assumption right now.

15 MEMBER HALNON: Dan, this is Greg, and I  
16 got a question. SHINE mentioned that they were --  
17 their program was informed by the DG-5062. Do you  
18 have, maybe it's subjective, do you have a feel for  
19 how well they complied with that or followed that  
20 relative to their program? Or are you approving a  
21 program that deviates quite a bit from that?

22 MR. WARNER: From what we reviewed and  
23 what we received in the RAI responses, I think they  
24 have -- what I've read is fairly consistent with what  
25 I read in the fuel cycle rulemaking in the draft

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 guide.

2 MEMBER HALNON: Okay, so it's similar.  
3 When all that is issued, would you be able to say that  
4 they're reasonably in compliance with the regulation  
5 and the reg guide? I say reasonably to give you some  
6 wiggle room. I guess I'm looking, you know, are they  
7 setting up precedents?

8 MR. WARNER: I mean, to be honest, and I'm  
9 speaking for myself here, that is kind of what the  
10 intent of this was. We're in situation where we're  
11 going to have different types of facilities coming in  
12 that are going to be different than what we've  
13 typically regulated at the NRC.

14 And we are trying to put together an  
15 approach that will be a fairly generic approach that  
16 can be used at different types of facilities. You can  
17 even see a similar approach is being looked at for  
18 advanced reactors that will help provide some  
19 consistency when applying cyber security to these  
20 different types of facilities.

21 So the fuel cycle rulemaking has a lot of  
22 really good stuff. A lot of good work was put into it  
23 for the background, and I think it provides a decent  
24 framework that can be applied at different types of  
25 facilities fairly simply.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MEMBER HALNON: Okay, fair enough, thanks.

2 MEMBER KIRCHNER: Hi, Dan, this is Walt  
3 again. I'm kind of revisiting my question again. I'm  
4 just trying to think through this. Would you -- would  
5 you consider their PICS system as a whole, looking at  
6 it as a whole system, as the critical digital asset?

7 Or do you get down to each of the  
8 controllers for every valve, pump? I'm sure this is  
9 all modern equipment, so I'm sure they're going to be  
10 reliant on programmable logic devices, etc., etc.

11 So does it get down to that level, or can  
12 they put them together in families? Or could you just  
13 say the PICS system is the critical (audio  
14 interference). How do you get the right answer from  
15 your perspective, which is not to have a cyber  
16 incident result in a consequence of concern matter  
17 without making it a bureaucratic nightmare?

18 MR. WARNER: I mean, at this point, that's  
19 for SHINE to determine. It's our responsibility, and  
20 this is what we've done with power reactors, is set  
21 the program and put the program in place, and then  
22 allow the licensees to implement the program. And  
23 then we come and inspect to determine how well we  
24 think they're doing.

25 At this point, I cannot give an answer on

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 this. It's really up to SHINE.

2 MEMBER BALLINGER: Yeah, this might be a  
3 better question to ask the SHINE folks. They're out  
4 there.

5 MS. RADEL: Yeah, this is Tracy. You  
6 know, the evaluation does get down to the individual  
7 component level. And you are able to group those  
8 components then when looking at the control sets  
9 applied to those digital assets. But it's evaluated  
10 down to the individual component level.

11 MEMBER MARCH-LEUBA: Yeah, but many of the  
12 modern actuators, they all have a microprocessor in --  
13 built in. So did you go to the chip level or did you  
14 got to the component level? In the component level,  
15 PICS is a critical asset. It's one critical asset  
16 that has hundreds of components inside.

17 MS. RADEL: We went to the component level  
18 in it.

19 MEMBER BALLINGER: Okay.

20 MEMBER MARCH-LEUBA: This is to place a  
21 statement on the record. A comment before you close.

22 MEMBER BALLINGER: Sure.

23 MEMBER MARCH-LEUBA: Yeah, so this is  
24 going to be above the pay grade for everybody in the  
25 conference, so this is not an action item. But what

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 I was saying before of denial of access for the  
2 production of the facility is something that is not  
3 part of the regulation. It's not part of the rule,  
4 it's not part of the license for operation. But it's  
5 something that maybe needs to be considered.

6 And I would like for the Committee to  
7 discuss it and maybe bring it up as one of the things  
8 that we propose to the Commission that is -- needs to  
9 be -- needs to be considered. For example, the attack  
10 they had on the Colonial Pipeline. Didn't kill  
11 anybody, didn't challenge anybody. We can spend a  
12 little more at the pump station. So it was a serious  
13 attack for society.

14 Same thing can happen with moly-99. And  
15 the approach we have of regulation, protecting a  
16 radiation dose that can challenge somebody's health is  
17 a must. It's a necessary condition. I'm asking is it  
18 sufficient.

19 And maybe we need, we as a committee,  
20 talking about the ACRS, need to discuss this among  
21 ourselves and propose it up. At least have people  
22 start thinking about it.

23 CHAIRMAN REMPE: So you're not really  
24 saying -- you may have a note in the letter that might  
25 say that some additional consideration might be given.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 But then you're also say, just like we have a couple  
2 of members, one's online still, saying the safety goal  
3 topic is something.

4 So this is something you'd like to  
5 consider beyond outside the scope of this. And that  
6 sounds like a working group that you should lead, but  
7 we can talk about that at P&P.

8 MEMBER MARCH-LEUBA: Let's not overdo the  
9 paperwork, but --

10 CHAIRMAN REMPE: No, but you want to  
11 discuss it or you want to like have a retreat or  
12 something to discuss it.

13 (Simultaneous speaking.)

14 MEMBER MARCH-LEUBA: Yeah, if ACRS --

15 CHAIRMAN REMPE: -- something for P&P to  
16 decide in the future.

17 MEMBER MARCH-LEUBA: If ACRS concerns  
18 itself only whether the regulation is satisfied, I  
19 don't think we're doing our job. We should be raising  
20 questions higher.

21 CHAIRMAN REMPE: So, P&P --

22 (Simultaneous speaking.)

23 MEMBER MARCH-LEUBA: We'll work offline.  
24 We don't need to do it on the record.

25 CHAIRMAN REMPE: Okay, thank you.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MEMBER MARCH-LEUBA: And it's not an  
2 action item for SHINE or the staff at this moment.

3 MEMBER BALLINGER: Okay, we're at a  
4 transition point where if there aren't any questions,  
5 additional questions related to the cyber security, we  
6 need to transition at least on the schedule to the  
7 technical spec presentation, and I guess my question  
8 to the staff is, with respect to the software  
9 lifecycle, where do you want to put that?

10 MR. BORROMEO: Oh, we can go after tech  
11 specs.

12 MEMBER BALLINGER: Okay, after that, okay.

13 MR. BORROMEO: Yeah, and that will be  
14 SHINE.

15 MEMBER BALLINGER: Okay, okay, got it.

16 MEMBER BROWN: Before you do that,  
17 addressing Jose's question? I'm trying to backtrack  
18 to the last, when we've had the discussions on one of  
19 the earlier projects.

20 All we really worked with -- and this is  
21 not a production facility like this. This was on the  
22 power plant, you know, for producing electricity. We  
23 focused on the protection system and what we call the  
24 plant systems, which were blocked off and shown coming  
25 into a network.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1           And what we did there was insist -- those  
2 were the control functions. That's where you turn  
3 stuff on and off and all that other kind of stuff.  
4 Anything that went into that network had to be, was a  
5 unit directional type of thing.

6           And we got pushback on that because this  
7 was not -- that's a cyber security issue, but it's not  
8 really a cyber security issue because it's internal to  
9 the plant controls. You can't put cyber security  
10 software into the actuator for stuff like this.

11           You've got to isolate or not and that's  
12 what we -- you know, at least we got it isolated at  
13 the network level so that nothing would come through  
14 the network. It was all unit directional going up to  
15 it.

16           Here, you've got a lot of other  
17 subsystems. I mean, in looking at Chapter 7, there's  
18 a bunch of stuff. I've forgotten the count, but it's  
19 a large number of --

20           MEMBER MARCH-LEUBA: Anything from air  
21 conditioning to the lights in the room.

22           MEMBER BROWN: That's why I asked the  
23 ethernet question. If you isolate the ethernet, then  
24 that's where the controls are operating from and then  
25 they go out. Now you've put yourself back into a case

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 where you're dealing with physical security on access,  
2 people coming in and making changes.

3 If you connect that, any of that stuff to  
4 an outside source, then now you're dealing with a  
5 separate security system, and if you go through a  
6 network, you can deal with it at the network as long  
7 as the network goes backwards unit directional back to  
8 those other things.

9 So, without seeing how this thing is  
10 hooked up, and if you go read 5.71, 5.71 addresses a  
11 lot of -- it even addresses the CDA can be a cell  
12 phone that somebody communicates with because it's got  
13 some type of a link that it can put some information  
14 someplace.

15 So, you can go way down in the weeds on  
16 this and it gets down to an individual basis. I tried  
17 to focus on the regular power plant stuff on isolating  
18 all of those with unit directional transmissions, even  
19 up the main control room.

20 What we didn't get to do in the main  
21 control room, because we don't see the architecture of  
22 the main control room, how does that get out to the  
23 TSC? Well, we showed the TSC over here getting  
24 information only from the systems. So, if you have --  
25 so, I mean --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1                   MEMBER MARCH-LEUBA: My point, Charlie, is  
2 that there is more than one attack vector.

3                   MEMBER BROWN: Oh, yeah, absolutely.

4                   MEMBER MARCH-LEUBA: When I used to work  
5 in nonproliferation, I used to tell my sponsor that  
6 our meetings should be in Las Vegas and going to see  
7 every single magic show in Las Vegas, because if I  
8 control the stage, I can make an elephant disappear.

9                   MEMBER BROWN: I agree with you.

10                  MEMBER MARCH-LEUBA: It never worked.  
11 They never paid us to go, but it was a story. You  
12 have USB drives, you have fake components from Western  
13 Digital or from North Korea Digital. There are so  
14 many attack vectors, the famous aquarium in the  
15 casino, but this is more a topic for the work group,  
16 eventually. We shouldn't be wasting time, SHINE's  
17 time.

18                  MEMBER BROWN: Well, but your question, I  
19 think, deals with us and we, I think, and how we  
20 discuss this. Any plant controls, safety controls, et  
21 cetera, none of those systems can you embed virus  
22 protection software because you've got to constantly  
23 update it, so somehow -- and we're not dealing --

24                  We have not been able to convince people  
25 to separate the variables. In other words, here's a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 set of stuff and here is all of the other stuff in the  
2 plant that's not connected to the controls.

3 MEMBER MARCH-LEUBA: And these viruses are  
4 very difficult to detect because they activate only  
5 once.

6 MEMBER BROWN: And --

7 (Simultaneous speaking.)

8 MEMBER BROWN: And that's not -- you're  
9 always reacting. All cyber security software  
10 basically, other than some, are reactionary.

11 MEMBER MARCH-LEUBA: Definitely we need to  
12 set up a Friday afternoon for a work group.

13 CHAIRMAN REMPE: I think that this should  
14 be a working group topic and I think the chairman,  
15 chairmen of the working group, and you can figure it  
16 out, but let's talk at P&P because that's the way this  
17 process should work. That's at least my understanding  
18 of it, but yeah, I think it's worth exploring.

19 MEMBER BALLINGER: Okay.

20 MEMBER KIRCHNER: I don't want to belabor  
21 it, but I wanted to follow up on Charlie. So we're  
22 getting the PICS presentation in October?

23 MEMBER BALLINGER: Yes.

24 MEMBER KIRCHNER: So, the question I would  
25 ask just to prepare the SHINE people is I would be

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 very interested in how that ethernet system is laid  
2 out for the plant, the equivalent of plant operations  
3 and controls, not the size on the trip protection  
4 system and the ESFAS system.

5 Because I think they could do a lot to  
6 make themselves not entirely immune, but first order  
7 much more secure. And as Charlie said, we in the past  
8 with power plants haven't been quite so worried about  
9 the balance of plant --

10 MEMBER MARCH-LEUBA: What SHINE needs and  
11 every facility needs is one person that is paranoid  
12 and looking over their shoulder all of the time that  
13 owns the problem, and unfortunately, the smaller the  
14 facilities they are, the less capability you have to  
15 have one person in charge of only one thing.

16 But what you need is somebody looking over  
17 their shoulder all of the time and asking questions.  
18 What can possibly go wrong? How can I attack this?  
19 I've said enough.

20 MEMBER BROWN: Well, we took a shot at  
21 trying to get -- I'm more worried about an NRC  
22 strategy and that if they -- we keep isolating systems  
23 that don't matter, but you've still got to protect  
24 where you can embed software and systems that have  
25 functionality in terms of the plant that can't have

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 any of that.

2 Then there is -- and we keep getting one  
3 group talking, you know, past and through another  
4 group, and you can't set up a strategy for how you can  
5 deal with this and the plant types out of it, whereas  
6 in the business stuff, the other, you know, collecting  
7 records for maintenance or whatever it is, they can do  
8 whatever they want to.

9 You can embed stuff in there because you  
10 can let it be constantly updated and just pray that  
11 nothing happens, but you ought to be sweating bullets  
12 if it does.

13 And there's not a grand strategy. The  
14 5.71 doesn't, it's got the zones, but it doesn't deal  
15 with the overall arching strategy of you can't embed  
16 software in control functions, virus software, can't  
17 do it.

18 Otherwise, if you can't do constant  
19 updates, you'll be constantly compromising that system  
20 and that's not recognized by the staff right now in  
21 terms of how we operate or how we deal with applicants  
22 and others.

23 MEMBER BALLINGER: Okay.

24 MEMBER BROWN: Is this on the record by  
25 the way?

1 MEMBER BALLINGER: Yes.

2 MEMBER BROWN: Good, because I'll forget  
3 what I said later.

4 MEMBER BALLINGER: With much fear and  
5 trepidation, are there any other questions from the  
6 members? Okay.

7 MEMBER BROWN: Has the staff presented on  
8 this yet? Are they going to present on this cyber  
9 part? Are they next? Oh, I saw the SHINE part.

