Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
NuScale Subcommittee Open Session

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Tuesday, February 7, 2017

Work Order No.: NRC-2867 Pages 1-93

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

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.

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

NUSCALE SUBCOMMITTEE

+ + + + +

OPEN SESSION

+ + + + +

TUESDAY

FEBRUARY 7, 2017

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 1:01 p.m., Michael Corradini, Chairman, presiding.

COMMITTEE MEMBERS:

MICHAEL L. CORRADINI, Chairman

RONALD G. BALLINGER, Member

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR. Member

MARGARET CHU, Member

WALTER L. KIRCHNER, Member

JOSE A. MARCH-LEUBA, Member

DANA A. POWERS, Member

HAROLD B. RAY, Member

JOY REMPE, Member

GORDON R. SKILLMAN, Member

JOHN W. STETKAR, Member

MATTHEW W. SUNSERI, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

JOSEPH M. ASHCRAFT, NRO

TOM BERGMAN, NuScale

LUIS BETANCOURT, NRO

GREGORGY CLARKSON, NuScale (Rock Creek Innovations)

GREG CRANSTON, NRO

DAVID CURTIS, NRO

ROBERT GAMBLE, NuScale

DAWNMATHEW KALATHIVEETTIL, NRO

MARVIN LEWIS, Public Participant*

STEVEN POPE, NuScale

JASON POTTORF, NuScale

OMID TABATABAI, NRO

DINESH TANEJA, NRO

ANDREA D. VEIL, Executive Director, ACRS

*Present via telephone

TABLE OF CONTENTS

P R O C E E D I N G S

1:01 p.m.

CHAIRMAN CORRADINI: This meeting will come to order. This is a meeting of the NuScale Subcommittee. My name is Mike Corradini, chair of the subcommittee. ACRS members in attendance currently are Ron Ballinger, Margaret Chu, Dick Skillman, Harold Ray, Dennis Bley, John Stetkar, Walt Kirchner, Charles Brown, and Joy Rempe. We have a couple other members who will be joining us, such as Matt Sunseri and our consultant, Myron Hecht.

Christina Antonescu is the Designated Federal Official for this meeting.

The purpose of the meeting is for the subcommittee to review NuScale's Topical Report, TR-1015-18653, Highly Integrated Protection System Platform, Revision 1.

We will hear presentations from the NRC staff and representatives from NuScale.

The subcommittee will gather information and analyze relevant issues and facts and formulate proposed positions and actions, as appropriate, for deliberation by the full committee.

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

this meeting previously published in the Federal Register. And as shown in the agenda, some presentations will be closed in order to discuss information that is proprietary to the applicants and its contractors, pursuant to U.S.C. 552(b)(c)(3) and (4).

Specifically for the agenda, an overview of the design of highly integrated protection systems platform will be given in open session and then later, if we need to discuss proprietary matters, we will go into closed session to do that.

And I will just go off script and ask either NuScale or the staff to identify if we start asking questions that take us where we need a closed session, just hold us off and we will go and discuss that in closed session. Attendance at this portion of the meeting dealing with such information in closed and will be limited to the NRC staff and its consultants of those individuals and organizations who have entered into an appropriate confidentiality agreement with them. Consequently, we will need to confirm this from the eligible observers and participants in the room at the time of the closed session.

We have received no written comments or

requests for time to make oral statements from members of the public regarding today's meeting. And as always, we have one bridge line established for interested members of the public to listen in.

Also, the bridge line will be opened at the end of the open session to see if anyone has additional comments from the public.

In addition, a second line has been arranged for the vendor, as applicable, to be able to participate in the meeting. Again, once we get off here, I want to make sure that line is open and members of NuScale that may be far away can participate. And as I had noted, this line is only for NuScale and NRC support staff who have an active role. And this line can be used during the closed portion of the meeting.

A transcript of the meeting is being kept and will be made available, as stated in the Federal Register notice. Therefore, we request that participants in the meeting use the microphones located throughout the meeting room. When addressing the subcommittee, participants should first identify themselves and speak with sufficient clarity and volume so that it may be readily heard.

Also, again, please silence all cell

phones, pagers, iPhones, iPads, and other appropriate and sundry appliances.

We will now proceed with the meeting and I will call upon Dave Curtis of the Office of New Reactors to start the presentation.

Before you start, Mr. Curtis, can I get someone from the second line, which has NuScale staff and NRC staff to just confirm you are on, if questions go your way?

Anybody out there?

PARTICIPANT: This is Ann from OGC.

CHAIRMAN CORRADINI: Okay, fine. All right, so somebody is out there.

So, Mr. Curtis, please start us off.

MR. CURTIS: Good afternoon. My name is David Curtis. I am the Acting Chief for the Instrumentation, Controls, and Electronics Engineering Branch in the Office of New Reactors.

I just wanted to start by thanking NuScale on two fronts. We really appreciate the quality of NuScale's Topical Report because it made it much more straightforward for the staff to be able to identify their safety findings.

And I also want to thank NuScale for their participation with us throughout the review

process through each stage of the process and that also made coming to our determinations much more straightforward.

The only other point that I wanted to make just sort of starting out is that this Topical Report is platform-specific. We have received NuScale's DC application and it is currently being assessed for acceptance. And when we have moved to the next stage and we have reviewed that DC, then we are going to be coming back to you to talk about our safety findings in regards to that. Staff will go into much more detail about that as they make their presentation.

Omid?

MR. TABATABAI: Thank you, David. Thank you, Dr. Corradini and ACRS members. Thanks for your time.

Just quickly I just wanted to bring to members of the public who are listening to this presentation that we have made a very minor change to the agenda. The latest one also reflects that change that the staff's presentation was supposed to be during the closed meeting but we have moved it up to the open portion of this meeting. So if you are using the old agenda that shows that staff's

presentation starts at 1:30, we have -- I'm sorry 3:30 or so, we have moved it up to the open portion. It starts at 1:30. So you don't have to hang up.

CHAIRMAN CORRADINI: Yes, I think we have the correct one. And just to reemphasize what you said, since it is open, if we have questions on the open session that dive into proprietary matters, we will postpone them and take them up when we go into closed session.

MR. TABATABAI: That's correct. Thanks for that reminder.

And also for folks on the bridge line, please, if you are using the private line, if you are not speaking, put your phones on mute so there is no background noise in the room.

Other than that, I don't have anything else and I will let NuScale present.

CHAIRMAN CORRADINI: So NuScale will come up?

MR. TABATABAI: Yes.

CHAIRMAN CORRADINI: Okay, we will have a change of place cards.

Jason, are you going to start us off?

MR. POTTORF: Yes.

CHAIRMAN CORRADINI: Okay. Go ahead.

MEMBER BROWN: Before they start, can I make --

CHAIRMAN CORRADINI: Charlie, as long as you have a green light, you can talk.

MEMBER BROWN: That's why I got permission first.

I had taken a quick look at the nonproprietary slides and I have gone through the proprietary slides. There is a good possibility when you listen to the non-proprietary part, it is in words, not necessarily in figures, and some may not be straightforward. The proprietary closed part of this will pretty much, I think, provide a lot of definition and too much back and forth during the nonproprietary session would -- I'm just cautioning, as Harold did in the last meeting, would not be as productive.

So I will try to flag those if I think -

-

CHAIRMAN CORRADINI: So are you telling me you are going to control yourself?

MEMBER BROWN: No, that is not a possibility.

CHAIRMAN CORRADINI: It was a question.

MEMBER BROWN: There are several that

are not controllable in this process and I am just -- - all I am trying to do is make you aware that the number of my questions, once I got the slides last night, I was able to come to some slightly different conclusions or at least eliminated some questions.

So anyway, I am just trying to give you a heads up, that's all.

CHAIRMAN CORRADINI: Okay, that sounds good. Jason, take it off. Go ahead.

MR. POTTORF: Thank you and good afternoon, everyone. It is a pleasure to be here. My name is Jason Pottorf. I am a Lead Engineer in Instrumentation and Controls with NuScale Power. I have been with NuScale Power for over eight years now.

In about 2010 at NuScale we partnered up with Gregg Clarkson and the Rock Creek Team to develop a new custom protection system architecture. We have been working on that since then.

Gregg Clarkson is here with me today. Do you want to go ahead and introduce yourself?

MR. CLARKSON: Yes, Gregg Clarkson with Rock Creek Innovations. Like Jason said, I partnered with NuScale in 2010, became a strategic partner in 2012 and also have decided to invest in

NuScale as of 2012 and have had the pleasure of designing a custom protection system for NuScale Power Reactor Design.

MR. POTTORF: Okay. We also have Vice President of Engineering at NuScale here, Robert Gamble.

MR. GAMBLE: Hello. Good to be here. I am a relatively newcomer to NuScale. I joined within the last year but have crossed paths with many of you in my earlier days with GE on the ESBWR design.

CHAIRMAN CORRADINI: That's why you look so familiar. We have seen you before.

MR. GAMBLE: That's right.

CHAIRMAN CORRADINI: Okay, good.

