Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: ACRS NuScale Committee Open Session

Docket Number: N/A

Location: Rockville, Maryland

Date: August 23, 2018

Work Order No.: NRC-3861 Pages 1-242

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

+ + + + +

THURSDAY

AUGUST 23, 2018

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., Michael Corradini, Chairman, presiding.

COMMITTEE MEMBERS:

MICHAEL L. CORRADINI, Chairman

RONALD G. BALLINGER, Member

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR. Member

WALTER L. KIRCHNER, Member

JOSE MARCH-LEUBA, Member

JOY L. REMPE, Member

GORDON R. SKILLMAN, Member

MATTHEW SUNSERI, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

*Present via telephone

CONTENTS

P R O C E E D I N G S

(8:31 a.m.)

CHAIRMAN CORRADINI: Okay, the meeting will come to order. This is a meeting of the NuScale Subcommittee. My name is Mike Corradini, Chair of this subcommittee meeting. ACRS members in attendance are Ron Ballinger, Dennis Bley, Dick Skillman, Matt Sunseri, Joy Rempe, Jose March-Leuba, Charlie Brown, soon to be Walt Kirchner, and our consultant, Myron Hecht. Christina Antonescu is the ACRS staff -- of the ACRS staff is the designated Federal official for this meeting.

The purpose of this meeting is for NuScale to give an overview to the subcommittee on the NuScale Design Certification Application Chapter 7, Instrumentation and Control, and for the staff to give a presentation to the subcommittee on their Safety Evaluation Report on Chapter 7 with open items.

The ACRS was established by statute and is governed by the Federal Advisory Committee Act, or FACA. That means that the committee can only speak through its published letter reports. We hold meetings to gather information to support our deliberations. Interested parties who wish to provide comments can contact our offices requesting time.

After the meeting, the Federal Register Notice is published. That said, we set aside about 15 minutes for extemporaneous comments from members of the public attending or listening. Written comments are also welcome.

The ACRS section of the U.S. NRC's public website provides our charter, bylaws, letter reports, and full transcripts of all our full and subcommittee meetings, including all slides presented at the meetings. We will hear a presentation from NuScale and the NRC staff today. The subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions as appropriate for deliberation by our full committee.

The rules for participation at today's meeting have been announced as part of the notice of the meeting published in the Federal Register, and we have received no written comment or request for time to make oral statements as a member of the public in today's meeting. As always, we have one bridge line established for interested members of the public to listen in in the open session.

Also, the bridge line will be open after the open meeting session to see if anyone would be listening to make additional comments. 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 this meeting use the microphones located throughout the meeting room when addressing the subcommittee. Participants should identify themselves, speak with sufficient clarity and volume so they may be readily heard.

Please also silence all your cell phone, pagers, iPhones, etcetera, so we do not have any buzzes or noises through the meeting. We will now proceed with the meeting. One extemporaneous point is this is the second of our meetings look at the DCD. We talked about Chapter 8 back in June. We are now going to discuss Chapter 7. Our intent is most likely to combine our comments and suggestions on seven and eight when we talk at the full committee in September.

So I think I am going to be calling upon Robert Caldwell of NRO to start us off with some introductory remarks. Mr. Caldwell?

MR. CALDWELL: Yes, hello. My name is Bob Caldwell. I am the Deputy Division Director for the Division of Engineering and Infrastructure in the Office of New Reactors, and I would like to thank you all for giving us the opportunity to present our

findings on Chapter 7 of the DCD.

Right now, before we present our -- do our presentation, before we get started, I would like to point out that NuScale recently informed us that there was a delta between Chapter 5 and 7 of the DCD which they are looking at. These discrepancies involve a remove shut-down station. During our presentation, we will be providing you our findings based on the DCD details that we have done the evaluation on.

So while NuScale is resolving these discrepancies that they find, there is the need for a change in Chapter 7. We will take a look at it and see if we need to change the SE. If there is a need for the change for the SE, we will come back to the subcommittee as appropriate.

CHAIRMAN CORRADINI: Charlie?

MEMBER BROWN: Just to make clear, so we understand this, what you mean is they want to delete the remote shutdown station? Is that my understanding?

MR. CALDWELL: No, I do not know exactly what their path forward is at the moment. We hope to find out. This is --

MEMBER BROWN: But you do not know those details? It is kind of -- the information passed

around, it was not real clear, and I just wanted to make sure it was clear to the other members.

CHAIRMAN CORRADINI: But the only thing we know for sure is what you reviewed is not necessarily what is the current design thoughts.

MEMBER BROWN: With respect to the remote shutdown. With respect to Chapter 7.

MR. CALDWELL: Yes, with respect to the remote shutdown stations.

CHAIRMAN CORRADINI: Shutdown stations.

MEMBER BROWN: Chapter 7 uses the RSS, calls it out in many places.

MR. CALDWELL: Right.

CHAIRMAN CORRADINI: Okay. So we have to be aware of that.

MR. CALDWELL: Yes, just be aware of that. That is the only ones we cross. Thank you.

CHAIRMAN CORRADINI: Thank you. So, we should turn to Paul. Are you going to lead us off?

MR. INFANGER: Yes, I am Paul Infanger. I am the Licensing Project Manager for Chapter 7. I appreciate the opportunity to present our technical details in support of the staff's SCR. I appreciated working with the staff on Chapter 7. We have received the SCR with no open items related to Chapter 7. The

only open items are related to turning back to some open items in Chapter 8 and expected open items in Chapter 15. But there are not Chapter 7-related open items.

We will relay, the issue on the remote shutdown panel will be addressed during our presentation. Just want to say a little bit about my background. I have been with NuScale for about three and a half years. Prior to that, I was working on the Korean reactor for Barakah, and also prior to that, at UniStar for the Calvert Cliffs COLAs, and prior to that, 25 years as Licensing Manager at various operating sites.

MEMBER BLEY: Mr. Paul, you mentioned Chapter 8. When we went through Chapter 8 with you, there were a few issues that came up that you deferred to Chapter 7. Are you going to talk about those in particular?

MR. INFANGER: Yeah, there were several timers that we discussed in Chapter 8 that were really I&C issues, so we are prepared and have information in our presentation on those.

MEMBER BROWN: Those are the 24-hour timers you are talking about?

MR. INFANGER: Yes.

MEMBER BROWN: Okay. And how they interface with the DC?

MR. INFANGER: Right.

MEMBER BROWN: Okay, thank you.

MR. INFANGER: So with that, I would like to introduce the lead speaker will be Brian Arnholt.

MR. ARNHOLT: Good morning. I am Brian Arnholt. Thanks for the opportunity to present to the subcommittee this morning. I am the I&C Supervisor with NuScale Power.

I have been with NuScale three and a half years. I am responsible for the design and licensing of the instrumentation and control systems for the NuScale plant design. Prior to that, I was with B&W on the mPower project in a very similar role, and then prior to that, was with GE Energy. I performed detailed design of the non-safety plant control system for the ESBWR and other global power generation projects that GE had at the time.

Started my career at Exelon Corporation as a Reactor Engineer at the Byron Nuclear Power Station, and transitioned into roles in real-time process systems and plant operations. And I received my degree in Nuclear Engineering from the University of Michigan, so please excuse my counterpart who is an

OSU grad.

MR. INFANGER: Yeah. Ohio State. Sorry.

MR. ARNHOLT: You might have to separate us two. With me today is Rufino Ayala. He is an I&C engineer on our team. Do you want to quickly introduce yourself?

MR. AYALA: Good morning. My name is Rufino Ayala. As Brian mentioned, I have been a part of the I&C Engineering Group. I have been supporting the project now for about a little over six years. Prior to NuScale, I was with Bechtel working at Watts Bar Unit 2 mainly focused on the refurbishment of their safety-related protection systems there. Prior to that, I graduated from the University of Houston. Got my Bachelor's in Science and Electrical Engineering.

MR. ARNHOLT: Okay, the purpose of today, we are going to provide an overview of the instrumentation and control design as it is presented in the Chapter 7 of the NuScale Final Safety Analysis Report. I have an abbreviation slide here for you. We use a lot of abbreviations and acronyms throughout the presentation, so this is a good point of reference for you to refer back to if you do not recognize any of the abbreviations we use.

The NuScale Design Certification for Chapter 7 follows the structure of the design-specific review standard for the NuScale design. I think the subcommittee has seen that over the years. So this is the first application for a Chapter 7 submittals that follows this new DSRS framework. So we structured the presentation to kind of correspond with the DSRS framework.

So there is Section 7.0 that goes into the architecture and system overview. Section 7.1 goes through the fundamental design principals. And then Section 7.2, discussing system features as they relate to conformance to IEEE 603 and IEEE 7-4.3.2.

I am going to start off with the Section 7.0, and we are going to start at a high level and kind of work down into the details. So the I&C system design basis, we leverage the NuScale passive safety and passive safety design and the simplicity of the design in our safety-related I&C platform. It is a digital I&C system based on field programmable data arrays.

We get a couple of benefits from the use of FPDAs. We leverage their capability for inherent diversity to address common-cause failure issues with digital I&C systems, and also, we leverage the

simplicity that an FPDA-based system affords you in the design. And that follows along with the theme of the NuScale plant design and its simplicity.

So what that means is the safety function is the removal of power. It is as simple as that. There is no safety-related electrical power either AC or DC that is required for the I&C systems to perform their required safety functions. So we de-energize electricity to field components and valves and things of that nature.

They will fail to their as-designed or safe position. We remove power to reactor trip breakers to shut down the reactor. We have no safety-related components that require active control. And so again, just the removal of power is the safety function in its simplest form.

The figure on the left is not all-encompassed, but to give you a visual depiction of the systems that are related to the safety-related I&C system protective functions.

So this slide, and I see folks have the detailed figure that came out of the FSAR figure 7.0-1. I can talk to that if there are questions, but this is more of a high-level picture overview of the entire I&C architecture. It is not to convey the

building blocks that comprise the I&C systems.

So starting at the lower left, we have our safety-related module protection system, and there are -- there is one independent module protection system for each NuScale power module. We do not share safety-related functions between any of the modules. They are completely independent.

On the lower right, we have our non-safety-related module control system that performs non-safety-related balance of plant power generation control functions, asset protection, things of that nature.

Moving up to the plant level, we have a plant-protection system that performs common plant-protective functions. For example, control room habitability, system actuation, radiation monitoring are two of the primary functions that that performs at the common plant level.

And then we have a non-safety-related plant control system that performs common plant functions such as site service water cooling control, electrical distribution control for common plant systems, things of that nature.

MEMBER BROWN: What that means, for those who have not been steeped in this, is the plant

control system, if you have got 12 modules, it applies to all -- those systems, it applies to all 12 modules.

MR. ARNHOLT: Yes, that is correct.

MEMBER BROWN: Okay. And the plant protection system, if I read my notes, that is also applicable to all 12 modules? Those units?

MR. ARNHOLT: That is right.

MEMBER BROWN: Those functions apply to all, but it is common across all of them?

MR. ARNHOLT: That is correct. The next slide I will show, the next two slides, I will show a little bit more in detail what these systems do and their classifications and give a little bit more detailed discussion on that.

MEMBER BROWN: Okay. So the only two that are plant-specific are the module protection system and the module control system -- yeah, the module control system?

MR. ARNHOLT: That is correct. But we have some other systems, like our Incore instrumentation system that provides our Incore instrumentation assemblies that are module-specific, but I have got a little bit more detail in the next few slides.

MEMBER BROWN: Okay.

MR. ARNHOLT: The box on the upper-left shows the interaction with the operator that is supplied in the main control room. Where the operator spends the majority of his time is at either a plant control system or a module control system workstation.

And that is where he performs his normal control systems startup, shutdown, refueling, maintenance activities are performed from those workstations. We do provide both module-specific and plant-level safety display and indication systems, and that provides the operator with long-term post-accident monitoring indication for those types of plant conditions.

CHAIRMAN CORRADINI: So, I am just listening. This is -- every time I listen to I&C, I re-learn it, and then I forget it. Remind me one more time what is the difference between the plant control system and the module control system?

MR. ARNHOLT: The plant control system controls and interfaces with systems that are common all 12 modules.

CHAIRMAN CORRADINI: Okay, fine. Thank you.

MR. ARNHOLT: Like a site cooling water system is a common plant system.

CHAIRMAN CORRADINI: Okay, thank you.

MR. ARNHOLT: And module control system would be turbine generator control.

CHAIRMAN CORRADINI: Okay. Thank you.

MEMBER BROWN: And the plant protection system is the protection function for those common -- separate from the plant control system itself?

MR. ARNHOLT: Yes, that is correct. The plant protection system, if you will bear with me just a minute.

MEMBER BROWN: Have at it.

MR. ARNHOLT: I will talk to a little bit more detail in the next slide or two. But I did miss one. We also show that we have a remote shutdown area. And I will make a few remarks about the comment before the meeting. So the remote shutdown system is provided as an alternate location for the operators to monitor the plant during shutdown conditions in events where they would need to evacuate the main control room.

So a typical scenario where the operators would need to evacuate the main control room, they would perform three things before they evacuate. They would manually trip all 12 reactors, they would manually initiate containment isolation for all 12

modules. At that point in time, the reactors are shut down, are being passively cooled by DK heat removal, and they're in safe shutdown.

They would then evacuate the main control room, staff the remove shutdown station, and at that point in time, there are no additional operator actions to perform. It is a monitoring-only mode. And that is, again, leveraging that passively-safe design that we built into the NuScale plant.

So those reactors, all 12 modules can stay in safe shutdown for an indefinite period of time without any operator action. So that is the scenario. And there is some language in Chapter 7 that suggests that -- and I need to back up. There are controls available.

We have a complement of module control system and plant control system workstations that provide the operator the capability for non-safety control should he or she need that. But it is not required nor necessary.

MEMBER SUNSERI: By indefinite period of time, you mean however long the water in the pool lasts?

MR. ARNHOLT: Exactly. That is correct. So the important terms are safe shutdown and passive

cooling, and the modules can sit like that in the reactor pool indefinitely.

MEMBER BLEY: And for your design, the words safe shutdown have no temperature connotation?

MR. ARNHOLT: We have a defined tech spec mode of safe shutdown that is less than -- reactor coolant system temperature less than 420 degrees.

MEMBER BLEY: Okay. So the minute the shut them down, you are not there yet, so it takes a little while.

MR. ARNHOLT: Right. So you have mode one power operations. Mode two is what we call hot shutdown, and that is where a reactor coolant system temperature is above 420 degrees Fahrenheit. And then they passively cool and transition to safe shutdown where RCS temperature is less than 420 degrees Fahrenheit.

MEMBER BLEY: Okay. And that takes how long, roughly?

MR. ARNHOLT: I do not want to misquote numbers as far as timelines. I would imagine there are figures maybe in Chapter 15.

CHAIRMAN CORRADINI: We could take it up later if that is desired.

MEMBER BLEY: Hour is not a long time.

CHAIRMAN CORRADINI: Because I remember in our previous meeting, that was given to us. I just do not remember what it is, either.

MEMBER BLEY: Yeah, I do not either. It was just that Brian kind of said. They will shut down all of it and then they will leave, and it will be on safe shutdown. But not quite yet.

MR. ARNHOLT: Yeah.

MEMBER BLEY: It's headed that way.

MR. ARNHOLT: Yeah. So what they do is they -- but there are no additional actions to take. But we do provide the capability of isolating, but we do have hardwired switches in our main control room for these manual actuation functions. So similar to existing plant designs.

We provide the capability to electrically isolate those switches with a series of switches in the remote shutdown. That mitigates potential spurious actuations due to fire concerns in the main control room. But we do provide that capability in the remote shutdown station.

MEMBER BLEY: I have a question about indications. An early question.

MR. ARNHOLT: Sure.

MEMBER BLEY: You will get to this later.

We were out there to visit four or five years ago. I do not remember how long ago.

CHAIRMAN CORRADINI: Sounds right.

MEMBER BLEY: And watched a lot of exercises in the simulator, and at that time, we looked at lot at the displays, and I personally found the approaches that had been taken and tested with a bunch of operators to be fairly convincing on how you could diagnose things from the large panel.

And I think I have gotten hints that that has changed over time. Is that set in concrete at this point in time? The kind of displays for all 12 modules that show up in the main control room? And are you going to talk about that?

MR. ARNHOLT: I will not talk about it in detail. I am happy to answer questions. The displays that we have for our module control system, plant control systems where the operator spends most of their time are based on our human system interface style guide that has been submitted for review.

And then the design of our safety display and information system regarding post-accident monitoring. So we have defined, and it is available in Chapter 7, what variables the operators will monitor for post-accident monitoring conditions. So

that is fixed as part of the design.

MEMBER BLEY: There were a number of color-coding schemes and transitions as plants moved -- as modules moved through toward safe shutdown.

MR. ARNHOLT: Those are --

MEMBER BLEY: Are those fixed, or are those not fixed in the design?

MR. ARNHOLT: I think right now we have concepts that are described in our human system interface guide through now we have just completed our integrated system validation of those concepts, and what changes result from that, I do not know the specifics of that.

MEMBER BLEY: We will get to that either in the human engineering or in the conduct of operations?

MR. ARNHOLT: And that would be, yeah, a topic that certainly would be best to discuss in a Chapter 18 discussion.

MEMBER BLEY: That is fine.

MR. ARNHOLT: So just a couple of concluding remarks. So there is some language in Chapter 7 that might lead the reader to conclude that there are controls that are necessary, and that is not the case, and I want to make that clear to the

committee. There are no controls necessary for the operator to manipulate at the remote shutdown station, because the modules are in passive cooling and remain and stay in a safe shutdown condition.

Through some internal reviews in the past couple of weeks, we identified some discrepancies in Chapter 5 related to the design of the DK heat removal system. We have identified those as part of our corrective action program, and we are going to make those necessary changes.

MEMBER BLEY: There is nothing there that is necessary if everything was done right before you left the control room.

MR. ARNHOLT: Exactly.

MEMBER BLEY: IF things somehow were not exactly done right and you cannot get back in the main control room, do you have the capability to carry out those three basic actions you described from the remote shutdown system?

MR. ARNHOLT: Not from the remote shutdown system, but using available plan operating procedures, you can make in-plant evolutions to manually --

MEMBER BLEY: --- specific breakers, that sort of thing, okay.

MR. ARNHOLT: Similar to existing plants

where if the reactors did not trip from the main control room, you would dispatch a local operator to open -- try to manually open the reactor trip breakers locally.

MEMBER BLEY: Not after similarity, after what you got.

MR. ARNHOLT: Right. All right, moving on.

MEMBER BROWN: Yeah, go backwards. The box labeled manually-enabled hardwired signal for each, what does that apply to? It is just a box hanging in there between all the other stuff. Lower right-hand corner.

MR. ARNHOLT: We do have the capability -- I will talk about this in more detail, but I can address it now. We do have the ability to manually control, take manual control of safety-related components from our non-safety-related module control system. So to back up a little bit.

MEMBER BROWN: This is enable non-safety-related, enable -- disable, whatever that --

MR. ARNHOLT: It is enable non-safety control switch. It is a hardwired switch. Acts almost like a permissive or an interlock.

MEMBER BROWN: You are going to talk about

that later, are you not?

MR. ARNHOLT: I will talk a little bit about that later.

MEMBER BROWN: Okay. While you are on this picture, just one more question. And you will have to correct me if I am wrong, because I am referring back to the HIPS subcommittee meeting. When we talked about these little boxes, circles called iso, which are isolated communications, one-way communications, we did not have the rest of this picture on there.

Those were described -- this is where you may need to correct me -- as communication devices where the receive and or, depending on which end you are on, they are fiber optic. They are serial data links. But they consist of gateway-style, I guess I would call it, to make it receive only. You would clip -- you do not even connect the transmit fabric. Is that -- am I correct?

MR. ARNHOLT: You are exactly correct.

MEMBER BROWN: Okay. Still on the right page here. When we get over to the module control system and the plant control system connections to the plant network, you show those as the same little iso type things. However, on your major diagram, even

though it is not talked about in the written word of Chapter 7, those are referred to as unidirectional data diodes. That is different.

If you go look at all the literature I have ever been able to find, those are different from the bidirectional -- the gateway style unidirectional. In other words, they are hardware-based, and that is -- although it does not say hardware anywhere in the text, either. It just says data diode.

And I am just trying to calibrate myself in terms of the difference between the two. Is my statement correct? The ones from the module control system and PCS down to the plant network are data diodes and they are hardware-based?

MR. ARNHOLT: So I can just point out there are two parts to this. There is communication. If we take the module protection system as an example, there is communication isolation that is performed by a monitoring and indicating bus communication module that was described in the HIPS Topical Report. That isolates communication one way from the module protection system to the module control system. Once you get into -- so that is isolated communication --

MEMBER BROWN: That is the little iso on the MPS blocks?

MR. ARNHOLT: That is what is shown on this box.

MEMBER BROWN: And that is a gateway? That is a --

MR. ARNHOLT: That is through a communication module.

MEMBER BROWN: I understand that, but it has got to have an outflow. And is the transmitting, is that literally one of the fabrics that transmit, in that case that receives or cutoff?

MR. ARNHOLT: Yes.

MEMBER BROWN: That is different than I am talking about. I understand that. We went through that in terms of the MIBs.

MR. ARNHOLT: I will talk to the second one that you are referring to. So once you are at the level of the module control system

MEMBER BROWN: Or the PCS.

MR. ARNHOLT: Or the PCS, we show on our overview, our protection overview, architectural overview, a unidirectional data diode. That is for communication from the MCS up to a plant-level --

MEMBER BROWN: And I understand that.

MR. ARNHOLT: -- and things of that nature.

MEMBER BROWN: I got that.

MR. ARNHOLT: Two separate devices, two separate types of --

MEMBER BROWN: And I am trying to articulate the difference between the gateway style and the data diode. All the literature I have read relative to remote access, preventing it, is air gap with a data diode if you really want the most secure. And that is typically a hardware base, yet there is nothing in the pictures -- there is nothing in the words. It just says it is a unidirectional communication device off to the plant network.

MEMBER BLEY: Which could be a software control.

MEMBER BROWN: It could be a software. Yeah, it could. And that is my real question.

MEMBER BLEY: That is his real question.

MR. ARNHOLT: We will specify that in our application, if it is digital or hardware or software based. We monitor the attributes of how that device works.

MEMBER BROWN: Well, we will be having some other discussions on that issue. Every other new plant that we have looked at has incorporated those remote access items in being hardware based, not --

with no software control at all.

MEMBER BLEY: Brian, I did not quite understand what you said. You said at some point, that will be specified? In what kind of document?

MR. ARNHOLT: When you get into like a detailed design, equipment requirement specification for that device. What we have laid out in the application are the design attributes that those devices have to be designed to.

MEMBER BLEY: I guess what you are hearing, and there is more than one of us who lean this way, is that is the sort of thing that would be really good to spell out.

MR. ARNHOLT: Now.

MEMBER BLEY: Now, and not wait to see what somebody puts in the detailed design document that is not going through the kind of review at a higher level that the design is going through.

MEMBER BROWN: The concern here is to not be sure that no communications off to the plant network are software configurable and have no software associated with them.

MR. ARNHOLT: Certainly take that away.

MEMBER BROWN: Be a straight hardware based data diode. So I mean, the simplest of all of

the gateways is like an RS-232 where you click one or the other.

MR. ARNHOLT: You have a transmit only connection.

MEMBER BROWN: Exactly.

MR. ARNHOLT: All right.

MEMBER BROWN: You will probably hear more on that as we talk today, if you had not figured that out by now.