10 MEMBER BALLINGER: Yeah, there's a reason  
11 why you didn't see the staff part.

12 (Simultaneous speaking.)

13 MEMBER BROWN: Did I really? I thought I  
14 had the slides up. That's okay.

15 CHAIRMAN REMPE: Let's go to the technical  
16 specification.

17 MEMBER BALLINGER: Can we work on this?  
18 Okay, so the SHINE people are up. Thank you very  
19 much, I hope.

20 MS. KOLB: Yeah, all right, this is  
21 Catherine Kolb, Senior Director of Operations for the  
22 SHINE facility and I'll be talking about technical  
23 specifications now.

24 So, we'll go over the different sections  
25 of our technical specifications, our proposed

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 technical specifications, including the introduction,  
2 safety limits, and limiting safety system settings,  
3 limiting conditions of operation, surveillance  
4 requirements, design features, and administrative  
5 controls.

6 So, the technical specifications that we  
7 have proposed for our medical isotope production  
8 facilities, these are requirements of 10 CFR 50.36.  
9 We used guidance provided by ANSI/ANS-15.1, the  
10 standard for the development of technical  
11 specifications for research reactors, the guidance in  
12 NUREG-1537, and for rules of usage, we used NUREG-  
13 1431, which is the standard tech specs for  
14 Westinghouse plants.

15 And we'll talk about that in a little bit,  
16 how we used those, but overall, the technical  
17 specifications used those guidance documents, but also  
18 incorporate the safety-related controls that were  
19 identified in our SHINE safety analysis in order to  
20 implement them.

21 So, the introduction section of the tech  
22 specs includes the definitions and descriptions of  
23 logical connectors as well as some introductory  
24 paragraphs about the purpose and scope. So, the  
25 definition section is primarily based on the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 definitions that are provided in ANSI/ANS-15.1.

2 We've made some facility-specific  
3 modifications of certain terms. For example, the  
4 definition of safe shutdown is specific to our  
5 facility. The definition of facility secured is  
6 specific to us, and we have added some new facility-  
7 specific terms. For example, we have defined what a  
8 neutron driver assembly system is for our main  
9 production facility and things along those lines.

10 The logical connector usage rules are  
11 based on the descriptions that are found in NUREG-  
12 1431.

13 MEMBER HALNON: Catherine, this is Greg.  
14 Did you use those because that's where you came from  
15 and they're familiar or was there a reason you went to  
16 the Westinghouse?

17 MS. KOLB: The parts that we used from 1431  
18 are, you know, similar across most of the standard  
19 tech specs that we looked at, but, yes, the staff that  
20 was responsible for writing the tech specs were  
21 primarily, you know, Westinghouse power reactor  
22 background people.

23 MEMBER HALNON: Okay, thanks.

24 MS. KOLB: Next slide? And in terms of  
25 pressure and temperature for the irradiation unit

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 primary system boundary and for process tanks  
2 containing irradiated uranyl sulfate solution in the  
3 radioisotope production facility, so there's different  
4 temperature and pressure actual limits depending on  
5 which piece of equipment it is, but those are all  
6 limits based on those types of perimeters.

7           Eliminating safety system settings are the  
8 variables and their allowable set points for our  
9 safety-related entry control system. That would be  
10 the target solution vessel reactivity protection  
11 system or the TRPS, and then engineered safety  
12 features actuation system or the ESFAS, and these are  
13 defined to ensure that the automatic protected actions  
14 are initiated prior to exceeding any of the safety  
15 limits that we've identified.

16           The next section, Section 3 of our  
17 proposed tech specs, includes the limiting conditions  
18 for operation. Those are the administratively  
19 established constraints and our equipment and our  
20 operational characteristics. They define the lowest  
21 functional capability or performance level for safe  
22 operation of our facility.

23           The rules of usage, as I mentioned before,  
24 are based on NUREG-1431. We used power reactor  
25 guidance because the SHINE facility is a commercial

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 entity. We have an expected operational cadence that  
2 is more similar to a continuously running power plant  
3 than to a typical research reactor.

4 So, we didn't use much of the, you know,  
5 technical items in the NUREG, but the front matter  
6 and, you know, the section in 3.0 where it describes  
7 how to use the limiting conditions of operation and  
8 how to use the tech specs. We used that quite  
9 liberally.

10 We have defined actions to be taken upon  
11 the discovery of a failure to meet an LCO and  
12 specified completion times are generally provided for  
13 each of the LCOs. That is different than a typical  
14 research reactor tech spec and much more like  
15 commercial power reactor tech specs because of the  
16 goal of the SHINE facility, which is 24/7 operation.

17 The LCOs provide -- we provide exceptions  
18 to the LCOs to allow the performance of specific  
19 startup tests. We discussed some of those at a  
20 previous ACRS meeting on how we need to measure  
21 different reactivity parameters. That is not possible  
22 following the normal usage LCOs, so we defined  
23 exceptions and compensatory measures in order to do  
24 those specific startup tests.

25 We've also included exceptions for the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 performance of defined recovery actions, so, for  
2 example, actor and actuation of the TRPS or ESFAS  
3 system in order to get back to an operational state in  
4 order to reset those things, those actuations, to  
5 reopen valves that had been closed. We needed some  
6 exceptions to our technical specifications.

7 Any questions on our approach to LCOs?  
8 All right, we have also defined surveillance  
9 requirements. This, the format of how we did these is  
10 also similar to commercial power plants where we've  
11 identified surveillance requirements for, you know,  
12 one or more for each LCO.

13 Typical research reactor tech specs might  
14 have those in two separate sections even though  
15 they're interrelated. We have them on the same page.  
16 That is to increase readability and, you know, for  
17 human factors considerations so that it's clear which  
18 surveillance requirements apply to which LCOs.

19 The surveillance requirements describe the  
20 frequency and the scope of the surveillances that  
21 demonstrate the minimum performance levels for each  
22 LCO.

23 The frequencies that we chose, you know,  
24 how often the surveillance requirements need to be  
25 performed, those are generally based on the guidance

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 in ANSI/ANS-15.1, the research reactor standard, where  
2 similar areas exist between equipment addressed in  
3 that standard and equipment used in the SHINE  
4 facility.

5 For the cases where there were no  
6 similarities -- in most cases, there were  
7 similarities, if not in specific instruments or  
8 specific components, in, you know, scope of what it's  
9 trying to accomplish, there were similarities there,  
10 so we used those, but in the couple of cases where  
11 there were no similarities to the research reactor  
12 ones, we did use industry experience and some  
13 commercial reactor guidance there.

14 The Section 4 of our technical  
15 specifications are design features. Those are the  
16 design characteristics of the site to the facility  
17 that are described in the tech specs to ensure that  
18 major alterations to our safety-related components or  
19 equipment are not made without appropriate safety  
20 reviews or prior approval if necessary.

21 The design features we have identified  
22 include descriptions of the sites and the location of  
23 our sites, physical characteristics of the main  
24 production facility, some important features of  
25 equipment that are assumed in the safety analysis such

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 as efficiencies in the carbon delay beds, ventilation  
2 features, shielding characteristics that exist in our  
3 facility, how we've described the limit that we have  
4 on uranium enrichment, and our margin of  
5 subcriticality for areas outside of our target  
6 solution vessel.

7 MEMBER MARCH-LEUBA: Sorry, this is Jose.  
8 You've been talking for too long. On the margin for  
9 subcriticality, does the tech spec put in on terms of  
10 dollars or in terms of a measured power? Because  
11 subcriticality is very difficult to measure.

12 MS. RADEL: So, this is Tracy. That  
13 margin of subcriticality is related to the criticality  
14 safety program, so that is the required margin for our  
15 criticality safety calculations. It's not related to  
16 the reactivity in the target solution vessel.

17 MEMBER MARCH-LEUBA: So, why does it  
18 belong in tech specs? I mean, this is just an entity  
19 of calculations, right?

20 MS. RADEL: The specific margin was  
21 approved or is going to be approved as part of the  
22 criticality safety review, and I believe that it was  
23 included there as part of like originally some of the  
24 discussions with some of the criticality safety.

25 That was done a while ago. I'm not

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 exactly sure of the discussions we had about why it  
2 was there, but it was of sufficient importance so that  
3 we wanted to put it in the technical specification --

4 (Simultaneous speaking.)

5 MEMBER MARCH-LEUBA: There is nothing  
6 wrong with being over-prescriptive. I was just  
7 wondering. I mean, it's okay. It's perfectly good to  
8 have it there.

9 MR. BALAZIK: This is Mike Balazik from  
10 the NRC staff. The ANSI 15.1 standard in design  
11 features actually talks about, it talks about  
12 effectiveness for storage, resident storage, so I  
13 think that kind of has a link with why SHINE put it  
14 there.

15 MEMBER MARCH-LEUBA: Yeah, I was asking  
16 why it's in tech specs, and normally an operator looks  
17 into an instrument, makes a reading and sees that it's  
18 within tech specs.

19 If it's an input to your subcriticality  
20 calculations, I mean, it's okay to have it there, but  
21 it doesn't make any -- you're never going to not  
22 satisfy it.

23 (Simultaneous speaking.)

24 MEMBER MARCH-LEUBA: There's nothing wrong  
25 with it.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MS. RADEL: Yeah, I think you're exactly  
2 right there. This is the design features portion of  
3 our tech specs, so most of the things listed in this  
4 section are things that aren't readily changeable by  
5 operators, you know, thickness of shielding and the  
6 fact that the site is located at this address, you  
7 know, things that aren't readily changeable by people  
8 except for major modifications, so that's why it's in  
9 this particular section.

10 MEMBER KIRCHNER: But your definition of  
11 design features includes components or equipment in  
12 the introduction there, and obviously you don't want  
13 someone going in and changing the diameter of pipe,  
14 for example, because that will impact the margin of  
15 subcriticality if it has a fissile fluid in it.

16 MS. RADEL: Yes, this is Tracy. That is  
17 correct. So, our margin of subcriticality is what  
18 defines our single parameter limit, which then define  
19 the size of our vessels and tanks, and rather than  
20 putting all of those, you know, tank diameters,  
21 thicknesses, and the link into tech specs, you know,  
22 we're able to capture all of that just by putting the  
23 margin of subcriticality that defines, ultimately  
24 defines those design features.

25 MEMBER BIER: Another question, for

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 equipment that might be used either in operation or in  
2 a safety mode, but that would interfere with  
3 operation, are there procedures to bypass so that you  
4 can test them on a regular basis without interfering  
5 with production or whatever?

6 MS. RADEL: Yes, so things of that nature  
7 are defined in our Section 3 in the limiting  
8 conditions for operation section. For those  
9 instruments, you know, for example, that can't  
10 calibrate when you're not in the mode or other  
11 condition of applicability, we have put in provisions  
12 to the specific LCOs, you know, that the instrument  
13 can be bypassed for up to two hours in order to  
14 perform the surveillance requirements. Those are  
15 listed specifically to which instruments those apply  
16 to where you can't readily do it in other modes.

17 MEMBER BIER: Thank you.

18 MS. KOLB: All right, my last slide is  
19 about Section 5 of our proposed technical  
20 specifications.

21 So, this section mirrors the sections that  
22 we have in Chapter 12 of the FSAR that we covered in  
23 the conduct of ops ACRS presentation last time, and it  
24 includes the organization, the structure, our minimum  
25 facility staffing, selection and training of

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 personnel, activities, and features of the review and  
2 audit committee that we have discussed, radiation  
3 safety program, procedures and rules about their usage  
4 and development at the SHINE facility, programs, which  
5 I'll come back to in a second, required actions for  
6 cases where if we exceeded safety limits or other  
7 specific reportable events, what the required actions  
8 are there, reports that we're required to make and  
9 records that we're required to keep.

10 The portion of Section 5 administrative  
11 controls that is different from Chapter 12 is in the  
12 program section. So, here is a list of mostly  
13 programs that were identified by our safety analysis  
14 as programmatic administrative controls.

15 These include things like maintenance and  
16 the fact that we have a nuclear criticality safety  
17 program, things of that nature to ensure that it is  
18 captured in our technical specifications and those  
19 programs be established, implemented, and maintained.

20 Under the configuration control program,  
21 one of the programs that we are required to have,  
22 we've also listed a table that includes features that  
23 were identified in the SSA as controls, in our safety  
24 analysis as controls, but didn't readily fit into the  
25 design features section of the technical

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 specifications.

2 We did this to ensure that all of the  
3 credited safety-related controls that were identified  
4 in the SSA are somehow reflected in the technical  
5 specifications in order to ensure that they would be  
6 maintained and keep our bases behind the safety  
7 analysis.

8 And this is my final slide on technical  
9 specifications. Are there any other questions?

10 MEMBER BALLINGER: Hearing none, can we  
11 transition to the staff? While you're transitioning,  
12 this is one person's opinion on this. When we review  
13 a light water reactor, we pretty much all know what  
14 the technical specifications are likely to be, but in  
15 a facility like this, we don't know or there are  
16 certainly deviations.

17 And so, the order of review, waiting until  
18 this time to do Chapter 14 or at least part of it, to  
19 me is probably too late. It's probably not a bad idea  
20 to try to at least introduce the reviewers to the  
21 technical specifications so that we know, we each have  
22 the definitions, actually, and have some of that  
23 information even if we don't connect the dots until we  
24 actually hear a presentation on a chapter where those  
25 technical specifications are discussed.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1           So, it's just, for me, it's a lesson  
2           learned. It's like in Chapter 3.1, you know, the  
3           design criteria, it's kind of a better idea to have  
4           them up front than wait, so, just for our own personal  
5           information. So, okay, I'm not sure how the members  
6           might feel about that.

7           MEMBER SUNSERI: Excuse me, this is Matt.  
8           I just want to add, Ron, you know, I've had technical  
9           specifications as part of the FSAR since, I don't know  
10          when this was issued, but I guess it's an old operator  
11          habit in me that whenever I review a system or  
12          something, I always go check the tech specs.

13          So, I've been following them all  
14          throughout the course of this review and I just went  
15          -- I was thumbing through as Tracy was going through  
16          this and I think it was a very comprehensive set and,  
17          you know.