MR. POTTORF: Okay, we will jump into the presentation. The first slide is our standard acknowledgment and disclaimer for the DOE cost sharing for the NuScale work.

So the presentation today, the purpose of the presentation is to provide a high-level overview of the design of the highly integrated protection system or HIPS, as we refer to it, the HIPS platform topical report.

I will briefly cover the history of the

NRC interactions on the topical report. I will cover the design approach that we took for the HIPS platform, briefly cover the scope of what is in the topical report, and then I will walk through at a high-level kind of a representative architecture to help show the safety data path through the HIPS platform.

I have a slide on the prototype effort that we have recently completed and I will wrap up at the end.

This is a slide -- slide 4 is all of the acronyms that we have used in the presentation.

So slide 5 lists all of the interactions and I will just summarize this slide in the interest of time. We have had a lot of very, very good interactions with the NRC throughout the review of the topical report. To summarize, we submitted in late 2015, Revision 0 of the HIPS platform topical report. We received the first set of RAIs towards the middle of 2016. We responded to those in the fall.

And just here recently, in fact last week, the NRC performed their audit of what we refer to as the MPS or module protection system prototype in the U.K. which utilize a lot of the design

concepts of the HIPS platform in that.

MEMBER STETKAR: Jason, again, turn me off if it is proprietary. Does that system in the U.K. replicate four divisions, whatever you call them?

MR. POTTORF: Yes, quickly, we had --

MEMBER STETKAR: Two out of four type, I mean is it that level of --

MR. POTTORF: It is two out of four.

MEMBER STETKAR: It is not one out of two.

MR. POTTORF: And I have a slide and I will cover that, what was covered in the prototype on that slide.

MEMBER STETKAR: Okay, sorry.

MR. POTTORF: No problem. Okay, so the HIPS Platform is designed to provide a robust platform for safety-related and important safety applications. And the fundamental design objective for the HIPS platform was to take advantage of the benefits of the analog architectures that you will find in existing commercial nuclear power plants, as well as to take advantage of digital technologies, all while incorporating the design I&C principles of independence, redundancy, diversity, and

predictability and repeatability.

Now if you are familiar with those existing analog architectures, you will know that the trip determination channels in those systems all function independently of each other within a division of input. And each of those trip determination channels then provides its trip determination to the voting portion of those systems via one-way physical point-to-point connections. And then actuation of safety components in those systems is performed by way of master and slave setup, where a master-slave communicates with multiple slave relays.

MEMBER BROWN: Are you talking about analog, your equivalent to the -- you are talking about the analog systems, the classic older systems right now.

MR. POTTORF: That's right. That's right.

MEMBER BROWN: I just wanted to clarify that. Thank you.

MR. POTTORF: And so the final actuated equipment is actually via this master-slave point to multipoint communication where each slave relay would then actuate a final component.

Now, as I am sure you are wondering, why am I describing these analog architectures. I am describing that because the design of the HIPS platform components enables you to implement a protection system very much akin to those analog systems, while taking advantage of the benefits of digital technology by way of the use of field programmable gate arrays or FPGAs.

And I guess I would say that if you are only familiar with some of those microprocessor-based digital protection systems that have come before the NRC, I would recommend that you set aside your concepts of how those operate because it will be harder for you to understand how our system operates. You should look at the HIPS platform as really a distributed set of FPGAs. Each of those FPGAs performs a very specific and simple function and there will be many FPGAs in the platform. So, it is quite different but we really tried to take advantage of those benefits of the existing analog and proven protection systems in the current plants.

Now as far as the topical report scope, the HIPS platform consists of HIPS chassis, which includes a backplane and a back panel and then also a system of modules that are interchangeable between

chasses.

The platform is designed to work with different module types configured to the individual application, where multiple chasses can be connected to create a larger system, if needed. The different HIPS modules and platform inputs and outputs are then connected to each other through the backplane and back panel of the chassis.

On Slide 7, I have listed the four module types that part of the HIPS platform. The first of those is a safety function module or SFM for short. The purpose of the safety function module is to provide signal conditioning and actuation determination for safety functions. It also provides scaled value of input process to non-safety controls and other safety displays for monitoring purposes. This module includes an FPGA as well as analog components on it.

MEMBER STETKAR: Jason, just for clarity, because people use term safety functions differently. In your construct, a safety function module monitors particular plant parameters and compares them to set points.

MR. POTTORF: That's correct.

MEMBER STETKAR: So a safety function

module does not initiate the function of auxiliary feedwater or the function of high pressure injection, with a function of blowdown or something like that. It is simply what used to be a bistable.

MR. POTTORF: That's correct.

MEMBER STETKAR: Okay.

MR. POTTORF: Yes.

MEMBER STETKAR: It is just a different connotation of safety function than is used elsewhere.

MR. POTTORF: Okay, the second module of the HIPS platform is the communications module or CM for short. And the purpose of the Communications module is to control, collect, and transmit information between other HIPS modules or to external components from the platform. This module includes an FPGA, as well as analog components as well.

The third module is the equipment interface module or EIM and it provides final equipment actuation output. This module includes analog priority logic circuitry on the board used for automatic and manual actuation inputs. This module include an FPGA as well as analog components, too.

And the final module is the Hardwired module or HWM and this is a relatively simple module. It converts hardwired contact inputs into logic level signals to make that available on the backplane of the chassis and HIPS platform. And it is analog only.

I do have a note here on the bottom that the HIPS platform is FPGA-based and, therefore, has no executable software in runtime environment for the platform.

CHAIRMAN CORRADINI: So I am probably one of the less knowledgeable on this. So explain -- can you at least remind us what an FPGA is or is this not the right time? Are you going to do it later?

MR. POTTORF: I hadn't provided any slides that speak specifically. Actually, I do have --

CHAIRMAN CORRADINI: I get smirks from some of my colleagues who probably know what it is.

MR. POTTORF: Maybe you can probably explain.

MR. CLARKSON: I think a simple explanation would be is imagine you had a surrogate board with a lot of individual components

representing logic dates and they were wired together, all of them were wired together with copper traces and you chose to make a specific sequential logic circuit out of that. You could go in an cut away the logic, the copper wire that you don't want connected, and leave behind what you do want connected. And by doing that, you would result in a specific circuit, that sequential logic circuit.

The FPGA does this on a piece of silicone.

CHAIRMAN CORRADINI: Okay so it is hardwired but on a very small scale.

MR. CLARKSON: Correct. Yes, that is correct.

CHAIRMAN CORRADINI: To perform a single function.

MR. CLARKSON: To perform a specific function.

CHAIRMAN CORRADINI: A specific function.

MR. CLARKSON: Just like you would with individual logic gates, yes.

CHAIRMAN CORRADINI: Okay.

MEMBER BROWN: FPGA means field

programmable gate array, right?

MR. CLARKSON: Yes.

MEMBER BROWN: It is a bunch of gates. They select which ones you want to use, which ones you don't want to use.

CHAIRMAN CORRADINI: Just teeny-tiny.

MEMBER BROWN: Tons of logic units. Tons, I would say -- how many are in an FPGA, 100,000? More than that?

(Simultaneous speaking.)

CHAIRMAN CORRADINI: I have got it. Let's go on.

MEMBER BROWN: Okay.

MR. POTTORF: Okay, on Slide 8 I provided a portion, a block diagram of a portion of a representative architecture. And there is a section in the topical report where we talk about a representative architecture and this is really not part of what we are looking for approval of but we included that in the topical report because it helps demonstrate some of the key or all of the key design concepts of the HIPS Platform components.

So on this slide you will see these two major boxes. The one on the upper part of the slide represents a single division of input. We call

those divisions separation groups. So this would be one of four separation groups of input to the representative protection system architecture.

The colored blocks in that bigger box there represent HIPS platform modules. The brown and green ones are the safety function modules, where you would bring in process inputs and perform trip determination on those boards. We have colored those green there because this is where triple redundant safety data paths begin in the safety data path.

So on the FPGA on the SFM there will be triplicated independent logic on a single FPGA but then, essentially, once you have made a trip determination, that is all that gets passed on down through the system from those SFMs.

The lines that you see in the middle of that big box represent the independent communication buses on the backplane of the chassis. You will see that we have a blue, purple, and red. These represent the independent communications for the three safety data paths. So all of the SFMs have independent components on the SFM that communication with each of those three safety data buses on the backplane.

The blue, purple, and red box at the bottom represent what we call a scheduling and bypass modules. These would be the master of the communications on those three safety data buses in that chassis for determination -- for trip determination.

CHAIRMAN CORRADINI: So I'm going to slow you down. So you gave us three things before, an SFM, a CM, an EIM, and an HWM. Now you have introduced an SVM. I assume that is a voting -- V for voting. What is the SBM?

MR. POTTORF: Yes, so I should clarify. The blue and the purple and the red boxes there are communication modules.

CHAIRMAN CORRADINI: Blue, red, and purple?

MR. POTTORF: Uh-huh.

CHAIRMAN CORRADINI: Okay.