MR. ARNHOLT: All right. Well, moving on. So here, just the next couple of slides, I have divided these next two slides into more detail on the module-specific systems. And there was a question about are there other module-specific systems. And we have got the MPS listed here, and that is a digital FPDA-based system that I talked about.

We have a Neutron Monitoring System. There are three subsystems related to Neutron Monitoring System. There is the safety-related Neutron Monitoring X4 System that does your X4 detecting for nuclear power monitoring source, intermediate and power range, and that provides signals to the MPS to perform protective functions based on a logic determination of those inputs.

And then we have our module control

system, and that is a digital distributed control system, and I will talk to that in just a second of what that is. And then we have our Incore instrumentation system which provides Incore neutron flux detectors, Incore inlet and Incore exit thermocouples for post-accident monitoring conditions.

Just a couple of notes on this slide. We have mentioned the safety classifications. So the module protection system and the NMS excore system are A1 safety classification in this classification, A1. The remaining systems are B2. There are no other A2 or B1 systems at the module-specific level.

So when I mentioned that the module control system is a distributed control system, there were some questions about what is a distributed control system.

MEMBER BROWN: Also the PCS is a distributed control system.

MR. ARNHOLT: Right.

MEMBER BROWN: So they are both -- I mean, you do not list that in here.

MR. ARNHOLT: It is on the next slide.

MEMBER BROWN: Okay. I have not gotten there yet.

MR. ARNHOLT: But this discussion will

apply to both. But a distributed control system is one where you can functionally allocate and geographically distribute control processors and input output equipment throughout your plant. And you can distribute control functions based on the particular plant functions that that system is designed to control.

So, for example, if I have a, for a NuScale power plant, I might have a control processor and input output set for controlling the main turbine, and that would be distributed either locally or geographically separate from other parts of the system. And then I might have a control processor at input output set to control my -- control that drive system. And those are where we physically allocate and physically separate control functions to different control processors.

There are many reasons why you do that, and on the NuScale design, we take that and leverage it from a common cause failure standpoint. We perform a segmentation. So we did an analysis, and I have got a slide later on, but I will talk to it now.

MEMBER BROWN: Let me back that up a little bit. And I do not know -- I may have the wrong perceptions. So you can correct me. If I look at the

existing plans today, and I look what were the two examples you used? You used what, the turbine generator --

MR. ARNHOLT: Turbine generator and control rod drive system.

MEMBER BROWN: Control rod drives. IF you go out and look at them, there is a set of equipment dedicated to that with some switches somewhere else that can make it do this, turn on, turn off, go up and down, whatever you have to do. In the distributed control system, you do not have those. They are all lumped in to a central processing unit where you -- when you talk about segmentation, you say there is a bunch of memory allocated to these four process functions.

There is another memory segment, memory set of -- memory units that are identified through this one, so on and so forth. And you identified, I do not know, four or five. You identified the major ones in the Chapter 7. There were three or four of them, I think, you identified.

And if the way I read the document, is that now all of the -- all the controls are lumped into a giant package of software that has its specific software identifier segmented into little parts of the

memory, and there is no -- there is not a separate voltage regulator other than the final thing which runs the field current up and down or whatever you want to call it. Is my perception correct or incorrect?

MR. ARNHOLT: Forgive me if I say it is incorrect.

MEMBER BROWN: That is fine. That is why I asked.

MR. ARNHOLT: Yeah, you had mentioned that it is lumped into a single, I will call it a control processing unit, and that is not --

MEMBER BROWN: That is the way it reads.

MR. ARNHOLT: Okay.

MEMBER BLEY: But go ahead.

MR. ARNHOLT: When we mention segmentation, we use physically separate control processors. And think of a control processor as a computer for lack of -- for simplicity's sake. And you allocate and only program into that control processing unit the software, the memory, the inputs and outputs to control that particular control function.

So in this case, let us pick control rod drive system. So the control processing unit for

control rod drive system only controls the control rod drive system. Only has input and output and memory allocated to it for the control rod drive system.

When we move to the designing the controls for the turbine generator set, you have a physically separate and independent control processing unit with its own set of input output, its own set of memory, and its own set of software that resides within the control -- physically separate control processor for the turbine generator set. It is just an example using those two systems.

MEMBER BROWN: So if I went out and I looked, I would see two boxes?

MR. ARNHOLT: You could.

MEMBER BROWN: Or boards or whatever.

MR. ARNHOLT: You could. Depending on how it was physically laid out.

MEMBER BROWN: It might be a big box, but they would be physically and electrically separated or whatever.

MR. ARNHOLT: In a distributed control system, the technology is there. When we bring that information into a network, into a control network, and we present that to an operator on a human system interface network where they are networked together

using conventional networking technologies. But at the control and input output levels, they are on physically separate control processors and physically separate input output modules.

MEMBER BROWN: Okay, so there is, just as an example, use the TG -- use the control rod drives as an example. I have a processor dedicated to the control rod drive actuation function. In other words, it drives a variable power supply of some kind that latches the rods up and down when you demand it.

And the only part, the input to that that says go up or go down, or unlatch and drop, whatever that is, that command exists in another processor somewhere in this network where the operators control multiple of these boxes, even though they may be in the same cabinet. I will put that aside. Is that then the way I would perceive this?

MR. ARNHOLT: Right. And those --

MEMBER BROWN: But what segment -- my memory -- I am not a programmer, okay, if that is not obvious. My memory of segmenting is allocating memory to segment, to hunks of stuff you want to do.

MR. ARNHOLT: And that is the advantage that the distributed control system gives you. You segment not only the software and the memory, but you

also segment --

MEMBER BROWN: Hold it. You said you have got it in another box.

MR. ARNHOLT: And you also segment the hardware. Physically different segments in the hardware. So let us use the term --

MEMBER BROWN: Okay, let me back up again. These extra boxes have all the memory in them. They are -- the memory box, the memory for the control rod drive mechanism does not have any other functionality or processes associated with it stored in that memory.

MR. ARNHOLT: For functions beyond its sole purpose of --

MEMBER BROWN: Other than the control rod drive mechanisms. It is physically addressably different --

MR. ARNHOLT: Yes, it is.

MEMBER BROWN: -- from every one of the rest of them, okay.

MR. ARNHOLT: That is right.

MEMBER BROWN: And I guess my view of segmentation was multiple of -- software being allocated to memory segments where you might have four -- it is like partitioning in a way.

MR. ARNHOLT: That is right.

MEMBER BROWN: Where it is all lumped in to one big thing, but when you call it, you do not have to go rooting around through all the other memory to actuate a particular function. That is the way to go read all this stuff. That is what -- that is long term memory ago.

MR. ARNHOLT: And this is typical engineering practice in process control industries, and you can --

MEMBER BROWN: Which part is typical here? What I just said, or what you said earlier?

MR. ARNHOLT: My view, where you segment both your -- and you separate both your software and your hardware into physically separate cabinets, control processors, input output cabinets, things of that nature.

MEMBER BROWN: Okay. Now, in Chapter 7, you identify in these major segments, there were like, three or four process functions that you had identified in a segment.

MR. ARNHOLT: Correct.

MEMBER BROWN: That again seems to go counter to the -- like the control rod drive mechanisms. There was a control -- the CDCS system. There was a containment -- I do not know whether it

was CM something, I do not know, I have forgotten the names of them. Containment isolation and --

MR. ARNHOLT: Maybe a containment evacuation system?

MEMBER BROWN: Maybe it is flooding or what have you. The flooding was separate. That was something else. But those were all in one segment. Does that mean their software is part of the control rod drive mechanism control software?

MR. ARNHOLT: Yes. And --

MEMBER BROWN: So I am right then? That is -- so I have got four functions of processes stuffed into one computer where you call upon any one of them whereas their memory may be segmented within that processor, but you have got four processes and one process controller?

MR. ARNHOLT: So I can give you a practical example of how we apply that to our design. And we performed what we call the segmentation analysis, and it is described in the FSAR. And we looked at all the major module controls system functions that have the ability to impact reactivity, coolant inventory, pressure. I have got a slide on this a little bit later, but I will talk to it now.

And we evaluated those from a postulated

common cause failure scenario. Maybe you lose a power supply. Maybe you have a network fault. Whatever the postulated failure is. And we evaluated the results of that failure and whether or not it was bounded by our Chapter 15 safety analysis. And if it was, then we could, with reasonable assurance, place those control function in the same control segment and postulate an entire failure in that segment and still be bounded by our Chapter 15 plant safety analysis.

So there is one example where we actually had to make a design change as a result of this analysis. And the two functions were the CV, the chemical volume and control system makeup, and chemical volume of control system letdown functions.

Originally, we had those on the same control segment because they were associated with the CVCS system. But we looked at that, and we had -- if we postulated a failure, we could also, we could impact coolant inventory adversely, and at the same time, core reactivity. And that was not bounded by our Chapter 15 safety analysis.

So we made a design change early in the process and separated those two segments. So now you can postulate a failure of the segment, the controls, the makeup to the reactor through the CVCS separately

from a failure of the letdown function of the CVCS.

So that is an example where the analysis actually resulted in a particular segmentation of two functions. And that was an example that we did describe in the Chapter 7. I do not know if you remember reviewing that.

MEMBER BROWN: I read it. I will not say that I understood you.

MR. ARNHOLT: So now those are on two separate segments, physically and software separated. So if you have a power supply failure, you would only postulate a power supply failure maybe on a CVCS letdown cycle and evaluate the potential effects of how that system would fail separately from a similar type of failure on the CVCS makeup segment.

And that is where the segmentation affords you the advantages to ensure that postulated failures of the non-safety systems conform to and are bounded by the analysis for the plant, safety analysis for the plant.

MEMBER BROWN: Okay. But it still boils down to where you have four process functions in one unit. If that processor just fails totally, whatever it is, you have lost four functions.

MR. ARNHOLT: That is correct.

MEMBER BROWN: And you have evaluated -- you made the argument -- and I am not plant savvy enough to know whether it is okay or not.

MR. ARNHOLT: Well, we did do --

MEMBER BROWN: Because they are all non-safety-related, the argument is, we do not need any of those, and if they all fail, we do not care.

MR. ARNHOLT: Right. And it is bounded by the plant safety analysis. Now, there is operational considerations, obviously, but from a pure effect on the plant safety analysis, we have evaluated that and determined that the failures that would result from that scenario are bounded by a Chapter 15 safety analysis.

MEMBER BROWN: Okay. Now back up to the previous slide again.

MEMBER SUNSERI: While you are doing that, let me interject here. Dr. Corradini had to step away for an obligation with one of the commissioners. He asked me to preside over the meeting until he returns, and heedfully that will be soon. So go ahead.

MEMBER BROWN: All right, I guess when you talk about -- you have got two distributor control systems. This is -- I am segueing back to the isolation from the plant network, which is the sole

external nexus to the outside world.

That is kind of a critical location, and why the emphasis I made earlier on the hardware nature of the data diodes, because once you get into either one of these, through its isolated connection, if somebody hacked it, you now have a bidirectional connection between the PCS and the MCS which would allow whoever got in to get into the other and take control of everything.

MR. ARNHOLT: On your non-safety control systems.

MEMBER BROWN: Yeah, all the non-safety control systems, which is whether they are non-safety or safety is -- it is really not a good idea to take -- have those get compromised. So that, it is a single point of vulnerability, and it applies to all your plant control, which applies to all the -- what, ten, 12, whatever the number of modules, NuScale power modules are, as well as the individual modules.

So that is why I was struggling to make sure I understood what you meant by segmenting and how they are all kind of interconnected and what is important about these two inputs from the external world and how important that isolation is to be non-software-based under any circumstances, and why the

emphasis we have placed on other designs to make that a hardware -- specifically and explicitly hardware based in their DCDs. So anyway, I think I have some -- are there any other questions on the distributed control system?

MR. HECHT: Yes, I have one.

MEMBER BROWN: Go ahead.

MR. HECHT: I thought I was clear until --

MEMBER BROWN: This is Myron. Give us your name, Myron. Oh, you got his name tag, I am sorry. Go ahead.

MR. HECHT: So before I understood that segment was composed of processors, but as a result of this discussion, I am not sure if segments are distributed within processors or there is a composition relationship where processors belong to segments.

MEMBER BLEY: What is what happened to me halfway through this discussion. I thought I followed it, and then I got lost.

MR. ARNHOLT: Processors are assigned to a segment. So you could have a segment, and again, it gets into the detailed design of your plant control system, but the processors within a segment are independent from the processors within another

segment.

MR. HECHT: Okay, so the composition is the distributed control system segments, the segments consist of processors.

MR. ARNHOLT: Correct.

MR. HECHT: Okay, thank you.

MEMBER BROWN: And I think you said in your earlier discussion within that processor, if you have got four processors or five, whatever they are, is there -- is their software segmented within those? Did you say that earlier? Or is it just jumbled around?

MR. ARNHOLT: Depends on how you architect the actual software.

MEMBER BROWN: I am not trying to design. I am just trying to understand.

MR. ARNHOLT: Right.

MEMBER BROWN: In terms of memory allocation and stuff. You have not specified to that. You are fundamentally segmenting by processors and processes within a processor that compacts the segment.

MR. ARNHOLT: I will give you a simple, everyday example. Everyone drives a car. You have your engine control module, and you think of that as

a segment, and then you have your infotainment module that handles your radio.

MEMBER BROWN: Not me.

MR. ARNHOLT: That is a separate segment. So if your infotainment module fails, or otherwise becomes inoperable, you still have your engine control module, and you can continue to drive down the road. That is a very simple everyday example of segmentation.

MEMBER BLEY: And there are some real good examples of people who have hacked through the entertainment module into the other modules.

MEMBER BROWN: Into the other module, yeah. Yeah. But I am glad I still have a distributor and a carburetor. They are so old.

MR. ARNHOLT: That is a simple, practical example of a segmentation.

MR. HECHT: To continue to onto Charlie's point, within an individual processor, I assume you have a real-time operating system?

MR. ARNHOLT: Typically, distributed, most of your modern commercially available distributor control systems are based on real-time operating systems.

MR. HECHT: But you do not specify that in

the Chapter 7?

MR. ARNHOLT: Or the MCS or the PCS, we did not get into that.

MR. HECHT: Okay. Well, I would assume, and I guess maybe does this turn into some kind of ASAI? But I would assume that these distributed operating systems keep all their tasks, each task related to some control function. Separate memory spaces. And that they are given their own time slice and given their own resource allocation after which they get done executing that they -- that it moves on and they are turned off until the --

MR. ARNHOLT: So I can answer that with a little bit of foreshadowing into the content that I have in section 7.1. We have our fundamental design principles. And largely, we discussed in our application how we applied the fundamental design principles to the design of the safety-related systems.

But we also did carry those design principles over to the non-safety systems. And to your point, we have a predictability and repeatability fundamental design principal that was parlayed into and put forth and carried into the design of your --

MR. HECHT: Well, that is a principal. I

am talking about the implementation now, and just to clarify to Charlie's point, that I would -- okay. It would seem to me that most conventional designs keep tasks that are associated with control functions and separate memory spaces, and if that's not clear in the application at this point, should it not be?

MR. ARNHOLT: It is not in the application, and it was not part of the framework of the DSRS when we put the application together for the non-safety systems. Those implementing details are -- just were not part of the application for the non-safety system.

MEMBER BROWN: If I am not mistaken, the point of this, I think, what I was hanging up on that was one of my -- thank you for leaping into this -- when you turn a switch and tell something to stop, start, increase, or decrease, you would like it to happen before you blink your eye.

MR. ARNHOLT: Exactly.

MEMBER BROWN: So that is a real-time operation. If it is like my computer here, and I ask it to do something, and I said, nothing is happening, takes five, ten, 15 seconds before something starts, that is not a good idea if I am not mistaken. So I guess how -- I would -- I am trying to connect the

repeatable and predictable to not being a real-time process. If you got repeatability and predictability and you applied that design principle to the MCS and PCS.

MR. ARNHOLT: I can offer this. I am not aware of a commercially-available distributed control system that does not function in a repeatable and predictable manner with a highly designed real-time operating system.

MEMBER BROWN: But if there was nothing, there was nothing in the Chapter 7 that talked about response time of the module control system and plant control system --

MR. ARNHOLT: That level of detail --

MEMBER BROWN: -- so all you do is say it needs to be repeatable and predictable, but it could be ten seconds or a minute, and that is repeatable and predictable.

MR. ARNHOLT: But we also do provide, you know, for balance plan and asset protection. So you know, you have a highly -- high-cost asset such as a turbine generator set. Those are design principles that you would want to apply to how you control and operate your turbine generator set from an asset protection standpoint.

MEMBER BROWN: Take an example. Is the overspeed protection system for the turbine generator set embedded in the module control system, or in the boxes mounted that come with the turbine generator set?

MR. ARNHOLT: Most likely that would be --

MEMBER BROWN: I went and looked at Chapter 8, and I went and looked at -- I think it was something else. I could not find it.

MR. ARNHOLT: The turbine generator designers and suppers that I am familiar with all have their own package control system that comes along with the turbine generator set itself.

MEMBER BROWN: So your distributed control system, through your process and your segmenting, will tell it, provides the commands to do the other things, and the inherent protection features are built into the unit that comes with it.

MR. ARNHOLT: And I can tell you, based on my experience, those are designed in a highly real-time system. For example, you have a fixed cycle at which a control processor works through all its functions. It might allocate ten percent to read all the inputs, 40 percent to perform all the logic, and then 50 percent to process all the outputs.

And that is a fixed sequence of events every single frame cycle of that control processor function. That is the typical way that most real-time distributed control systems function. But that level of detail was not in -- we did not put that into Chapter 7 for the non-safety systems.

MEMBER BROWN: Do you have anything else, Dennis?

MEMBER SUNSERI: I guess maybe I have a question, Charlie.

MEMBER BROWN: Have at it.

MEMBER SUNSERI: For Charlie and Myron. I guess it would help me to understand the context of this conversation of what is the so what. Are you expressing a concern or seeking to understand?

MEMBER BROWN: Just trying to understand, okay? This is a -- I mean, it is a -- they have been defined as non-safety systems, so --

MEMBER BLEY: And understanding implies you can think of the insults that might cause a problem.

MEMBER BROWN: Exactly. And that is --

MEMBER BLEY: That is the reason for digging into it.

MEMBER BROWN: I dug into this because I

wanted to understand the relationship between the possible external access, the ability to get into them, how interwoven are these interior to the -- you know, within the designs of these two systems.

MEMBER SUNSERI: I was not challenging. I was just trying to seek to understand myself.

MEMBER BROWN: No, this was strictly an understanding to make sure we understand, because we are not -- we are obviously not trying to design the non-safety systems. I mean, but we -- we do want to make sure that they are not susceptible to causing a problem in some other manner based on the way they are put together or accessed.

MR. ARNHOLT: And the takeaway I would like to leave you with is we have done that analysis and the results of that analysis and how we designed, at least from an architecture level, is reflected in the design that you see here today.

MEMBER BROWN: And now for -- go ahead, Dennis.

MEMBER BLEY: That is kind of comforting. If one drives the non-safety systems into places you do not ever expect them to be, they can create challenges for the safety systems that might be beyond your design capabilities.

MR. ARNHOLT: That is true. And there is --

MEMBER BLEY: So they are not non-safety in that sense. They can drive you into difficult situations.

MR. ARNHOLT: True. And the fact that we call them non-safety does not mean they are not important to the overall operation of the plant. We design them as such, to be highly reliable and work when called upon. And so we did describe, in Chapter 7, there is some language, and we call them preventative and limiting measures.

So there are things that you can do in design space. Segmentation is one. Error checking on your signal inputs, having redundant sensor inputs -- and this is non-safety I am talking about. So there are a whole series of preventative and limiting measures you can do and apply to your design that ensure the reliable operation of these systems.

And then we described some of those in the application, how we apply those. And that ensures that as the operators interface with the system, as the system operates, it operates as designed, in a reliable fashion.

MEMBER BROWN: Okay, let me ask, it does

not show up on this diagram. But on the other diagram.

MR. ARNHOLT: And I do have, in this presentation, if you want, at the very end, I can throw the more difficult --

MEMBER BROWN: Yeah, okay. Go ahead and put it up there. I do not know if anybody can read it. Now you cannot read that. Okay.

MR. ARNHOLT: I am happy to --

MEMBER BROWN: Now I guess my question is, if I look at this and if you will put it back up. No, go on back to the last thing just so if somebody wants to see it, they can.

MEMBER MARCH-LEUBA: Brian, you have the mouse. You can point.

MEMBER BROWN: Here.

MEMBER MARCH-LEUBA: So we can see what you --

MEMBER BROWN: Go up to the box. Go up to the right. Right hand. Now go over a little bit to the -- there are two boxes between the legend and the main control room. Right there.

MR. ARNHOLT: Right here?

MEMBER BROWN: Now down, go down one more. No, the next little box below it. It is labeled

technical support center.

MR. ARNHOLT: Okay. All right.

MEMBER BROWN: Let me see. It is up, up, right there.

MR. ARNHOLT: Right there. Okay.

MEMBER BROWN: That has a line down into plant control system, but yet when I try to define it -- and it has got some words like PCS power operations network. From reading the chapter -- and I could not figure it out -- it implied to me that the technical support center had some ability to control or operate the plant control system as opposed to just a monitoring function. I could not define it.

MR. ARNHOLT: No, that is not correct. The PCS workstations and the technical support center are for monitoring the plant level the operation of the plant. So each module control system's information --

MEMBER BROWN: I understand the workstation. I am talking about the other little box to the right where it says power operations, HSI network.

MR. ARNHOLT: Right. And that -- we have a network where all the human system interfaces connect to, and that is where that workstation is connected to. So you have an IO network, the way this

drawing is set up. You have an IO network that interfaces with the control network and so those are those IO modules that I mentioned.

The control processor's function on the control network level. And then you aggregate that up to you HSI operations network. And that is the network where the human system interfaces reside for the operator interfaces. And that is where this display would interface to.

MEMBER BROWN: Without any notes, I guess I would have interpreted that line to be a bidirectional line although based on what you just said, it ought to be a unidirectional. I do not care whether it is a gateway or whatever, but --

MR. ARNHOLT: It did not provide that level of detail in this drawing of that, but when you configure your -- and again, this is getting into the design details of how you --

MEMBER BROWN: I am not interested in getting -- I just want to make sure that people from the TSC cannot go initiate some action from the technical server --

MR. ARNHOLT: But there are user roles that you would assign for somebody to be able to access that. And these are on cyber security

principles of how you design systems that you have operator roles, engineer roles, technician roles.

MEMBER BROWN: But you are talking about they have to ask for information.

MR. ARNHOLT: Right.

MEMBER BROWN: From the plant control system.

MR. ARNHOLT: Right. And so it --

MEMBER BROWN: And that is why it is bidirectional.

MR. ARNHOLT: If you log in with a technical support center role, you would not have control capability. You would have monitor only capability, as an example.

MEMBER BROWN: Okay. You can go on back to your other slide now.

MEMBER MARCH-LEUBA: Going back to what -- that line is bidirectional.

MEMBER BROWN: Did you find it?

MEMBER MARCH-LEUBA: The line between the technical support center and the plant control, the PCS, is bidirectional.

MR. ARNHOLT: Yeah, we did not show it as a unidirectional line, but that is a typical --

MEMBER BROWN: Because it did not say

anything, I assumed it was a bidirectional line. Just based on the rest of the approach that you did with the rest of the figure. And why does it have to be bidirectional? I thought if you just sent all the information to technical support center, they do not have to ask for anything. It is always there.