18          MEMBER BALLINGER: I mean, no doubt it's  
19          an extensive and comprehensive list.

20          MEMBER SUNSERI: So, I agree that perhaps  
21          an overview up front might have been helpful, but they  
22          have been available and they have been used throughout  
23          the review.

24          MEMBER BALLINGER: Yeah, yeah.

25          MR. BORROMEO: So, this is Josh Borromeo,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 Chief of the NPUF Licensing Branch. You know, this  
2 may be an artifact of the way that we do license  
3 renewals for research test reactors. We go through  
4 the up-front matter of the FSAR.

5 You know, all of the other chapters in the  
6 tech specs is usually last because the design is set  
7 and where they want to operate is set, and then we  
8 collect everything at the end. We did a similar thing  
9 here for SHINE.

10 So, you know, I can certainly understand  
11 your perspective on this and will take that into  
12 consideration.

13 MEMBER BALLINGER: Okay.

14 MR. BALAZIK: All right, can everybody  
15 hear me okay?

16 MEMBER BALLINGER: Yeah.

17 MR. BALAZIK: All right, good afternoon.  
18 My name is Balazik. I'm a project manager in the  
19 Office of Nuclear Reactor Regulation and I'll be  
20 presenting the staff's evaluation of SHINE's proposed  
21 technical specifications. Next slide, please?

22 So, I'm going to go through the regulatory  
23 basis real quick. 10 CFR 50.34 requires the applicant  
24 to include proposed tech specs prepared in accordance  
25 with the requirements as detailed in 50.36.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1           50.36 specifies what needs to be included  
2           in the tech specs and 10 CFR 50.40 and 50.57 specifies  
3           common standards and findings for issuance of an  
4           operating license. Next slide, please?

5           So, for this review, the staff utilized  
6           the guidance in 1537 and the interim staff guidance  
7           augmenting 1537, also ANSI-15.1, which is the guidance  
8           for the development of technical specifications for a  
9           research reactor. While we couldn't use all of the  
10          guidance contained within that document, there was a  
11          lot of similarities that we could apply to SHINE.

12          And as Catherine said earlier, unique to  
13          this review, the staff also used NUREG-1431, standard  
14          tech specs, and we use this for Westinghouse plants  
15          and we use this for review of the usage rules and the  
16          logic connectors in the action statements.

17          Most of the research and test reactor tech  
18          specs, a majority of them do not use action statement,  
19          logic connectors, or have completion times, so a  
20          little bit of a new review for us. Next slide,  
21          please?

22          First, I just quickly want to go through  
23          a summary of the application. The principle purpose  
24          of the tech specs is to maintain system performance  
25          and ensure safe operation of the facility, to promote

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 public health and safety. These tech specs will be  
2 included with the license.

3 In Section 1, SHINE proposed a lot of  
4 standard tech specs that are in ANSI-15.1 and NUREG-  
5 1537, but SHINE did identify a lot of site-specific  
6 definitions, and they also described the use of logic  
7 connectors and/or with completion times.

8 In Section 2, SHINE proposed safety limits  
9 for both the utilization and production facility with  
10 limiting safety system settings to prevent the  
11 exceedance of those safety limits. Next slide,  
12 please?

13 In Section 3, SHINE proposed limiting  
14 conditions for operation and surveillance requirements  
15 with the application of usage rules, action  
16 statements, and completion times.

17 One item I did like that SHINE did is the  
18 combination of the LCOs and their surveillance  
19 requirements. I think it makes the tech specs a lot  
20 straightforward for the operators that are using them.

21 I think for a majority of the RTRs, it  
22 might be for all of them, but the tech specs of their  
23 surveillances are separated, so again, a little bit of  
24 a usability improvement here.

25 Tech spec Section 4.0, SHINE identified

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 major design features. We talked about one earlier,  
2 the margin of subcriticality. And these are features  
3 that we don't want to be altered or modified that  
4 aren't captured in Sections 2 and 3 of the tech specs,  
5 so SHINE identified a lot of site-specific design  
6 features.

7 And 4 is mostly administrative controls.  
8 A lot of this aligned with ANSI-15.1, but SHINE did  
9 identify additional organizational and procedural  
10 control for the facility. Okay, next slide?

11 All right, so when the staff initially  
12 evaluated SHINE's proposed tech specs, it was Revision  
13 5 that was submitted to the NRC on January 26 of this  
14 year.

15 And in earlier SE sections that we  
16 presented to ACRS, we first had the technical  
17 reviewers take a look at the tech specs, look at the  
18 values, and ensure that they found the values  
19 acceptable for tech specs, so that was like the early  
20 on review.

21 So, we had them look at Sections 2, 3, and  
22 4, along with the surveillance requirements that are  
23 specified in tech specs. And so, based on a lot of  
24 the conversations or discussions with SHINE on the  
25 different chapters of the FSAR, you know, SHINE has

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 been revising the tech specs throughout the process.

2 One thing I would like to add is there is  
3 one outstanding section of the tech specs that we  
4 still need to include in the evaluation and that's for  
5 digital I&C. It's tech spec Section 3.2 and we plan  
6 to present that to the ACRS members on October 21.

7 Okay, so the next step in our evaluation,  
8 the NRC licensing and project management staff, so  
9 that's the staff within DANU, and we also used the  
10 power reactor tech spec branch, we evaluated the tech  
11 specs in a different manner.

12 We looked to ensure the consistency,  
13 clarity, and formatting of the tech specs and mainly  
14 focused on definition, the logical connectors in tech  
15 spec Section 1, the usage rules in Section 3, and  
16 administrative controls in Section 5.

17 And the NRC did audit the tech specs and  
18 we are preparing an audit report. It should be issued  
19 by next week, and if ACRS members want to see that, we  
20 can share that report with them.

21 Based upon that audit, SHINE also, you  
22 know -- Holly, could you go back one slide? There's  
23 one thing I want to touch upon. Based upon that  
24 audit, there was, you know, a lot of discussions on  
25 the tech specs, and SHINE did revise the tech specs

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 and they submitted a complete version of the tech  
2 specs, which is Revision 6, and that's the version  
3 that came in earlier this week that members saw pop up  
4 in their box.

5 Now, SHINE has shared this version with us  
6 earlier, but I just wanted to let members know that  
7 that's the version that showed up in ADAMS a couple of  
8 days ago.

9 MEMBER BIER: Quick question, is there  
10 either an audit report or a markup showing the  
11 difference in the tech specs?

12 MR. BALAZIK: Yeah, well, what we've done  
13 with the audit report is we have Revision 5 and we  
14 have comments out next to the tech specs, and so it's  
15 not going to show the strikeouts, but I guess you  
16 could compare the two and what we looked at, the  
17 comments we had, and then the adjustments that SHINE  
18 made, but it's not going to show the red line  
19 strikeouts.

20 MEMBER BIER: That's fine. Thank you.

21 MR. BALAZIK: Okay, so for the evaluation  
22 of findings and conclusions, SHINE's proposed tech  
23 specs are consistent with the guidance in NUREG-1537,  
24 and the ANSI Standard 15.1, and NUREG-1431.

25 As required by 1536, the SHINE operating

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 license application includes a summary statement of  
2 the basis or the reason for the proposed tech specs.  
3 As required by 1536(b), the operating license  
4 application includes proposed tech specs derived from  
5 the analysis and evaluation included in the SHINE FSAR  
6 as supplemented.

7 The SHINE's tech specs specify safety  
8 limits on the wall, temperature, and the differential  
9 pressure across the primary system boundary, and the  
10 pressures within the process tanks containing the  
11 target material, and the connective piping, and to  
12 reasonably protect against uncontrolled release of  
13 reactivity and the specified limiting safety system  
14 settings that satisfy 50.36(c)(1).

15 SHINE's proposed tech specs include LCOs,  
16 limiting conditions for operation, which are the  
17 lowest functional capability for performance levels of  
18 equipment that are required for safe operation of the  
19 facility that meet the requirements of 50.36(c)(2).

20 Next slide?

21 SHINE's proposed tech specs include  
22 surveillance requirements which relate to testing  
23 calibration to ensure the necessary quality of systems  
24 and components is maintained and that facility  
25 operation will be within the safety limits and the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 LCOs will be met to satisfy the requirements of  
2 50.36(c)(3).

3 The tech specs also include design  
4 features or those features of the facility such and  
5 materials of construction, geometric arrangements,  
6 which, if altered, would have a significant effect on  
7 safety, and that satisfies 50.36(c)(4).

8 And SHINE also included administrative  
9 controls also which discuss the organization and  
10 management procedures, recordkeeping review and  
11 audits, and the necessary reporting to ensure  
12 operation of the facility is operating in a safe  
13 manner, and it satisfies C5 of 50.36.

14 And they also included requirements for  
15 initial notification, written reports, and records  
16 that satisfy 50.36(c)(1)(2) and (7), and also  
17 identified special reports to be reported in  
18 accordance with 50.36(c)(8).

19 And also that the issuance of the  
20 operating license for the facility would not be  
21 inimical to the common defense or security, or to the  
22 health and safety of the public.

23 One thing I would like to add is that as  
24 a result of Revision 6 of the tech specs, the staff  
25 will need to go back and evaluate any impact to the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 previous SE chapters.

2 For example, I don't remember exactly when  
3 we were presented Chapter 4. I think that was in the  
4 spring of this year. While none of the technical  
5 values have been impacted, some of the wording has  
6 been, and that was to ensure clarity and consistency  
7 of the tech specs.

8 So, the staff will go back and take a look  
9 at that wording to make sure it's consistent with Rev  
10 6. If the staff does identify any, I'll say  
11 significant impacts, we can present that information  
12 to the ACRS members during the October 21 subcommittee  
13 meeting.

14 That is my last slide. I don't know if  
15 there's any additional questions that I could answer.

16 One thing, Professor Ballinger, I would  
17 like to add is we did have the technical staff take a  
18 look at the tech specs early on, but we wanted to make  
19 sure that those FSAR chapters, SE chapters, you know,  
20 that they were satisfied with those before we moved on  
21 with the tech specs.

22 So, we did have an early look at them even  
23 though I know we're presenting them today, but there's  
24 been lots of changes that have happened over the last  
25 couple of years for tech specs.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MEMBER BALLINGER: Yeah, I would have  
2 assumed that. Okay, thank you. Okay, we're at the  
3 end of this phase or section if you will. Are there  
4 questions from the members?

5 Okay, if that's the case, then we have one  
6 more presentation and that's by the SHINE folks  
7 related to life cycle overview, and so I don't -- who  
8 is going to do that presentation?

9 MR. BARTELME: Jeff Bartelme from SHINE.  
10 We're just, we're waiting. We're running ahead of  
11 schedule here, so we're just waiting on the -- oh, I  
12 see. Jason, are you here?

13 MR. POTTORF: Yes, I'm on, Jeff.

14 MEMBER BALLINGER: Okay.

15 MR. BARTELME: With the slides shared, we  
16 can get started.

17 MR. POTTORF: Do you want me to share the  
18 slides or are you going to do that on your side, Jeff?

19 MR. BARTELME: I'll share them. I'm just  
20 getting them pulled up.

21 MR. POTTORF: Okay.

22 MR. BARTELME: All right, can everyone see  
23 the slides?

24 MEMBER BALLINGER: Okay, we're ready to  
25 go.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MR. BARTELME: All right, go ahead, Jason.

2 MR. POTTORF: All right, good afternoon,  
3 everyone. This is Jason Pottorf with Rock Creek  
4 Innovations. I'm the Director of Engineering here.

5 Today, I'm going to give an overview of  
6 the programmable logic lifecycle process that we  
7 implement here at Rock Creek, and I want to start off  
8 here on this first slide by pointing out that the  
9 programmable logic development is a part of our  
10 overall system design and control process for Rock  
11 Creek.

12 The programmable lifecycle process  
13 includes five phases, starting with planning and then  
14 requirements, design, implementation, and test.

15 During the planning phase is where we will  
16 identify all system level requirements and trace those  
17 into customer requirements and documents that are  
18 provided from, say, SHINE from the TRPS and ESFAS  
19 system.

20 I want to point out that the V&V  
21 activities that we do for programmable logic  
22 development is performed in accordance with IEEE  
23 Standard 1012, 2004 version, and we will create a V&V  
24 plan for every project that provides a clear mapping  
25 of what we're doing in our lifecycle to those tasks

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 and activities in IEEE Standard 1012. Next slide,  
2 please?

3 So, this figure here is a really high  
4 level figure to show kind of how we approach an  
5 overall system development, you know, that consists of  
6 both hardware and programmable logic.

7 So, we start out there in the beginning in  
8 a planning phase, and that really covers both hardware  
9 and programmable logic where we'll identify system  
10 level requirements, and then after we complete that  
11 first planning phase is where we split the lifecycle  
12 kind of into a hardware path and a programmable logic  
13 path.

14 The programmable path there is shown in  
15 green and that coincides with what we call the system  
16 design phase. So, in the system design phase, we'll  
17 be developing things like hardware design specs for  
18 the individual HIPS modules that are needed for a  
19 specific application.

20 And then we have a separate programmable  
21 logic lifecycle that we go through for all of the  
22 modules, and it's important to know that we actually  
23 implement the full programmable logic lifecycle for  
24 every individual FPGA that will go on a separate  
25 module.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1           So, say, for example, a safety function  
2 module, we will implement the entire programmable  
3 logic lifecycle with the requirements phase, design  
4 phase, implementation phase, and test phase for that  
5 module, and we'll do it separately for every module.

6           You know, and that makes sense because if  
7 you look at a HIPS-based system, each of the FPGAs  
8 that are implemented on a module operates completely  
9 autonomously from each other, so we take the approach  
10 that we can develop the requirements for that module  
11 separately, create the logic, and do all of the  
12 testing, implement it on that hardware and then test  
13 that hardware separately for each module.

14           MEMBER MARCH-LEUBA: Can I interrupt you?  
15 This is Jose. Is there a feedback loop from the test  
16 phase to any of the previous three?

17           Even all the way to requirements, when you  
18 test and you find out that you cannot meet the  
19 requirements or that you probably need additional  
20 requirements, design, or implementation? So, does  
21 your plan for lifecycle plan have feedback loops?