MR. POTTORF: So these herein the middle are communications modules. We refer to them as SBMs or scheduling and bypass modules in the representative architecture, whereas down in this voting and actuation chassis shown at the bottom, we refer to those as scheduling and voting modules. This is where the voting would be performed.

All of these in the middle of the system are communications modules. Those lines in-between the communications modules, those are the point-to-point communications for trip determination. And because we are only showing one of the four separation groups, you will see the other three being input to each of the communications modules down at the actuation chassis set of equipment.

MEMBER BROWN: Let me provide one hopefully helpful comment. There are four separation groups. They can have lots of SVMs, one, two, three, four, eight, nine. It depends on how many input pieces of data you put in. And then there is three other, a group A, B and -- a B, C and D. Every separation group has three SBMs total. Those are safety bus --

MR. POTTORF: They are the master --

MEMBER BROWN: -- masters or something like that. I have forgotten exactly what SBM -- but it is fundamentally an organization and sorting and transmission task.

MR. POTTORF: Correct.

MEMBER BROWN: It doesn't do anything other than that.

MEMBER STETKAR: Except for what you

call voting modules.

MEMBER BROWN: I haven't gotten there. You are way ahead of me. John, let me finish.

Those exist in four separation groups. There will be 12 of those.

Once you leave that upper box, you go down to the divisions. There is two divisions of reactor trip and safeguards each. Two divisions of reactor trip. Two divisions of ESFAS. And that is where the SVMs are located. Those are voted -- now they are called scheduling and voting modules. That is where the two of four voting is done.

You will also then hear another calibration later, the EIMs take these, they are going to talk about three triple module redundancy at some point. So there is three paths, which become clear in the proprietary section that pass through into the two fundamental divisions. Division 1 has reactor trip and ESFAS Division 2.

So I have gone from four separation groups to two divisions of reactor trip and ESFAS. The voting modules then collect the data from the other groups. That is the SGV --

MR. CLARKSON: No, that I got.

MEMBER BROWN: -- all that type of

stuff.

So, there is three SVMs per division and three -- yes, three SVMs per division and they do everything. The EIMs only do take the triple module redundancy and they go to the two out of three so you can have three -- all these trips get processed three times. They are voted on as three times. And then they are processed into the EIMs where you say okay, two out of three of those will cause me to trip. That is the extra redundancy and failsafe if you have a path fail.

So, that is the big picture block diagram. There was another figure that was not included in any of these. That is why I went through this dog and pony show.

CHAIRMAN CORRADINI: Keep on going.

MEMBER MARCH-LEUBA: Hold on. While we have these, these are two analogs. They work on a clock, right?

MR. POTTORF: Correct.

MEMBER MARCH-LEUBA: Where is the master clock and does it connect to everybody? He will be interested in that.

MR. POTTORF: So there is no master clock. And that is kind of why when we refer to

those as scheduling and bypass modules, the SBMs, that is because that SBM is responsible for scheduling the communications within that chassis.

MEMBER MARCH-LEUBA: So there is intercommunications between devices --

MR. POTTORF: That's right.

MEMBER MARCH-LEUBA: -- not the master clock.

MR. POTTORF: Yes, that's right. Yes, you will see in the closed portion the details of how that communication scheme works.

MEMBER BROWN: And there are some more questions that are useful in the closed session but not here.

CHAIRMAN CORRADINI: Green light on.

MR. HECHT: On the top part of the diagram, SFM #2 doesn't have any connection. Is that deliberate or did you just leave --

MR. POTTORF: Yes, that is an error.

MEMBER BROWN: Say that again. I missed it.

MR. POTTORF: Yes, there should be similar --

MR. HECHT: The question was just making clear that the connectivity of all the functional

SFMs are the same.

MR. CLARKSON: Actually, to clarify, if you had an SFM with process inputs that you only needed for monitoring and indication, that is an example of how you would connect it.

If it wasn't performing a safety function, if it was just taking the inputs in to bring in for information, that as an example, I don't know if that was the intent, Jason, but that is a good example of that.

MR. POTTORF: That's a good point. You could use an SFM to simply bring in -- to monitor non-safety parameters in a plant.

MR. HECHT: And then they go out on the MIB?

MR. POTTORF: That's right. It only goes out on the MIB. You would only program the FPGA to communicate with the MIB. But the intent for this presentation was to connect all those.

So if it was performing a safety function, it would have connections to all of the --

MEMBER STETKAR: No, the intent was explicitly to demonstrate that capability.

MR. POTTORF: Okay. Okay, we'll move on.

Okay so the prototype effort. So in late 2015, we initiated development of a prototype module protection system and the scope of that prototype includes -- the hardware scope includes two safety function modules and four communications modules. So, the three scheduling bypass modules and monitoring and indication communications module for one separation group of input. The other three separation groups or divisions of input were simulated with LabVIEW in the prototype.

As for the actuation portion of the system, the hardware scope included two EIMs an four communications modules, three scheduling and voting modules, as well as a monitoring and communications module for one division of ESFAS.

And we just here recently completed the FAT on that system last week at the NRC. We went out to Wimborne Minster and performed an audit of that FAT and testing.

MEMBER STETKAR: Jason, because this is on the record, what is a FAT?

MR. POTTORF: It is a factory acceptance test.

MEMBER STETKAR: Thank you.

MR. POTTORF: And the factory

acceptance test went very well. No issues were identified as part of that testing.

MR. HECHT: Is there any significance of that FAT, other than just satisfying you as the developer that things work together in an integrated test?

MR. POTTORF: That was the main purpose of the FAT was to demonstrate that the concepts of the HIPS platform function and to identify any risks going forward with the platform licensing.

MR. HECHT: So it is really an early integration test. It is not really a factory acceptance test, where it is going into a plant.

MR. POTTORF: No, that's right. It was acceptance of the prototype equipment. So yes, it will have no input into licensing activities, that is for sure.

MR. HECHT: Thank you.

MR. POTTORF: To summarize, the HIPS platform is based on the fundamental I&C design principles of independence, redundancy, diversity and defense-in-depth, and predictability and repeatability.

The platform was developed to provide a simple and reliable solution for nuclear power plant

I&C applications, which support meeting the guidelines and the requirements of the NRC's regulatory guides and IEEE standards applicable to safety-related and important safety applications.

The platform is based on FPGA technology, which has been previously used by the NRC for safety-related -- approved by the NRC for safety-related applications. And the licensing topical report for the HIPS platform demonstrates how the key design concepts for the HIPS platform meet those fundamental I&C design principles. The topical report also describes the testing and diagnostics concepts and how the key design concepts are implemented to achieve overall simplicity in the platform.

And that is the end of my opening portion of the presentation.

There are some supplemental slides attached to this that we will get into more detail in the closed session.

CHAIRMAN CORRADINI: Okay, any questions for the current presentation? Otherwise, we are going to switch to the staff.

Okay we will change out and the staff will join us. Thank you.

Who is going to lead us off, Luis?

MR. BETANCOURT: I am.

CHAIRMAN CORRADINI: Okay.

MR. BETANCOURT: So, good afternoon, everybody. My name is Luis Betancourt. I am the I&C lead clinical reviewer for this topical report. Why don't we have everybody here on my side is Dawnmathew Kalathiveetti, who is an electronics engineer in the Office of New Reactors and he is going to be my co-presenter for this presentation.

On the right I have Dinesh Taneja, who sit he Senior I&C technical reviewer for the NuScale DC application and we also have Joe Ashcraft, who is an electronics engineer in the Office of New Reactor.

So today we are just going to be presenting the staff findings of the design of the highly integrated protection system platform.

So for today's agenda, we would like to provide you like a brief background of the major milestones that happened in the review, followed by the scope of the staff review and evaluation and a summary of the staff findings.

This slide is a brief summary of the presentation that NuScale provided. So in late

2015, the applicant submitted Revision 0 of the topical report. That was followed by February 2016, when we accepted the topical report of Revision 0.

Since then, the staff has expended about 1500 hours which has involved the four engineers that you see in front of you. I would like to mention that the actual hours are actually consistent with the estimated hours that was in the acceptance letter. So that is a big win for us at the NRC and the applicant that we were able to meet the schedule within the allowable hours.

During this time, we had several public meetings and there were two audits that happened. I would like to mention the last we just completed, the audit of the factory acceptance testing of the prototype. It went really well. We were able to assert the prototype. We were able to have a little feel of the platform acceptabilities and we confirmed that the topical report actually claims conform with the applicable regulations.

We had no observations during the audit and there were no ROIs submitted as part of that.

Regarding the ROIs, we had the applicant respond to over 18 questions in one round of the ROIs. And then in November 2016, they submitted

Revision 1 of the topical report, which included the -- and they incorporated their responses of the questions.

As part of the next steps, we expect to issue the set evaluation, depending on the comments that we get from the subcommittee by late March 2017.

Any questions on the audit or anything else? No? Okay.

So the scope of the staff review was a top-down review approach that was based on the fundamental design principles that are outlined in the NRC design-specific review standard for NuScale. I would like to note this is the first time that we actually used the DSRS to perform a review of a topical report.