MR. ARNHOLT: Yes. You can. I am sorry, did you have a question?

MEMBER KIRCHNER: I thought the protocol would be the control would remain with the operator, not the technical support center.

MEMBER BROWN: Well, he just said that.

MEMBER KIRCHNER: Okay.

MEMBER BROWN: If I am not mistaken.

MR. ARNHOLT: When I say bidirectional, I mean typical ethernet networking technologies. TCP/IP. We do not use any special --

MEMBER MARCH-LEUBA: What someone is reading there is "hackable."

MEMBER BROWN: Yes.

MR. ARNHOLT: And the way this architecture is laid out is, is we have a defensive architecture with multiple layers of security, so your innermost layers are where your safety systems reside. There is no physical possibility to even remotely

access the systems.

Once you get out, we have the unidirectional data diode that we talked about earlier, and once you get out to that, up to the plant network, you have firewalls. So we do have multiple defensive levels that are going to -- designed within this architecture from a --

MEMBER BROWN: Well, your firewalls from the plant network on out to the world is a bidirectional firewall, so that is useless. I will not phrase it in the way I normally phrase it.

MR. ARNHOLT: And I will add, I have got a slide on this, too, but we -- part of our application, we did not submit a cybersecurity plan. We have a --

MEMBER BROWN: I am not working on cybersecurity. I am only looking at remote access, okay? And that -- it is the data diodes from the plant control or machinery and module control system. If you have a bidirectional firewall, whatever it is that you want to screw around with and try to make it smart all the time, that is your business.

I just want to make sure the penetration of that firewall to the plant network cannot allow any communication at all under any circumstances to the

other two.

MR. ARNHOLT: I certainly understand the line of the questions.

MEMBER BROWN: To SNMCS, because if you are open to total vulnerability to the entire plant whether you call it non-safety or whatever, from that standpoint.

MR. HECHT: This is Myron Hecht again. Can I ask a question about that connection that you were just talking about? You said it was a TCP/IP-type connection. And then, you said that, basically, the role-based log-in would prevent an operator or a person in the TCS, or TSC -- excuse me -- Technical Support Center from controlling the network. Yet, TCP/IP is inherently a bidirectional connection. So, that means that the prevention of control or inhibition of control from the TSC is based on software-based, on the log-in function and the software which basically says a person with a TSC role cannot control the plant. Just to make that clear.

MEMBER BROWN: Yes, that's what I understood.

MR. HECHT: Okay.

MEMBER BROWN: I don't particularly care for that, but that's beyond us right now.

MR. ARNHOLT: Yes, and I would say that the details of those designs were in progress in that detail design phase, but you won't find that level of detail in the application that's currently used right now.

MEMBER BROWN: Okay.

MR. HECHT: But, on a hardware level, it is bidirectional. It's only on the software level that we inhibit the --

MEMBER BROWN: Yes.

MR. ARNHOLT: And there are multiple technologies and engineering attributes you can apply to the design of these systems to make them robust from an interaction and communication standpoint.

MR. HECHT: Thank you.

MEMBER MARCH-LEUBA: Where is the Technical Support Center located physically? Inside the plant or outside the plant?

MR. ARNHOLT: I don't know the answer to that question without having to --

MEMBER BLEY: Usually inside.

MEMBER MARCH-LEUBA: Yes, but if it was located 10 miles away --

MEMBER BROWN: No, no, I agree with Dennis; the ones we've seen before is just a building

outside --

MEMBER MARCH-LEUBA: If it's inside the fence --

MR. BERGMAN: This is Tom Bergman.

It's inside the control building.

MEMBER BROWN: It's inside the control building?

MR. BERGMAN: Yes.

MEMBER BROWN: Okay.

MEMBER MARCH-LEUBA: Then, it doesn't matter.

MEMBER BROWN: Right.

MR. ARNHOLT: And there's other security-level controls. There's, obviously, physical security controls that afford you the most protection, being able to physically secure your digital I&C equipment. I mean, the most bang for your buck is in how you apply physical security.

MEMBER MARCH-LEUBA: If it's a copper line, with TCP/IP, I can go there with a little needle and put any TCP/IP package I want to in there. But, if it's in the secured area, then I cannot do that. I might as well go to the blue PCS --

MEMBER BLEY: They usually have connections to the company network in that area, too.

MEMBER BROWN: Well, in this case, they're not showing that.

MEMBER MARCH-LEUBA: Not in that way.

MEMBER BROWN: It has to go through the plant control system, which it's a unit. That's a good way to do it.

MR. ARNHOLT: Any other remaining questions here?

MEMBER BROWN: Okay. Yes, you can go on back to your other one.

MEMBER BROWN: I'm just trying to make sure we understand what we're looking at.

MR. ARNHOLT: All right. So, I've covered this slide, and I just have a similar slide that discusses the plant-level systems. I've talked about most of these.

I do want to make a couple of points regarding the design of the plant protection system and the safety display and information system. While these are non-safety, non-risk-significant systems, this doesn't mean we don't design them with a high level of design quality. We've applied augmented design requirements for these.

For example, the plant protection system -- and you may have read this in the application -- is

actually based off of the same platform technology as our module protection system. So, we leverage all the design attributes that make that a safe and reliable system and apply that to the plant protection system.

In turn, the plant protection system does perform very important functions. It will actually control inhabitability under a certain set of conditions for protection of the operators in the main control room, and it also has some important radiation-monitoring functions that made us supply these augmented design requirements to it.

MEMBER BLEY: Brian?

MR. ARNHOLT: Yes?

MEMBER BLEY: When you say non-safety-related, I understand. When you say non-risk-significant, is that from the I&C designer's point of view or is that from the point of view of the PRA that tried to find ways to make this system create risk-important scenarios?

MR. ARNHOLT: That risk determination was performed as part of our design reliability assurance program. So, throughout the design of --

MEMBER BLEY: Which isn't connected to the PRA?

MR. ARNHOLT: The PRA informs this, but

the process for performing DRAP evaluations that's described in Chapter 17 explains how we came up with the risk determination for these systems.

MEMBER BLEY: Which chapter?

MR. ARNHOLT: Chapter 17.

MEMBER BLEY: Seventeen.

MR. ARNHOLT: Describes our design reliability assurance program.

MEMBER BLEY: I will look at that. Also, we haven't reviewed the PRA in detail yet. I want to make sure they look for ways that, in fact, this could become a significant --

MR. ARNHOLT: For many years, we had an active -- and still do have an active -- DRAP expert panel, and we apply the principles that we've described in our DRAP program to the design of all the NuScale --

MEMBER BLEY: In Chapter 17.

MR. ARNHOLT: Yes.

MEMBER BLEY: Okay.

MR. ARNHOLT: But that's where the risk determination comes from in this context.

The safety display and information system, it's actually a unique display system. It's non-safety-related, but we do apply FPGA-based technology

to this. And as I mentioned earlier, there are some benefits in simplicity and diversity that we carry through, even into our safety display and information systems, and those are the primary systems that provide the display of post-accident monitoring information to the plant operators.

MEMBER BROWN: My memory tells me that's redundant pluses. There's a safety design. There's a division 1 SDI and a division 2 SDI?

MR. ARNHOLT: There's actually 26 physical displays, two divisions for each module or module-specific information. And then, we have a redundant --

MEMBER BROWN: I've read the number. My point is, all the information from all the plants goes through just -- and it's not shown on your other -- if you go back to figure 8, it's not shown on figure 8. No, it was back earlier. That one. The next one.

MR. ARNHOLT: We don't show that level of detail here, but --

MEMBER BROWN: Yes, you show it, but it's shown on the figure as, and the implication is, the monitors, you've got a lot of those.

MR. ARNHOLT: We do.

MEMBER BROWN: But it only shows a

division 1 and 2. And the way I read that was there is an SDI for each and every NPM.

MR. ARNHOLT: That's correct.

MEMBER BROWN: Is that?

MR. ARNHOLT: Yes.

MEMBER BROWN: Okay. All right. So, they are segregated by NuScale Power Modules?

MR. ARNHOLT: Yes.

MEMBER BROWN: Okay. That was my question. Thank you.

MR. ARNHOLT: I mentioned most of these, and I'd just mention the last set of systems is a radiation-monitoring system. This largely is a series of plant-level radiation monitors throughout the plant, fixed-area radiation monitors. We do have a set of module-specific radiation monitors. So, this kind of crosses both paths, but we apply both analog and digital technology to the design of the system.

So, dropping down into a lower level of detail, looking at the module protection system, the module protection system is the NuScale specific implementation of the highly-integrated protection system platform that the ACRS Subcommittee has previously reviewed. The NRC has approved our Topical Report for that.

An important takeaway of that, we have taken no deviations from what was presented as part of the HIPS platform in the design of the NuScale specific module protection system. So, we conform to the same regulations and take no exceptions to IEEE 603, IEEE 7-4.3.2, or the Staff Requirements Memorandum for SECY-93-087 that explains the diversity attributes of your I&C systems.

The major components of the MPS. We have four separation groups of sensor inputs and electronics and trip determination. You may remember this from the review of the HIPS platform. We have Class 1E DC-to-DC power converters, and that provides isolation between the non-safety related, non-Class 1E DC power system provided by the highly-reliable DC system to the safety-related module protection system. So, that is our isolation point for the power feeds to MPS.

We have reactor trip and pressurizer heater breakers, two divisions of reactor trip and ESFAS divisional voting and outputs to field actuation components. We also provide two divisions of hardwired manual actuation switches. If you recall the NuScale design, there are no required operator actions to perform the safety-related functions. So,

the MPS performs all of its required safety functions automatically without any input from the operator. However, we do provide the capability for backup manual action by the operator if the case would arise.

We have non-safety-related 24-hour timers, and I'll talk to this just shortly in the next slide. These are the 24-hour timers that came out of the Chapter 8 discussion. I'll talk a little bit more about how those function and how the I&C systems respond to that.

And then, we have some non-safety-related maintenance workstations that allow us to perform calibration and maintenance of the module protection system.

Also, part of the MPS, we had the discussion previously about the remote shutdown station. We do provide isolation switches that isolate those hardwired actuation and enable non-safety switches in the main control room. We provide the capability to isolate those electrically from the main control room and the remote shutdown stations. That helps mitigate any potential issues, if there were a fire in the main control or if those switches to become compromised.

MEMBER BLEY: At least somewhere in here

I'm assuming, but I might be wrong, that the manually-enabled hardwired signal for each component that we talked about on the overall architecture drawing is described. Is that one switch that sets up the hardware control for everything or is there a separate switch for each item?

MR. ARNHOLT: It's an excellent question, and I can clarify a little bit. We have system-level manual actuation switches. When I say "system-level," I mean we actuate the reactor trip function. We actuate the containment isolation function at the system level. There is one switch per each division. And we do have a pair of --

MEMBER BLEY: And that's hardwired --

MR. ARNHOLT: Hardwired, copper wires to a hardwired module inside the module protection system.

MEMBER BLEY: Everything else continues to work automatically when you engage that switch?

MR. ARNHOLT: Yes.

MEMBER BLEY: It just adds one more signal?

MR. ARNHOLT: The inputs for these manual switches are hardwired, and they actually input -- and I've got a slide that at the end I can make sure I

point out.

MEMBER BLEY: Okay.

MR. ARNHOLT: But it inputs, actually, downstream of any digital or software-based component.

MEMBER BLEY: Okay.

MR. ARNHOLT: So, it bypasses all the software and actually inputs at the very end to drive the actuation command.

MEMBER BLEY: But does that switch actually send a signal or that just enables? Then, you have another push button or something?

MR. ARNHOLT: What it does is it tells, it interfaces with our actuation part of the logic and tells our equipment interface module to remove power from the --

MEMBER BLEY: Okay. So, it actually creates a function?

MR. ARNHOLT: Exactly.

MEMBER BLEY: Okay.

MEMBER BROWN: So, it's not totally downstream? It still interfaces with the actuation priority logic --

MR. ARNHOLT: Priority logic.

MEMBER BROWN: -- which is in the EI --

MR. ARNHOLT: Exactly.

MEMBER BROWN: -- in the equipment --

MR. ARNHOLT: Equipment interface module.

MEMBER BROWN: -- interface module.

MR. ARNHOLT: But downstream of any digitally-based component.

MEMBER BROWN: All the digital stuff?

MR. ARNHOLT: Right.

MR. HECHT: In an answer to one of the questions that the staff had raised, you made the point that this hardware switch is a non-safety function and that, in the APLs modules, the application priority logic modules, that if there was an indication of an RTS or an ESF condition, that the manual signal would basically be ignored. Is that correct?

MR. ARNHOLT: Yes.

MR. HECHT: So, is that the only condition under which the manual switch is ignored?

MR. ARNHOLT: If there were an active manual or automatic signal, and you attempt to manipulate the switch -- it's a momentary contact switch -- that signal would be ignored. If you had normal conditions and you wanted to take control of safety-related equipment using this switch, and so, say you enabled the switch, and you were in the

process of performing control of safety-related components, if during that time you were to receive a valid automatic or manual actuation signal, that switch input would drop out and the automatic and manual signal would be automatically processed at the highest priority. That's another condition.

And then, if the operator wanted to re-enable control from the non-safety systems, he would have to physically manipulate that switch yet again. So, anytime an automatic or manual signal occurs, the design of the APL completely ignores any input from that switch and you have to work through the sequence of events to re-enable that control again. The keyword is it "takes deliberate operator actuation" to re-enable the capability for that non-safety-related control.

MEMBER BROWN: The APL is all just logic, solid-state --

MR. ARNHOLT: Logic components.

MEMBER BROWN: Transistor logic, whatever you want to call it. In the old days, it was TGL or something like that.

MR. ARNHOLT: For those of the Committee members -- I don't know if you've been to see our prototype in Corvallis, where we have an actual card

of the APL. But I can't show a picture of it in an open --

MEMBER BROWN: I'm just remembering the figure and the discussion from the HIPS thing. And my memory was that it was all just hardwired -- the way we made computers in the 1960s.

MR. ARNHOLT: Exactly. Ironically, quite complicated in design space to do, but we did it.

MEMBER BROWN: I hate to say I remember that.

(Laughter.)

MEMBER SUNSERI: They were made out of wood, weren't they?

(Laughter.)

MEMBER BROWN: And hammers and non-magnetic nails.

One other question on this. You talked about you could actuate back through the module control system. And you haven't gotten to this enable safety switch. Is that another pathway into actuating the module protection system, with the enable safety control switch? It's not listed here as an input.

MR. ARNHOLT: It is, and it's an excellent question. For the operator to be able to take component-level control from the non-safety-related

module control system, we have to enable the non-safety -- you have to have no active protective signal enabled. You have to manipulate this, enable the non-safety switch. And then, the operator has to take control functions from his MCS workstation.

Those outputs are actually via hardwired, non- -- there's no digital communication. They're actually hardwired outputs from the non-safety system into our hardwired module to drive the logic-level commands to control safety-related components. So, that input, yes, that is an isolated input into the MPS, but through a hardwired non-digitally-communicated interface.

MEMBER BROWN: Okay. And somewhere I read that -- and I'm just looking at my notes now; I can't remember if it was in the CSR or the Chapter 7 -- that this enable safety control switch, whatever you call it, is a momentary switch.

MR. ARNHOLT: That's correct.

MEMBER BROWN: Does that mean you have to hold it in place while you do something else?

MR. ARNHOLT: No. It --

MEMBER BROWN: You say you have to enable that and, then, go do something else?

MR. ARNHOLT: You do not have to maintain

it. It's a swaying-return-to-center switch, and it creates a logic-level signal that allows --

MEMBER BROWN: But that locks in?

MR. ARNHOLT: It locks in.

MEMBER BROWN: It locks in the logic-level signal. So, then, you can go operate the control?

MR. ARNHOLT: If you were to get a --

MEMBER BROWN: Okay, I've got the picture now.

MR. ARNHOLT: Okay. Then, that would automatically go away if you got a valid protective signal.

MEMBER BROWN: Yes, I've got it.

MR. ARNHOLT: You've got to re-enable it to restart that scenario.

MEMBER BROWN: Okay. Thank you.

MR. AYALA: One thing I just want to add to that is, so it is two divisions of those switches. Let's say you wanted to do component-level control of a safety-related component. Your division 1 switch, you control on that valve. You would disable the division 1 control. Then, you move on to division 2 and use that switch. So, you would have to -- it's not a single switch capable of allowing you to control two divisions of safety-related components.

MR. ARNHOLT: All right.

MEMBER BROWN: Thank you for the clarification, by the way.

MR. ARNHOLT: All right. There was some discussion during the Chapter 8 ACRS Subcommittee meeting on loss of AC power scenario and the design function of these 24-hour timers that we talked about. I'm going to walk through that here.

To set the stage, you just want to remember your frame of mind is the safety-related I&C systems require no safety-related or Class 1E electrical AC or DC power to perform their safety function. Remember, the removal of power is the safety function.

However, we do want to provide the capability for long-term post-accident monitoring. For that, you do need electrical power. So, what I've shown here is kind of a diagram of the flow of both AC and DC electrical power, and I've got a sequence of events there on the bottom. But, to do that, we take advantage of our highly-reliable DC power system that's, again, non-safety-related. And that's arranged into four power channels, power channels alpha, bravo, charlie, and delta. Power channels alpha and delta have batteries that provide up to 24

hours of power supply to its required loads, and power channels bravo and charlie provide up to 72 hours for long-term post-accident monitoring.

So, in order to ensure power is available for long-term post-accident monitoring, we monitor for and detect a loss of AC power to the input of the EDSS battery chargers. So, on a detection -- you can kind of follow along there at the bottom -- on a detection of a loss of AC power, and we have volted sensors that monitor the AC power input to the batteries, upon a loss of AC power, the module protection system automatically initiates a reactor trip, containment isolation, and decay heat removal actuation. And what that does is that removes non-essential loads related to what's required to be powered for this scenario, and it starts these 24-hour timers. The 24-hour timers, remember, are non-safety-related functions, and their sole purpose is to ensure that we are capable of supplying power to meet our long-term post-accident monitoring requirements.

So, we call this mode an ECCS hold mode. The important part is here we want to reduce the loads on the batteries to just those related to, for the first 24 hours, just related to post-accident monitoring, and we want to continue to maintain power

to the ECCS valves to make sure that they remain closed. We do not inhibit the ability for either an automatic or a manual operator-initiated ECCS actuation. So, there is no way that they can inhibit a valid ECCS actuation demand that one were to call for. They're simply there to keep power supplied to the ECCS valves to prevent an unnecessary or spurious ECCS actuation for the first 24 hours.

We chose 24 hours. It's a reasonable amount of time to make restoration of AC power and also keep power applied to the ECCS valves and ensure they're closed.

At the end of the 24-hour period, if AC power is not restored, we would remove power from the reactor trip system and the engineered safeguards features chassis. And so, that removal of power would, in turn, remove power from the ECCS valves, and they would open on that loss of power.

And then, we would transition to what we call -- and you may have read it in the application -- is a PAM-only mode, post-accident monitoring only mode. So, the only loads powered at that time are those loads related to sensor electronics or sensor loop power and the power to the safety display and indication system. And we would sit there and provide

that power for the 72 hours for long-term monitoring.

MEMBER SKILLMAN: So, the 24-hour hold is intended to enable repowering whatever it is that caused the casualty, so that you could go back to power? The flip side is you prevent going on ECCS, so you don't have to go through an ECCS reset? Is that what you're doing?

MR. ARNHOLT: That's correct.

MEMBER SKILLMAN: I understand. Thank you.

MR. HECHT: To confirm on Gordon's question, the ECCS hold really means ECCS inhibit, right?

MR. ARNHOLT: No.

MR. HECHT: No?

MR. ARNHOLT: We do not -- and I mentioned previously -- we do not inhibit the capability to automatically actuate ECCS. If an ECCS condition is warranted, ECCS will actuate either automatically or manually via the operator. This scenario is assuming there is not a demand for an ECCS actuation.

MR. HECHT: Okay. Thank you.

MR. ARNHOLT: That's the important distinction. If, during that 24-hour period, the operators were to notice conditions that would warrant

an ECCS actuation, they would have the capability to manually initiate an ECCS actuation.

MEMBER BLEY: But, at the end of the 24 hours, you actuate, which means we get there, if everything's working right, before the batteries start to decay?

MR. ARNHOLT: Right. And it's important to note, the DC-to-DC power converters, those are a Class 1E isolation device. And that's where we provide our protection from any under-voltage conditions, power surge transients from the AC power system, things of that nature. That's what those devices are intended to do, protect the downstream safety-related equipment within the MPS.

MEMBER SKILLMAN: What is the -- let me ask this question very carefully because I don't wish to be pejorative -- what is the advantage that the designers envisioned, other than draining the batteries? How often might the designers of the NuScale facility think this event might occur?

MR. ARNHOLT: How often?

MEMBER SKILLMAN: Yes.

MR. ARNHOLT: I don't know what the postulated frequency of a loss of AC power event is. Do you know what Chapter 15 assumes?

MR. INFANGER: No. We don't have a specific -- it's in the PRA. Chapter 19 has a loss of outside power frequency. Typically, in the industry it's about once every 20 years.

MEMBER BLEY: But it varies around the country.

MR. INFANGER: Yes.

MR. ARNHOLT: But the takeaway is, AC power or DC power is not required for performance of a safety function.

MEMBER SKILLMAN: Yes. Thank you.

MR. ARNHOLT: Just a note about, we mentioned earlier or heard a discussion earlier about application specific action items, and this is just a takeaway. The HIPS Topical Report provided 65 application specific action items. So, we did a detailed cross-referencing in the NuScale Chapter 7 application that showed where we addressed within the chapter all of the 65 action items. And we've got a detailed table that provides that cross-referencing for review. And then, that way, it gives you the pointer to the content in the chapter where those pieces of information were addressed.

I've got a little bit lower level of detail of the module protection system top-level

architecture, and the color coding is important here. The color coding is meant to convey this inherent diversity attribute, but the Committee has seen this figure before. So, for separation groups alpha and charlie in ESFAS in reactor trip division 1, that's based on one FPGA technology. And for separation groups bravo and delta, and reactor trip in ESFAS divisions 2, that's based on a different FPGA technology. So, we apply the exact same diversity attributes that we described in our HIPS Topical Report to the NuScale plant design. That's what the color coding was meant to convey.

The gray boxes down at the end indicate that those prior-to-logic functions do not contain any embedded digital technology.

MEMBER BROWN: Just if you don't remember from the HIPS meeting what that means on the two technologies, one of them is a one-time program or flash FPGA operation; the other one is an SRAM or static random access memory. The one-time programming is, if my memory serves, that's a non-volatile set of stuff.

MR. ARNHOLT: Correct.

MEMBER BROWN: The SRAM is a volatile set of FPGAs which, when you lose power, everything goes

away. I mean, you don't have any memory. It has to be reset.

MEMBER BLEY: But the common point is the logic you've put in by either method.

MEMBER BROWN: That's right. In one case the memory is retained, and the other one the memory is not retained. But they're two different, they're just two different approaches in terms of the FPGA technologies.

MR. AYALA: Just a minor clarification, though. They both still have some level of non-volatile memory.

MEMBER BROWN: Well, everything --

MR. AYALA: Yes.

MEMBER BROWN: -- has some level of non -- otherwise, you couldn't start it up.

MR. AYALA: Right. So, on the SRAM, when it starts up, the SRAM loses its configuration.

MEMBER BROWN: Yes.