22           MR. POTTORF: Yes, absolutely, yeah, all  
23 through each step of the lifecycle for programmable  
24 logic, you know, V&V will be performing testing and  
25 doing reviews of the design activities, and should

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 they find any anomalies or specific tests that are  
2 failed, yeah, that would then trigger us to go back up  
3 and make modifications, you know, either all the way  
4 up to, say, system requirements at the top, or at the  
5 programmable logic level, we would go back and update  
6 requirements and then go back through the phases.

7 MEMBER MARCH-LEUBA: I do know it is human  
8 nature, but none of us like to do documentation.  
9 Whenever something like this happens, your plan  
10 requires extensive documentation of what happened, why  
11 it happened, and how it was solved? Because failures  
12 are full of good intentions, last-minute modifications  
13 and things like that.

14 MR. POTTORF: Yeah, absolutely, we will --  
15 we do maintain configuration control of all of our  
16 documentation and we would be required to go back  
17 through and update all of that documentation.

18 MEMBER MARCH-LEUBA: I'm not saying keep  
19 the documentation as built, but keeping the  
20 documentation of what failed and probably a root cause  
21 of why it failed, and making you think through it,  
22 something that you want to just go and fix it because  
23 you know this full loop was not properly closed or  
24 something like this, but trying to learn from the  
25 mistakes.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MR. POTTORF: Oh, yeah, definitely, we  
2 would certainly, as part of our programmable logic  
3 development process, you know, we'll categorize any  
4 anomalies found, you know, based on severity, and then  
5 we'll also, you know, we also have your corrective  
6 program as part of our quality assurance program for  
7 Rock Creek where we would identify any specific issues  
8 or major issues like that where we would want to do a  
9 root cause analysis and get that fixed in our program,  
10 definitely, yeah.

11 MEMBER MARCH-LEUBA: You used the right  
12 key words, corrective action. That's the way to go.  
13 Thank you.

14 MR. POTTORF: Yeah, you bet. So, once we  
15 complete that programmable logic set of phases for  
16 each module and complete it for all of the modules  
17 that in the system, then we can move on down into  
18 those lower boxes there where we would integrate.

19 At that point, we would then consider each  
20 module to be a piece of hardware. We would have fully  
21 tested the logic that was implemented in the hardware  
22 and then move into integrating different modules into  
23 chassis, chassis into cabinets, and then cabinets  
24 together and testing them. So, those activities would  
25 then be performed in what we call the system

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 implementation and test phase there.

2 The rest of my presentation will primarily  
3 focus on the green boxes here. I do have, I want to  
4 say three slides where I talk about the details of  
5 what we do in the planning phase, and then I have a  
6 single slide of each of the green boxes here, and then  
7 my final slide kind of covers those last two, the  
8 system implementation and test phase.

9 MEMBER BROWN: Can I ask you a question  
10 before you go on? You can finish what you're doing,  
11 but I just didn't want you to skip it before I ask a  
12 question.

13 MR. POTTORF: Yeah, sure, go ahead.

14 MEMBER BROWN: After you finish the  
15 modules, you've got the modules assembled into a  
16 system, and this is, I think, down in your  
17 implementation and system test phase, is there some  
18 way you, not model, but is kind of a little  
19 engineering model setup where you have the inputs and  
20 then you have a mockup of some type of thing that  
21 you're trying to control the system you're trying to  
22 control, you know, a motor starts, or a valve opens,  
23 or something moves something from point A to point B?

24 Have you got a little mockup to show that  
25 you get the proper outputs before it ever gets into

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 the plant or is the plant the actual first  
2 combinational overall system test?

3 MR. POTTORF: So, yeah, we would  
4 definitely -- that type of testing would be performed  
5 down there at that system test phase. We actually use  
6 speed good equipment which --

7 MEMBER BROWN: I don't know what that is.  
8 Is that a software system that you can program to look  
9 like your final actuated system?

10 MR. POTTORF: Yeah, it's basically a set  
11 of equipment where we can provide simulated inputs,  
12 whether those are 4 to 20s, or R2D, or discrete inputs  
13 --

14 MEMBER BROWN: Okay.

15 MR. POTTORF: -- and then also receive  
16 real-time, you know, outputs from the system,  
17 providing real-time inputs and outputs to the system  
18 and then running through kind of those system level  
19 tests to simulate operation of the actual equipment.

20 MEMBER BROWN: Okay, and that's before you  
21 actually go down into the plant when it's built and  
22 doing your overall installation and confirmation  
23 tests?

24 MR. POTTORF: Yeah, that's --

25 MEMBER BROWN: That's probably a wise

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 thing to do. That's why I asked.

2 MR. POTTORF: Yeah, definitely.

3 MEMBER BROWN: Okay, thank you.

4 MEMBER MARCH-LEUBA: Before you get  
5 comfortable and start going back again to your  
6 presentation, I know we're talking about software  
7 lifecycle mostly because that is a well-defined term,  
8 but are you planning for hardware obsolescence? And  
9 what I'm thinking is the reason there aren't that many  
10 customers for a HIPS system.

11 Are you planning 25 years from now there  
12 won't be a supplier for it and then how are you going  
13 to maintain your system for 40 to 60 years? Is this  
14 part of the lifecycle analysis?

15 MR. POTTORF: Not explicitly, and I would  
16 say the FPGA-based modules lend themselves quite well  
17 to managing that kind of obsolescence down the road.  
18 You know, and the way that we would do that, when we  
19 -- so we actually have diverse FPGAs, so different  
20 types of FPGAs from different vendors that we're  
21 implementing across the division of the TRPS and  
22 ESFAS.

23 So, when we go through logic development,  
24 requirements phase and design phase, and then at the  
25 very beginning of the implementation phase is where we

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 will generate hardware description language from the  
2 logic models that are created in the design phase.

3 That hardware description language is  
4 agnostic of the hardware that it actually gets  
5 implemented on in the implementation phase. So, you  
6 know, for now, what we're implementing for, say, TRPS  
7 and ESFAS is specific to, say, Intel or Xilinx FPGA.  
8 That hardware description language, that HDL code  
9 really isn't specific to any of that hardware.

10 So, say, 25 years from now, you know,  
11 whatever the available hardware is, that HDL is really  
12 a generic implementation of logic in whatever the  
13 hardware happens to be.

14 So, yeah, there would be some work  
15 required down the road for whatever that hardware  
16 looks like 20 or 30 years from now, but it lends  
17 itself to being able to implement the exact same logic  
18 on whatever the hardware ends up being.

19 I don't know, Gregg, if you want to jump  
20 in here and provide any more on that topic?

21 MR. CLARKSON: Yeah, I can jump in on  
22 that. Yeah, actually the obsolescence issue is one of  
23 the key reasons we wanted to target utilizing FPGAs,  
24 and so there's, you know, in addition to what Jason  
25 said, there's another aspect to this and that is make

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 the design as simple as possible.

2 So, the rest of the supporting hardware on  
3 a module or on a circuit board, make that as simple as  
4 possible and reduce the component count as much as you  
5 can, and that just, that translates to less hardware  
6 obsolescence issues down the road.

7 So, get the logic all put into the HDL,  
8 the hardware description language, the test factors,  
9 you know, all of the stuff that's required to describe  
10 the logic, and then test for the logic is completely  
11 portable so that ten years from now, you can target a  
12 different FPGA or a different type of device, in fact,  
13 and retain the design exactly as-is and the test  
14 factors exactly as-is, you know, on their first  
15 deployment.

16 MEMBER MARCH-LEUBA: Have you given any  
17 thought of -- I mean, we're designing plants for 40,  
18 60 years, and I was watching on the plane a Big Bang  
19 Theory show where he keeps his most important file on  
20 an eight-and-a-half-inch floppy. You cannot read it.

21 So, do you have any configuration control?  
22 I mean, are all of these files stored in somebody's  
23 hard drive or -- it's not easy to ensure that you'll  
24 have access to these things and be able to read them  
25 and understand them in, what, in 2080.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MR. CLARKSON: Yeah, we take a systematic  
2 approach to that. So, everything that we do is within  
3 what we call a repository, an aversion control system.  
4 See, so that's important so that you keep everything  
5 together that's required for a project, so if you  
6 happen to pick it up 20 years from now, you would have  
7 all of the files.

8 But then the question arises, well, what  
9 about the applications to look at the files and, you  
10 know, many, many, many other concerns that you have?

11 So, the systematic approach is to have  
12 everything captured in a repository, create, you know,  
13 virtual machines of the entire environment, including  
14 the applications required to view those files, you  
15 know, and make that to where it's as portable as  
16 possible.

17 But then finally, there's nothing that can  
18 replace just good documentation. We call them  
19 artifacts, but they are, in fact, the documents that  
20 come out of this process.

21 The specifications, the logic  
22 descriptions, the logic drawings, all of that, keep  
23 that also as a hard copy and just, you know, really  
24 make sure you capture all of those artifacts so that  
25 worst-case if all you had was that hard copy, you

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 would have the exact logic implemented. You would  
2 have the exact listing of the test factors.

3 You know, you'd have to go recreate them  
4 in another tool at that time, but you could recreate  
5 it, and that's what's important.

6 MEMBER BROWN: You're going to keep paper  
7 in other words?

8 MR. CLARKSON: That's right. We're going  
9 to keep something to where somebody can look at it  
10 physically and not rely on a three-and-a-half-inch  
11 floppy from eBay, you know, to make sure it works.

12 MEMBER BROWN: I ask that question for two  
13 reasons because Jose's comment about the floppy rang  
14 a bell. I mean, I still have my Windows XP computer  
15 that I bought back in 19, I don't know, '98 or  
16 something like that and I can still read my floppies  
17 fortunately. But that's an interesting way to do it,  
18 the paper with the HDL. I guess the way you're doing  
19 it, you can do that fairly well.

20 One of my worries in a previous program,  
21 and I don't know that you'll face this or not because  
22 this was a software-based system not a FPGA-based  
23 system, was even the language in which you do your  
24 programming in becomes obsolete.

25 Right now, it's C++, so we developed

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 standard modules to perform functions so that we knew  
2 what the inputs and outputs were, and then we could  
3 program that module even if D++ came along and it  
4 actually worked. It was kind of a generic approach.  
5 Otherwise, the cost was going to drive us crazy. I'm  
6 talking 100 applications to put this in, not just one  
7 plant.

8 MEMBER MARCH-LEUBA: But I'm glad --

9 MEMBER BROWN: So, you guys seem to be on  
10 the right track from what I can see. Thank you.

11 MEMBER MARCH-LEUBA: I'm glad you're  
12 thinking about this even though it's not the standard  
13 for lifecycle and making some thoughts and effort into  
14 it.

15 Because with the old large light-water  
16 reactors and you had your I&C, you just pulled the  
17 card, take a picture of it, and reverse engineering.  
18 You just look at the coils and the resistors and  
19 figure out what resistor you have in there.

20 MEMBER BROWN: Even the integrated  
21 circuits and --

22 MEMBER MARCH-LEUBA: Yeah.

23 MEMBER BROWN: -- even the logic circuits,  
24 you could do that with.

25 MEMBER MARCH-LEUBA: But now systems are

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 so complex that unless you document it ahead of time,  
2 two years from now, you won't be able to do it, so  
3 please do a good job of keeping records. Thank you.

4 MR. CLARKSON: Yeah, a key thing, you  
5 know, Charlie, to go along with what you said there on  
6 the software system, the key difference between an  
7 FPGA-based system or a logic-based system and a  
8 software system is, you know, when you get the  
9 software, ultimately it comes down to its machine code  
10 for whatever the underlying machine that it was -- you  
11 know, whether you read it in C++, FORTRAN, or PASCAL,  
12 whatever the programming language was, it ultimately  
13 gets compiled down into machine code, but if you don't  
14 have the underlying machine to execute it, it doesn't  
15 do you any good.

16 What's neat about the FPGAs is what  
17 results in the FPGA is actual logic, you know, gate  
18 level logic. So, I could presumably go and build a  
19 fully hardware version of what's in that FPGA using  
20 individual logic gates.

21 So, you're not reliant on that underlying,  
22 you know, software machine, you know, the computer if  
23 you will, and so it makes it much more like hardware.  
24 You're designing hardware, you know, with a hardware  
25 result.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1           So, it gives you a lot -- and you can do  
2 a simpler design that way and it gives you just a lot  
3 of tools to deal with that future obsolescence that  
4 you know you're going to see. It's just part of it.

5           MEMBER BROWN: No, I really like, I do  
6 like the FPGA approach to doing this stuff. I found  
7 in my other program even changing the compiler to  
8 compile your code can screw up the functionality of  
9 what you're trying to accomplish.

10           That actually happened. That's why I can  
11 make that statement. So, we had to find a way around  
12 that. You can do it, just we didn't think of it  
13 before. Everybody thinks you compile the code. You  
14 compile the code. You gets ones and zeroes and --

15           MEMBER MARCH-LEUBA: You probably won't  
16 understand me, but what you have to do is disable  
17 optimizations.

18           PARTICIPANT: Okay, yeah.

19           (Laughter.)

20           MEMBER BROWN: Okay, well, thank you.  
21 Thank you for the explanation and the expansion of the  
22 comment. Thank you.

23           MR. POTTORF: All right, if we're ready to  
24 move on, I guess we can jump to the end of the  
25 planning phase. This is fairly standard stuff here.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 We start out within the life cycle is design and  
2 review, reviewing all -- all things provided from the  
3 customer which is SHINE in this case. I have a list  
4 here of typical things that we would review and put  
5 under configuration control at the start of a project.

6 For SHINE'S TRPS and ESFAS, those main  
7 inputs for us are their design criteria documents, as  
8 well as their functional requirement specs, that we  
9 would bring in and put under configuration control.

10 Next slide.

11 So what we do, we start out by creating a  
12 design input list, what we call the design input list  
13 to formally track those documents that are the  
14 requirements for the system design. Anything that we  
15 receive informally from the customer, we would track  
16 that as an unverified assumption so we have what we  
17 call our UVA process to track anything like that and  
18 our life cycle does require that before we do any kind  
19 of baselining of program and logic testing or system  
20 testing that we must have closed all of those  
21 unverified assumptions that might be created during a  
22 project.