The design-specific are applicable, regardless of the technology, analog, or digital and they actually work together to ensure that the safety functions will be accomplished when needed. That is, that the design should demonstrate compliance with all of them, rather than one versus another.

We also spent a lot of time reviewing the capabilities of the platform regarding the

calibration testing and diagnostics. Some of the items that you see application-specific action items were items that were outside the scope of the staff review. An example of those is the quality assurance and the qualification because design-application specific activities that are dependent on the vendor that it decides to implement the HIPS system. For those aspects, we have established application-specific items for the uses of the platform to demonstrate compliance with Appendix B on the regulatory requirements.

MEMBER STETKAR: Luis, are the details -- I don't know which -- when to ask questions of the staff in open session or closed session. Are the ASAIs considered open information?

MR. BETANCOURT: Yes, that is open.

MEMBER STETKAR: They are?

MR. BETANCOURT: Yes.

MEMBER STETKAR: Okay. I had a lot of questions on the ASAIs so I might as well launch into them. Let me find my notes on them.

One of the ASAIs, and it is number 21, says an applicant or a licensee referencing the SE must provide redundant power sources to separately supply the redundant power conversion features

within the HIPS platform.

What does the staff mean by redundant power supplies? Because I can interpret that a variety of different ways. If I have four trains of DC power in my plant, A, B, C, D, I could interpret that as I need power to one division from train A and train D or I could interpret it as I need two separate Division A power supply train A to Division 1. What does the staff mean by that? Because it seems contrary to what I understand about the design that I can't talk about in open session.

MR. TANEJA: Right.

MEMBER STETKAR: So what do you mean by that?

MR. TANEJA: So in the topical, their chassis, one box, is like you can use it into a one separation group or one -- let me see.

CHAIRMAN CORRADINI: Go ahead.

MR. TANEJA: So in the topical report, one chassis design represents an application into a one division or one separation group.

MEMBER STETKAR: Now when you talk about separation groups, here we get into semantics because divisions and separation groups are different things.

MR. TANEJA: Right. So if you take a look at just one chassis, let's talk about that one box.

MEMBER STETKAR: A chassis.

MR. TANEJA: A chassis. So their design is what I want to use the word is it is a single failure-proof design, not in a one point of failure. So you could lose a power supply so the chassis continues to function.

So you could have two separate power inputs that provide you with a capability to you know --

MEMBER STETKAR: Okay but --

MR. TANEJA: -- lose a power supply and allow that failure but continue to function.

MEMBER STETKAR: As I understand that, though, both of those inputs could come from the same DC bus.

MR. TANEJA: Now that is application-specific. So that is where a person who is applying this thing in their architecture could make a decision how they want to supply those different power sources.

MEMBER STETKAR: Okay. I am now going to use this in my application. So I want to make

sure that I really understand what the staff means by this. So I have an application now that has two and only two trains in the whole plant, train A and train B.

MR. TANEJA: Right.

MEMBER STETKAR: I got two DC buses in my plant. Does that mean that I have to supply each division of my protections system from both DC train A and DC train B because those are my only redundancies?

MR. TANEJA: And then you lose your independence between them.

MEMBER STETKAR: Yes, you do. So how do I comply with this application-specific action item in that application? I can't, can I?

MR. TANEJA: No, see -- I give you one example that --

MEMBER STETKAR: I don't want to belabor this because we don't have a lot of time. My biggest questions on these ASAIs as I thought about them, trying to implement them in the real world, they are not specific enough. They don't tell me what your expectation is.

It is nice to say you have to have redundant power supplies but you had better darn

tell me what that means because, otherwise, I don't know how to wire up my plant.

Because their interpretation, my understanding of redundant power supplies is different from what I think your interpretation might be and if they are different, that is a problem.

MR. TANEJA: Yes. Well you know, good comment. We will take that into consideration on clarifying some of these ASAIs.

MEMBER STETKAR: Okay, that is on ASAI. I am going to belabor this because I was really disappointed in the ASAIs. I didn't learn much from them.

ASAI 40 says an applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for sensitive command features to provide protection against the resulting condition of a nonsafety system action that has been caused by a single credible event, including its directing and direct consequences.

Is a single credible event a seismic event, fire, internal flood, external flood? Those are single credible events to me. Or do you mean a single failure in electrical things that you can

think about?

MR. TANEJA: I am trying to the SER section.

MEMBER STETKAR: It is ASAI 40, forty. I quoted it verbatim.

So I want to know when I design this thing, what is a single credible event, especially in its effects on nonsafety system signal inputs in my platform.

MR. BETANCOURT: No, this is specific design basis.

MR. TANEJA: You know we put in these SER reference sections. So the context of these is really as a whole. When you read that section it will probably get more apparent as to what this thing stands for.

MEMBER STETKAR: It wasn't apparent to me and I have read a lot of things. So, what is a single credible event in the staff's interpretation?

If these are things that I need to do to make my application-specific platform satisfy NRC staff expectations, those expectations ought to be clear.

Don't try to do it real-time. We don't have much time. I have got a bunch of -- I want to

make my comments on the record so that you have them and can go back and think about things because there are several.

ASAI 57, five-seven, an applicant or licensee referencing the CSE must configure the slave modules to alarm and assume a failsafe position. I cannot find the term slave module anywhere in the topical report. So I have no idea what a slave module is.

MR. BETANCOURT: Well, in the case of the slave module, in this platform are the SFMs and the EIMs.

MEMBER STETKAR: Well, you probably ought to refer to those things, since that is what you are writing it on.

MR. TANEJA: So I think in the closed portion of the meeting, NuScale has the communication details on how the master and slave interact.

MEMBER STETKAR: They don't use the term slave anywhere.

MR. BETANCOURT: Well the slave --

MEMBER STETKAR: No. I'm trying to say that if the staff is making specifications for things, acceptance criteria, you ought to be precise

and I ought to know what your expectations are.

MR. BETANCOURT: Okay.

MEMBER BROWN: John, I am just now key wording it and I have found three references. Master-slave protocols --

MEMBER STETKAR: Sure.

MEMBER BROWN: -- inlays and it is one of the acronyms.

MEMBER STETKAR: In their discussion of the analog analogy they use that phrase.

MEMBER BROWN: Well no, it's under the communication engine part.

MR. BETANCOURT: The protocol that they use is a master-slave configuration. That is what we meant about the slave model.

MEMBER STETKAR: Just make sure somebody understands what that is.

MEMBER BROWN: We will get it with the request package from the master as a unique identifier of the slave. When it is received, it is only the slave that corresponds, blah, blah, blah.

MR. HECHT: Well that is for a bus master.

MEMBER BROWN: Well, bus master, all I am saying is it is a bus master but there is a slave

inside. There is one in each end that you have got to communicate between.

MR. HECHT: I guess that kind of reinforces John's point because a slave module and master is a slave protocol is different than a slave module whether it is Division A and Division B.

MEMBER STETKAR: Other places just to not -- there is going to be a long discussion in the proprietary stuff.

I found a lot of duplication in the ASAIs, 62 and 63, 19 and 56, 22 and 52, 32 and 25, 33 and 54, 43 and 45. So, it is -- clean it up, please.

MR. BETANCOURT: I cannot ask why we have some of them like duplicates. The reason is when we received the topical report the Revision 0 and Revision 1, the applicant they proposed to say a size and the way that -- hold on. Let me finish. So the way that they actually set it up was more on the class by class compliance with the 603 7-4.3.2. So that is the reason that you see that some of them are duplicates, even though they mean the same. The whole idea is to show like there will be an ASAI to a specific bus, to the 603 7-4.3.2 and so on.

CHAIRMAN CORRADINI: I didn't understand

that. So, it was consciously duplicated why?

MR. BETANCOURT: The reason is that the way that the applicant proposed the ASAIs was a class by class on 603 7-4.3.2, I-04 and the SRM.

So some of the ASAI may be the same, even though like they are specific to a specific class to the standard requirement. So I can see why he was confused on that.

MR. TANEJA: Yes, like IEEE 7-4.3.2 is a daughter standard to IEEE 603. So the 7-4.3.2 addresses the digital side of the protection system that is described in 603. So there may be overlapping statements in these two standards. So the application-specific action items are addressing how to meet a certain criteria or clause of 603 or clause of 7-4.3.2, or clause of our ISG on communications. So there may be overlaps but it is like I do this to meet this clause, do this to meet this clause, do this meet this clause.

MEMBER STETKAR: So if I am an applicant now, I have to address each one of those and it costs me money to do that, even if I have to say go see this other thing. You say well, that wasn't quite what we intended by that. Why do you make me say the same things two or three times?

MR. TABATABAI: We are trying to take care of that in the BSRS as much as we can.

CHAIRMAN CORRADINI: John, do you have other things?

MEMBER STETKAR: No, I don't.

CHAIRMAN CORRADINI: Okay, let's keep on going.

MR. HECHT: I have a question about things which what is in the ASAIs and what is general, and what might fall through the cracks as a result.