MR. AYALA: So, it has to look at the non-volatile memory and say, okay, how should I be configured? And then, it configures itself.

MEMBER BROWN: But that's got programmable read-only memory somewhere in there that the SRAM goes and sucks stuff out to reprogram itself. It just

takes time to do it; that's all.

MR. AYALA: Yes.

MEMBER BLEY: It's lacking a few switches. Never mind.

(Laughter.)

MR. ARNHOLT: So, one of the last takeaways here, and just so it's clear in everyone's mind, we have four separation groups of signal inputs, trip determination, and that feeds into two divisions of voting logic and actuation commands to field components. So, just as a point of clarification.

MEMBER BLEY: Just from your point of view -- this is not a technical question -- how helpful did it turn out to be for you to have done the Topical earlier before you did the review of Chapter 7 with this there?

MR. ARNHOLT: I think the way that NuScale did it was extremely advantageous to us. And obviously, we took no exceptions to it. So, the staff review that was performed for Chapter 7 leveraged a lot of what was reviewed and approved in the HIPS Topical Report. Very helpful.

MEMBER BROWN: I would actually echo that, from our standpoint. If I had had to do both of these coming up to the same meeting, my head would have

exploded, as if it didn't in the first place.

MR. ARNHOLT: And just remember, the way we've designed the HIPS system and applied it to the NuScale design for the module protection system, it's a very simple system. And it affords us a lot of -- it's easy to review, and there's just a lot of benefit to that.

Just a quick slide. We do have reactor trip breakers. We have four reactor trip breakers, two aligned to each reactor trip system division. And we do provide the capability for manual trip of those breakers. And we have a similar complement of pressurizer heater trip breakers that are a safety-related function to remove power upon demand actuation from the pressurizer heaters.

And just to note, these breakers do have both a safety-related under-voltage coil, and to go back to the removal of power is the safety function. But we also do apply a non-safety-related diverse shut trip circuitry capability, too, just from a breaker operation --

MEMBER BLEY: Experience has shown that's a really good idea because, depending on how well you do the maintenance, the under-voltage --

MR. ARNHOLT: We've leveraged a lot of

operating experience into the design of these breakers.

We've talked about this in great detail. I don't want to spend any more time on this. If we need to, I can entertain additional questions. But that list of five effects down at the bottom, that was how we evaluated those systems from the segmentation. And we looked at the system's ability to impact, as I mentioned, reactivity, coolant pressure, temperature level increases or decreases, or radioactive release to the environment. So, that kind of formed the framework by which we did our evaluation and allocated segments to parts to the control system.

MEMBER SUNSERI: Brian, this looks like a good place for a break.

MR. ARNHOLT: Absolutely. I was going to say we're concluded with the Section 7.0 section.

MEMBER SUNSERI: All right. So, let's pause here for 15 minutes. Return at 20 after on this clock up here.

Thank you.

(Whereupon, the foregoing matter went off the record at 10:03 a.m. and went back on the record at 10:20 a.m.)

CHAIRMAN CORRADINI: Okay, why don't we

get started?

I was asked to make a reminder that, thanks to the diligence of the members, we get close to proprietary, and we leave it to you to tell us to back off, so that we can save those questions for the afternoon closed session.

MR. ARNHOLT: Understood.

CHAIRMAN CORRADINI: Okay.

MR. ARNHOLT: I haven't got there yet this morning, and I'm not have any prepared information for a closed session, but if discussions need to go there, we can --

CHAIRMAN CORRADINI: But you just warn us, so we don't --

MR. ARNHOLT: Thank you.

CHAIRMAN CORRADINI: Keep on going.

MR. ARNHOLT: All right. Before I jump into the Section 7.1 information, I just want to make sure that people were clear on a discussion we had on the previous section about our enable non-safety control switch. And I can't remember if I misspoke, but it is a momentary contact switch.

MEMBER BROWN: Yes, I asked you that question.

MR. ARNHOLT: Okay.

MEMBER BROWN: And you answered it.

MR. ARNHOLT: Okay. Thank you.

MEMBER BROWN: And explained why it was okay to be momentary.

MR. ARNHOLT: Okay. Good.

So, the Section 7.1 instruction on these fundamental design principles of independence, redundancy, predictability, and repeatability, diversity and defense-in-depth, and simplicity. As I wrap up the presentation, I'll talk a little bit more about the simplicity attribute and how we applied that.

Working on the independence principle, this is a figure that those of you who were part of the review of the HIPS Topical Report may have seen in the past. The MPS and NMS are two safety-related systems. They're designed with physical-electrical communication and functional independence.

We've talked about this in previous discussions, but just to reemphasize, we have one-way communication from safety to non-safety systems through isolated data paths. So, that's a communication-independence attribute.

We separate safety and non-safety-related communications on the separate communication buses.

And I'll point to this figure and walk you through a couple of examples.

If you look at the top of that figure, and at safety function module No. 1, that safety function module may perform a safety-related function, say, to monitor pressurizer level and initiate a reactor trip on a high or low pressurizer level function. And you can see we've drawn some arrows between these three safety data buses that are part of the safety data communication path, and we also provide that data onto a separate, completely separate and independent communication bus that we call a monitoring communication bus.

So, we have three safety, redundant safety data buses here, and you can see those connections from that safety function module. And we have an isolated independent non-safety-related communication bus that's our monitoring and indication bus. That's that isolated data path that we talked about earlier that provides information to MCS through these communication modules.

If you look at safety function module --

MEMBER MARCH-LEUBA: That yellow box is the isolation?

MR. ARNHOLT: That is where the electrical

and communication isolation occurs.

So, if we look at safety function module No. 2, you will not see connections to the safety data bus. And these are physical connections on the actual FPGA circuitry. Physically, when we manufacture and design and build the system, we physically do not make those connections. And we only apply data to, and connect data to, this monitoring and indication bus.

An example of that might be a sensor input that's used for post-accident monitoring that has a non-safety-related function, but we would still bring it into the MPS because, then, we can leverage the reliability of the MPS and take advantage of the highly-reliable DC power system for that long-term post-accident monitoring.

So, here's just a pictorial description of how we've implemented at a practical level this concept of independence in communication in the system.

MEMBER MARCH-LEUBA: So, even though you don't need it to be in the safety box, you put the sensor in the safety --

MR. ARNHOLT: We do. And really, what drove us to that decision was a simplicity standpoint. We wanted to maintain the overall architecture as

simple as possible, and by doing it this way --

MEMBER MARCH-LEUBA: I was going to ask the opposite, how come -- that's not simplicity. That's complicated, the safety box, which is the one you want to be simple. It's simplifying your life.

(Laughter.)

MR. ARNHOLT: And then, we talked about this again, the control of safety-related components of the hardwired isolated inputs for the module control system. We mentioned earlier that that is performed by hardware connections that communicate no data.

Moving on to the next fundamental principle, redundancy, we talked about this again, but just how we've implemented it into the architecture and design, four separation groups, two divisions of module protection system. We have four channels of safety-related neutron monitoring system that provide inputs from the X4 detectors into the MPS to perform protective functions on this inputs.

The NMS and the MPS are designed to meet single failure criteria and through those redundancy attributes. We also apply redundancy into our post-accident monitoring functions. We have no, NuScale has no Type A post-accident monitoring variables that

are associated with required safety-related operator actions. We do have Type B and C variables. And for those functions, we do meet the single failure criterion, as required by IEEE 497.

And I had mentioned this earlier. We do even carry these principles into the design of the non-safety-related systems. And again, the end goal there is a for a highly-reliable system for asset protection and to reliably operate your plant.

Just a couple of notes and takeaways on predictability and repeatability. There's a pretty detailed discussion in the Highly Integrated Protection System Topical Report. Some of that is of a proprietary nature, and I won't discuss it here. But we directly apply those principles into the design of the FPGA-based MPS system.

And we do account for this fixed response time. We describe how we calculate that response time, and that is directly accounted for in the safety analysis as part of the actuation delays that are assumed in the Chapter 15 analysis.

Lastly, looking at the diversity and defense-in-depth, I had mentioned earlier we leverage the diversity between the two different types of FPGA technologies, as I talked about, from an architecture

standpoint, how we do that with the platform technology diversity. And that's where we get most of our advantage and provide defense against digital-based common-cause failures.

Now the NuScale design does make use of some first-of-a-kind sensors for safety-related functions, but have digital technology in them. And when I say "digital technology," based on the sensor design, the sensor electronics and processing makes use of digital processing technology. Now what the actual inputs to MPS are, are actually analog inputs. So, it's just the sensor processing that is performed by a digital function, but we still would input that as an analog input to the MPS, as I say, as a 4-to-20-milliamp signal or a 0-to-10-volt signal.

MEMBER MARCH-LEUBA: Is it planned to build a complete system, a complete four-channel protection system, plug it into a simulator, and run it for three years before you go into the real system?

MR. ARNHOLT: I don't know that that's part of our plan. We'll go through the normal digital I&C development life cycle where you build. You'll do component-level testing, integrated system testing, factor acceptance testing, site acceptance testing. But to do a long-term --

MEMBER MARCH-LEUBA: Because it is one-of-a-kind, you are going to mess up somewhere.

MR. ARNHOLT: For most of our first-of-a-kind technology, we do have in-progress activities that we're doing proof-of-concept and prototype development. For example, we have a working prototype of a single channel and single division of a module protection system. That's been built and we've had that in operation up in our Corvallis simulator for the last 18 months or so.

MEMBER MARCH-LEUBA: How likely is it that you will build the same system when you build the plant? I mean, you'll probably use different components.

MR. ARNHOLT: We could. But, you know, there are certain design attributes that we applied, just because it was a prototype. We maybe didn't use rigor in the design of chassis or how the carbs are physically assembled into the chassis, things of that nature.

MEMBER MARCH-LEUBA: Yes, I mean, being one of a kind, you will mess up. I will rather that you test it on a computer instead of on the real plant.

MR. ARNHOLT: Yes, and as part of our

first-of-a-kind development program, we do proof-of-concept. We have a whole qualification program that is laid out as part of our design schedule.

Just for point of clarification, I had mentioned our safety display and information system is an FPGA-based system.

MEMBER MARCH-LEUBA: Uh-hum.

MR. ARNHOLT: We expect to have a prototype fully tested and built by the end of this year. So, in the next several months, we'll have a working prototype. And that, the large benefit to that is we had talked earlier about the human-system interface and colors, and how do graphics interface with the operator. So, we're able to validate that because using FPGAs to perform display and monitoring, it's a unique and novel concept, and we'll work out a lot of those challenges with our prototype development.

But, with these digital-based sensors, we did want to address the digital-based common-cause failure with those. And to do that, we addressed it as part of a coping analysis. And so, there's an extensive summary of this in the FSER Table 7.1-18, where we walk through the digital-based sensors for pressure, level, and flow, and looked at those

potential common-cause failure scenarios as they relate to how the Chapter 15 analysis laid out.

Remember, a coping analysis uses best estimate methods. So, the takeaway is we performed our coping analysis using best estimate methods, and we met all of our acceptance criteria. And that largely was related to two different scenarios. Once you apply best estimate methods, the particular scenario that you evaluate for never gets to a point where you have to challenge the safety system. So, it just becomes a "no, never mind". And in other cases, we would have had diverse non-digital-based sensors that provide us the backup protective function. So, the takeaway here is we perform an extensive coping analysis to address these digital-based sensors and postulated common-cause failures, and the results were acceptable.

That concludes 7.1. Any remaining questions related to the content in 7.1?

(No response.)

All right. Moving into Section 7.2, and we've talked about this extensively this morning, but I do want to have a brief discussion on the control of access attributes.

The design of the module protection system

conforms to the control-of-access requirements in IEEE 603 and Regulatory Guide 1.152. That sets the regulatory basis for how we've evaluated and presented that in Chapter 7.

I've mentioned the No. 1 security aspect that we take advantage of is physical protection. We lock our safety-related cabinets in physically-protected rooms.

The MPS design, physically, you cannot perform any remote access to the FPGA-based logic, and that's one of the other attributes that you get a benefit from with FPGA-based systems. They're highly secure, and once they're put into the runtime configuration, there is physically no way to alter the runtime application without actually removing a card from service, physically removing it, and performing whatever manipulations you need to change the logic on that.

We do have a limited set of what we call tunable parameters, things such as calibration constants or setpoints that we use our maintenance workstation for to update. And you can update that on the system in a running configuration, but very limited to just a few select number of parameters as far as calibration of the system goes.

A quick note on automatic and manual controls, and to reemphasize, there are no safety-related manual operator actions required for the NuScale design. The MPS performs all of its RTS and ESFAS functions automatically. However, we do provide these series of -- and they're listed here -- of manual actuation switches that backup. There's one switch per division, and that is purely to give the operator a backup to the automatic functions that the MPS provides.

This next slide, I included this to discuss the actuation prior to logic. And you may have seen in the application we provide the logic diagrams for all the MPS functions. So, this figure is straight out, is representative straight out of the FSER, and it's an attempt to show that your automatic and manual protective functions have the highest priority. And you can see, there on the left, they input at the lowest point downstream to where the voting logic occurs for command and actuation to the final actuated component.

And we talked earlier about this enable non-safety control switch. You can see where the logic comes as you walk through this. The way the logic represents -- and I talked about it before -- if

the operator had enabled non-safety-related control using his procedures, and if an automatic or manual actuation signal were to occur during that scenario, this logic would drop out that input from the enable non-safety-related control switch and remove any non-safety-related control commands until the operate took deliberate action to reenable that.

And just a point to take away, to remember, this is a non-digital-based component. It's actually a separate circuit within our equipment interface module. It is comprised of non-digital discrete components. So, there is no software-based or digital-based circuitry involved with that.

MEMBER BROWN: Non-digital --

MR. ARNHOLT: Non-digital.

MEMBER BROWN: -- that's digital. I mean, it's digital logic. It's just hardware-implemented; that's all.

MR. ARNHOLT: Yes, discrete components.

MEMBER BROWN: It's no software.

MR. ARNHOLT: Exactly. I just had a note here --

MEMBER BROWN: Non-digital, though, it's just no software.

MR. ARNHOLT: I'm going to back up one

slide, two slides. I just wanted to mention -- I don't have it written up here -- but we do have a COL action item I mentioned this morning to submit a cybersecurity plan. So, this application does not submit that as part of the NuScale DCA, but it is a COL item to submit a cybersecurity plan.

So, to wrap up, in conclusion, I mentioned the FSAR follows the Chapter 7 DSRS structure. Overall, we thought it was a huge success to follow that structure versus the old SRP. I thought it led to efficient review. We had a lot of interactions with the NRC staff, and really a lot of benefit with that, the way that the DSRS worked out. I've been involved with it for a number of years, and this is the culmination of the result of that effort.

CHAIRMAN CORRADINI: Well, if you talk to anybody above the staff you're talking to, to higher-ups within the Agency, that would be good to know.

MR. ARNHOLT: Okay.

CHAIRMAN CORRADINI: Because I think at the higher levels they wanted to make sure that this was a benefit.

MR. ARNHOLT: In my view, I think to speak on behalf of NuScale, it was a very, very large benefit to this.

CHAIRMAN CORRADINI: Okay.

MEMBER BROWN: Well, the object of the -- and this is a personal opinion -- but the DSRSes were to provide an overall framework within which we should evaluate stuff, as well as more in one place succinctly describe the things that you need to look at underneath that overarching framework. That's why I think it's been useful for us, or at least it has been for me.

MR. ARNHOLT: It can achieve the desired result.

The foundation of the regulatory conformance, there we've taken no departure to the regulations and the regulatory guidance that exists. And that helps the review.

And just a couple of notes about the simplicity. We tried to leverage the overall passively-safe, simple design of the NuScale power module. And you see that in the design of the I&C systems. We don't have closed-loop control from a safety-related standpoint. It's actuate-only, and the actuation function is the removal of power. So, very simple functions. Typically, your safety-related protective signal conditioning and trip determination functions are greater than and less than functions,

simple comparators, simple functions to perform that, and again, leverages the simplicity attributes that we set forth.

And that concludes my presentation. I don't know if there are any other remaining questions. I'm happy to answer them.

CHAIRMAN CORRADINI: Take silence as a success. Thank you.

We'll move on to the staff.

And for an I&C Subcommittee, we are almost by uncertainty on time.

MEMBER BLEY: We are?

(Laughter.)

CHAIRMAN CORRADINI: Well, I mean, staff was supposed to start at 10:15. So, this is pretty close to on time.

(Laughter.)

It's in the same hour.

MEMBER BLEY: It may speak to having done the Topical.

CHAIRMAN CORRADINI: Huh?

MEMBER BLEY: That may speak, also, to having done the Topical earlier.

CHAIRMAN CORRADINI: Yes.

You know, the army is coming. Careful.

(Laughter.)

Luis, are you going to start us off or is Omid? You'll start us off? Okay.

This is now a testament to the complexity of I&C or just the complexity of the staff? What is it?

MEMBER BROWN: Both.

(Laughter.)

CHAIRMAN CORRADINI: Okay. Omid, you're up.

MR. TABATABAI: Good morning, everyone. Good morning, Chairman. Thanks very much for giving us an opportunity to present to you the staff's evaluation of NuScale's Chapter 7 instrumentation and controls chapter for the design certification application.

We have, as you said, a team of experts here, but that is not all of us. As you can imagine, there are a lot more branches and technical disciplines involved in this review. And Luis will touch on that.

Actually, before we get started, I would like to remind members of the public who are listening on the phone, we have a public version of the Safety Evaluation Report available in ADAMS. If they need

the ML number, they can contact me or Greg Cranston.

CHAIRMAN CORRADINI: Or Christina.

MR. TABATABAI: Or Christina, to get the ML number.

Dr. Bley, you also mentioned about Chapter 17. You had a question about the DRAP process and the classification of risk significant systems. I just want to tell you --

MEMBER BROWN: Not quite, but go ahead.

MR. TABATABAI: I'm sorry, it was Mr. Skillman. I think you asked the question during NuScale's presentation.

MEMBER BLEY: Well, I asked where their evaluation of non-risk-significant came from.

MR. TABATABAI: Right.

MEMBER BLEY: And they pointed me to Chapter 17, which I haven't seen.

MR. TABATABAI: Right. And I happen to be the PM for Chapter 17 as well.

MEMBER BLEY: Oh, okay.

MR. TABATABAI: So, we finished the SER, the safety evaluation for Chapter 17. I can provide a copy of that to you ahead of time.

MEMBER BLEY: Okay, great.

MR. TABATABAI: So, that's all --

MEMBER BLEY: Through Christina, yes.

MR. TABATABAI: Of course, yes.

Aside from that, I don't have any more remarks. I would like to ask Luis Betancourt to start the technical discussions.

CHAIRMAN CORRADINI: Thank you.

MR. BETANCOURT: Well, good morning. My name is Luis Betancourt, and I am the Acting I&C Branch Chief. With me here today we have -- front and center are two main presenters for today, which is Sergiu Basturescu as well as Dawnmathews Kalathiveettil, and Dinesh Taneja, who is also the I&C technical reviewer for the NuScale design. And at least in the audience we've got, also, some of the members that, in the case that we need to draw them, we will also put them in the line of fire.

That being said, for today's agenda, what we want to do, I will provide a high-level background of the I&C staff review team, how we interface with all the disciplines in the NRC as well as some of the high-level milestones that we go through in the review.

Following my presentation, Sergiu will talk about the philosophy of the safety-focused review that we employed in this review, followed by the high-

level overview of the I&C architecture. And he will present three of the four fundamental design principles.

Then, Dawnmathews will be talking about the fundamental design physical of D3, as well as some of the questions that we got in the morning on the no cementation analyses as well as the assumption of ATWS.

We also plan to have a slide to talk about the comments that we got from Chapter 8, from the Subcommittee members. So, we're going to cover the story from the staff, and then, high-level conclusions.

MEMBER BLEY: Luis, were you planning to talk about or would you talk about how you folks saw the utility of having done the Topical ahead of time?

MR. BETANCOURT: Yes, I will.

So, very quickly, this is the I&C review team as well as the quality management team.

The purpose of this slide is to show that, even though we're seeing today a Chapter 7 review, this actually involved a lot of the disciplines that you see on this slide. In the slide you will see the different disciplines that are called out, and we actually interacted with five Divisions across three

different offices.

One of the things, it was really helpful in the DSRS that these interfaces were clearly delineated. So, that really helped us to start with the review, or who are all of these people that we need to start to talking to in order to be able to perform the review of Chapter 7.

To address your question, Dennis, one of the things that we found out as part of the pre-application activities is that we actually had a lot of interactions with the pre-applicant. And as part of those pre-applications, we also had the HIPS Topical Report at that time. And when they came in, one of the things that they found out is in this area of built-in diversity. That was the first time that we saw that. We actually had a lot of questions with them at that time. It actually helped us to understand their diversity early in the game.

So, when we received the application in late 2016, we already knew what were these safety-focused areas that we want to do on the staff. So, even though we had this pre-application between late 2016 to March 2017, when we were doing our acceptance review, there were some of the major technical issues that were addressed as far as the Topical Report. So,

we were able to focus on other areas that were more application-specific in the NuScale design.

Since then, I wanted to point out that, in April 2017, we had the full Committee on the HIPS Topical Report, that the members were briefed on the platform. And around that time, between March 2017 to December 2017, we were able to have five public meetings. We were able to issue nine RAIs that contained existing questions, and we had one audit regarding the FMAA/SR analysis and the no cementation technical basis.

MEMBER BLEY: So, you got way ahead, that sounds --

MR. BETANCOURT: Yes.

MEMBER BLEY: That's good to know.

MR. BETANCOURT: Right. And then, by that time, by 2017, we were able to close all of their RAIs. So, when we submitted the SER, the Draft SER with Open Items and Projects, at that time there were no open items. So, all of the issues that we found were resolved with the RAIs.

And in March 2018, they submitted the application and Revision of the DCD, and it took us a month to verify that all the confirmatory items were incorporated in Revision 1. And since then, that's

why we are here today.

One of the things that I want to commend both the staff and NuScale is that, since 2014 all the way to today, we have had a very open, collaborative environment with the applicant that we were able to actually express with very frank conversation. These are the technical issues that we found in the application. And we were able to have that dialog that actually helped us to get where we are today.

As of today, we don't have any I&C specific open items in the SER. You will see that there are some more open items, but they're actually from the interfaces that we have from other chapters; for example, Chapter 8, Chapter 15, and Chapter 18. But, as of today, we don't have any open items that are specific to I&C.

Any more questions on this before I turn it over to Sergiu?

(No response.)

Okay. Oh, Charlie, you had a question?

MEMBER BROWN: Yes. So, all open items are closed?

MR. BETANCOURT: For I&C.

MEMBER BROWN: For I&C?

MR. BETANCOURT: Right.

MEMBER BROWN: Okay. Good.

MR. BETANCOURT: So, we'll now turn it over to Sergiu here, and he's going to take over.

Sergiu.

MR. BASTURESCU: Good morning. My name is Sergiu Basturescu.

And go to slide 6. On this slide, we are presenting the safety-focused review. The NRC established the enhanced safety-focused review approach, which lined up with the framework of the DSRS, which was developed by the Instrumentation and Control staff.

Use of risk insights to enhance the safety-focused review of the NuScale SMR design is consistent with the fundamental I&C safety design principles of independence, redundancy, predictability, and repeatability, diversity and defense-in-depth, and simplicity. We will look at these fundamental principles on the later slides.