23 Also, in the planning phase, we will  
24 create all of the plans that drive the work for the  
25 life cycle so -- and I have those listed here. We

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 create a quality assurance plan, programming and  
2 logical development plan. That document would specify  
3 all of the individual FPGAs that we're going to  
4 develop logic for and test in the system.

5 We'll create a configuration management  
6 plan, separate V&V plan that covers V&V of all the  
7 program and logic. We'll create a qualification plan,  
8 if required, and a separate test plan as well for all  
9 testing activities.

10 Then we also do a security assessment. We  
11 do have a HIPS platform security plan and in the  
12 security assessment what we do there is evaluate the  
13 proposed system architecture for cyber security  
14 vulnerabilities and how we're going to address those  
15 in the system, and identify any security-related  
16 requirements for the system there.

17 Next slide.

18 Then the next important design documents  
19 that we create in the planning phase would be a system  
20 requirements spec. So this is where we're taking  
21 those high level system requirements from SHINE, say  
22 for the TRPS and ESFAS, and detailing those out into  
23 atomic testable requirements for the system, both  
24 hardware and programmable logic and user or  
25 programmatic-type requirements for the system design.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 So we'll document that in our SyRS system requirement  
2 spec and we'll establish traceability from each of  
3 those requirements up to SHINE's input, design input  
4 documents.

5           Once we complete a system requirements  
6 spec, then we create a system design specification.  
7 And this is where we identify the -- all of the  
8 individual components for the HIPS-based system. So  
9 any divisions, cabinet chassis, and modules that will  
10 comprise the system. And this is where we will  
11 allocate those system requirements to those individual  
12 pieces of hardware so we know which programmable logic  
13 requirements are going to be implemented on which  
14 FPGAs or modules.

15           That system design spec will include  
16 listing of all inputs and outputs for each piece of  
17 hardware, including the tag names and descriptions of  
18 them, what are the types of the signals and the ranges  
19 for those inputs and outputs.

20           Any questions on planning phase before I  
21 move on?

22           If not, next slide.

23           So now we move into programmable logic  
24 specific phases. And so these activities are, as I  
25 showed in that figure before, they are performed in

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 conjunction with the system design phase. It includes  
2 requirements of the design implementation and tests  
3 for programmable logic.

4 For each of those four phases, we will  
5 create -- the V&V organization will create phase  
6 summary reports as part of the formal exit criteria  
7 for moving on to the next phase in the life cycle.  
8 As I mentioned before, we do implement this entire  
9 life cycle for each field programmable gate array, the  
10 logic gets implemented on each one. And we do perform  
11 all of the logic development activities within Rock  
12 Creek's secure development environment and the  
13 isolated development network.

14 Next slide.

15 For the programmable logic requirements  
16 phase, this is where we are documenting all of the  
17 programmable logic requirements for a given FPGA.  
18 This is to translate those system level requirements  
19 into the specific detailed programmable logic  
20 requirements.

21 As I mentioned before, we create a  
22 separate VLRS for each FPGA within the system. We  
23 establish feasibility for each of those programmable  
24 logic requirements up to the system requirements spec  
25 at that time. These requirements are required to be

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 adequate enough to support the implementation and  
2 verification of the design.

3 In each of the programmable logic  
4 requirements specs, we do provide a virtual  
5 description of the logic functions and provide the  
6 level of detail to implement that verification of the  
7 design. So the programmable logic requirements and  
8 their associated traceability are independently  
9 reviewed by our V&V organization where they would  
10 provide any anomalies identified associated with those  
11 and then those would be required to be addressed by  
12 the design organization.

13 Next slide.

14 So the next phase, programmable logic  
15 design phase. During this phase, we'll create at  
16 least one logic model associated with each  
17 programmable logic design spec. For an application,  
18 it should be a one-to-one. For every programmable  
19 logic requirements spec, we'll create a programmable  
20 logical design spec in one single model to implement  
21 all the logic for that programmable logic requirements  
22 spec.

23 The programmable logic design spec  
24 provides a description of the logic architecture,  
25 control logic, any data structures, I/O format,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 interfaces needed for that logic, and algorithms  
2 necessary to implement the programmable logic  
3 requirements. These logic models are developed  
4 following formal modeling standards, as well as Rock  
5 Creek's model based development procedure.

6 Review of the logic model is then  
7 performed by V&V to verify that it meets the  
8 requirements and then the V&V organization would  
9 perform the programmable logic testing for that  
10 specific model. The results of that testing would  
11 then be reviewed by the design organization to  
12 validate that meets the requirements.

13 There are two levels of testing that we  
14 perform for the logic. So we have a HIPS platform  
15 core logic that we logic that we develop separately  
16 that would be used. These are kind of library blocks  
17 of logic that we would expect to be implemented in  
18 just about every application. We will combine those  
19 HIPS library blocks, logic library blocks, with logic  
20 blocks that we create that are specific the  
21 application for the system. So for say a TRPS system  
22 for SHINE, we'll create a separate set of logic to  
23 implement that logic specifically. We'll test that  
24 separately and then we'll integrate it with the HIPS  
25 platform library blocks and then test the integration

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 of those together.

2 Also in this design phase is where we  
3 would begin preparation for testing of the logic once  
4 it is implemented in hardware. And so this includes  
5 what we call a module test plan and test designs.

6 The module test is -- would be akin to  
7 what is normally called a system-acceptance testing  
8 for like a typical software-based system where you're  
9 implementing, you know, kind of one piece of software  
10 for an entire system. Once you implement all that  
11 software into hardware and you do your final  
12 acceptance testing, that would be akin to what we are  
13 calling the module test because of -- because each  
14 module is autonomous and independently operates of  
15 itself, we do that kind of acceptance testing at the  
16 module level here, so that's what we call module  
17 tests. And so in this phase is where we start to  
18 create those test plans and test designs to perform  
19 that once the logic is implemented in hardware.

20 Next slide.

21 MEMBER MARCH-LEUBA: Before you go on, did  
22 you're talking about all the testing -- first, an  
23 observation, are you using future tense for almost  
24 everything? We didn't towards the end of the project,  
25 right? When are we going to have a final anything?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 And I see this stuff is right or you want them to  
2 answer?

3 MR. BORROMEO: Yes, we can certainly  
4 answer. So where we're cutting off the licensing  
5 review is the requirements phase and then the rest of  
6 the phase we'll look at it in the oversight phase.  
7 This is similar to the framework that we've used for  
8 HIPS.

9 MEMBER MARCH-LEUBA: What kind of scale  
10 are we talking about? Are we talking Christmas? Are  
11 we talking 2055?

12 MR. BORROMEO: So they're on track to be  
13 completed with the requirements phase in October.

14 MEMBER MARCH-LEUBA: All right. So my  
15 next question is related to this. FPGAs are not --  
16 this is for SHINE. If FPGAs are not as vulnerable as  
17 software systems to memory leaks, database collection,  
18 things that build up over time, so whenever we have a  
19 module finalized, I would like to see for at least a  
20 couple of months before I declare it -- as part of the  
21 testing, there should be an extended burnout to ensure  
22 that whatever FPGAs are vulnerable over heat up or  
23 damage over time, get tested.

24 I wouldn't feel comfortable with less than  
25 two months with any of my equipment. What do you

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 think, SHINE, Jason?

2 MR. POTTORF: Gregg, you want to tackle  
3 that one?

4 You know, what I would say we've had -- so  
5 we've developed all the hardware already for the TRPS  
6 and ESFAS. And we've put out preliminary versions,  
7 sometimes multiple versions of the programmable logic  
8 models and implemented those. So we've actually had a  
9 golden -- what we call a golden unit which is with  
10 preliminary sets of logic implemented and running on  
11 the actual hardware so -- and we've had that running  
12 for close to two years now, I believe.

13 I would also say, you know, this same type  
14 of hardware and logic was implemented at Wolf Creek  
15 and has been running there since Gregg --- that would  
16 have been 2010, '11-ish?

17 MR. CLARKSON: 2009, but to answer -- I  
18 hear the question and yes, so one of the approaches we  
19 take, as like Jason mentioned, is we build what we  
20 call a golden unit as early in the project as we can,  
21 even back into the conceptual phases of the project so  
22 that as you're capturing the system requirements,  
23 system design, allocating that out down into the  
24 individual modules and allocating that programmable  
25 logic, you can conceptually start to implement early

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 instances of that logic into the hardware and run it,  
2 you know, and see it running and see it interacting.

3 So this golden unit evolves through the  
4 project all the way to the end when you finalize the  
5 design and you have your final logic for each of the  
6 individual modules implemented into the hardware and  
7 then all running as a final, final system.

8 So it gets you that, like you said, those  
9 counter overruns or stack -- in this case, we're not  
10 stacks or EAPs or anything because we don't have  
11 executable code, but it gets you those timing element  
12 aspects a good look at those to make sure you don't  
13 have any unexpected temporal effects of the system  
14 running.

15 MEMBER MARCH-LEUBA: Yes, when do  
16 software, you always get surprised when you're running  
17 more than a few hours. Memory leaks build up. Whenever  
18 you do design instrumentation I have all these fights  
19 with everybody else because I want to reboot every  
20 night, say I can test the equipment I send you for 24  
21 hours guarantee, we'll go for 24 hours, but no more  
22 than that. So then I will reboot. And everybody was  
23 supposed to dial completely because that's what I  
24 tested it for.

25 So certainly when we have the final, let's

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 make sure we run it for a week or two, not just a spur  
2 of the moment.

3 Another question, with respect to cosmic  
4 rays and high-energetic cosmic rays, is there any  
5 component on FPGA that could slip a bit and give you  
6 the wrong output? If I send you a single event extra  
7 gamma ray.

8 MR. CLARKSON: Yes, so if you have like a  
9 single event upset or a single upset or however you  
10 want to state that, so you know, what that would do is  
11 that would impact some physical portion of the silicon  
12 on the device. And so presumably, it would take out  
13 a transistor or a group of transistors.

14 So one of the things that we do is we  
15 develop three legs of the logic in the upper portion  
16 of the system, what we call a safety function module.  
17 We develop three individual instances of logic that  
18 are physically independent from one another and then  
19 that three legs of the safety data bus we call it or  
20 the safety path, that stays intact through the whole  
21 system all the way down to what we call the equipment  
22 interface module. That's very effective for a lot of  
23 different reasons, but one of them is it's very  
24 effective against a single event upset situation. So  
25 that if you had a cosmic ray or something -- mutual

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 bombardment, you come in and you take out some  
2 physical aspect of that -- of a particular FPGA. That  
3 logic that's associated with that physical aspect will  
4 no longer function properly. It will then behave  
5 differently than the other two that weren't impacted  
6 by that physical event. And you'll be able to detect  
7 that.

8 MEMBER MARCH-LEUBA: Yes. Just remember  
9 that SHINE is going to be very unusual, there's going  
10 to be an awful lot of 14 MeV neutrons running around.  
11 I imagine you have a lot of shielding, but there's  
12 going to be a lot of 14 MeV neutrons out there. So we  
13 may have -- you may have to consider final testing for  
14 single event scenarios. 14 MeV neutrons are very  
15 difficult to shield, believe me.

16 Okay, those are all my questions. Thank  
17 you.

18 MR. POTTORF: Okay, sounds good. Next  
19 slide.

20 So next phase would be implementation of  
21 the programmable logic in the hardware is where we're  
22 integrating the logic to the target hardware. During  
23 this phase, the beginning of this phase, we will  
24 generate the hardware description language code from  
25 the logic models and trace each of those code

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 statements to programmable logic design model  
2 elements.

3 V&V will review and analyze that code to  
4 ensure compliance with the requirements and then we  
5 will perform synthesis and the placement routing of  
6 the code and do a review and analysis of that activity  
7 as well, the results of that.

8 Also, after that during this phase, the  
9 designer would generate all the programming data and  
10 program-specific FPGA hardware.

11 At the end of this phase, we would then  
12 finish up the planning activities for testing of all  
13 of the programmable logic, so we will be do post-  
14 synthesis testings. We'll create the test plans,  
15 designs, cases, and procedures to perform the post-  
16 synthesis testing, as well as develop the specific  
17 module test cases and test procedures.

18 Next slide.

19 And in the programmable logic test phase,  
20 this is where we'll execute those -- the post-  
21 synthesis testing and generate the reports, as well as  
22 perform the final module testing once the logic is  
23 implemented in hardware -- and produce those test  
24 reports as well.

25 Once all of that is complete, then V&V

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 will prepare what we call module final report,  
2 summarizing all of the V&V activities associated with  
3 each of the programming logic -- each programmable  
4 logic that gets implemented on each FPGA, so the  
5 outputs from this phase are sure to be complete and  
6 approved. This is the control point before we move on  
7 into that system portion of our overall life cycle  
8 where we do the system integration of hardware  
9 components and testing of that.

10 Next slide.

11 So this is the -- kind of summarizes those  
12 two blocks at the end of the figure I showed earlier  
13 wherein the system implementation phase is where we'll  
14 integrate all the different hardware components. So  
15 this will be a programmed HIPS modules, installing  
16 those in the chassis and those chassis in the cabinets  
17 and do the integration testing, consistent testing,  
18 and acceptance testing. So we'll have some separate  
19 tests for -- specific to integration of hardware.  
20 What we call system testing, that will be more  
21 specific to proving that we've met our HIPS platform  
22 requirements whereas our acceptance testing is more  
23 for proving that we've met all of SHINE's TRPS and  
24 ESFAS functional requirements for the system.

25 So the test cases and procedures for

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 performing for tests are prepared and approved during  
2 the implementation phase which would then lead to  
3 executing those test cases and procedures in the  
4 system test phase.

5 All the hardware and programmable logic  
6 design must be baseline prior to performing the system  
7 acceptance testing in the system test phase. We call  
8 that our test baseline. Once we create a test  
9 baseline, that is where we are required in our process  
10 to begin formal design change control.