There are some general questions related particularly to the communications bus and to the application -- and to the specifics of the implementation of general purpose FPGAs and those are primarily related to communications. I can understand an applicant not wanting to get into the details of the implementation of the RS-422 protocols or their protocol engine or a number of other things which are common across all modules but you are not asking for that information here. How do you get to those architectural basic level quality assurance issues and all of the things that one might normally expect in Reg Guide 1.152, 1.168, 1.17, et cetera?

MR. TANEJA: So the QAs we have the ASAIs specifically for the development life cycle activities, which these reg guides pertain to and we expect the user of this platform to address those in their application for whether it is a design certification or a license amendment to explain how they are going to meet that life cycle development process, whether they are meeting and how they are complying with these.

MR. HECHT: But the developer isn't going to be developing the communication bus FPGAs.

MR. TANEJA: The FPGAs are going to be developed -- oh the communication protocol is very specific to the architecture.

MR. HECHT: Is specific to the what?

MR. TANEJA: This prototype or this platform, it is unique to this platform design, how the communication protocol works. The physical area is RS-422 but the communication protocol, which I expect NuScale to cover in the proprietary portion of the meeting, is proprietary to the design, how that works.

MR. HECHT: Okay. That was my understanding. So you expect that communication protocol to be used in every NuScale control system.

MR. TANEJA: Well, any application, whether it is NuScale or anybody. Right.

MR. HECHT: Well so my question is shouldn't that be part of the evaluation of the platform, as opposed to being an evaluation of the application or why wasn't it?

MR. TANEJA: It was part of the platform evaluation.

MR. HECHT: Well, is the quality assurance part of the platform?

MR. BETANCOURT: No. What we have over here -- well, let me tell you why it was not covered over here.

In the past, the platforms that we have received in the NRC, they have already been built. So in the case of NuScale, they are building this platform scratch. It is still on paper. It is still a design. So in the past what we have done is a commercial grade application review and we look upon the QA process, the secure development process and so on.

In this case, it hasn't been built so we have an ASAI for any -- right now NuScale may decide to use Ultra (phonetic), may decide to follow a different vendor. So what they have is a set of

requirements and specs that it can give to any single vendor and they can tell them build me this design in accordance with Appendix B. So that is the reason that we have that ASAI.

MR. HECHT: So, if Plant A has this communication protocol and Plant B has this communication protocol, you would expect both of them to send you the same information on how the architectural and foundation features of this NuScale design are implemented, even though they are common?

MR. TANEJA: Well, see one is a requirement specification and then you know the reg guides that you are referring to, those are really the life cycle activities that you must perform in order to develop an architecture.

Even the fabrication of the equipment has to follow a QA process of Appendix B. So if I am looking at a requirement spec, the requirement spec requires the vendor to build a system in accordance with the RQA program or whatever the QA programs that are stipulated in the purchase order.

So the ASAIs are asking the user of this topical report to impose the QA requirements on the system that they would be buying to build this

architecture.

MR. HECHT: I don't think we are closing on this question but I don't want to take too much time on it.

MR. TANEJA: Okay, fair enough.

CHAIRMAN CORRADINI: All right.

MEMBER STETKAR: I've got one more.

MEMBER BROWN: John, before you go, can I amplify Myron's a minute on the QA piece?

MEMBER STETKAR: Sure, sorry.

MEMBER BROWN: I guess what I was trying to get out of this interchange is right now NuScale, they have got their plant design and they have proposed an architecture for the integrated protection system.

MR. TANEJA: Correct.

MEMBER BROWN: Well, a part of an architecture. It is a proposed implementation in terms of components, et cetera. It is a platform, as you say.

You did not address the ideas, as Myron pointed out, QA, SDOE, all that stuff that you grind through, making sure that you have got a consistent product when you come out, and it makes sense and it is protected. They don't have to go what is it,

Rock Creek, who is building this. This topical report could go to somebody else.

MR. TANEJA: That's correct.

MEMBER BROWN: And I think that is, in a way, you want to end up with the same consistent quality --

MR. TANEJA: Exactly.

MEMBER BROWN: -- and product but yet, there was nothing in the SER explicitly talking about how you -- you are expecting that to come with all the other reg guides and rules that we have?

MR. BETANCOURT: Well, any use of this platform, they have to come back to us at the NRC. It is a part of our license amendment requirements or a DC application.

In the case of NuScale --

MEMBER BROWN: You said you have a DC application now.

MR. BETANCOURT: Right. In this application, NuScale is already addressing that and they are going to be building the platform in accordance with Appendix B.

Any operating power plant or any new reactors they can reference we want to use this platform but they have to address that as a specific

item in the QA program. They have to develop in accordance to the requirements that have already been specified.

MEMBER BROWN: Okay so that will springboard into the requirements that you all talked about and imposed on other applicants.

MR. BETANCOURT: Right and we will be able to review that when it comes in-house.

MEMBER BROWN: Okay, I agree. I have got my answer here. We will move on. Is that okay, Mike?

CHAIRMAN CORRADINI: Yes, I'm just listening.

MEMBER BROWN: Yes, I want to get on.

MR. BETANCOURT: I think you had a question before we move on.

MEMBER BROWN: Oh, John, I'm sorry.

MEMBER STETKAR: There is this Section 3.8.2.4 of the SER. There is a discussion of Section 2 digital I&C Interim Staff Guidance 04, in particular on command prioritization.

And in several subsections under there, parts of the discussion, there are statements like the following. This happens to be a quote from one of them: The staff agrees that an evaluation of

point 4 is not applicable because all priority logic capability within the HIPS platform is performed by discrete logic components, i.e., analog technology. Therefore, this SE does not address the evaluation against point 4 of staff position 2. There are, I don't know, three, four, five of those.

Okay, where does the staff address those functional requirements for command prioritization in their review of either this platform or some application-specific implementation of this platform? Because this says well, we are not addressing that because it is not software related somehow.

MR. TANEJA: Yes, this evaluation was specifically against the ISG-04. The ISG-04 was the set of points in there are dealing digital data communication.

MEMBER STETKAR: Software-based?

MR. TANEJA: Software-based digital data communication. So in the HIPS platform, the priority logic is discrete. It does not use any software whatsoever.

MEMBER STETKAR: I understand that.

MR. TANEJA: So that is why it was the evaluation was not relevant to these areas of the

ISG-04.

MEMBER STETKAR: Where does the staff review the hardware implemented priority in this platform and have assurance that, indeed, it is implemented fine or specified fine? And the staff does that and when is it done?

MR. BETANCOURT: As you just mentioned, this point was specific to software-based system and the -- hear me out. Hear me out.

MEMBER STETKAR: Okay.

MR. BETANCOURT: At the APL, which is the activation priority logic, the applicant has made a statement about the priority logic that they will use to implement. All of the activation logic it will be having the highest priority, followed by the manual actuation actions. That will also be on ASAI. If I recall very well, we are going to be reviewing that aspect.

MEMBER STETKAR: I didn't get the last part of that.

MR. BETANCOURT: I think there will be an ASAI on that but I have to --

MEMBER STETKAR: I couldn't find one, which is the reason why I kind of asked this because it strikes me that you are saying you are not

reviewing specific aspects of this proposed design because oh, they are not software-implemented aspects. And I couldn't find any places where you were reviewing aspects of the design that are hardware-implemented aspects.

MR. BETANCOURT: Okay, we will take it back.

MEMBER STETKAR: In particular, under these parts, that ISG-04 priority --

MR. BETANCOURT: I understand. We will take it back.

MEMBER BLEY: Think about this one in general, not just this specific case. Because when you go through and X things out because they don't fit what you designed it for, the functional concept that was there needs to be picked up somewhere. This should just be an example.

MEMBER STETKAR: See, if I read that -- for example, if I turn off this notion of software and hardware, in the ISG under Command Prioritization sub-item 2 says priority modules used for diverse actuation signals should be independent of the remainder of the digital system and should function properly, regardless of the state or condition of the digital system. If these

recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.

It doesn't say anything about software there. It just says priority modules. And you say well, you don't have to review that here because that function is not implemented via software, that priority module function.

And I think what we are saying is somewhere there ought to be assurance that someone in a staff review, whether it is at the topical report for the platform, which to my mind seems -- setting what that priority logic is, what is more important than A or B is clearly an application-specific function. You know what gets higher priority than another.

But the way that that logic is implemented seems to be a platform review issue.

MR. TANEJA: We did review it and we have a very good understanding of it. We will make sure that we go back and see where we documented it in our safety evaluation.

MEMBER STETKAR: Okay.

MR. TANEJA: Okay?

MEMBER STETKAR: Okay.

MR. TANEJA: So, we will go back and take a look at it.

MEMBER STETKAR: Thanks.

CHAIRMAN CORRADINI: Any more questions before we move on?

MEMBER STETKAR: No, I didn't. That was it.

CHAIRMAN CORRADINI: Why don't you guys go ahead, then?

MR. BETANCOURT: Okay, let's move on to the next slide.