MEMBER BLEY: Sergiu, a couple of years ago or more, I guess, we were briefed on the safety-focused review approach and the kind of tracking tables and things they had developed. Did you use that kind of as we might have seen it a couple of years ago or has it evolved a lot?

MR. BETANCOURT: So, I was actually part of that safety-focused review team as well as Joe Ashcraft, who is in the audience. And, yes, we were able to use that table at the beginning of the review to be able to narrow down --

MEMBER BLEY: Was it helpful?

MR. BETANCOURT: It was.

MEMBER BLEY: Did it really focus things?

MR. BETANCOURT: Yes.

MEMBER BLEY: Okay.

MR. BETANCOURT: It really helped us to focus on how the I&C system interfaced with the other safety systems in the plan. So, it really helped us to narrow down the technical issues.

MEMBER BLEY: It kind of "smelled" like it should, but it's nice to hear that you had experience with it.

MR. BETANCOURT: Yes.

MEMBER BLEY: Do you know if other parts of the NuScale review are using that same approach?

MR. BETANCOURT: Oh, they will need to answer that.

(Laughter.)

MR. TABATABAI: To the extent practicable yes.

MEMBER BLEY: Is it? Okay.

MR. TABATABAI: Yes. Yes, we are.

MEMBER BLEY: And it's helping in other areas as well?

MR. TABATABAI: Yes, we are using that approach.

MEMBER BLEY: Okay. Thank you.

MR. BETANCOURT: So, I think Chapter 14 is actually using a safety-focused review as part of the initial task plan. So, that's an area that they are focusing the safety-focused review, as just one example.

MR. BASTURESCU: Okay. So, moving on --

MR. HECHT: Can I ask a real trivial question? What does the "A" stand for in the SFRA?

MR. BASTURESCU: Safety-focused review.

MR. TABATABAI: Oh, the "A", the approach.

(Laughter.)

MR. BETANCOURT: And I forgot to mention, we have a lot of acronyms.

MEMBER BROWN: It was new.

MR. BETANCOURT: Yes. We have a lot of acronyms in the slides. So, I'll point you to slides 20 and 21. It's a mapping of all of them. We will try our best to clearly define the terms in each one

of the slides.

MR. BASTURESCU: Okay. On this slide, we are presenting our Safety Evaluation Report, SER, on the NuScale design, which is partly presented in Tier 2, Chapter 7.

In Tier 1, Sections 2.5 and 2.6, of the DCD, in conjunction with Chapter 7, we evaluate --

MEMBER BROWN: Can I stop this for a minute? I forgot something. If you don't mind? I guess I go back to Luis.

MR. BETANCOURT: Okay.

MEMBER BROWN: You said there were no open items. Yet, in --

MR. BETANCOURT: Specific to I&C, right.

MEMBER BROWN: I've got to go back and find what I found a minute ago.

In 7.1.3.6, conclusions --

MR. BETANCOURT: 7 --

MEMBER BROWN: .1.3.6 of your SER, under "redundant power sources within the module protection system" --

MR. BETANCOURT: Yes.

MEMBER BROWN: -- you all commented that, "Due to the open items in Section 7.1.5, 7.2.13, and 8.3, the NRC staff cannot reach a conclusion." That's

in the version of the SER I have.

MR. BETANCOURT: Yes. And I actually noted that before coming to the ACRS. That's cleanup work that we have to do.

MEMBER BROWN: That's what?

MR. BETANCOURT: Cleanup work that we have to do. That's an editorial --

MEMBER BLEY: It's editorial? It's not --

MR. BETANCOURT: Right. There's no open items now in 715. So, that was something that --

MEMBER BROWN: Well, it says "7.2.13" also.

MR. BETANCOURT: I can tell you right now that's something that we need to fix internally in the report.

Oh, we've got somebody over here.

MR. HALVERSON: Yes, Derek Halverson.

The 7.2.13 one just points to a Chapter 8 one as well. It's pointing out where --

MEMBER BROWN: And 7.8.3?

MR. HALVERSON: The 7.2.13 --

MEMBER BROWN: There's one in 8.3, Section 8.3 also, that statement. All I'm trying to do is get --

MR. BETANCOURT: No, no, to answer your

question, Charlie, that was a missed oversight from our part. That language should not be there. That's the language that it was sent to Projects originally back in January. So, that's something that we forgot to clean up. And in reality, there should not be that language in the --

MEMBER BLEY: So, it's editorial and not technical?

MR. BETANCOURT: Right. Correct.

MR. TABATABAI: Right. I think at the beginning Luis mentioned that between receiving Revision 1, new revision -- they had finished their SER based on Revision 0, and then, Revision 1 came in. They confirmed all of the items were closed, but in terms of updating the SE, we kind of fell behind, yes. And we plan to clean that up for the full Committee in September.

CHAIRMAN CORRADINI: Great, but the sooner, the better. Otherwise, the old people that are sometimes known as "members" will forget and ask you the same thing all over again in September.

(Laughter.)

MR. BETANCOURT: Yes, understood. That's something that we have to do.

MEMBER BROWN: Yes, another part of the

SER, I mean, like Section 3.1 also -- well, excuse me. Under 7.2.3, it also identifies -- and it throws in 3.1 as well. So, there were some inconsistencies. I'm not saying there's anything wrong. You're saying they're all --

MR. BETANCOURT: It was because of the timing when it was sent to Projects and when it went to review. So, it's something that it was a missed oversight on our part. We will clean it up before it goes to the full Committee. That's an action that we have to take.

MEMBER BROWN: Okay. Thank you.

MR. BASTURESCU: So, going back to in the Tier 2 section, we validated the documents incorporated by our IBRs, which were two Technical Reports and one Topical Report. The Topical Report is the Highly Integrated Protection System, the HIPS, Platform, which is based on the fundamental design principles, and included the 65 application specific action items, ASAIs. All of these ASAIs were addressed in Chapter 7 and evaluated by the staff during our review of Chapter 7.

Besides Chapter 7, we also supported evaluations in Chapters 9 and 14. Today we will be focusing on Chapter 7, but we will be participating

during the review of those chapters.

In the exemption section --

MEMBER BLEY: Despite the wonderful list of acronyms, I don't see "IRB" on your list.

MR. BASTURESCU: It's "incorporated by reference".

MEMBER BROWN: Incorporated by reference.

MEMBER BLEY: Oh, okay. Thank you.

MR. BASTURESCU: We apologize for that.

So, yes, on the right side, we are showing the exemptions, and those exemptions were the ones that the staff looked at. The staff evaluated the ATWS exemption, and the that you will find in Chapter 7 of the SER. And we will be discussing that in a later slide. As for the three-mile exemption, that one is documented in Chapter 8, SER.

Now moving on, unless there's any questions?

(No response.)

Okay. So, this is the I&C architecture. We saw this in the morning, and we are showing it as an example, also, during the HIPS platform presentation.

We have this figure. Also, we have it loaded in Visio. So, we can zoom-in on any area

you're interested in looking at.

Besides the architecture, for NuScale, it was the starting point of our review, and it was the first thing we looked at and studied when we started this project.

MEMBER BROWN: Okay. Before you leave this --

MR. BASTURESCU: Yes?

MEMBER BROWN: And to echo back to the discussions we had with NuScale, and if I can find your page here fast enough, page 44 -- that's the problem with not having paper in front of you. Here we are. You made a statement in here where you said that, "The unidirectional data diode," which you talk about from the PCS and the MCS, you described it as a unidirectional data diode "firewalled connection". And I don't know why we're combining those two words. "Firewalled" is a far more generic term, which would imply that this can be -- that's not listed in Chapter 7. I couldn't find the word "firewalled" relative to this anywhere in Chapter 7.

So, I'm just asking, do you know something that we don't? Or that NuScale, that I didn't communicate properly with them earlier relative to the data diode characteristics of being hardware, not

software-configured? Not allowing the option to be software-configured as part of the overall design? That's listed in a couple of places, both for the module control system and the plant control system, data diodes. And the figure just says --

MEMBER BLEY: Charlie's earlier point was we don't find anywhere in writing that requires that.

MEMBER BROWN: Yes, that it be hardware-based. But, in addition to that, you use the word "firewalled" in the SER, which has a more generic implication of being, sounding like something else that would be software -- they can be software-controlled if you just talk about firewalls. I hate to mouse-note this, but I don't want to leave any contradiction in terms of where you think --

MR. BETANCOURT: No, no, I hear your comment.

MEMBER BROWN: -- you stand relative to the hardware-based --

MR. BETANCOURT: Right.

MEMBER BROWN: -- data diode approach as opposed to any software-based.

MR. BETANCOURT: Right.

MEMBER BROWN: And I did do a data search of the various vendors that make this stuff before I

came here and found that there were units called "data diodes," but, yet, had significant software in terms of their configuration. There were other vendors that had units that very specifically called out hardware-based and touted their hard-based design as opposed to those that were software-based.

MR. BETANCOURT: Right. And I remember the discussion that we had in the morning, that what you heard in the morning is consistent --

MEMBER BROWN: We're still in the morning, by the way.

MR. BETANCOURT: -- in the application.

(Laughter.)

Right. Well, yes.

MEMBER BROWN: I haven't gone to sleep yet.

(Laughter.)

MR. BETANCOURT: Okay. Point taken.

To answer your question, yes, the application does not specify whether this diode is going to be software-configured or hardware-based, and I can see why the confusion when you read the SER and the word "firewall" attached to it. So, we need to remove that because it's basically with what was discussed in the morning. So, I can see what was the

confusion that you had before.

MEMBER MARCH-LEUBA: I'm looking at the SER, and it says, "unidirectional diode," comma --

MR. BETANCOURT: Yes.

MEMBER MARCH-LEUBA: -- "firewalled connection".

MR. BETANCOURT: Yes, I have that over here.

MEMBER MARCH-LEUBA: So, it implements a firewall function with that hardware --

MR. BETANCOURT: Right, and I can see why the confusion.

MEMBER BROWN: There's a comma in between there, I'll agree with that. But, still, that just means it just confuses it even more.

MEMBER MARCH-LEUBA: No, I mean, there is a firewall function.

MEMBER BROWN: It's just "firewalled connection".

CHAIRMAN CORRADINI: I think they get it.

MR. BETANCOURT: We got it. We will take that comment.

MEMBER BROWN: Okay.

MEMBER BLEY: Are you going to correct it?

MR. BETANCOURT: Yes. Yes, by the full

Committee.

(Laughter.)

MEMBER BROWN: But you also ought to -- there's no definition of a data diode in Chapter 7. There's no definition of a data diode as a hardware-based device in the SER.

MR. BETANCOURT: That's correct.

MEMBER BROWN: And I only suggest that that appear. Whether Chapter 7 gets revised or not is another issue, but I would suggest that that be very explicit in any SER that you all issue, that that data diode is a hardware-based data diode.

MR. BETANCOURT: I'll take that back since right now the application does not contain that wording. So, we need to do some discussion internally.

MEMBER BROWN: We ought to have that resolved.

MR. BETANCOURT: Right.

CHAIRMAN CORRADINI: So, that's one member.

MEMBER BROWN: Oh, absolutely, I'm one member.

CHAIRMAN CORRADINI: But I do think there's a high probability event that, if it isn't

clarified, you might see a letter report that --

MR. BETANCOURT: That has that comment. I understand. I understand that.

CHAIRMAN CORRADINI: -- that says it should be clarified.

MR. BETANCOURT: I understand that. Okay.

CHAIRMAN CORRADINI: Okay. Fine. Let's move on.

MR. BASTURESCU: So, here we're going to be looking at the safety classifications. The safety classifications have been determined by NuScale and reviewed by the staff for Chapters 15, 17, and 19, and they are documented in Chapter 3.

We have had interactions with staff on these chapters in order to validate these classifications. With the incorporation of risk insights, I&C systems may be classified as safety-related/risk-significant, which is A1; safety-related/non-risk-significant, which is A2; non-safety-related/risk-significant, B1, and non-safety-related/non-risk-significant, B2.

In keeping with the safety-focused review project direction, the staff primarily focused on evaluations of the A1 systems, that is, the module protection system and the neutron-monitoring system,

the MPS and the NMS. There were no I&C systems for the A2 or B1 classifications.

The scope of our review for the B2 systems was to verify --

MEMBER BLEY: And when you determined that, did you base that, A2, did you base that determination on the PRA or something else? And if you didn't base it on the PRA, how do you know there are no risk-important/not-safety-related systems?

MR. BETANCOURT: So, I guess this goes back to the table that you were mentioning at the beginning of the discussion. Before the presentation, NuScale provided a high-level -- these are all the functions that we planned to actually send to the staff. So, we went through that at that time. When we received the application --

MEMBER BLEY: Kind of based on looking at their list and your judgment that it was reasonable?

MR. BETANCOURT: Correct. So, we actually went back to the --

MEMBER BLEY: But no comparison to the PRA, to safety? Did any of these things crop up as risk --

MR. BETANCOURT: So, that's where our interface with the PRA --

MEMBER BLEY: I didn't hear.

MR. BETANCOURT: That's where our interface with the PRA group actually came in. So, we actually went and talked to the DRAP people.

MEMBER BLEY: Okay.

MR. BETANCOURT: We also went to the Chapter 15 analysis to verify that there's no function that will be classified under A2. So, what we confirmed is that --

MEMBER BLEY: Should have picked up anything in the PRA.

MR. BETANCOURT: Correct.

MR. ASHCRAFT: Yes, this is Joe Ashcraft from the staff.

In Chapter 17, I think it's Table 17-4 that lists the conclusions based on NuScale's input and the PRA.

MEMBER BLEY: We'll look for that. We haven't seen that yet.

MR. ASHCRAFT: I understand.

MR. BETANCOURT: Oh, there is a question here.

MR. HECHT: It's Myron Hecht.

On one of the RAIs, there was a mention of an MHS, which is a module heating system. And I don't

see it on this list, and I had not heard of it before. It was pretty well-explained in the answer, but are there other systems which don't appear on this list, and why not?

MR. BETANCOURT: So, these are the only I&C specific that appear in the architecture. The MHS should appear in 17.4, for these are the only I&C specific systems that were under review.

MR. HECHT: I see. So, the MHS is more like an actuator system? So, it's not really an I&C system?

MR. BETANCOURT: Yes. Yes.

MR. HECHT: Okay.

MEMBER BROWN: What does it heat?

MEMBER SKILLMAN: It is the module heating system that is an auxiliary system that is used to start the plant by injecting heat through the CVCS from 0 to 15 percent power. So, it is basically a thermal hydraulic bootstrap when there is no residual decay heat being produced. It's in Chapter 9, but it's very obscure. But it is buried down in Chapter 7, you're right. I went digging after this because I said, what is that? But it's not an I&C system. It's a plumbing system. It's an aux boiler system, one each for six modules apiece, is what it is.

MEMBER BROWN: Okay. Since I'm not this plant understanding, it's a method to prevent the plant from getting too cold or is it to allow you to start up, to start up heating?

MEMBER SKILLMAN: It can be helpful on shutdown.

MEMBER BROWN: But is it with power? I mean, the reactor is critical or is this without -- this is independent boiler steam circulation?

MEMBER SKILLMAN: You can have a cold, brand-new, fresh core, no decay heat.

MEMBER BROWN: Okay.

MEMBER SKILLMAN: And if you wish to start the system, you use a module heating system with heat from the auxiliary boilers.

MR. ARNHOLT: Brian Arnholt with NuScale.

I would just offer, because NuScale is a natural circulation plant, you don't have heat input from the active reactor coolant pumps when you start the plant up. So, the module heating system provides you that source of heat to initiate and maintain natural circulation until you begin nuclear heating and you start the reactor up.

I hope that helps.

MEMBER BROWN: Well, it does. Thank you.

I think I even read that. I just forgot it.

(Laughter.)

MEMBER KIRCHNER: Just for clarity, the CVCS system is part of the module control system?

MEMBER BROWN: The module heatup system, you mean?

MEMBER SKILLMAN: It just delivers the hot water.

MEMBER KIRCHNER: So, where does it reside?

MR. TANEJA: CVCS is a plant system, right? It's a plant system for that nuclear module. The I&C systems are -- MCS, module control system, controls CVCS functions.

MEMBER KIRCHNER: No, I understand all that.

MR. TANEJA: Okay. Right. But it's a plant system. So, here we are just focusing on what the I&C architecture and the I&C systems are.

MR. HECHT: I guess the confusion is because the second "C" in CVCS is "control" and the second "C" in I&C, or the first "C" in I&C is "control".

(Laughter.)

MR. TANEJA: I can see that.

MEMBER KIRCHNER: I'm not really confused. The CVCS system is part of the module control system or? Where is the actual instrumentation and control reside?

MR. ARNHOLT: This is Brian Arnholt again.

CVCS, the control of CVCS is one of those module-specific, non-safety-related control systems. The module heating system is a common plant system, but it interfaces through the CVCS heat exchange.

MEMBER KIRCHNER: That's the way you get it into the vessel, yes. Thank you.

MR. BASTURESCU: So, back to B2 systems. The scope of our review for the B2 systems was to verify that it met the pertinent regulatory requirements and to evaluate for any adverse impact to safety functions or placing the plant in an unanalyzed state.

Even though the plant protection system, PPS, and safety display and indication system, SDIS, are B2 systems, they both require an augmented level of quality. The PPS provides monitoring and control plant systems. They are common throughout the 12 nuclear NuScale power modules. Specifically, the PPS provide automatic actuation functions for the control and habitability system and the normal control in

heating and ventilation and air conditioning system; and also, for the spent fuel pool and reactor pool level indication. The SDIS provides accurate, complete, and timely information pertinent to the MPS and PPS status and information displays.

So now, we're moving to the portion of our presentation where we are going to focus on the I&C safety design principles. The first safety design principle is independence. And the four areas of independence we reviewed was physical, electrical, communications, and functional.

The physical independence. For physical independence, the staff found that the equipment associated with the module protection system, MPS, and heat monitoring system are located in separate seismically-qualified equipment rooms, and cabling is routed in physical separate cable trays in risers.

For electrical independence, the staff found that the electrical isolation between the safety-related MPS and associated non-safety-related systems is provided by galvanic isolation between the non-safety-related sensor inputs to the MPS, transmit-only and receive-only fiber optic boards, DC-to-DC in galvanic isolation at the hardwired modules, and isolation device in the electrical power supply.

MEMBER SKILLMAN: What do you mean by "galvanic isolation"?

MEMBER BROWN: They're electrically isolated by fiber optics. There's no electrical connection. Galvanic.

MEMBER BLEY: I think, typically -- you guys can correct me on this -- you want the ground systems not to be common.

MEMBER BROWN: I think what they're talking about galvanic, there's not an electrical connection between an input and an output.

MR. BETANCOURT: It's what was called an isolation amplifier.

MEMBER BROWN: Yes. So, you so isolate it.

MR. BETANCOURT: But it is for the power line. This is a power line.

MEMBER BLEY: This is power?

MR. BETANCOURT: This is power. And this already followed the scope of the HIPS Topical Report. All of these features were already addressed during that review. So, the reason that we review over here, how was that implemented throughout the whole architecture?

MEMBER BROWN: It was kind of the

electrical independence between divisions -- or between segments, I mean, excuse me, separation groups and --

MR. BETANCOURT: And communications.

MEMBER BROWN: -- the communications to other functions like the NIB and maintenance workstation, and a few things like that, as well as the MCS and PCS.

MR. TANEJA: Like the module control system component-level controls are interfaced with the module protection system using hardwired connections, and they are isolated using these isolation devices to provide electrical isolation between the module control system and the protection system. So, any faults that may occur on the non-safety side of it does not promulgate into the safety side. And that's the isolation device that provides that capability.

MEMBER BROWN: Thank you.

MR. BASTURESCU: The communications independence. As part of our evaluation, the staff found that, to the exception of divisional voting, that the communications within the MPS separation group is independent and does not rely on communication from outside the respective separation

group or division to perform a safety function.

For voting purposes, the communication uses a point-to-point fiber optics between the scheduling and bypass modules and the scheduling and voting modules. There are no digital communications from the non-safety-related to the safety-related side.

Independence of module control system interfaces with the MPS for performing manual component-level controls is achieved via Class 1E isolation devices.

MEMBER BROWN: But that's, again, with this enable switch.

MR. BETANCOURT: Right.

MR. BASTURESCU: Yes.

MEMBER BROWN: So, I mean, literally, that's a hardwired -- bypassed into the APLs.

MR. BASTURESCU: Right. That's basically it.

MR. HECHT: Can I ask a question with respect to the communication independence? You have three safety data buses, all of which are controlled by communications modules which are called bus masters. And the bus master is working based on a construct, a logical construct, called a finite state

machine for communications. And we don't have any information about how that is implemented and we don't have any information about the different FPGA technologies that would be used to implement it.

How are you sure that a bus master on one of the safety buses which is connected to all of the functional modules might not take them all down because of some kind of jabbering? And I understand there are three separate safety data buses, but one of those safety data buses might start basically launching a denial-of-service attack, not intentional, but unintentional, whereby it takes down all of those SFMs.

MR. TANEJA: So, Myron, what you're looking at is one separation group. So, this is a tripper module redundant architecture, the TMR architecture. What this offers is added dependability and reliability.

From the safety perspective, I can lose this whole separation group A and still be able to perform my safety function, because within the separation group I have added redundancy offered to provide additional, I guess reliability benefit and operational benefit. So, I am not prone to -- it's a more fault tolerant system, in other words.

So, even though I think we looked at that in detail when we looked at the Topical Report on how these FPGAs were configured for these communication protocols, but having three different buses, what it allows me to do is I can lose communication to one of the safety buses. I just need the other two to be functional to still maintain my function. So, it just gives me a lot more fault tolerant capabilities. That's what it does, you know.

MR. HECHT: I guess my question really isn't on the safety buses. It's what the safety buses can do to the SFMs.

MR. TANEJA: That's okay. I mean, I could lose this whole separation group, but it does not have any adverse impact on the independent separation groups that are running independent of this.

MR. HECHT: So, basically, you're relying on the fact that you have replication of four separation groups and you basically believe that there is no circumstance in which there could be a common failure across all those separation groups?

MR. TANEJA: Right, right.

MR. HECHT: Yet, you don't have any details on the implementation of the bus masters?

MR. TANEJA: Like I said, during the

Topical Report for the HIPS platform, we went into that detail review --

MR. HECHT: Well, it didn't say anything there, either, because that was supposed to be one of those application-specific items, and it doesn't seem to be occurring now. So, when would it be addressed?

MR. BETANCOURT: So, which ASAI are you talking about?

MR. HECHT: I don't remember which one.

MR. BETANCOURT: Okay.

MR. HECHT: But the point is that --

MR. TANEJA: Let me understand the concern here. Are we worried about having a failure due to the bus master malfunction?

MR. HECHT: Some logical error --

MR. TANEJA: Right.

MR. HECHT: -- in the bus master which could happen across multiple separation groups.

MR. TANEJA: We don't have any sharing between multiple separation groups.

MR. HECHT: No, it's a common design, right?

MR. TANEJA: No. We have diversity in the technology also, right? We have two separation groups using one FPGA technology, and the other two

separation groups using a different FPGA technology. So, that right there is the level of diversity that offers -- so, I could lose those two with the same FPGA technology, those two separation groups. We have a slide that will show you how the failures of multiple separation groups can still offer us with the success of achieving a safety function.

MR. HECHT: So, for example, one might be using -- I forgot what they call it -- that flash technology --

MR. TANEJA: Right.

MR. HECHT: -- and the other one might be using some kind of fusing technology?

MR. TANEJA: Right.