11 That is really it for the presentation.  
12 Any questions?

13 If not, I'll turn it back over.

14 MEMBER BALLINGER: Okay, curiosity  
15 question. Jason, have you ever fished in Rock Creek?

16 MR. POTTORF: What's the question?

17 MEMBER BALLINGER: It's a Friday afternoon  
18 question. Have you ever fished Rock Creek in Montana?

19 MR. POTTORF: I have not.

20 MEMBER BALLINGER: Put it on your list.  
21 Beautiful place.

22 MR. POTTORF: All right, will do.

23 CHAIRMAN REMPE: So Member Ballinger, I  
24 have a question, but it's not on this particular  
25 topic. It pertains to all three of the topics

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 discussed today.

2 MEMBER BALLINGER: Yes.

3 CHAIRMAN REMPE: I'm thinking about the  
4 memos and when the lead members will be providing  
5 their memos to you. And because you're going to be  
6 gone during October full committee week, I'd suggest  
7 that the decision be made that that November 15th  
8 subcommittee meeting be used to discuss the memos.  
9 And I believe that's allowed, but Larry Burkhart can  
10 weigh in and say yes or no, but I think since the  
11 memos were kind of out of our normal routine, then you  
12 could have that during that --

13 MEMBER BALLINGER: I'm responsible for one  
14 of them.

15 CHAIRMAN REMPE: Well, yes, so that's why  
16 I'm bringing it up now because it's different folks  
17 that are responsible for them. Is that --

18 MEMBER BALLINGER: That's fine. It's just  
19 that we now need to expand the -- from half day to a  
20 full day.

21 CHAIRMAN REMPE: Well, there's a tentative  
22 subcommittee meeting for the 15th, and you're going to  
23 be talking about the letter and we could do a full day  
24 or something earlier, but that's why I'm bringing it  
25 up now because the SHINE folks as well as the staff

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 may want to be present.

2 MEMBER BALLINGER: Yes, that's fine.

3 CHAIRMAN REMPE: And Larry, are you out  
4 there? And do you want to start then in the morning  
5 on the 15th instead of the afternoon?

6 MEMBER BALLINGER: I don't have the --

7 CHAIRMAN REMPE: It's Tuesday, November  
8 15th and it's currently scheduled -- we're going to be  
9 in-person to start at 1 p.m.

10 MEMBER BALLINGER: I'm just trying to get  
11 at the October --

12 MR. BURKHART: This is Larry. What's the  
13 question?

14 MEMBER BALLINGER: The October  
15 subcommittee is virtual, right?

16 CHAIRMAN REMPE: The October subcommittee  
17 is virtual and it's on PICS in the phased approach and  
18 it's a whole day. You're going to be gone. And  
19 normally, we would do this at the full committee  
20 meeting.

21 MEMBER BALLINGER: I'll be here for the  
22 October subcommittee meeting.

23 CHAIRMAN REMPE: Yes, you'll be gone  
24 during the October full committee meeting and you've  
25 got these memos, there's three topics. And so are

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 there three memos? Is that a correct assumption?

2 MEMBER BALLINGER: I don't -- there's  
3 definitely two. I don't know about the life cycle.  
4 That's not a chapter.

5 CHAIRMAN REMPE: Okay, so maybe just two  
6 memos. And so if that's the case, I don't think you  
7 don't have need to have an agenda change or the time  
8 start change.

9 MEMBER MARCH-LEUBA: I think Josh wants to  
10 say something.

11 MR. BORROMEO: Yes, so life cycle will be  
12 part of Chapter 7.

13 MEMBER BALLINGER: Okay, so there may --  
14 that's Charlie's.

15 MR. BORROMEO: Yes, that's software life  
16 cycle.

17 MEMBER BROWN: I don't remember reading it  
18 when I read Chapter 7.

19 MEMBER MARCH-LEUBA: It's under  
20 development. We need the SER.

21 MR. BORROMEO: We're well aware.

22 MEMBER BALLINGER: So we have to do a  
23 little offline talking.

24 MEMBER BROWN: A lot of offline talking  
25 because we'll bring up the other issues. Let's go

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 ahead and finish this.

2 MEMBER MARCH-LEUBA: No, let's finish this  
3 because I have a delicate question for SHINE.

4 MEMBER BROWN: What was Joy talking about?  
5 We're talking about?

6 MEMBER BALLINGER: She's suggesting that  
7 we have -- whatever product we produce by way of a  
8 memo for this discussion, gets presented and talked  
9 about during the November --

10 CHAIRMAN REMPE: November subcommittee.

11 MEMBER BALLINGER: November subcommittee.  
12 We have a half day.

13 CHAIRMAN REMPE: You have the November  
14 full committee week that we can discuss it, too. It's  
15 up to you, but I just was wondering when will this be  
16 discussing, it won't be during October. I'm just  
17 trying to figure it out.

18 Yes, we have five letters. November is  
19 very full. We don't have SHINE on the agenda.

20 MEMBER BROWN: Is there another memo on  
21 this for the discussion? You're talking about these  
22 little memos, we talked about?

23 MEMBER MARCH-LEUBA: Yes, and it should be  
24 part of Chapter 7 and as I told you earlier many times  
25 since I was in the Army and you never volunteer for

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 nothing, but I want to volunteer to send you a  
2 paragraph or two on this.

3 MEMBER BROWN: Right now, I've got 1.152  
4 Chapter 7, CCF; and I've still got some Chapter 7  
5 thing that I'm supposed to do plus the PICS is coming  
6 up in another two weeks.

7 MEMBER MARCH-LEUBA: I'll send you two  
8 paragraphs on life cycle for you to attach to the  
9 letter for November.

10 CHAIRMAN REMPE: We're not talking about  
11 November full committee week. We have too many things  
12 going on. We're talking about November subcommittee  
13 week.

14 MEMBER BROWN: I'm looking at the little  
15 green box. I call that the rainbow chart.

16 CHAIRMAN REMPE: Good. That's what you  
17 should -- yes, and so -- it's either that -- I mean  
18 the full letter gets done December full committee  
19 week, and so that's not the time to do it.

20 MEMBER BALLINGER: Okay, yes.

21 MEMBER BROWN: I read all of Chapter 7.

22 MR. BORROMEO: So this is in the FSAR  
23 Chapter 7. The staff has not yet completed their  
24 review of life cycle.

25 MEMBER BALLINGER: Okay, so now my

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 question is when?

2 MR. BORROMEIO: October 21st. So the plan  
3 that we were aware of was we're going to -- because  
4 there was a lot of questions last time, we wanted to  
5 grease the skids -- this is what life cycle looks  
6 like.

7 MEMBER BALLINGER: Oh, I see. Okay.

8 MR. BORROMEIO: So right now, you don't  
9 have an SER from us.

10 MEMBER BALLINGER: So life cycle is just  
11 a separate issue. We're talking about now cyber  
12 security and the tech spec.

13 MR. BORROMEIO: Those are done.

14 MEMBER BALLINGER: Okay. So now let's get  
15 back to the --

16 CHAIRMAN REMPE: You have two memos, cyber  
17 security and tech specs, during the November  
18 subcommittee on the 15th.

19 MEMBER BALLINGER: Now wait a minute, we  
20 will have -- we will have had a discussion of -- we  
21 will have had a presentation on the PICS in October,  
22 right? So we're talking about November three, at  
23 least three memos because now we have to include the  
24 PICS.

25 CHAIRMAN REMPE: So you'll have three

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 memos during November 15th subcommittee meeting. Now  
2 I hear you're going to get a chapter 7 SDE on October  
3 21. When is that discussion going to occur? Will  
4 there be any other discussion?

5 MEMBER BALLINGER: That's out of sight of  
6 any --

7 MR. BORROMEO: So for Chapter 7, we  
8 presented the safety related system, the RPS&S.

9 MEMBER BALLINGER: Yes.

10 MR. BORROMEO: Right? We have life cycle  
11 and case that's still outstanding.

12 MEMBER BALLINGER: Okay.

13 CHAIRMAN REMPE: So then by December,  
14 you're going to -- are you going to have a memo on  
15 Chapter 7 or are you just going to go gung-ho for the  
16 final letter and not have a memo in Chapter 7?

17 MEMBER BALLINGER: It's a piece of Chapter  
18 7.

19 CHAIRMAN REMPE: Okay, so we have to have  
20 -- we won't have any other memo on all of this stuff.

21 MEMBER BALLINGER: Right.

22 CHAIRMAN REMPE: We're just going to go  
23 gung-ho for the final letter.

24 MEMBER PETTI: But the only question it  
25 might be given the timing most expeditious is to just

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 take a couple of paragraphs as Jose has agreed and put  
2 it and modify it -- go with another revision of the  
3 Chapter 7 memo that exists.

4 MEMBER BROWN: But there is no -- I haven't  
5 written it --

6 MEMBER PETTI: Oh, you haven't written it  
7 yet.

8 MEMBER BROWN: No, I just got the template  
9 for it two days ago, three days ago, whenever Chris  
10 sent me a template.

11 MEMBER BALLINGER: Well, now we have an  
12 opportunity because if you can supply a couple (audio  
13 interference) to Charlie, you can kill two birds with  
14 one stone.

15 MEMBER BROWN: I don't mind merging them,  
16 it's just --

17 CHAIRMAN REMPE: That's not us, that's  
18 somebody else on the line.

19 MEMBER BROWN: Look, I'm going to ask one  
20 other question. Right now, all I've heard is dates,  
21 dates, memo here, memo there, whatever. Send me an  
22 email. Tell me when the X memo is supposed to be  
23 prepared for whatever meeting we attend, and when.

24 CHAIRMAN REMPE: You're the subcommittee  
25 chair.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 MEMBER BROWN: I want it in writing, okay?  
2 Then I have to produce a memo for something. Right  
3 now, it's been up in the air now for months. I was  
4 waiting to do the PICS thing to go along with it.

5 MEMBER BALLINGER: It's never been up in  
6 the air for months.

7 MEMBER BROWN: Sorry. I've never seen a  
8 schedule. All I know is it's just been talky-talk.  
9 Okay?

10 MEMBER BALLINGER: We've already published  
11 the schedule 20 times. Never mind. Okay.

12 CHAIRMAN REMPE: Okay, so I think I heard  
13 that you'll send a memo to Charlie about when the  
14 schedule is due. And I've heard that some memos will  
15 be discussed on this November 15th and you may like to  
16 have the whole day is what I'm hearing.

17 MEMBER BALLINGER: Well, I'm just saying  
18 that you suggested that we do -- go through a draft of  
19 the letter on that day as well.

20 CHAIRMAN REMPE: Right.

21 MEMBER BALLINGER: So to me that's half a  
22 day. And now you're talking about this which is fine  
23 which means --

24 CHAIRMAN REMPE: -- a whole day.

25 MEMBER BALLINGER: You can't put ten

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 pounds in a five pound paper bag.

2 CHAIRMAN REMPE: Well, let's do a whole  
3 day. That sounds good. I'm bringing it up now  
4 because I'm thinking about the future. That's the end  
5 of that topic.

6 I have another topic that I'd like to talk  
7 about that's not pertaining to this subject and I'll  
8 be quiet for a while if you want to go first, okay?

9 MEMBER MARCH-LEUBA: Yes, I wanted to go  
10 back to Jason and the SHINE -- you guys missed earlier  
11 this afternoon the cyber security interesting  
12 discussions. When you generate the FPGAs and do the  
13 compiling and building the hardware, do you have a  
14 cyber security program or plan for your machines you  
15 use to do the compiling, right? Because it's a low  
16 probability event, but I can be very devious and  
17 install an Easter egg in the hardware that only gets  
18 triggered on Christmas 2028. You'll never test that.

19 So yes, I think when this comes from the  
20 staff and I'm going to ask you guys to see what type  
21 of cyber security we have on the generation of highly  
22 reliable HIPS systems by going to the -- those are the  
23 crown jewels of the protection system.

24 MR. BORROMEO: Understood.

25 MR. POTTORF: I was just going to point

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 out, yes, Rock Creek, we do have a secured development  
2 environment and isolated development network program  
3 complete with all its own procedures and forms and  
4 plans, so yes, we do all --

5 MEMBER MARCH-LEUBA: When you submit the  
6 final, half a page on the report, saying that you have  
7 considered it. It's a very low-probability event that  
8 would be difficult to do, but Easter eggs have  
9 happened. Okay. Thank you.

10 MEMBER BROWN: So for Chapter 7, we're  
11 expecting Chapter 7 on the systems that operate SHINE  
12 to do their thing. That was the I&C part.

13 There's a cyber section as well, right?  
14 Who's going to do that?

15 MEMBER MARCH-LEUBA: Me.

16 MEMBER BROWN: You're going to prepare a  
17 couple on the life cycle.

18 MEMBER MARCH-LEUBA: On the life cycle.

19 MEMBER BROWN: I thought the cyber meeting  
20 was later. We've not heard cyber today.

21 MEMBER MARCH-LEUBA: I can work on this  
22 until after we come back.

23 CHAIRMAN REMPE: At this point are we done  
24 with things that need to be on the transcript and I'll  
25 let the court reporter go and then we'll stay and do

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1716 14th STREET, N.W., SUITE 200  
WASHINGTON, D.C. 20009-4309

1 the organizational thing.

2 MEMBER BROWN: Yes, that's fine.

3 CHAIRMAN REMPE: So court reporter, we're  
4 going to end this topic and you don't need to record  
5 any more, okay?

6 MEMBER BROWN: We have to do public  
7 comments.

8 CHAIRMAN REMPE: Oh, wait, court reporter,  
9 are you still there? Thank you so much, I forgot.

10 Yes, Ron.

11 MEMBER BALLINGER: Okay, so we need to  
12 have -- go out for public comments. If you're a  
13 member of the public and you would like to make a  
14 comment, please, if you're on the Teams thing, just  
15 unmute, and give us your name and make your comment.  
16 If you're on the phone, you'll have to do the \*6 and  
17 make your comment. So please do so.

18 Hearing none, we're done.

19 CHAIRMAN REMPE: Okay. Again, I'll try it  
20 this time. Unless I hear otherwise, I think we're done  
21 with the court reporter.

22 (Whereupon, the above-entitled matter went  
23 off the record at 3:45 p.m.)