MEMBER BROWN: Luis, would you be a little careful? You are kind of --

MR. BETANCOURT: Yes, I know. It is kind of sensitive.

MEMBER BROWN: You are going to snap his eardrums out if you are not careful.

MR. BETANCOURT: Sorry for that.

So let's move on to the topics of independence. We were able to review the design table so the platform that we were able to confirm that the platform independent features that provide the capability to implement the system designs that can satisfy the systems independence requirements.

So evaluation was focused in these four

areas that you see on the screen on the physical, electrical, communication, and function independence.

Any questions on this topic?

CHAIRMAN CORRADINI: This is where I am confused. I am trying to figure out what action that -- so, this is just me who is trying to understand what action the committee is going to take on this, given the number of ASAIs that are listed at this point in time.

What you are kind of saying is things look okay, assuming they satisfy 65 things. How does one come to a conclusion for a letter back to the staff and informs the applicant that can't say anything more than as long as you satisfy 65 additional things, we are kind of okay? I'm struggling.

MR. TANEJA: Well you know this is an interesting one. I don't think there has ever been a topical on a digital platform in front of the ACRS. I think this is the first one that we are doing.

CHAIRMAN CORRADINI: Because?

MR. TANEJA: I don't know.

CHAIRMAN CORRADINI: Because they are

already pre-built and you just have to qualify them from a QA standpoint?

MR. TANEJA: You know because those are topicals and they are not licensing actions. So since this is really, at this moment, it is not a licensing action unless I have an applicant that refers to this topical in their application, whether it is for design certification or license amendment request.

So when we come back with the NuScale review, that is where they are referring to this topical report and they are addressing all of the ASAIs in there. And that is when we will get into the details of the regulatory compliance and all the safety features and how they are implemented.

MR. BETANCOURT: Right because the finding that we are making is only at the platform level but we still need to complete a story on how the platform interacts with the system.

CHAIRMAN CORRADINI: Okay. So, I wrote down -- I had a feeling you were going to go this way. So I wrote down the plant protection or the HIPS or whatever this thing is called is a box that you are trying to decide if the box satisfactorily fits into the architecture.

MR. BETANCOURT: Correct.

CHAIRMAN CORRADINI: Okay. So if that is the case, other than this as being informational for the members, is that all it is? It strikes me as we are a bit early in the game to write anything with a conclusion if it is strictly they are building a box and the box has got to fit into a bigger box and it looks okay; but until we see how the box fits -- connects to the bigger box, there can be no conclusion.

MR. BETANCOURT: Right and that is the reason that we were basically saying like the platform -- if we have an applicant, a licensee that uses this platform, we believe that this that is why we used the wording it first complies with the regulations.

CHAIRMAN CORRADINI: Okay, fine.

MEMBER STETKAR: Just for the record, at least I haven't tracked down whether it came to the full committee but I know that the US-APWR, the subcommittee -- I am trying to read at the same time I talk and I don't do that well -- did review the topical report on digital I&C and, in fact, the ACRS wrote a letter on June 25, 2009 at least on the Diversity and Defense-in-Depth aspects.

MR. TANEJA: Was it topical or technical?

MEMBER STETKAR: It was a topical report. We wouldn't write a letter on a technical report. The June 25, 2009 letter is Safety Evaluation for Mitsubishi Heavy Industry's Topical Report MUAP-07006-P Revision 2, Defense-in-Depth and Diversity Related to US-APWR but we discussed the whole platform.

MR. TANEJA: Yes, what happened in that case --

MEMBER STETKAR: So just it has come before us in the past.

MR. TANEJA: -- so that applicant changed that technical topical report into a technical report for their design.

MEMBER BROWN: This really isn't worth our committee time.

CHAIRMAN CORRADINI: All right but I just wanted to make sure I was understanding where it would fit in.

MEMBER BROWN: Yes, my understanding of what they were trying to show, to do with this, is NuScale has proposed a design and a set of digital components set up in a certain configuration that,

if connected properly, would be capable of demonstrating the fundamentals and the other design aspects, in terms of communications or stuff -- a bunch of stuff we don't need. We have no idea what networks are going to be in this plant, how you are going to connect in and out.

We can talk about the memory that they have and if it is not accessible, then we can make sure -- we can say hey, it can be covered. But we don't see it until we have seen it.

CHAIRMAN CORRADINI: Okay.

MEMBER BROWN: How they connect the other stuff into this platform and everything else is not defined in this. This just shows how you get four separation groups into two divisions of trips and will they trip or not.

MEMBER STETKAR: I find it easier to think of this as NuScale has not proposed this topical report. Rock Creek has proposed it and it might be used in the NuScale application.

MEMBER BROWN: That is one way of looking at.

MEMBER STETKAR: That is one way of thinking about it.

MEMBER BROWN: Yes, that is one way of

looking at it.

MEMBER STETKAR: Is the proposed design by Joe's Electronics, if you will -- seriously, it is a way of thinking about this disjoint between ASAIs and looking at the platform itself being proposed by a vendor, which could be used in NuScale. It could be used in a Westinghouse plant.

CHAIRMAN CORRADINI: Oh, that I understand. I just want to understand the connection to the architecture and I think I have got it. So keep on going.

MEMBER BROWN: Oh, and from the time I got here in 2008, I can't remember reviewing a topical report of this nature for any of the -- I understand the point about the diversity, that one aspect that we talked about on the US-APWR but we didn't do that on the other projects that I have looked at. We did the DCD and we used the technical spec or the technical report or a topical report to look at to make sure we could understand how it operated. That is the way I have done it in the past.

MR. BETANCOURT: Okay, before I move on on this slide, do you have any questions on independence?

MEMBER BROWN: We will have to take your word for it.

MR. BETANCOURT: Okay, let's move on.

CHAIRMAN CORRADINI: That's very unlike us but keep on going.

MR. BETANCOURT: Okay, in the

MEMBER BROWN: Okay in area of redundancy, we were able to confirm that the proposed design exhibits redundancy in the areas of power supply, safety function module, communication redundancy, equipment interface and at the platform level.

So all of these redundancies affected to result in a highly reliable system.

MEMBER KIRCHNER: Let me ask a question now because I'm following your slides and the NuScale slides. So what you are saying is that all the bullets that are in the NuScale, which is extracted from the topical report, you have checked all those and you agree with all of those.

MR. BETANCOURT: Yes. Yes, and there is already areas that we spend our time --

MEMBER KIRCHNER: These are the backup slides.

MR. BETANCOURT: Okay, yes.

MEMBER KIRCHNER: Okay.

MEMBER BROWN: Go on.

MR. BETANCOURT: Okay, so I guess I am now going to turn it to Dawnmathew Kalathiveettil on the remainder of the presentation.

MEMBER BROWN: Now before he says anything, this is a different picture than you are going to see later. This is just a functional depiction, not box depiction of their proposed system. You don't see an SBM and you don't see an SVM. I can tell you where the SVM is. I can't tell you where the SBM --

CHAIRMAN CORRADINI: I don't want to know right now.

MEMBER BROWN: You don't want to know. I am just telling you this is a functional depiction of what this system is supposed to look like.

You have got the four groups, separation groups, breaking down into two divisions of voting. That's all you are seeing. That is the limits of its intelligence.

MR. KALATHIVEETTIL: Okay, good afternoon, everyone. My name is Dawnmathew Kalathiveettil and I will be continuing --

CHAIRMAN CORRADINI: You have got to say

that slower. I --

MR. KALATHIVEETTIL: Slower?

CHAIRMAN CORRADINI: You guys speed up from person to person.

MR. KALATHIVEETTIL: It is Kalathiveettil.

CHAIRMAN CORRADINI: Okay.

MR. BETANCOURT: It is a long name and a long last name.

MR. KALATHIVEETTIL: All right, so moving on with diversity of the HIPS platform. So the HIPS platform basically uses two diverse FPGA technologies to achieve equipment diversity.

The example in the topical report, the four separation group, protection system is based on using one FPGA technology with two of the separation groups and a number of kind FPGA technology with the other two separation groups. This is shown as yellow and red from the figure.

In such an arrangement, additional CCF associated with one FPGA technology would not defeat the safety function, since you still have two separation groups which remain unaffected. And because of the diversity, the unaffected separation groups will be able to accomplish the safety

function.

Along with the equivalent diversity, there is also associated shift design diversity because vendors use different development tools to actually make the final configured FPGAs and also the HIPS platform provides functional diversity with the use of different protection logic on the SFMs associated with each safety function or safety function group.

All right, so this table here basically tries to explain the built-in diversity of the HIPS platform. The first event you see is a regular transient accident situation with no CCF at all. And in that situation, you have all four separation groups modules, the SFM, CM, and EIMs all being available to do their particular safety function.

Case 1 we see that there is --

MEMBER SKILLMAN: Excuse me, sir. When you say available, that word connotes the device is powered, it is actuated, it is waiting for a signal and it is going to produce the correct signal at the right point in time. Is that what you were communicating when you say it is ready?

MR. KALATHIVEETTIL: Yes, it's available.