MR. HECHT: But underlying both of those is common VHDL, right?

MR. TANEJA: Well, it's different toolsets.

MR. HECHT: But the VHDL itself could -- the error might have been manifested there. So, the question that I would have is, I mean, there are ways of dealing with that through QA and through whatever design constraints you're putting on, but that's not specified here in the application, as far as I can tell, or in the report.

MR. TANEJA: The software QA process is laid out in the application. So, there is a very rigorous development process that requires to be followed in developing these platforms. So, there is an Appendix B which dictates the overall quality assurance program. And then, there's a specific software QA assurance manual that dictates development of the module protection system design. So, it's essentially a controlled process in developing the whole thing all the way down to site acceptance testing. Not only just factory acceptance testing, it takes it down to the site acceptance testing.

MR. HECHT: Testing will take you so far, but --

MR. TANEJA: No, I'm just talking about, it's a managed process that starts with your conceptual design to intermediate design, to detailed design, to integration, to module testing, you know, the little software design module testing.

The only thing that I can offer is that, when we were looking at the HIPS platform, we had the opportunity to actually participate in the -- the vendor built a prototype. We had an opportunity to participate in the factory acceptance testing of the prototype. Okay?

Now that prototype did not, you know, it was not built following this QA process that they are required to follow for the NuScale design. But that prototype, during the test, there were 17 --

MR. BETANCOURT: That may be proprietary.

MR. TANEJA: No, I don't think I'm saying anything proprietary.

There was a number of multiple failures that occurred before I lost the function within one chassis. Okay? I'm not talking separation --

MEMBER BLEY: We have closed session scheduled.

MR. TANEJA: Right, but I'm just -- this is a generic statement. There were multiple failures within a controller before I could lose that function capability. So, it's just built in, level of diversity that's built into it. And then, there is this rigorous development life cycle activity that has to occur for developing the actual platform.

MEMBER BLEY: I think everybody has that, but it seemed to me Myron was suggesting a failure or error mode that could create situations we haven't thought about. Is that right?

MR. HECHT: Right. Well, where I was hoping to get to is that there would be a formal

specification of those finite state machines or communication engines, and that those would be proven as part of the development process. And I didn't hear that being stated here. I'm just wondering why.

MR. BETANCOURT: I would prefer to talk about that in the closed session since --

MR. TANEJA: So, the state diagrams were laid out in the HIPS Topical Report, right? So, those state diagrams are there. Those are finite state diagrams; they were there. Now, like I said, that was the details on the platform.

Now the actual development that occurs for the NuScale equipment development, it has to follow a formal development process, meaning that you do do intermediate verification and validation. And one of the key parameters that goes into that QA program is independent V&V that has to occur at the end of each life cycle activity. Okay?

MR. HECHT: It all starts fundamentally from having --

MR. TANEJA: Exactly.

MR. HECHT: -- a sound --

MR. TANEJA: Requirement spec. Right. Yes.

MR. HECHT: So, I was trying to deal with

it from that aspect again, but maybe I'm taking up too much time of the Committee, unless there's other interest.

MR. TANEJA: Maybe NuScale can offer some more insight into that.

MEMBER BROWN: Let me back us out of that, if you would, for a minute. Okay?

MR. TANEJA: Okay.

MEMBER BROWN: I remember having some of this discussion back in the HIPS process. And I'm going to be generic relative to this. I'm trying to look at this relative to the thought process.

Within a separation group, the safety data buses don't communicate between separation groups, No. 1.

MR. BETANCOURT: That's correct.

MEMBER BROWN: So, if you had a safety data bus with a bus master controlling it, blowing up one of the separation groups, that would not be a problem. And the only place we have an interaction between separation groups is right there, and that is not a bus master. It's a digital --

MR. BETANCOURT: It's a point-to-point --

MEMBER BROWN: It's a point-to-point --

MR. BETANCOURT: Fiber optic --

MEMBER BROWN: -- up/down, 1/0, whatever you want to call it, to the voting unit processor within the SVM.

MR. BETANCOURT: Correct.

MEMBER BROWN: So, I'm not trying to hammer my consultant here. Okay?

(Laughter.)

I'm trying to get a better understanding of why a specific problem with the state machine, or whatever they're called, since I have no idea what anybody is talking about when you do that, compromises this when you have that much separation or that much electrical -- that much independence between each separation group and any connection between separation groups is isolated to a 1/0-type, on/off signal, not a serial data link which is connected to a safety data bus.

MR. BETANCOURT: That's correct.

MR. HECHT: Do you want me to answer that?

MEMBER BROWN: You can try.

MR. HECHT: Okay.

MEMBER BROWN: As long as it's short.

CHAIRMAN CORRADINI: Yes, I was going to say --

MEMBER BROWN: And as long as I understand

it.

CHAIRMAN CORRADINI: -- you guys are way beyond stuff that I understand, but I do understand time. I do want to make sure we get through their presentation before lunch.

MEMBER BROWN: Myron?

MR. HECHT: All right. With the Chairman's permission, it's similar argument that you would make with software common-cause failures. And you could argue that you have all this isolation between separate processes on separate channels, and there can be several problems that can occur in the algorithms of those bus masters. I don't think they're simple. I don't remember seeing state machines that -- or that completely describe the bus master performance. And given the fact that all divisions are receiving the same signals in roughly the same sequence, there's just --

MEMBER BROWN: All separation groups.

MR. HECHT: Yes.

MEMBER BROWN: But they're not.

MR. HECHT: What? All separation groups.

MEMBER BROWN: They're separate.

MR. HECHT: Yes.

MEMBER BROWN: That's why I'm having a

hard time understanding.

MR. HECHT: Well, if you don't believe that it's credible that the separation groups are getting the same signals that could cause common problems, then --

MEMBER BROWN: But they're not getting the same signals. There's no connection of the safety data buses between separation groups.

MR. HECHT: But from the plant.

MEMBER BROWN: The only place you've got plant input is the detectors themselves. They've got independent sensors going to each one of the SFMs.

MR. TANEJA: They're not sharing anything. I mean, that's really the review, our review, on independence, was focusing on just those things that Charlie is highlighting. The independence is at the input level. Independence is in the cross-communication between the separation groups. Independence is at the EIM level, where it's really controlling the component. So, really, we are not doing any crosstalking other than the voting. That's the only crosstalking that's happening.

MEMBER BROWN: And that's not a data bus issue.

MR. TANEJA: Right.

MEMBER BROWN: That's the way I walked away from the HIPS meeting at the high level.

MR. TANEJA: That's a correct understanding that you have.

MR. HECHT: I think that that's true, but I guess the point is that the SFMs could react the same way to the plant inputs that they're getting.

MEMBER BLEY: Because of the logic inside them.

MR. HECHT: Yes.

MR. AYALA: Not necessarily. Because each SFM is different from each other. So, it's as if it has its own function. They don't share the same functions.

MR. TANEJA: So, I'll offer another solution to this thing. Okay? We were convinced, looking at the design, because of the divorced FPGA technology, that the potential for a common-cause failure of all four separation groups was reasonably -- reasonably -- low. Okay?

Now there is that "What if?" Right? So, we asked that question to ourselves, "What if the hell breaks loose and all four of them go crazy?" So, we have these manual system level actuations. Looking at the physics of the NuScale modules, they're very, very

slow transients. And you've got basically system-level actuation. You can trip the plant; you can initiate the DHRS; you can initiate the ECCS totally independent of the digital logic. They come in at the APL, and you can take care of that.

You know, you don't have to worry about any of these things working. I mean, that's the beauty of this whole plant that buys you that additional confidence that, you know, hey, manual actions are there as a defense-in-depth mechanism. They are always there for me.

But, you know, just staying focused on safety, we were okay with that.

MR. TABATABAI: I just want to clarify, when he says "beauty of this plant," he means I&C systems.

(Laughter.)

CHAIRMAN CORRADINI: I think we've got all sides of the argument. Can we move on?

MEMBER BROWN: Yes, we can move on.

MEMBER BLEY: Well, almost. This is real short. I want to take us back to the galvanic isolation.

I'm remembering back to the sixties where this first came up as an issue. And what it really

means -- I went back and double-checked a couple of things -- is, as somebody said, no copper connection between different electrical segments. We used to think we had separation if we had the batteries all separate, but, then, we had common grounds coming back. And we got ground loops and we got all kind of crap. So, it means no copper connections between them. It can be any other kind of connection, inductance, capacitance, light pipes, whatever, but no copper anywhere.

MEMBER BROWN: That's the way I read the ISO that we've got. They are electrically isolated because it's converted to an optical signal that goes from point A to point B.

MEMBER BLEY: And that problem was really a ground problem once upon a time.

MEMBER BROWN: Yes. Well, you can -- I hate to say this -- but if you have ground loops in your power supplies, if you do that particularly with auctioneered stuff, you can create huge problems.

MEMBER BLEY: Very interesting situations, too.

MEMBER BROWN: I mean, still situations you have to deal with in the design. Changing a wire from No. 12 to No. 4 bus bar can remove your common-

cause, your common-mode failures relative to little signals running along --

MEMBER BLEY: If you have copper connections.

MEMBER BROWN: If you have copper connections.

CHAIRMAN CORRADINI: We'll talk about this over lunch. Let's go.

(Laughter.)

MR. BASTURESCU: So, the second design principle we look at is redundancy.

MEMBER BROWN: We've got plenty of time.

(Laughter.)

We've got all day, Mike.

MR. BASTURESCU: This slide, this is the review of redundancy, which is commonly used in safety systems to achieve system reliability, goals, and conformity with a single failure criterion.

The HIPS platform is based on a triple module redundant architecture that provides for high reliable and full design, such as use of three safety buses, three voting modules, three bypass and schedule modules within a separation group and a division.

Use of redundant equipment interface modules for key safety application allows protection

against spurious actuations, fault tolerance, online testability, and supports self-diagnostics. Also, the PPS and the SDIS consist of two independent and redundant divisions.

MEMBER BROWN: Go ahead.

MR. BASTURESCU: The predictability and repeatability. This is the third I&C design principle we'll look at. Predictable and repeatable system behavior refers to a system that will produce the same output for a given set of inputs, input signals, within well-defined response time limits, to allow timely completion of actions.

The staff found that the MPS is designed to complete the reactor trip system and engineering safety feature actuation system function in less than or equal to one second, which satisfies the allocated time in the safety analysis of one second for these functions. And this is done in a predictable and a repeatable manner.

And if there's no other questions, I will turn it now over to Dawnmathews.

MR. KALATHIVEETTIL: Thank you, Sergiu.

Good morning, everyone. My name is Dawnmathews Kalathiveettil, and I will be resuming our presentation by diving straight into diversity and

defense-in-depth, or D3, as we like to call it in the I&C community.

So, the figure that you see in front of you is basically the module protection system, or MPS, design. As you can see, the MPS is made up of two separation groups for each division, and in total, there are four separation groups for the entire design. Division 1 is the yellow color, while division 2 is shown in red, so that it's easier to understand.

Let's start off with the inputs to the MPS. As you can see, on top, there's PTL, et cetera. That's the pressure-temperature level sensors. As you can see, these sensors come into the input submodule versus the signal condition A, B, C, et cetera. And they are additional sensors. They're analog sensors. But, for the purpose of D3 assessment, our focus on the sensors was mainly towards the digital-based sensors, and the ones that actually have safety functions related to it, and which could actually be affected by additional base common-cause failure.

These were identified to be the digital-base level pressure and flow sensors. However, the coping analysis demonstrated that, even if these additional sensors did have additional common-cause

failure, the plant can cope up with it.

To discuss the actual MPS, the FPGA portion of the safety function module, the communication module, and the equipment interface module are the only portions of the MPS that could be affected by additional common-cause failure. Hence, the MPS uses two diverse FPG architectures, like I said, in order to achieve this equipment diversity.

So, if division 1 is made up of one type of FPGAs, then division 2 would be made up of another kind. And the whole idea is that the same digital common-cause failure cannot simultaneously take out both divisions, and at least one division would be available to complete the required safety functions.

MEMBER BROWN: To be clear, the divisions are the bottom line, and the separation groups are the top line?

MR. KALATHIVEETTIL: Exactly. So, when it comes to the division level, what you see is the ESFAS and the RTS; whereas, in the separation group, you actually see it come through A, B, C, and D.

So, in addition to the equipment diversity that I just discussed, the diverse FPGA technologies also result in an associated level of design diversity, since FPGA vendors use different

development tools to provide the final configured FPGAs. These tools have inherent diversity due to the FPG architectures and the programming methods which are used.

The MPS also provides functional diversity for the use of protection logic on the safety function module, which Luis was trying to mention earlier. So, the way that they are, there are different functions associated with different safety function modules. So, the actual logic in that would be slightly different, which adds to more functional diversity.

MEMBER SKILLMAN: Dawnmathews, may I ask this question, please?

MR. KALATHIVEETTIL: Sure.

MEMBER SKILLMAN: How will a technician know the difference between an FPGA of one architecture versus an FPGA of a different architecture?

MR. BETANCOURT: As part of the identification requirement, they're supposed to be labeled in that throughout the plant either by markings or colors. So, that's how a technician will know what FPGA technology will be present in whatever division.

MEMBER SKILLMAN: That sounds great. So,

I'm a technician, and I put two of them in my pocket and I walk around for two afternoons. Then, I pull them out of my pocket and I say, "Oh-oh, what do I do with these?" How do I know which one goes where?

MR. BETANCOURT: We actually asked that question regarding, let's say, for example, that you have an SFM that pertains to separation group A, and by mistake, you want to put that into separation group B. So, the platform has these self-testing features that will be identify whether or not you're putting the wrong module to other cabinets. So, it will tell the operator, in that case an alarm, that you're putting the wrong SFM to whatever cabinet.

MEMBER SKILLMAN: Thank you. Thank you.

MEMBER BLEY: It will fit? Physically, it will fit? It's just you need the test --

MR. BETANCOURT: Correct.

MR. TANEJA: Also, physically, there are some modules that are designed to a -- there's a special key that won't let you plug them in.

MEMBER BLEY: That's really convincing if we --

MR. TANEJA: Yes.

MR. ARNHOLT: Brian Arnholt with NuScale Power.

What Luis said is correct, but, also, if you get to Corvallis and you look at the prototype, we can actually demonstrate it. But the cards, each card is physically keyed so that you cannot physically insert the one card in the wrong slot.

MEMBER SKILLMAN: Thank you.

MR. KALATHIVEETTIL: All right. So, the table here tries to explain the effects of additional base common-cause failure on the MPSes in diversity. There are three events which are shown in the table. A green tic basically implies that the particular module is available to do its function, while the cross just says that it's not available.

All right. So, let's look at event one, where the scenario is that you have a transient or a design basis event happening, but there is no common-cause failure. In that situation, you have the modules of all four separation groups available to perform their function. Event two is a situation where you have a transient or design basis event concurrent with an additional base common-cause failure.

And what is happening here is we are assuming that there is functional diversity of the SFM in addition to the equipment diversity. So, this is

only affecting the SFM in separation group A and C. As you can see, the communication module and the equipment interface modules of A and C, along with both B and D, are available to do their function.

And the final scenario is one where, once again, you have the common-cause failure, but in this case, for whatever reason, the entire separation group A and C modules are gone. So, the reason is that we are only considering equipment diversity, no more functional diversity. The particular kind of FPGA which is available in division 1 has been taken out, but you still have all the modules and the different type of FPGA in division 2 available to do the safety functions.

And just to add, in addition to this, like Dinesh mentioned earlier, you have the diverse system-level manual actuations which actually bypass the MPS logic. And so, if needed, that adds an additional level of diversity and defense-in-depth.

Next slide.

All right. So, simplicity has been a focus of NuScale design, and NuScale has been able to incorporate the fundamental design principles into its I&C architecture and the systems while adhering to simplicity.

This is very evident since the design uses simple reactor trip systems and ESFAS functions. There are no closed or open loops, and all safety-related functions are de-energized to actuate. In other words, the safety-related functions happen by the removal of electrical power.

MEMBER BLEY: I really liked this part. We wanted this to be one of the principles, but in many applications it's just not feasible, given the kind of systems people are buying. This is an excellent characteristic of this system.

MEMBER BROWN: It's a very subjective one, but it's also important.

MEMBER BLEY: It's subjective, but, boy, when you look at problems that crop up, you eliminate -- and the ability to review and understand and test -- you eliminate a lot of potential situations by having simplicity.

MR. KALATHIVEETTIL: All right. So, until now, we've talked quite a bit about the safety side of the NuScale design. On the non-safety side, the module control system and the plant control system are segmented to ensure that a failure of these non-safety systems does not adversely affect the MPS.

MEMBER BROWN: Okay. You can stop right

there, please.

MR. KALATHIVEETTIL: Okay.

MEMBER BROWN: I have a hard time understanding this. Since the MPS is separate, not communicated with, why does segmentation of the MPS and/or PCS affect the operation of the MPS if it's not segmented? I mean, that's a unidirectional -- if you look at your diagram, it's unidirectional and there's no feedback. The only feedback you ever get to is when you operate the enable safety control switch, where you can take manual control, which applies only getting into the APL or the actuation and priority logic.

MR. TANEJA: So, let me try to answer that, Charlie.

MEMBER BROWN: You're going to have to try real hard.

(Laughter.)

MR. TANEJA: I'll give you a good example. See, when the safety analyses are performed in Chapter 15, there are certain failures assumed. Loss of feedwater, for example, would be one failure, right, or turbine trip or turbine bypass values. So, those are the different design basis events that are postulated to see if the plant transient can deal with

that, right?

So, with the module control system, what we were looking for was could you have multiple failures or spurious failures on the module, you know, on the balance-of-plant side that can challenge safety from the thermal hydraulic point of view, not the electrical interfaces or not actuating equipment, but the impact on the thermal hydraulic of the plant. And that is really the concern here.

And I think, like NuScale presented this morning, that there were these five goals that they were trying to achieve from the segmentation, which was essentially looking at an impact to the reactivity, release of radiation. So, these were safety of the plant. So, they had to basically assign function to different segments, so they don't have a common-cause failure that they cut multiple functions and result in one of those unsafe conditions.

MEMBER BROWN: Yes, but that's a plant safety issue, not a response of the module protection system issue.

MR. TANEJA: It is a module protection system issue if you don't do it right. If you put controls on the same controller, multiple, you know, if you put like -- this morning I think Brian gave a

very good example of two functions being on the same controller would have resulted in unsafe plant conditions.

MR. ARNHOLT: Brian Arnholt with NuScale. I might be able to maybe clarify what Charlie is asking.

I think he's saying that there is no -- since we've isolated the MPS from the MCS, there's no possible maybe adverse feedback the other way. Is that your point?

MEMBER BROWN: Yes, it's you can't -- the MPS will respond to the input it gets. And you're not going to change that, regardless whether you have or don't have segmentation. Whether you have multiple plant systems failures that result in some analyzed transient that you haven't analyzed under your accident condition that the module protection system, even though it responds, doesn't result in adequate protection, you know, protecting the plant, that's not the MPS's failure. It's not a matter of compromising it. That's what I was trying to understand, but the segmentation does not --

MEMBER BLEY: Let me try to parrot what he said because it's something I brought up earlier. He's talking about the module control system. So, can

you drive the plant itself, the physical plant, from problems there into conditions that challenge the protection system, that get the plant in a situation that's beyond what's been analyzed?

MEMBER BROWN: But that's different from adversely affecting the MPS functions. It functions, but they may have missed a transient --

MEMBER BLEY: Well, it's different from adversely affecting operations within the MPS. It can affect the MPS function because you don't get what you expected to get other than --

MEMBER BROWN: Yes, I would --

MEMBER BLEY: But the problem seems a real one.

MEMBER BROWN: I understand your point, and I understand --

MEMBER BLEY: Are you arguing words or are you saying the problem is not a real one? I'm sorry to get us going.

You guys can just sit back and relax for a minute.

MEMBER BROWN: Well, no, no, that's right, we're having fun.

(Laughter.)

We're going to get there, Mike, don't

worry.

CHAIRMAN CORRADINI: But I want to make sure -- I don't hear it as substantive. I hear about you don't like how they word this, but --

MEMBER BROWN: No, I don't like the implication --

CHAIRMAN CORRADINI: Right.

MEMBER BROWN: -- that there is some failure in the MCS, whatever that is, that now can adversely affect the ability of the MPS to respond to its sensor inputs. That's all I'm saying. That is wrong.

MR. TANEJA: No, that is not what we are saying.

MEMBER BROWN: I totally understand that you can have compounding things in the MCS that could result in a plant response when the MPS does not have the proper inputs --

MR. TANEJA: Correct.

MEMBER BROWN: -- to respond. That's a different issue. That does not adversely affect the MPS functions. That's all. It's a little bit broad. This sends a message in your SER. They don't say that in Chapter 7, by the way. NuScale doesn't say that, but it is --

MR. TANEJA: No, it's a broad statement that we made. It is that the MPS functionality, whether it's not getting the correct input at the given situation -- so, the inputs are part of the MPS structure, you know. So, what we were saying was that, a transient on the balance of plant does not give me what I need to create a turbine trip, I mean a reactor trip or an ESFAS function, because the input conditions did not come in at the right time --

MEMBER BROWN: I understand that.

MR. TANEJA: Yes. Right.

MEMBER BROWN: I understand that. But, right now, we've got pressure-temperature level, neutron, whatever else would come in there. If you need another function to get generated because of some other combination of things, it won't be there because of the MCS failure. You're saying if you -- the way they physically -- if we had combined all these things in what I would have called "memory segmentation" only, with all the control functions tied up in a big pile of software, but they physically, at least what they said, they physically separated them out by processors --

MR. TANEJA: Right.

MEMBER BROWN: -- with their own

individual software. And that's a physical separation of the data.

MR. TANEJA: Right.

MEMBER BROWN: But even that doesn't give you a big -- it looks very difficult to have four of those things that you can control from the MCS with a common command set or software set. You've still got four different response systems downstream from what you can control. So, I just think we're working overtime on this.

CHAIRMAN CORRADINI: But I just want to make sure what we're arguing about. The way they state this here is what you're objecting to, not what they meant to say?

MEMBER BROWN: I don't like the message that somehow there's something that impacts the MPS and it doesn't. We may not have covered it from a protection standpoint, from a plant transient in terms of failures in the plant standpoint. We didn't provide enough input to the MPS. We didn't provide a proper --

MEMBER BLEY: It's not screwing with the MPS internally.

MEMBER BROWN: That's right. That's what this --

MEMBER BLEY: It's feeding it unexpected information.

MEMBER BROWN: And to me, this implies that an MCS failure can adversely affect it. And that's why we segment. That's not --

CHAIRMAN CORRADINI: Okay. Do you guys get it?

MEMBER BROWN: That's not why they're doing it.

CHAIRMAN CORRADINI: So, do you guys get it?

MR. TANEJA: Right.

CHAIRMAN CORRADINI: And you agree with it?

MEMBER BROWN: I understand what they did.

(Laughter.)

MR. ASHCRAFT: This is Joe Ashcraft. I just want to make a quick comment.

And so, maybe this slide is misleading. I think the overall, what they are trying --

MEMBER BROWN: Well, it's in the SER also.

MR. ASHCRAFT: I think what we're trying to say is that the MCS/PCS does not affect the MPS.

MR. KALATHIVEETTIL: It doesn't unnecessarily challenge it.

MR. ASHCRAFT: In other reviews that we've had that was a big issue. So, maybe it's not worded correctly here or maybe it's confusing, but that was the goal, to just ensure that the non-safety side does not impact the safety.