24

25

# **Advisory Committee on Reactor Safeguards**

## **SHINE Medical Technologies Operating License Application**

### **Cybersecurity**

**September 9, 2022 – Non-Proprietary**

**Dan Warner  
Cyber Security Branch  
Division of Physical and Cyber Security Policy  
Office of Nuclear Security and Incident Response**

---

---

# SRM-18-0063

- In September 2019, the Commission issued Staff Requirements Memorandum (SRM) SRM-18-0063 for non-power production and utilization facilities intending to possess or use a Category II quantity of special nuclear material for the production of molybdenum-99 (Mo-99).
- In the SRM, the Commission approved the staff's approach for addressing cybersecurity at these facilities through development of appropriate license conditions based on the facilities' operating license applications.
- SHINE is the first applicant to submit a license application that is subject to the requirements of this SRM.

---

# Cybersecurity Process Development

- Staff reviewed the proposed rulemaking on cybersecurity for fuel cycle facilities and developed a similar model for use at SHINE and similar facilities.
- Staff provided SHINE feedback to consider when identifying applicable consequences of concern which are events that occur as a result of the compromise of a critical digital asset (CDA) that have the potential to adversely impact public health and safety or common defense and security.
- Staff reviewed the SHINE application to determine if there was adequate protection for CDAs that could result in a consequence of concern.

---

# FSAR Review

- Staff reviewed the Final Safety Analysis Report (FSAR) for discussions of cybersecurity with a focus on safety systems. Several sections discuss protections for the Highly Integrated Protection System (HIPS) platform for safety systems.
- FSAR Chapter 7 Section 7.4.2.2 – Target Solution Vessel Reactivity Protection System (TRPS) System Design Criteria and Section 7.5.2.2 – Engineered Safety Features Actuation System (ESFAS) System Design Criteria include Criterion 3 that identifies the TRPS and ESFAS systems will incorporate design or administrative controls to prevent/limit unauthorized physical and electronic access to critical digital assets.

---

# FSAR Review

- FSAR Section 7.4.5.3.2 – Cyber Security Design Features includes information on a defensive system architecture which includes features such as:
  - One-way isolated communication outside of safety systems
  - Maintenance workstation access only when a module is out of service
  - No capability for remote access to the safety system.

---

# FSAR Review

- FSAR Section 7.4.5.3.3 – Access Control identifies several features used to restrict access including:
  - Physical keys to prevent unauthorized use.
  - Locked cabinets for rack mounted equipment with administrative key control.
  - Modification or replacement of Field Programmable Gate Arrays (FPGAs) restricted when installed in the HIPS chassis.
  - FPGA modules only allow modification to setpoints and tunable parameters that may require periodic modification.

---

# Additional Application Reviews

- Physical Security Plan - Staff reviewed the Physical Security Plan for any information related to cybersecurity for security systems.
- Cybersecurity Audit - Staff conducted a regulatory audit with SHINE to gather more information regarding cybersecurity.
  - SHINE identified CDA access controls and protective features from the FSAR but indicated there was no specific cybersecurity program at SHINE.
  - For cybersecurity of physical security assets, SHINE only identified access controls.

---

# Cybersecurity RAIs

- SHINE submitted a revision to its initial Request for Additional Information (RAI) response based on NRC feedback received.
  - Provided information regarding the design, administrative, and programmatic controls that the SHINE Cybersecurity Plan (CSP) will provide.
  - Included how consequences of concern will be identified, how CDAs will be determined, how cybersecurity controls will be applied, and other programmatic controls to ensure that the cybersecurity program is documented and maintained.

---

# Staff Evaluation of Cybersecurity at SHINE

- Staff reviewed the SHINE application and then held a regulatory audit followed by issuing a set of RAIs to gather sufficient information to make a determination.
- Staff determined additional program elements were required to ensure adequate protection at the SHINE facility and developed a list of important cybersecurity program elements applicable to SHINE.
- Staff developed a license condition to address these additional program elements and determined the issuance of a SHINE operating license, as conditioned, in part, by the license condition, will not be inimical to the common defense and security or to the health and safety of the public and therefore, meets the requirements of 10 CFR 50.57(a)(6).

---

# Staff License Condition for Cybersecurity

- The licensee must have a CSP that describes how the facility's cybersecurity program provides reasonable assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks.
  - Similar to the approach followed in 10 CFR 73.54.
- The licensee may make a change to the CSP provided the cybersecurity program elements in the license condition and the performance objectives of the CSP remain met.

---

# Questions



---

# BACKGROUND

---

# Consequences of Concern

- For facilities intending to produce Mo-99, the following consequences of concern must be considered (but may not necessarily apply):
  - Latent Safeguards: The concern involves the compromise as a result of a cyberattack of a digital asset performing a security function, which would allow a malicious actor to exploit the degraded security function that was put in place to prevent the unauthorized removal of Special Nuclear Material (SNM) of moderate strategic significance or the loss of Material Control & Accountability (MC&A) for SNM of moderate strategic significance.
  - Active Safety: In this situation, the cyberattack compromises the function of a digital asset and directly leads to safety-related consequences as defined in the safety criteria found in the licensee's Final Safety Analysis Report.
  - Latent Safety or Security: The attack renders one or more digital assets incapable of performing its intended function. When called upon to respond to an event, separate from the cyberattack, the digital asset does not operate as expected and therefore the supported safety or security function is compromised, resulting in safety-related consequences like above, or loss or unauthorized disclosure of classified information or classified matter. In addition, MC&A functions whose compromise could lead to a latent safety consequence of concern, would need to be protected from a cyberattack.



# Cybersecurity Plan

JEFF BARTELME, DIRECTOR OF LICENSING

# Outline

- Requirement for SHINE to Develop Cybersecurity Plan
- SHINE Cybersecurity Plan Overview
- Consequences of Concern
- Identification of Critical Digital Assets
- Determination of Cybersecurity Controls
- Additional Programmatic Considerations

# Requirement for SHINE to Develop Cybersecurity Plan

- There is no explicit regulatory requirement for non-power production and utilization facilities to establish a site-specific cybersecurity plan.
  - Despite there being no explicit regulatory requirement to establish a critical digital asset-specific cybersecurity plan, cybersecurity considerations informed the design of digital systems at the SHINE facility.
- In December 2021, the NRC Staff notified SHINE of the plan to impose, via license condition, a requirement for SHINE to develop a site-specific cybersecurity plan, which accomplishes, in part:
  - Identification of digital assets that, if compromised by a cyber attack, would result in a consequence of concern
  - Determination of which digital assets require protection as critical digital assets
  - Identification and application of a graded set of cybersecurity controls for critical digital assets
  - Providing temporary compensatory measures to meet the plan performance objectives when a cybersecurity control is degraded
  - Reporting and tracking cybersecurity events

# SHINE Cybersecurity Plan Overview

- SHINE has developed a cybersecurity plan to document the design controls, administrative controls, and programmatic controls to prevent or limit the unauthorized physical and electronic access to critical digital assets.
  - SHINE defines critical digital assets as a digital asset for which no alternate means has been identified to prevent the associated consequence of concern.
- The cybersecurity plan was informed by the guidance of draft Regulatory Guide DG-5062, “Cyber Security Programs for Nuclear Fuel Cycle Facilities” (January 2017 Draft).
- The performance objective of the cybersecurity plan is to detect, protect against, and respond to a cyber-attack capable of causing a consequence of concern.

# Consequences of Concern

- The cybersecurity plan is design to protect against the following consequences of concern:
  - Latent Consequences of Concern – Safeguards
    - The compromise, as a result of a cyber-attack, of a function required to prevent unauthorized removal of special nuclear material (SNM) of moderate strategic significance.
  - Active Consequences of Concern – Safety
    - Exceeding the SHINE Safety Criteria as a direct result of a cyber-attack.
  - Latent Consequences of Concern – Safety
    - The compromise, as a result of a cyber-attack, of a function required to prevent or mitigate the consequences of an accident which could exceed the SHINE Safety Criteria.
- Site-specific documents are used to consider the potential consequences of concern from a cyber-attack.
  - The SHINE Safety Analysis (SSA) Summary Report is used to identify active and latent safety consequences of concern.
  - The Physical Security Plan is used to identify latent safeguards consequences of concern.

# Identification of Critical Digital Assets

- SHINE has established a process for the identification of critical digital assets that includes identifying digital assets associated with consequences of concern, consideration of the function of each digital asset to determine whether an alternate means exists that prevents the consequence of concern, and determination of the resulting critical digital assets requiring protection.
- An alternative means analysis is performed for identified digital assets that considers the function of the critical digital asset to determine whether an alternate means exists that could be credited or implemented to prevent the consequence of concern.
- If no alternative means exist for a digital asset that prevents the consequence of concern, the digital asset is determined to be a critical digital asset and requires protection.

# Determination of Cybersecurity Controls

- For each critical digital asset requiring protection, SHINE establishes and maintains cybersecurity controls specific to the associated consequence of concern.
- SHINE uses the guidance provided in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations,” to derive cybersecurity controls.
- Implementing procedures are established and maintained that identify and document the cybersecurity controls applicable to the identified critical digital asset.
  - Implementing procedures document, in part:
    - The location, interconnections, and operating environment of the critical digital assets;
    - The measures taken to meeting the performance specifications associated with the identified cybersecurity controls; and
    - The verification process for cybersecurity controls.

# Additional Programmatic Considerations

- Temporary Compensatory Measures
  - If it is determined that cybersecurity controls are not meeting defined performance specifications, SHINE implements compensatory measures to ensure adequate protection of critical digital assets.
- Configuration Management
  - The facility-wide configuration management program includes a cybersecurity impact analysis prior to the implementation of a change.
- Periodic Review
  - A review of the cybersecurity plan occurs at least every 36 months.
- Event Reporting and Tracking
  - SHINE informs the NRC Operations Center at the time of making an event-based notification if the event is a result of a cyber-attack.
  - SHINE records, and tracks to resolution: (1) Failures, compromises, discovered vulnerabilities, or degradations that result in the decrease in effectiveness of a cybersecurity control; and (2) cyber-attacks that compromise a critical digital asset associated with a consequence of concern.

# **Advisory Committee on Reactor Safeguards**

## **SHINE Medical Technologies, LLC Operating License Application**

### **Chapter 14 - Technical Specifications**

**Michael Balazik**  
Project Manager/Inspector  
Office of Nuclear Reactor Regulation

September 9, 2022

---

---

# Regulatory Basis

- Regulatory Requirements
  - 10 CFR 50.34, “Contents of applications; technical information”
  - 10 CFR 50.36, “Technical specifications”
  - 10 CFR 50.40, “Common standards”
  - 10 CFR 50.57, “Issuance of operating license”

---

# Guidance and Acceptance Criteria

- NUREG-1537, Part 1, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Format and Content,” issued February 1996;
- NUREG-1537, Part 2, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Standard Review Plan and Acceptance Criteria,” issued February 1996;
- Final Interim Staff Guidance (ISG) Augmenting NUREG-1537, Part 1 and Part 2, for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors
- ANSI/ANS-15.1-2007 (R2013), "The Devolvement of Technical Specifications for Research Reactors”
- NUREG-1431, “Standard Technical Specifications – Westinghouse Plants, Volume 1”

---

# Summary of Application

- Principal purpose to the Technical Specifications (TS) is to maintain system performance to ensure safe operation of the facility to promote public health and safety.
- TS Section 1.0, SHINE proposed standard and site-specific definitions and describes the use of logic connectors with completion times.
- TS Section 2.0, SHINE proposed safety limits for both the utilization and production facility with limiting safety system settings to prevent exceedance of a safety limit.

---

## Summary of Application (continued)

- TS Section 3.0, SHINE proposed limiting conditions of operation (LCO) and surveillance requirements with the application of usage rules, action statements and completion times.
- TS Section 4.0, SHINE proposed major design features (DF) for the facility. These DFs if altered or modified may impact safety of the facility.
- TS Section 5.0, SHINE proposed administrative controls that establish the organizational and procedural controls for the facility.

---

# Staff Evaluation

- The staff initially evaluated SHINE's proposed TS (Revision 5) submitted to the NRC on January 26, 2022.
- The NRC technical staff evaluated the TS values in Sections 2, 3, and 4, along with the surveillance requirements, as documented in the specific safety evaluation (SE) chapter.
  - Based on requests for additional information and audits, SHINE revised the proposed TS.
- The staff will include an evaluation of the TSs (TS Section 3.2, "Instrumentation and Control Safety Systems") associated with digital instrumentation and control in SE Chapter 7, "Instrumentation and Control Systems."

---

## Staff Evaluation (continued)

- The NRC licensing and project management staff evaluated the TS to ensure consistency, clarity, and formatting of the TS, mainly focused on the definitions and logical connectors in TS Section 1, usage rules in Section 3, and administrative controls in Section 5.
  - The NRC staff audited the TS and issued an audit report.
  - Usage rules establish general requirements for TS Section 3.0 for limiting conditions for operation and surveillance requirements.
- The audit resulted in SHINE revising its TS and submitting a complete version of TS (Revision 6).

---

# Evaluation Findings and Conclusions

- SHINE's proposed TS are consistent with the guidance in NUREG-1537, ANSI/ANS-15.1, and NUREG-1431.
- As required by 10 CFR 50.36(a)(1), the SHINE operating license application includes a summary statement of the bases or reasons for the proposed TSs, other than those covering administrative controls.
- As required by 10 CFR 50.36(b), the SHINE operating license application includes proposed TSs derived from the analyses and evaluation included in the SHINE FSAR, as supplemented.
- SHINE's proposed TSs specify SLs on the wall temperature and differential pressure across the primary system boundary and the pressure within process tanks containing irradiated uranyl sulfate and connected piping, which are the important process variable necessary to reasonably protect against the uncontrolled release of radioactivity; and specify LSSSs, that satisfy 10 CFR 50.36(c)(1)(i)(A) and (ii)(A).
- SHINE's proposed TSs include LCOs, which are the lowest functional capability or performance levels of equipment required for safe operation of the facility, for each item that meets one or more of the criteria specified in 10 CFR 50.36(c)(2)(ii).