MEMBER SKILLMAN: It is going to do what it is supposed to do?

MR. KALATHIVEETTIL: Right, that's what it means.

MEMBER SKILLMAN: Okay.

MR. KALATHIVEETTIL: So Case 2 is where, as you can see, there is additional CCF associated with the FPGA of the SFMs of separation groups A and C. But here we are crediting equipment diversity and module functional diversity because of the CM and EIM of separation groups A and C are still available, just as all the key modules of B and D are available.

And the last case scenario in Case 2 is one where we are assuming that a CCF has taken out the FPGA technology associated with A and C. So all three modules are not available for the safety functions. However, you still have separation groups B and D, which can actually accomplish the safety function because the FPGA is not affected by the same CCF.

Any questions?

MEMBER KIRCHNER: So B and D have the different field programmable beta rays?

MR. KALATHIVEETTIL: Yes.

MEMBER KIRCHNER: Okay, just checking.

MR. HECHT: What do you mean by functional diversity?

MR. TANEJA: Let me elaborate on this one. Typically, when we see a CPU-based digital platform, you have input boards with multiple input capabilities and then you have a CPU board which takes the information and does a processing and then you have the output boards that output the output to an actuated device.

In their design, the safety function module is dedicated to a specific function. So each module can only accept four -- it has four input sub-modules on them. So, it can accept four inputs.

So, there the design is essentially like if you are familiar with the old Westinghouse 7300 cabinets, where they had an input module which was essentially like a driver card that took in an analog input and then you went into a scaling, which kind of scaled that into a different analog circle and went into a bistable module.

So their design is, essentially, the application of that scheme. So the functional diversity is that each SFM is only designated to a one given function.

For example, for the NuScale, I think we are dealing with 22 safety functions. So there would be 22 separate safety function modules.

So I can lose a safety function module so I will lose that particular parameter. Let's say that is dealing with a pressurizer pressure. But I might be able to achieve a safety function using other plant parameters, which are running on a separate safety function module. So I have not lost the capability other than that specific one.

So in comparison to a digital system, where my analog input board goes, I may lose 20 inputs or 40 inputs, depending on how they are designed. And then I will lose like a whole division capability.

Here, that functional diversity allows me to lose maybe a subset of a function but I have other means within that separation group to achieve the same, I guess -- I don't want to say the same safety function but the intended consequences are dealing with that event.

MR. HECHT: Is the platform that we are talking about here, does it require such functional diversity? I used to call it analog -- I mean well some kind of redundancy, functional redundancy. You

are basically saying that you are using different sensors to get the same trip signal. Right?

MR. TANEJA: You are getting different plant process parameter to decipher same plant upset or transient condition, let's say. So you are using the level and the pressurizer pressure may be two separate ways of looking at this.

MR. HECHT: The term that I was looking for was analytical redundancy.

MR. TANEJA: Exactly.

MR. HECHT: So, is that required in the design or are you just positing it here for the purposes of this example?

MR. TANEJA: The example. This is an example and I think that is going to be an application-specific action item where the user of this platform has to show how they allocated different safety functions to various different inputs to achieve that feature.

MEMBER BLEY: Myron, in more general not in terms of just I&C. We have always protected against key accidents in multiple ways. So there is a design principle.

MR. HECHT: Yes, I get that. That is D3. But I --

MEMBER BROWN: Before there was a D3.

MR. HECHT: Okay.

MEMBER STETKAR: Well before we labeled it.

MR. HECHT: Okay. So is this an implicit or explicit requirement that there be this functional diversity as part of this platform?

MR. TANEJA: Well you know I guess I would say it is additional level of defense-in-depth by having that capability because you do have B and D on a different FPGA platform, which are not susceptible to a common cause failure, which would result in maybe only losing in two out of the four separation groups.

So the redundancy, you know you would have these same functions available to you on the redundant set also.

So it is just a level of defense-in-depth. I think that is what we are achieving by this purpose. It is not that -- I could, you know like in Case 2, I could lose A and C but I still achieve my functions.

MR. HECHT: Right. Well, I guess that case is kind of application-specific as to whether you have that middle case there.

MR. TANEJA: Right, exactly.

MR. HECHT: So it is not always there.

MR. TANEJA: You know the platform is flexible enough to be able to do that and a good designer should use these capabilities, I would say.

MEMBER BROWN: I would suggest that we move on but this will be examined in more detail whenever we get an actual plant architecture presented to us.

And I suspect -- you said something about all and just one observation. I know there is four processing plant parameter processings for each safety function module.

MR. KALATHIVEETTIL: Right.

MEMBER BROWN: I presume they would not put all four pressure signals onto one safety function module. That would defeat your purpose.

Well, somebody may not have heard that. I thought I heard that being stated here a minute ago. All right, go on.

MR. TANEJA: So the allocation of that has to be design.

MEMBER BROWN: I got it. Let's go on.

MR. KALATHIVEETTIL: Predictability and repeatability. The staff evaluated how data is

communicated in the HIPS platform and the response time characteristics of the system. The HIPS platform is FPGA-based design and does not use interrupts.

The staff reviewed that the HIPS platform operates on fixed cycles, where a deterministic sequence of: 1) acquiring inputs; 2) performing logic operations such as comparing a process variable against a trip set point to determine the partial trip status; and 3) generating output signals as followed without the use of any interrupts.

The staff basically finds that the platform conforms to 10 CFR 50.55a(h), specifically IEEE Standard 603-1991, Clause 4, Clause 5.2 and Clause 5.5.

MR. BETANCOURT: I would like to make a note that even though this might be single data path flow, NuScale is going to go into a lot of detail in the proprietary information on this topic.

This only shows like the scope of our review that we are excluding the fuel sensors and the fuel components. But from the inputs module, all the way to the EIM, that was the scope of our review.

MR. KALATHIVEETTIL: We are showing as the boundary.

MEMBER BROWN: Okay.

MR. KALATHIVEETTIL: Calculation testing and diagnostic capabilities, Section 8 of the topical report describes the diagnostics and maintenance features provided by the platform and directly addresses IEEE Standard 603-991, Clause 5.7.

The platform features detect and monitor the system's performance during operation and to initiate alarms if the system fails to perform deterministically and within the required time.

The platform uses cycling redundancy check to ensure that for data communication integrity. In addition, the staff also determined that the self-testing features of the modules do not affect the ability of any module to perform its safety function.

CHAIRMAN CORRADINI: Any questions?

MR. KALATHIVEETTIL: For regulatory conformance, the staff finds that the HIPS platform meets the applicable regulatory requirements associated with the fundamental design principles. As said, earlier, there are 65 ASAIs and out of

those, 55 were proposed by the applicant and the staff added an additional 10 to the list.

Those 65 ASAIs provided in Table 4-1 must be performed when requesting the NRC's approval of the HIPS platform for safety-related applications at nuclear power plants.

Any other questions?

CHAIRMAN CORRADINI: Any other questions by the committee?

Going once --

MEMBER BROWN: We're done.

MR. BETANCOURT: Okay, thank you.

CHAIRMAN CORRADINI: Okay. So we are going to be going into a closed portion.

So before we do that, why don't we see if there are members of the public that have comments on this portion.

So, can we -- is there anybody in the room that wants to make a comment? Otherwise, can we please turn on the mike for members of the public on the phone line.

Okay, anybody in the room? No.

Is anybody on the phone line from members of the public want to make a comment?

MR. LEWIS: Marvin Lewis, member of the

public.

CHAIRMAN CORRADINI: Marvin, Happy New Year.

MR. LEWIS: Thank you, same to you.

CHAIRMAN CORRADINI: Any comments you make, Marvin?

MR. LEWIS: Yes, just a small one. It appears that some very simple things haven't been coordinated just like knowing definitions but I always get in my lane abbreviations are used like a garden. And I find that us that are listening in from the public that you have got to get things hammered down before the meeting or at least introduce those terms for people who are on the line.

CHAIRMAN CORRADINI: Marvin, you are fading on us. So you seem to be pulling away from your phone or something.

So, get closer to your phone. Don't scream but move closer because you are fading on us. We lose every other word.

MR. LEWIS: I am getting some of the same thing on this side.

All right, just define your abbreviations, please. Thank you. Bye.

CHAIRMAN CORRADINI: Okay, anybody else on the public line?

Okay, not hearing any, could you please close the public line and we will now check the room and go into closed session.

(Whereupon, the above-entitled matter went off the record at 2:26 p.m.)