MR. BETANCOURT: This is it. I'm looking at Mike and the clock.

MEMBER BROWN: You don't want an MCS failure affecting three or four items that result in data not getting to the MPS that it needs to show protection for that set of failures. That's fundamentally what you're --

MR. BETANCOURT: I think we understand the comment. We're going to go back to the SE and find a better way to say it.

CHAIRMAN CORRADINI: That's probably the way to deal with it.

Okay. Let's move on.

MEMBER BROWN: What's next?

MR. KALATHIVEETTIL: All right. So, this is the 10 CFR 5062 exemption or the anticipated transient without scram exemption. The evaluation of this exemption was documented in Chapter 7 with assistance from Reactor Systems and the PRA Branches.

To give a brief history, NuScale requested

an exemption from the portion of the ATWS rule requiring diverse equipment to initiate a turbine trip under conditions indicative of an ATWS. They also stated that, since the design does not include an auxiliary or emergency feedwater system, the portion of the ATWS rule requiring diverse automatic auxiliary feedwater system initiation is not applicable to them.

Since the underlying purpose of the 10 CFR 5062 rule is to reduce the risks associated with ATWS events, staff evaluated three major aspects for this request.

First, staff evaluated how the design reduces the risk of an ATWS event through redundancy, diversity, and independence within the NuScale MPS. The built-in diversity of the MPS design reduces the probability of a failure to scram.

Secondly, the staff evaluated how the NuScale design responds to an ATWS event and found that the response is bounded by the design basis accident analysis.

Finally, staff's evaluation also showed that the MPS design results in an ATWS contribution to core damage frequency which is lower than the safety goal which is identified in the 10 CFR 5062 rulemaking documents.

Hence, staff concluded that the underlying purpose of the ATWS rule was met by the NuScale design.

MEMBER MARCH-LEUBA: Did NuScale submit a reference ATWS calculation? Because the SER mentions some numbers from Chapter 19 here and there, but I haven't seen a plot of what the ATWS response is. With respect to your bullet No. 2, how do you decide that an ATWS is better than anything in Chapter 15?

MR. KALATHIVEETTIL: We actually have Jim Gilmer here from Reactor Systems. He's the one who evaluated this portion of it.

CHAIRMAN CORRADINI: But we're going to see this, I guess --

MEMBER MARCH-LEUBA: Are we going to see it?

CHAIRMAN CORRADINI: Yes, we're going to see it.

MEMBER MARCH-LEUBA: That's the question. Are we?

MR. GILMER: Yes, Jim Gilmer, Reactor Systems.

NuScale has not submitted on the docket the calculation. However, during Chapter 19 audit as well as Chapter 15 audit, we reviewed all of their in

RELAP calculations and any supporting ANSYS stress analysis.

MEMBER MARCH-LEUBA: So, basically, we'll get to see that, Chapter 15 and Chapter 19 --

CHAIRMAN CORRADINI: If not, we're going to ask for it.

MEMBER MARCH-LEUBA: I'm not happy that there is no submitted on-the-record calculation for ATWS. It should be part of this.

MR. GILMER: I understand. We would like to see it, also, on the docket.

But the two particular ATWS acceptance criteria that were challenged in this design are the reactor coolant pressure, RCS pressure, and containment.

MEMBER MARCH-LEUBA: Yes.

MR. GILMER: And there were --

MEMBER MARCH-LEUBA: I'm willing to table it until Chapter 15 or 19.

CHAIRMAN CORRADINI: Okay. All right.

MR. KALATHIVEETTIL: Next slide.

All right. So, as the heading of this slide states, the purpose here is to address some of the ACRS comments from a NuScale Chapter 8 Subcommittee meeting.

First, there was a concern as to how the 24-hour timers were powered. The 24-hour timers are part of the MPS boundary. And so, they are powered the same source as the MPS is. The whole purpose of the 24-hour timers is simply to provide an ECCS hold mode and, also, any load-shedding which could, in turn, help with achieving their 72-hour capacity for the post-accident monitoring, or PAM-only mode.

Another concern was as to what happens if there are degraded voltage conditions. The MPS is capable of sensing any kind of degraded voltage condition, and if such a condition exists, then the MPS basically performs its safety function.

Next slide.

MEMBER MARCH-LEUBA: So, are you saying that MPS has an under-voltage sensor and a scram based on it?

MR. KALATHIVEETTIL: Yes, it actually had a predetermined value that it looks for. And the moment that it is hit, it actually goes ahead and does the RTS --

MEMBER MARCH-LEUBA: One of the scrams is local just to MPS?

MR. KALATHIVEETTIL: Yes. Yes, you are correct.

MEMBER BROWN: Okay. Is that separate from the timers?

MR. TANEJA: The degraded condition is not part of the timers. That is how the MPS is --

MEMBER BROWN: So, is there an under-voltage sensor that's fed into the MPS?

MR. ARNHOLT: Brian Arnholt with NuScale Power.

Yes, we monitor the AC voltage input to the EDSS battery chargers, and if we detect a low-voltage condition, there's logic within the MPS that will initiate a reactor trip, containment isolation, and decay heat removal system.

MEMBER BLEY: In fact, it's an ESFAS?

MEMBER MARCH-LEUBA: Is it --

CHAIRMAN CORRADINI: One at a time.

MR. ARNHOLT: Yes, both a reactor trip and an ESFAS function.

MEMBER BLEY: Back in the Chapter 8 meeting, we were concerned that what if the batteries didn't hold up as long as they're supposed to. Could we get individual valves drifting shut and weird stuff? And now, they're saying, well, you shouldn't because we have one more backup on the battery, and that's to initiate one of the safety functions.

MEMBER MARCH-LEUBA: But he said they're detecting the AC power coming from outside --

MEMBER BLEY: Which won't be there if we're running on batteries. So, it doesn't help us if we're on batteries.

MR. ARNHOLT: Now there's two parts to that. There's the AC voltage monitoring we perform, but also, if you remember, I mentioned we had those DC-to-DC power converters, those Class 1E isolation devices. Those monitor for any type of under-voltage or voltage-changing condition for the power feed into MPS. And just like they isolate --

MEMBER MARCH-LEUBA: So, if there's a drop in voltage, you also operate for that --

MR. ARNHOLT: A circuit breaker, for example, and then, they would remove power and isolate that power feed into the MPS as well.

MEMBER BLEY: And the setpoints on those are higher than the point at which, by testing, we know any of the valves would start to drift?

MR. ARNHOLT: Correct.

MEMBER BLEY: Is that true?

MR. ARNHOLT: That's true.

MEMBER BLEY: Where is the test reports?

MR. ARNHOLT: Oh, we haven't those -- we

haven't gotten that far yet. That's not --

MEMBER BLEY: You're going to test that? We'll be interested in seeing the test results.

MEMBER BROWN: I also did not read -- is there something in Chapter 7 or in, I guess Chapter 7, that talks about the sensor inputs, one of the under-voltage -- that's input to the MPS system?

MR. BETANCOURT: Yes. So, if you look under the DCD, there's a Table 7.1-4 that shows, and then, Table 7.1-3 that shows all of the inputs and the parameters for the ESFAS and RTS. So, Table 7.1-3 --

MEMBER BROWN: This is in the Chapter 7?

MR. BETANCOURT: Right. Reactor trip functions, and Table 7.1-4, Engineered Safety Features, Actuation System Functions. So, you will see those parameters to be on both of them.

MEMBER BROWN: Okay. I just missed that when I went through it. Okay. Thank you.

MR. KALATHIVEETTIL: This was the first time that staff used the design specific review standard, Chapter 7, to review an application. The approach of DSRS Chapter 7 resulted in a simple I&C architecture and HIPS design, while incorporating the fundamental design principles. The approach also resulted in the completion of the Safety Evaluation in

an efficient and effective safety-focused manner.

In conclusion, the staff finds that the I&C design is safe and that it complies with all the applicable NRC regulatory requirements.

MEMBER BROWN: And I have another question. Actually, I have two questions. Sorry, Mike. We've got a lot of time, three minutes.

Multi-unit stations, you all concluded that the setup and the controls, and everything, that multi-unit station setup is okay?

MR. KALATHIVEETTIL: Yes.

MEMBER BROWN: My question is, when do we see an evaluation of how people actually control the plant using this? Is that going to be in Chapter 18, HNI, or whatever it is?

MR. BETANCOURT: So, we reviewed the Chapter 21 input and RFCR in Chapter 7, but I think that will be for Chapter 18 and Chapter 15 it could be addressed.

MEMBER BROWN: But I didn't get much out of the multi-unit station discussion.

MR. BETANCOURT: Right.

MEMBER BROWN: It just says the I&C systems and the distributed control systems, et cetera, et cetera, provide the ability to control all

these things. It didn't say how am I going to control 12 modules with one DC system.

MR. BETANCOURT: Right.

MEMBER BROWN: How many operators do I need to do --

MR. BETANCOURT: So, that's a Chapter 18 topic.

MEMBER BLEY: And I understand, I've heard that the way they're doing that has evolved from what we saw several years ago when we were out there, which was three people in the control room, one guy running all the plants and, then, dropping them off. And it was pretty interesting. It worked very well. But we're really interested in seeing that whenever it comes up.

MEMBER BROWN: So, it's really Chapter 18?

MR. BETANCOURT: Yes.

MEMBER BROWN: Okay. All right. That's question one.

CHAIRMAN CORRADINI: Wait a minute. Now you brought it up, so it's your fault.

(Laughter.)

So, has the staffing regimen for the multi-units been settled or is it still an issue that's a policy issue to the Commission? I'm trying

to understand how many people are watching how many modules. It kind of interacts with the questions you were asking.

MEMBER BROWN: No, that's part of it, yes.

CHAIRMAN CORRADINI: Has that been settled and it's in the DCD, settled for review?

MR. TABATABAI: I cannot answer that question. Actually, I'm not the PM for Chapter 18. So, I don't want to provide --

MR. BERGMAN: Tom Bergman, NuScale.

That's still an active part of the review.

CHAIRMAN CORRADINI: Fine.

MR. BERGMAN: The staff has just recently observed some of our operator training. They have another audit coming out to see more of the testing. So, we haven't heard any concerns specifically raised, but it is still under review by the staff.

MEMBER BLEY: Tom, is it spelled out in the DCD now or is it --

MR. BERGMAN: Is what spelled out?

MEMBER BLEY: How they're going to operate or how you expect them to operate.

MR. BERGMAN: I don't know that the number of operators is specifically in the DCD. It will be in the appendix that certifies the design, Part 52.

So, the regulatory approaches are appendix and Part 52, which say COLs that incorporate this design by reference follow this approach in lieu of that in 5054(m). And that will say our approach is six operators will be in front, plus a senior reactor operator, STA, and supervisor. But, just like you saw when you were there, they are still the three people at the desks.

MEMBER BLEY: Okay. Thanks.

CHAIRMAN CORRADINI: Charlie, I'm sorry. You had one more question, Charlie?

MEMBER BROWN: Yes, but I've got to find it here.

Yes, it's you all had a comment or a paragraph where you talked about the MPS is an FPGA-based system. Traditional watchdog timers do not provide the same protections for FPGA systems as they do in microprocessor-based systems. The MPS addresses the need for "alabness," although I couldn't find that word anywhere, via the self-testing features of the MPS modules, EGVF-FM. In other words, it's under the built-in self-test features.

But, when I went and looked at that, all I could find was that throughout the testing you have individual -- at least the way I read it, each

individual piece has some type of an identification of its alabness or --

MR. BETANCOURT: Correct.

MEMBER BROWN: But there's no beginning-to-end check that anything ever finishes a complete cycle anywhere.

MR. BETANCOURT: Right.

MEMBER BROWN: In other words, from start to finish. I'm not talking about repeatability. Just the things actually get to the end.

MR. BETANCOURT: The feedback.

MEMBER BROWN: That's right. As you get with the watchdog timer. In other words, you're stepping through -- I mean, FPGA still has to go through and process data, result into a vote, and something has to happen.

MR. BETANCOURT: Right.

MEMBER BROWN: But there's nothing that says that that actually gets completed, other than individual pieces along the way.

MR. BETANCOURT: So, you're correct. Like the way that they are designed, it's like a piecemeal way.

MEMBER BROWN: Very piecemeal.

MR. BETANCOURT: Right. But, then, you

will still get that feedback at the control room that the actuation, or whatever function you're trying to activate --

MEMBER BROWN: If you actuate, but you don't actuate the protection.

MR. BETANCOURT: Right.

MEMBER BROWN: You don't actuate the trip systems.

MR. BETANCOURT: Right.

MEMBER BROWN: So, you don't ever know whether the thing is being voted and a signal is being out to the EIM.

MR. BETANCOURT: And that's where the piecemeal comes into play. It's like each one of the modules will actually do like a cross-check against each other. So, in other words, the EIM may be expecting a signal from one of the separation groups, and if it doesn't come in in the allotted time, it will send out an alarm, hey, I was expecting --

MEMBER BROWN: Where are those alarms identified?

MR. BETANCOURT: The specific alarms?

MEMBER BROWN: Chapter 7?

MR. BETANCOURT: Like you're talking about the failure?

MEMBER BROWN: Yes, I'm trying to figure out, if I don't say that I complete data processing from data input in whatever the sample size, you know, whatever the sample period is from beginning to end, and I either get a signal that either doesn't arrive or does arrive at an EIM -- I don't know what the endpoint is. Obviously, you don't want to actuate anything.

MR. BETANCOURT: I believe we had an RAI --

MEMBER BROWN: Or outputs from the voting unit that says, I'm finished; nothing's there; I don't have to trip. Something ought to be telling you that I have finished it somewhere.

MR. BETANCOURT: I believe there was an RAI and an ASAI, but it was clearly delineated, that concern, what is a safe state of a failure, whatever module. And I know that we had that on the SER. And there's a table that shows what is the safe state that is expected for each one of the modules.

MEMBER BROWN: I understand the safe state, but how do I know that it doesn't get to safe state? Is there an alarm triggered and where is the alarm specified?

MR. ARNHOLT: I might be able to help.

Brian Arnholt from NuScale Power.

I've got to be careful with what I say here because a lot of this detail is proprietary of how it works. But if --

MEMBER BROWN: I don't want to know how it works. I just want to know whether an alarm goes off if it doesn't complete a processing cycle --

MR. ARNHOLT: Yes, it does.

MEMBER BROWN: -- in 50 millicycles.

MR. ARNHOLT: The answer to your question is yes.

MEMBER BROWN: And where is that stated? That's not proprietary. That just means --

MR. ARNHOLT: That's a part of our self-testing and diagnostics that described in the HIPS Topical Report.

CHAIRMAN CORRADINI: And if you want more detail, let's do it after lunch in the closed session.

MEMBER BROWN: I guess I'll want more detail.

CHAIRMAN CORRADINI: I figured you did.

MEMBER BROWN: We can talk about it after lunch.

(Laughter.)

CHAIRMAN CORRADINI: Okay.

MEMBER BROWN: Because I don't remember -- I remember the BIST for each individual piece, but I never saw a start; I don't remember and could not find. I went and took a quick look at Rev 1 of HIPS, and I'm not going to talk about that anymore right now, but I couldn't find anything.

CHAIRMAN CORRADINI: Okay.

MEMBER SKILLMAN: Mike --

CHAIRMAN CORRADINI: No, no, I want to make sure I had the members --

MEMBER BROWN: That's my last --

MEMBER SKILLMAN: I have a question, sir, Mr. Chairman.

You have not introduced slide 23. Please do it. On this slide. You had to have been there to understand why this change in regulation came in 1980-1981. I recognize this is not a full P and it's not a full B. This is a hybrid in shutdown because this is a PWR with a very, very low pressure.

But I will tell you, from having been there in the control room, if you do not know what your pressurized level is, you do not know the condition of your core. And so, I don't know why staff finds pressurizer level not necessary. I understand you might say it's not necessary to achieve

cooling, but it's vital to understand the status of the core.

MR. BETANCOURT: And what I believe, that the intent of how NuScale is set to address this is that they're not relying on pressurizer level indication to get that function. They're relying on the RCS flow instead of the pressurizer level indication to be able to meet the intent of that regulation. So, they're saying that we still meet the intent, not using the pressurizer level indication. We're using the RCS flow indication to be able to verify there's natural circulation throughout the core.

CHAIRMAN CORRADINI: But I think what Dick is saying is, whether I'm a B or a P, in the P I find pressurized level, and if it's a B, I have a level indication in the reactor. What I think he is bothered by is I have neither.

MEMBER SKILLMAN: Bingo.

MR. TANEJA: Yes, the regulation, for regulation's sake, they don't need that information. But it is a post-accident monitoring variable that is available. The pressurizer level I believe is one of the variables that is displayed on the safety indication and display panel. So, it is one of the --

MR. ARNHOLT: One point of clarification. Brian Arnholt, NuScale Power.

The post-accident monitoring variable for this function is RPD riser level. And that's what we use to monitor inventory within the reactor vessel.

CHAIRMAN CORRADINI: The riser level is what -- where is that measured? That's within the downcomer after the steam generators?

MR. ARNHOLT: The riser is the central column of water coming out of the core.

CHAIRMAN CORRADINI: Oh, I'm sorry, just the opposite. What I call the shroud in the BWR. Okay. Fine. Okay. So, it's within that, which is physically below where the pressurizer control is?

MR. ARNHOLT: Correct. But that's our direct measurement for whether we --

MEMBER SKILLMAN: And would one put on the record that that is an adequate and accurate representation of the hydraulic level above the core? That's a yes or no.

MR. ARNHOLT: Could you repeat the question, please?

MEMBER SKILLMAN: Yes. Would one communicate that that riser level is an adequate and accurate indication of the hydraulic level above the

core?

MR. ARNHOLT: Yes.

MEMBER SKILLMAN: Thank you.

CHAIRMAN CORRADINI: Other comments by the members?

(No response.)

Okay. I think at this point I'd like to --

MR. BETANCOURT: Can I break up all of the actions that we have to do? Sorry. Or you want to do that after --

CHAIRMAN CORRADINI: Well, I think I want to go to public comments.

MR. BETANCOURT: Okay.

CHAIRMAN CORRADINI: We can do that, because we're going to have a closed session, and we'll have a full more, I'm sure.

Okay. So, I'd like to get the phone line open, if we could, please.

OPERATOR: The bridge is open.

CHAIRMAN CORRADINI: Thank you.

So, are there any members of the public out there who would like to make a comment at the end of our open session?

(No response.)

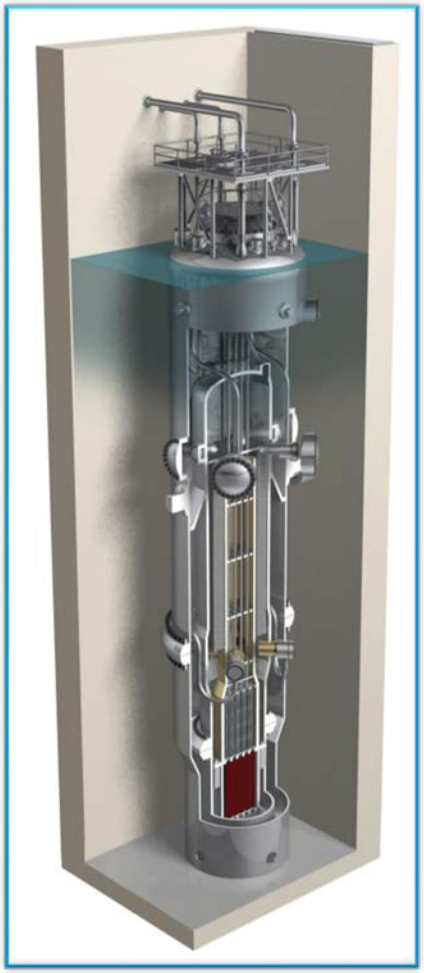
Okay. Hearing none, could you close the outside line?

And I want to ask, anybody in the audience that would like to make a comment?

(No response.)

Okay. Hearing none, we will break for lunch, and we'll come back at 1:15. I think that's okay if we give ourselves an additional five minutes, ten minutes. Okay? We'll see you back here at 1:15, and it will be in closed session.

(Whereupon, the foregoing matter went off the record for lunch at 12:09 p.m. and went back on the record in closed session at 1:16 p.m.)