---

# Evaluation Findings and Conclusions (continued)

- SHINE's proposed TSs include SRs, which relate to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within SLs, and that the LCOs will be met, that satisfy 10 CFR 50.36(c)(3).
  - SHINE's proposed TSs include design features, which are those features of the facility such as materials of construction and geometric arrangements, which, if altered or modified, would have a significant effect on safety, that satisfy 10 CFR 50.36(c)(4).
  - SHINE's proposed TSs include administrative controls, which are the provisions relating to organization and management, procedures, recordkeeping, review and audit, and reporting necessary to assure operation of the facility in a safe manner, that satisfy 10 CFR 50.36(c)(5). SHINE's proposed TSs also include requirements for initial notification, written reports, and records that satisfy 10 CFR 50.36(c)(1), (2), and (7) and requirements for special reports that the staff deemed necessary in accordance with 10 CFR 50.36(c)(8).
  - The issuance of an operating license for the facility would not be inimical to the common defense and security or to the health and safety of the public.
-



# Technical Specifications

CATHERINE KOLB, SENIOR DIRECTOR OF PLANT OPERATIONS

# Outline

- Overview
- Introduction
- Safety Limits and Limiting Safety System Settings
- Limiting Conditions for Operation
- Surveillance Requirements
- Design Features
- Administrative Controls

# Overview

- Technical specifications have been proposed for the SHINE Medical Isotope Production Facility to meet the requirements of 10 CFR 50.36.
- Guidance provided by:
  - ANSI/ANS-15.1-2007, “The Development of Technical Specifications for Research Reactors”
  - Appendix 14.1 of NUREG-1537, Part 1, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Format and Content”
  - NUREG-1431, “Standard Technical Specifications, Westinghouse Plants” (for rules of usage)
- Safety-related controls identified in the SHINE Safety Analysis (SSA) are incorporated into the SHINE technical specifications.

# Introduction

## DEFINITIONS AND USAGE

- Definitions section provides defined terms used throughout the technical specifications.
  - Primarily based on definitions from ANSI/ANS-15.1-2007.
  - Facility-specific modifications of certain terms (e.g., “Safe Shutdown”, “Facility Secured”) and new facility-specific terms (e.g., “Neutron Driver Assembly System”, “Main Production Facility”) are also provided.
- Use of logical connectors (“and” and “or”) and completion times for actions specified in limiting conditions for operation based on guidance provided in NUREG-1431.

# Safety Limits and Limiting Safety System Settings

- Safety limits (SLs) have been defined for the irradiation unit primary system boundary and process tanks containing irradiated uranyl sulfate in the radioisotope production facility.
- Limiting safety system settings (LSSSs) are defined as those variables and allowable setpoints for the two safety-related instrumentation and control (I&C) systems (i.e., target solution vessel (TSV) reactivity protection system [TRPS] and engineered safety features actuation system [ESFAS]) that ensure automatic protective actions are initiated prior to the safety limit being exceeded.

# Limiting Conditions for Operation

- Limiting conditions for operation (LCOs) are administratively established constraints on equipment and operational characteristics, defining the lowest functional capability or performance level required for safe operation of the facility.
- Rules of usage based on guidance from NUREG-1431.
  - Power reactor guidance was chosen because the SHINE facility, as a commercial entity, has an expected operational cadence different from a typical research reactor.
  - Actions to be taken upon discovery of a failure to meet an LCO, within specified completion times, are generally provided.
  - Exceptions are provided to allow for the performance of specific startup tests.
  - Exceptions are also provided to allow for the performance of defined recovery actions.

# Surveillance Requirements

- Surveillance requirements (SRs) are provided for each LCO, in the same section of the technical specifications as the LCO, to improve readability and for human factors considerations.
- SRs prescribe the frequency and scope of surveillance to demonstrate minimum performance levels established by the LCO.
- SR frequencies are generally based on guidance provided in ANSI/ANS-15.1-2007 for cases where similarities exist between equipment addressed in the standard and equipment used in the SHINE facility.

# Design Features

- Design features (DFs) describe design characteristics of the site and the facility to ensure that major alterations to safety-related components or equipment are not made prior to appropriate safety reviews.
- Design features include:
  - Site location and description
  - Main production facility physical characteristics
  - Features of equipment important in safety analysis assumptions (e.g., carbon delay bed efficiencies, ventilation features, shielding characteristics)
  - Uranium enrichment limit
  - Margin of subcriticality limit

# Administrative Controls

- Organization
  - Structure
  - Minimum facility staffing
  - Selection and training of personnel
- Review and audit committee
- Radiation safety
- Procedures
- Programs required to be established, implemented, and maintained
- Required actions
- Reports
- Records



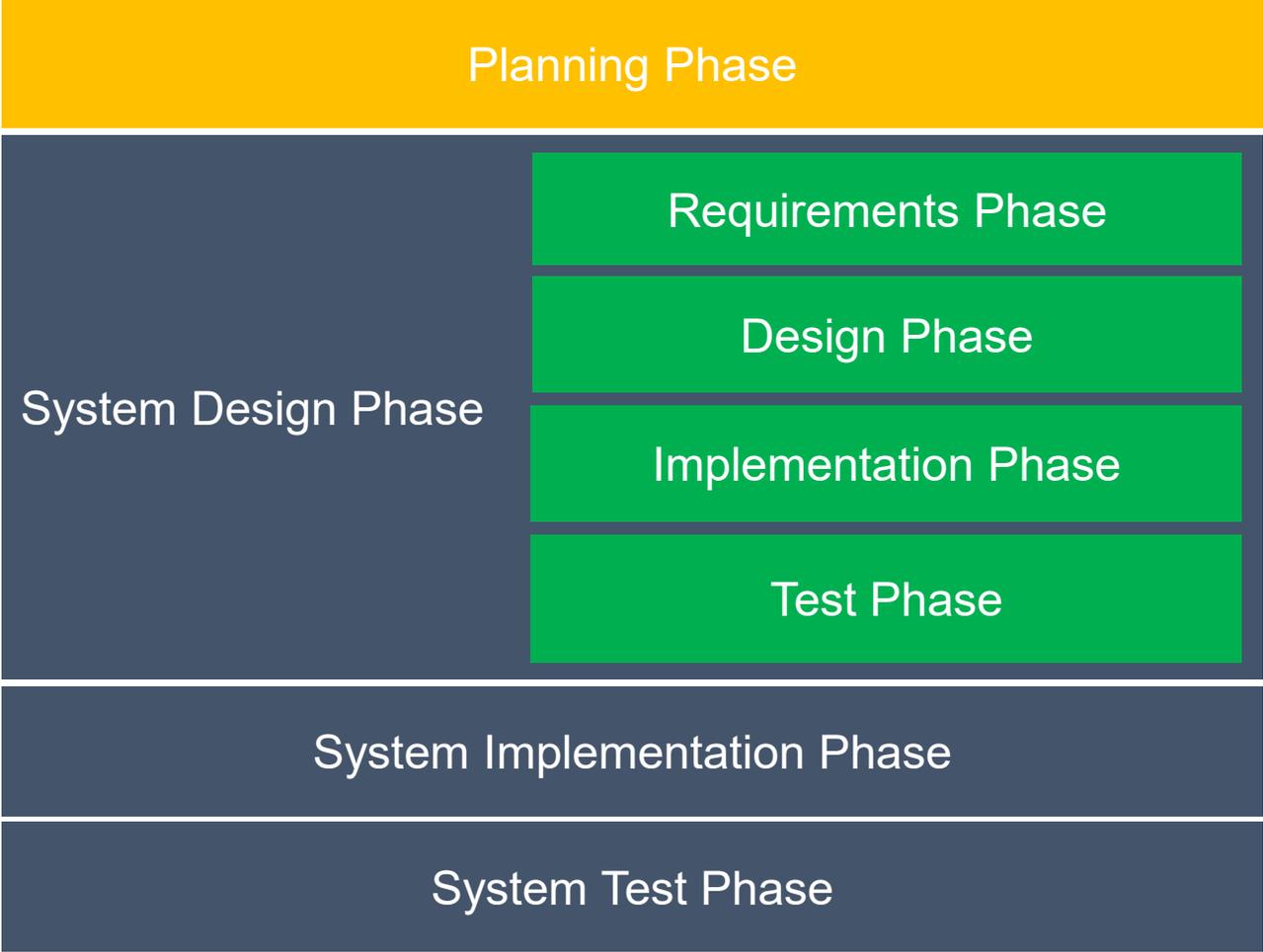
# Programmable Logic Lifecycle Overview

JASON POTTORF, DIRECTOR OF ENGINEERING, ROCK CREEK INNOVATIONS

# Programmable Logic Development and System Design Control

- Programmable logic development takes place as part of the overall system design control for the highly integrated protection system (HIPS) application to the SHINE facility.
- The programmable logic lifecycle process consists of 5 phases: Planning, Requirements, Design, Implementation, and Test.
- The Planning Phase includes system level requirements identification and tracing to customer requirements.
- Verification and Validation (V&V) of programmable logic activities is performed in accordance with Institute of Electrical and Electronics Engineers (IEEE) Standard 1012-2004, “IEEE Standard for Software Verification and Validation.”

# Overall System Lifecycle



-  Hardware and Programmable Logic
-  Programmable Logic
-  Hardware

# Planning Phase

- Design input review
  - Procurement requirements specifications
  - Input documents containing project requirements in the procurement requirements specifications
  - Following inputs are considered (if provided):
    - Purchase order
    - Customer requirements
    - Rock Creek Innovations proposal
    - Customer system drawings
    - Customer control room drawings
    - Customer wiring diagrams
    - Customer input/output database
    - Customer piping and instrumentation diagrams
    - Applicable regulatory requirements, codes, and standards

# Planning Phase (Cont'd)

- Design Input List (DIL)
  - Lists formally received customer and vendor design input documents
  - Design input received by non-formal means identified as an unverified assumption (UVA)
  - UVA process can be used to track design details needed or used which have not been received
- The following Planning Phase documents for the implementation of the programmable logic lifecycle process are developed:
  - Project Quality Assurance Plan
  - Project Programmable Logic Development Plan (PLDP)
  - Project Configuration Management Plan
  - Project V&V Plan
  - Project Equipment Qualification Plan
  - Project Test Plan
  - Project Security Assessment

# Planning Phase (Cont'd)

- System Requirements Specification (SyRS)
  - System design requirement details are defined and documented
  - Traceability to design inputs established
  - Requirements allocated to hardware and/or programmable logic in the SyRS
- System Design Specification (SyDS)
  - HIPS hardware components specified (i.e., divisions, cabinets, chassis, and modules)
  - System requirements are allocated to HIPS hardware
  - Includes input/output list for each module - tag names, descriptions, signal types, and ranges

# Programmable Logic Development

- The following programmable logic lifecycle process activities are performed in conjunction with the System Design Phase:
  - Programmable Logic Requirements Phase
  - Programmable Logic Design Phase
  - Programmable Logic Implementation Phase
  - Programmable Logic Test Phase
- Phase-specific summary reports prepared by V&V organization as part of the formal exit criteria for each phase.
- This lifecycle is implemented separately for the field programmable gate arrays (FPGAs) on each HIPS module within the project-specific system.
- These activities are performed within a Secure Development Environment (SDE) and Isolated Development Network (IDN).

# Programmable Logic Requirements Phase

- Generate programmable logic requirements specification (PLRS) to translate the project-specific system design requirements into detailed programmable logic requirements.
  - A separate PLRS is developed for the FPGA on each HIPS module within the project-specific system.
  - A traceability report is developed for each PLRS.
- Programmable logic requirements should be adequate to support implementation and verification of the design.
  - PLRS provides a functional description of the programmable logic functionality.
  - PLRS contain the level of detail that enables the development and verification of the design.
- Programmable logic requirements and traceability are reviewed by the V&V organization and any anomalies identified are addressed by Design.

# Programmable Logic Design Phase

- Create at least one logic model and associated programmable logic design specification (PLDS) document for each PLRS
  - Provides a description of the logic architecture, control logic, data structures, input/output formats, interfaces, and algorithms necessary to implement programmable logic requirements
  - Logic models developed following defined modeling standards and model-based development procedure
- Design review of the logic model is performed by V&V organization to verify the logic design meets programmable logic requirements
- Programmable logic testing is performed by V&V organization and reviewed by Design to validate the logic design meets requirements
  - Separate testing of application specific logic blocks
  - Testing of integration between HIPS Platform and application specific logic blocks
- Begin preparation for testing of the logic when implemented into hardware (Module Test Plans/Designs)

# Programmable Logic Implementation Phase

- HIPS platform hardware and programmable logic components are integrated into the project during this phase to provide the target hardware and incorporate the HIPS platform programmable logic that has been previously designed, developed, and tested.
  - Hardware description language (HDL) code is generated from the logic design models and code statements are traced to the programmable logic design model elements.
  - HDL code is review and analyzed to ensure it is accurate, consistent, verifiable, and complies with requirements.
  - Synthesis and place and route of HDL code is performed, reviewed and analyzed (synthesis, resource allocation, timing, and power reports).
  - Designer generates FPGA programming data and programs the target FPGA.
- HDL post-synthesis test preparation developed (Test Plans, Designs, Cases, Procedures)
- Hardware implementation test preparation continued (Module Test Cases, Procedures)

# Programmable Logic Test Phase

- During the Test Phase, requirements of the V&V Plan are completed.
  - Post-synthesis testing executed, and reports developed
  - Module testing executed, and reports developed
- V&V module final report(s) completed
- Output documents from the Test Phase are ensured to be complete and approved.
  - This serves as the control point to transition from the System Design/Programmable Logic Test Phase to the System Implementation Phase.

# System Implementation and System Test Phase

- System Implementation Phase
  - HIPS platform hardware components are integrated into the project system during this phase to prepare the system hardware for system component integration, system, and acceptance testing.
  - Test cases and procedures are prepared for each of system component integration testing, system testing, and system acceptance testing.
- System Test Phase
  - Hardware and programmable logic design is baselined prior to system acceptance testing – this is identified as the Test Baseline.
  - Change control begins after the Test Baseline.
  - Required tests are completed and output documents approved.