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Design of the Highly Integrated Protection System Platform

Presentation to the ACRS Subcommittee

February 7, 2017

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Agenda

- Background
- Safety Evaluation Scope
- Safety Evaluation Topics
  - Fundamental Design Principles
  - Calibration, Testing, and Diagnostics Capabilities
- Regulatory Conformance

Background - Timeline

Date	Activity
December 2015	Topical Report (TR) 1015-18653-P submitted for review
February 2016	NRC Accepted TR for Review
June 2016	NRC Sent RAIs
July 2016	First Audit at NuScale's Rockville Office
August 2016	NuScale Sent Response to RAIs
November 2016	Revision 1 of TR docketed
January 2017	Draft Safety Evaluation Issued
January 2017	Second Audit at Ultra Electronics (Wimborne, UK)
February 2017	ACRS Subcommittee Meeting
March 2017	Issuance of Final Safety Evaluation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

SE Review Scope

- The scope of the review was focused on:
  - Fundamental I&C design principles
  - Calibration, testing, and diagnostics capabilities of the HIPS Platform

- Application-Specific Action Items:
  - Quality Assurance
  - Equipment Qualification
  - Secure Development Process
  - MWS and PS Gateway
  - Human-Machine Interface
  - Displays

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Independence

- Physical Independence
- Electrical Independence
- Communications Independence
- Functional Independence

The staff finds that the TR provides information sufficient to support conformance with the independence requirements in RG 1.75, RG 1.152, RG 1.53, and DI&C-ISG-04, or establishes ASAIs as necessary to fully comply with the regulatory requirements for an applicant or licensee referencing this SE.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

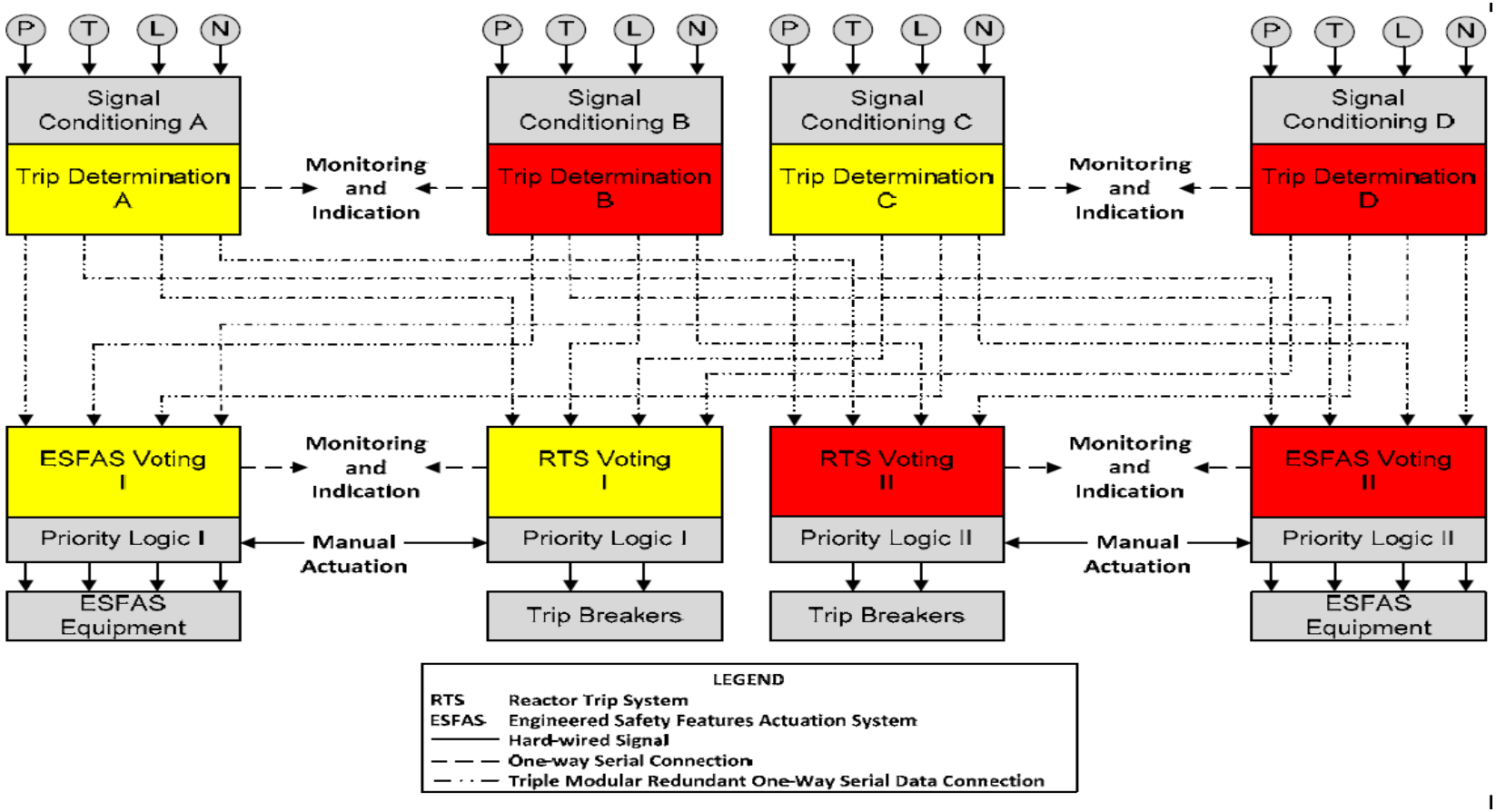
Redundancy

- Power Supply Redundancy
- Safety Module Redundancy
- Communication Redundancy
- Equipment Interface Redundancy
- Platform Redundancy

The staff finds that the TR provides information sufficient to support conformance with the regulatory requirements on the single failure criterion in RG 1.53, or establishes ASAIs as necessary to fully comply with the regulatory requirements for an applicant or licensee referencing this SE.

Diversity

FPGA Equipment Diversity Allocation in a Representative Architecture



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

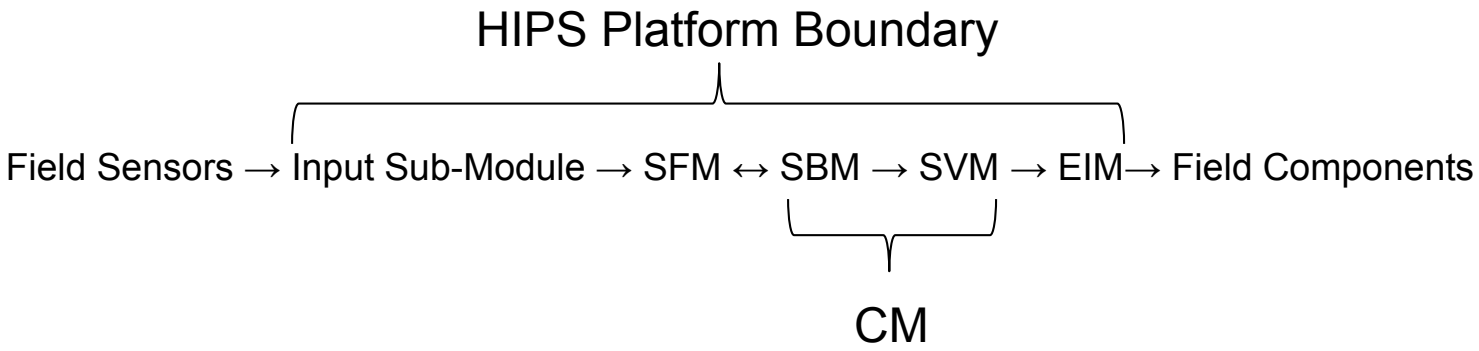
Diversity

Effects of Digital CCF for HIPS Diversity Strategy

Event	Module	A	C	B	D
Transient or accident (no CCF)	SFM	✓	✓	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or accident with CCF (Case 1 – equipment (FPGA) and module functional diversity)	SFM	×	×	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or accident with CCF (Case 2 - equipment (FPGA) diversity)	SFM	×	×	✓	✓
	CM	×	×	✓	✓
	EIM	×	×	✓	✓

Predictability and Repeatability

Typical plant signal data flow path in HIPS platform



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Calibration, Testing, and Diagnostics Capabilities

- Section 8, “Calibration, Testing, and Diagnostics,” of the TR describes the diagnostics and maintenance features provided by HIPS platform and directly addresses IEEE Std 603-1991 Clause 5.7.
- These features include the use of BIST, CRC checks, periodic surveillance testing, and other tests in each type of module as appropriate to verify normal operation.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Regulatory Conformance

- The HIPS platform design supports meeting the applicable regulatory requirements associated with the fundamental I&C design principles.
- 65 ASAIs have been established to identify criteria that should be addressed by applicants or licensees referencing this SE.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Questions

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Acronyms

- ACRS: Advisory Committee on Reactor Safeguards
- ASAI: application-specific action item
- BIST: built-in self-testing
- CCF: common-cause failure
- CM: Communication Module
- CRC: cyclic redundancy checksum
- DC: direct current
- EIM: equipment interface module
- ESFAS: engineering safety features actuation system
- FPGA: field programmable gate array
- HIPS: highly integrated protection system
- I&C: instrumentation and control
- IEEE: Institute of Electrical and Electronics Engineers
- ISM: input sub-module
- MWS: maintenance workstation
- NRC: U.S. Nuclear Regulatory Commission
- PS: protection system
- RAI: request for additional information
- RG: regulatory guide
- RTS: reactor trip system
- SBM: scheduling and bypass module
- SFM: safety function module
- SE: safety evaluation
- SVM: scheduling and voting module
- TR: topical report