ACRS Presentation: NuScale Instrumentation and Controls Design Overview

Brian Arnholt
Supervisor, I&C Engineering
Rufino Ayala
I&C Engineer
Paul Infanger
Licensing Project Manager

August 23, 2018

PM-0618-60212
Revision: 0

Template #: 0000-21727-F01 R4

Purpose

- Provide an overview of the NuScale Instrumentation and Control (I&C) systems and highlights of the I&C systems design described in NuScale Final Safety Analysis Report (FSAR) Chapter 7

Abbreviations

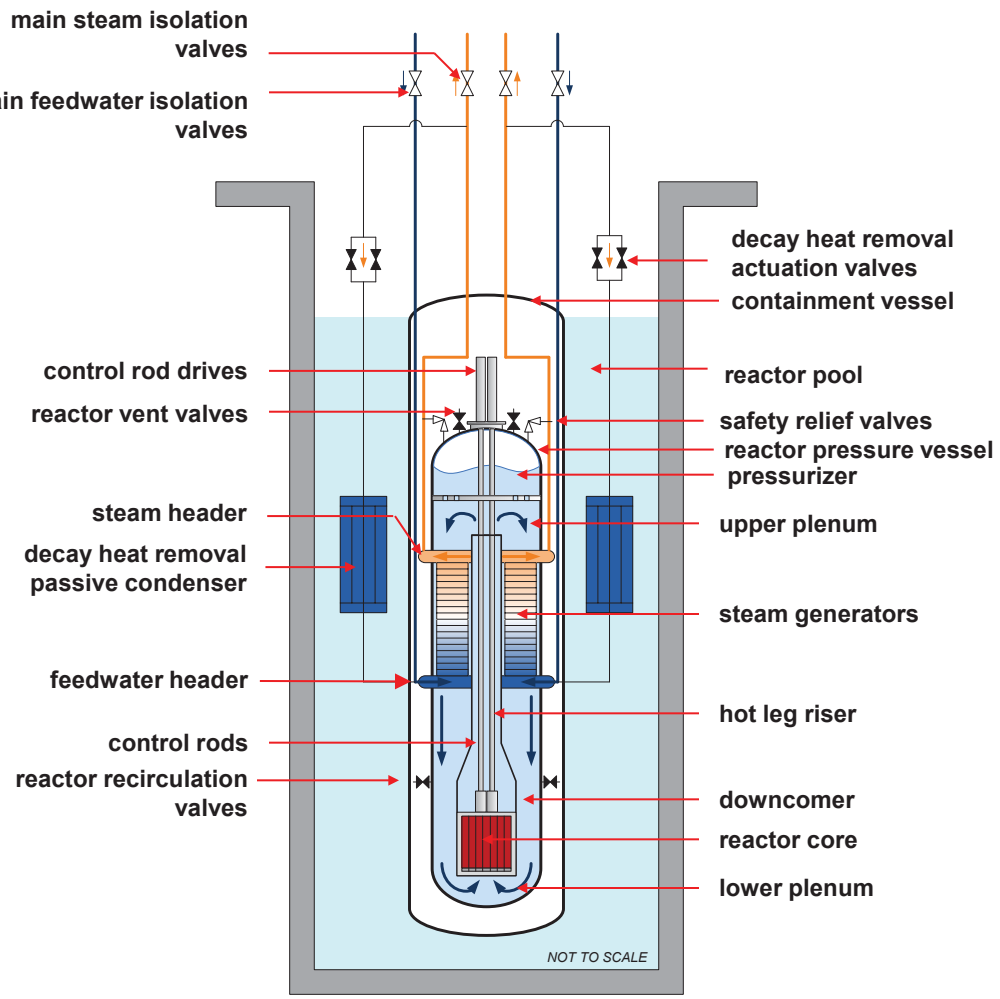
APL – actuation and priority logic
ASAI – application specific action item
CCF – common cause failure
CFDS – containment flood and drain system
CIS – containment isolation signal
CNT – containment system
CVCS – chemical and volume control system
D3 – diversity and defense-in-depth
DI&C – digital instrumentation and control
DHRS – decay heat removal system
ECCS – emergency core cooling system
EDSS – highly reliable DC power system
EDNS – normal DC power system
EIM – equipment interface module
ELVS – low AC voltage power system
ESFAS – engineered safety features actuation system
FPGA – field programmable gate array
HIPS – highly integrated protection system
HWM – hard-wired module
I&C – instrumentation and controls
ICIS – in-core instrumentation system
IEEE – Institute for Electrical and Electronics Engineers
ISM – input sub-module
MCS – module control system
MIB – monitoring and indication bus
MIB-CM – MIB communication module
MPS – module protection system
NPM – NuScale Power Module
NMS – neutron monitoring system
PAM – post-accident monitoring
PCS – plant control system
PPS – plant protection system
RMS – radiation monitoring system
RTB – reactor trip breaker
RTS – reactor trip system
SBM – scheduling and bypass module
SDB – safety data bus
SDIS – safety display and indication system
SFM – safety function module
SVM – scheduling and voting module
UTB – under the bioshield

NuScale DCA Chapter 7 Structure

- NuScale Chapter 7 Design Certification Application Follows Design Specific Review Standard Framework
  - Section 7.0: Instrumentation and Controls - Introduction and Overview
    - System Architecture and Overview
    - Key System Descriptions
  - Section 7.1 Fundamental Design Principles
    - Independence
    - Redundancy
    - Predictability and Repeatability
    - Diversity and Defense-in-Depth
    - Simplicity
    - Hazards Analysis
  - Section 7.2 System Features
    - Design and system characteristics in accordance with IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" and IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers and Safety Systems of Nuclear Power Generating Stations"

Section 7.0: Instrumentation and Controls - Introduction and Overview

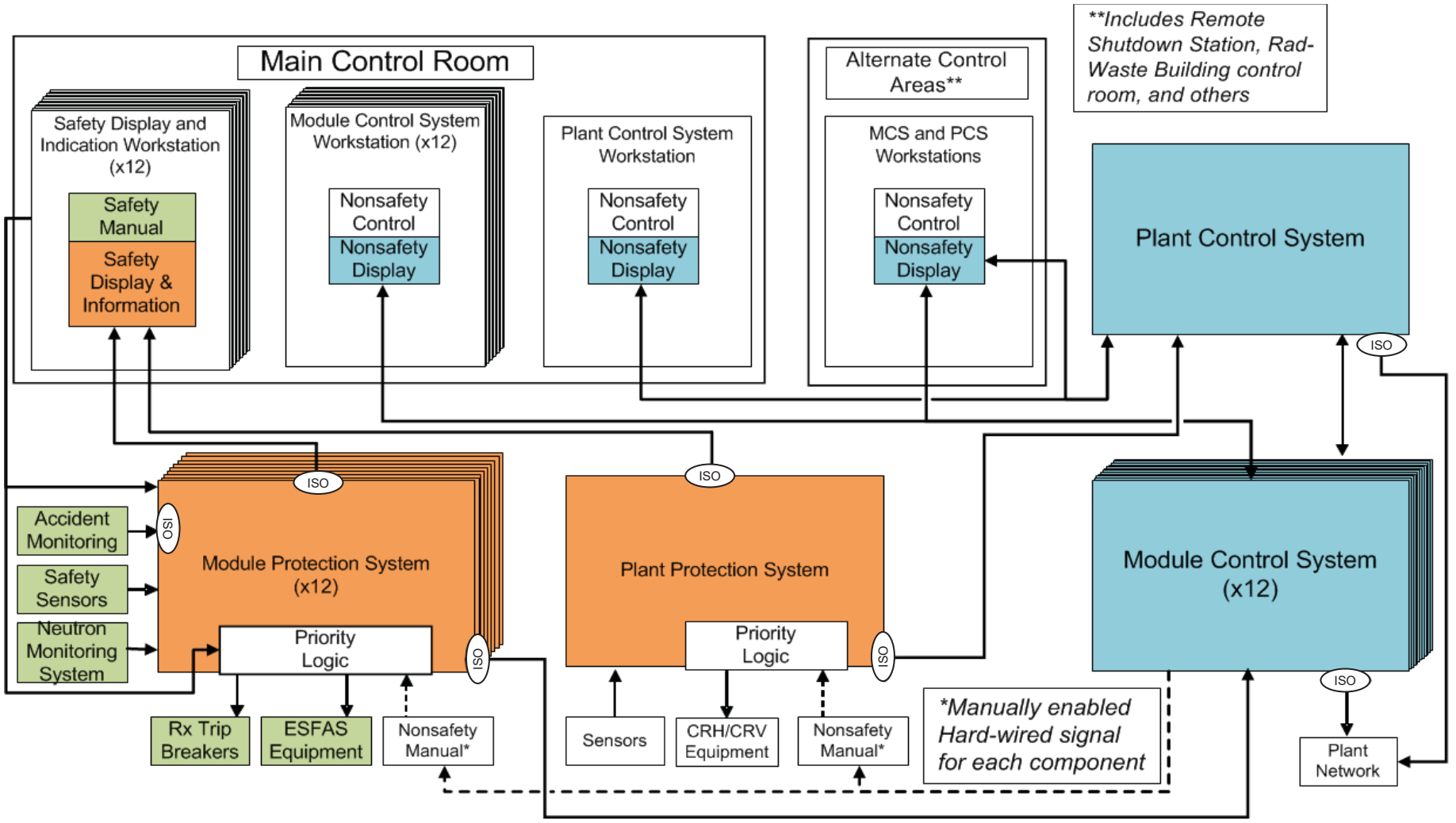
I&C System Design Basis



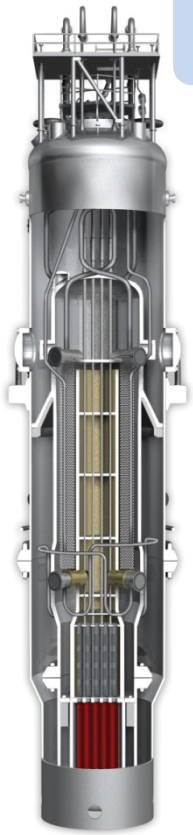
Safety I&C Platform

- Digital I&C system
- Use of FPGAs allows for diversification within the safety I&C platform
- Passive safety features result in a simpler safety I&C platform
- A simpler and more diversified design results in a more reliable safety I&C platform
- No safety-related pumps or fans to control
- Provide reactor trip breaker and pressurizer heater breaker trip signals
- Provide trip signals to solenoid operated valves
- On “loss of power” solenoids de-energize and associated valves fail in the “safe” position and reactor trip and pressurizer heater breakers open

I&C Architecture Overview



Module-Specific I&C Systems



Module Protection System (MPS) — Digital FPGA-based

The MPS is a digital, FPGA-based system that monitors process variables and provides automatic initiating signals in response to out-of-normal conditions, providing protection against unsafe NPM operation during steady state and transient power operation. Each NPM has a single dedicated MPS — A1

Neutron Monitoring System (NMS) — Analog

The neutron monitoring system (NMS) is an analog system comprised of three sub-systems:

- NMS-excore subsystem provides neutron flux data to the MPS for reactor trips — A1
- NMS-flood subsystem provides information to the MPS for post-accident monitoring during conditions when CNV is flooded — B2
- NMS-refuel subsystem provides neutron flux signals to the PCS during refueling operations (plant-level) — B2

Module Control System (MCS) — Digital-distributed control system

The MCS is a distributed control system which provides the Human System Interface and controls for monitoring and control of NPM specific plant components that are associated with the NPM balance-of-plant control functions. — B2

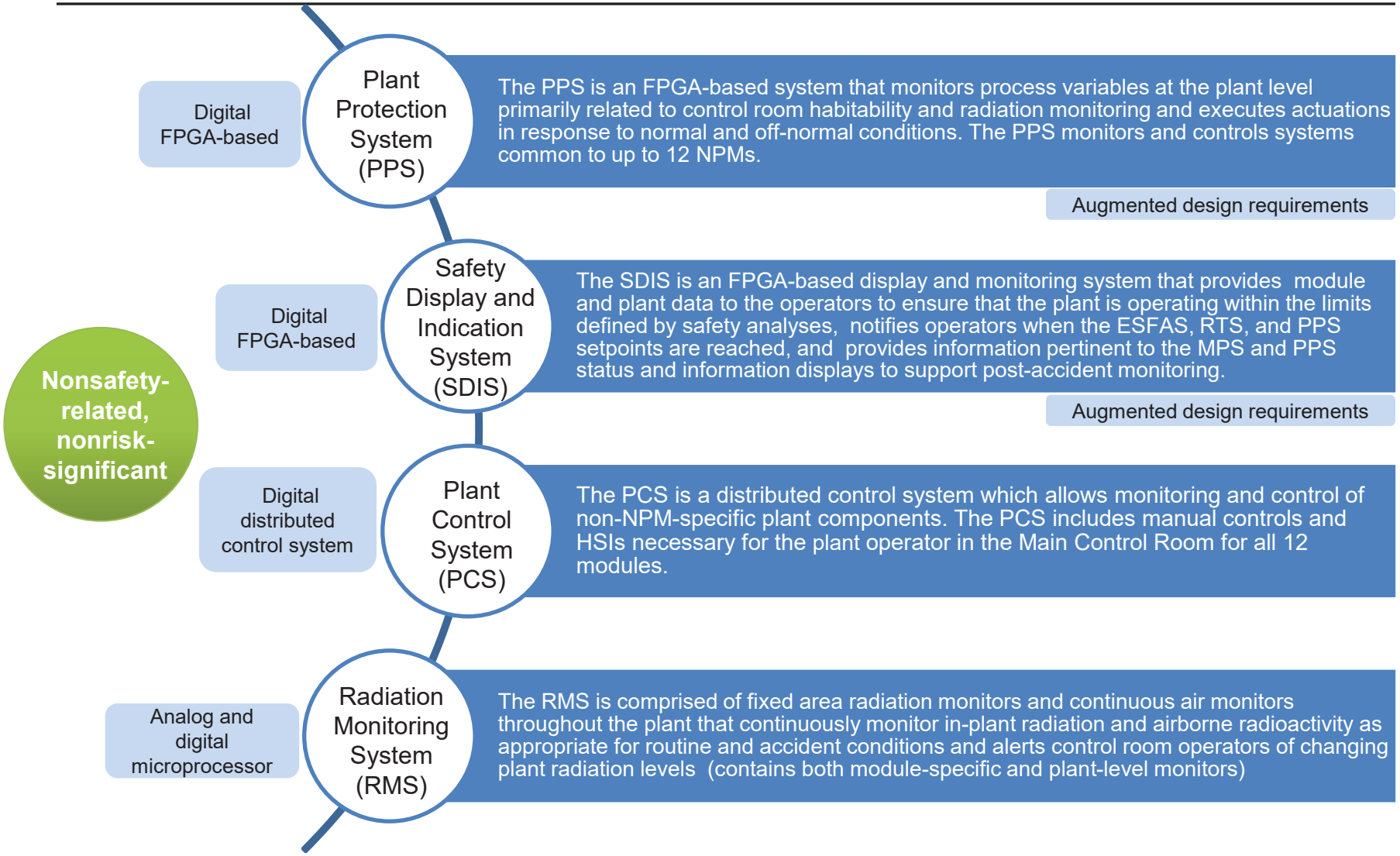
Incore Instrument System (ICIS)

The ICIS monitors the neutron flux distribution within the reactor core and provides core inlet and exit temperature information to the MPS for monitoring core cooling during post-accident conditions — B2

A1 - Safety-related, risk-significant

B2 - Nonsafety-related, not risk-significant

Plant-Level I&C Systems

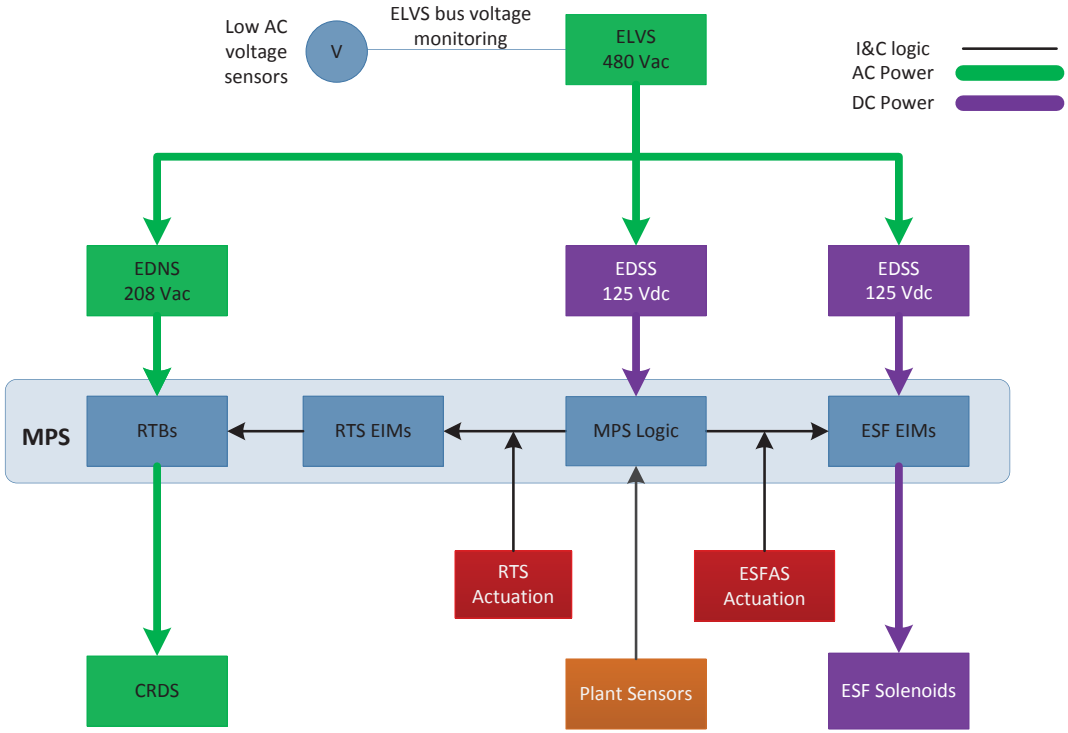


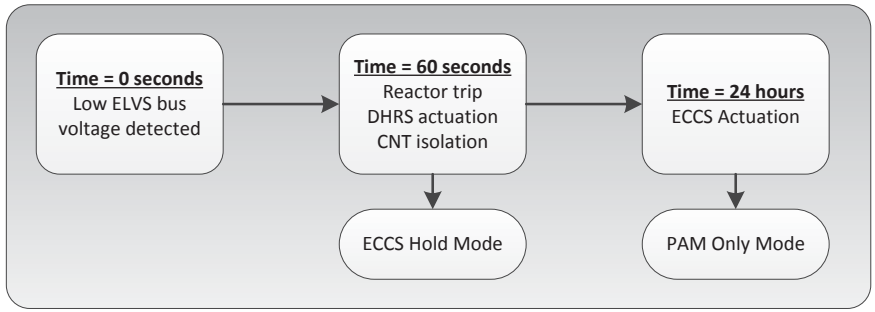
Module Protection System

- The NuScale safety-related MPS design is based on topical report TR-1015-18653-P-A, “Design of the Highly Integrated Protection System Platform” (HIPS TR).
- The safety-related I&C systems design basis conforms to the following without deviation or exceptions:
  - IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”
  - IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers and Safety Systems of Nuclear Power Generating Stations”
  - Staff Requirements Memorandum to SECY 93-087, “"Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-water Reactor Designs"
- Major components:
  - Four separation groups of sensor inputs, electronics and trip determination
  - Class 1E DC-DC power converters/isolation devices
  - Reactor trip and pressurizer heater trip breakers
  - Two divisions of RTS and ESFAS voting and actuation components
  - Two divisions of hard-wired manual actuation switches
  - Nonsafety-related 24 hour timers
  - Nonsafety-related maintenance workstations
- MCR isolation switches provided in Remote Shutdown Station.

Loss of AC Power

- NuScale I&C Architecture provides for nonsafety-related post-accident monitoring (PAM) functions.
- Performed by MPS, PPS and SDIS and MCS for Type B, C and D, and other systems for Type E
- MPS “PAM-only” mode supports long-term PAM variable monitoring
- Sensors that support long-term PAM functions remain energized for 72 hours.
- Battery Mission Times
  - EDSS-MS Channel A & D – 24 hours (ECCS Hold Mode)
  - EDSS-MS Channel B & C – 72 hours (PAM Support)
  - EDSS-C Division I & II – 72 hours (PAM Support)





HIPS TR Application Specific Action Items

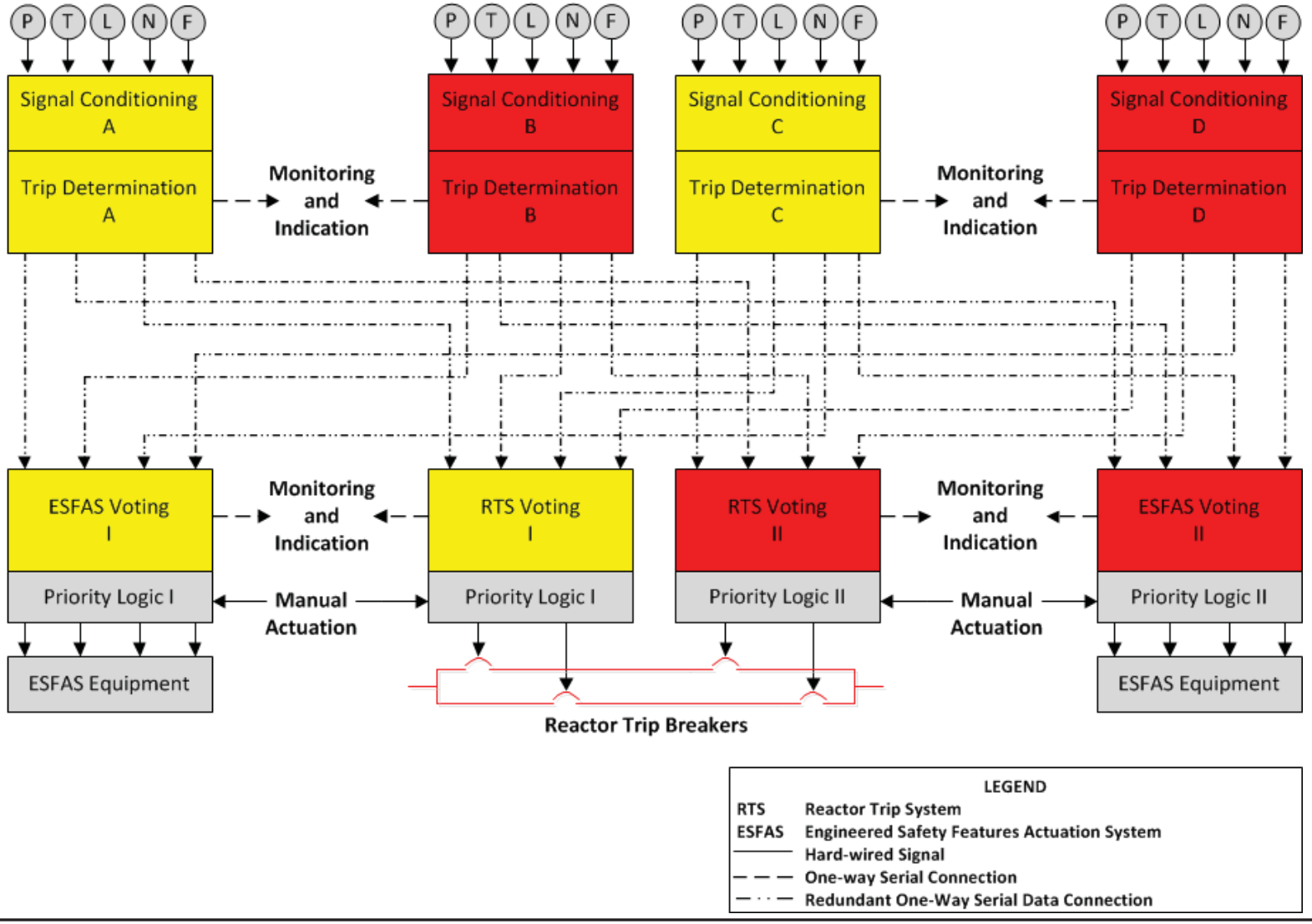
- FSAR addresses all 65 ASAIs in HIPS TR.
- FSAR Table 7.0-2 provides cross-references for all 65 ASAIs from HIPS TR.

Table 7.0-2: Highly Integrated Protection System Topical Report (HIPS TR) Application Specific Information Cross References

HIPS TR Application Specific Action Item Number	Section 7.0 - Introduction and Overview				Section 7.1- Fundamental Design Principles								Section 7.2 - System Characteristics													
	7.0.1	7.0.2	7.0.3	7.0.4	7.1.1	7.1.2	7.1.3	7.1.4	7.1.5	7.1.6	7.1.7	7.1.8	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5	7.2.6	7.2.7	7.2.8	7.2.9	7.2.10	7.2.11	7.2.12	7.2.13	7.2.14	7.2.15
1	x				x																					
2				x																						
3[1]					x																					
▪ ▪ ▪																										
▪ ▪ ▪																										
▪ ▪ ▪																										
63									x																	
64									x																	
65									x																	

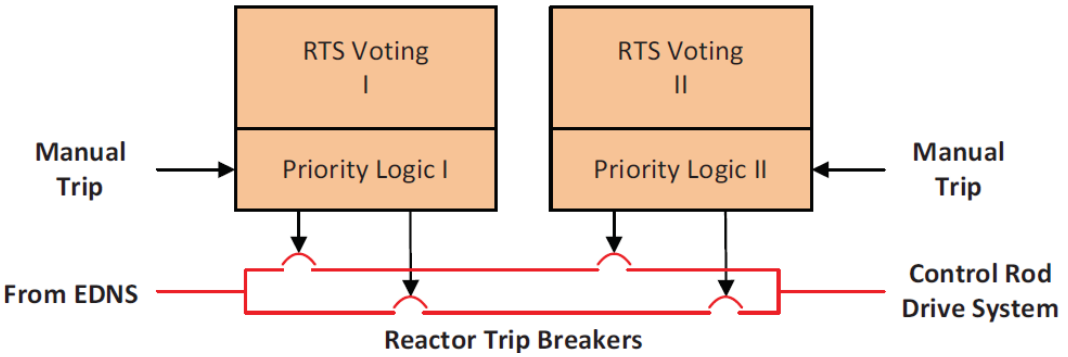
Note 1: For ASAIs 3 through 6, the overall conformance of the MPS to IEEE Std 603-1991, IEEE Std 7-4.3.2-2003, Digital I&C ISG-04 and SRM for SECY-93-087 is described in Section 7.1.1.

MPS Top-Level Architecture

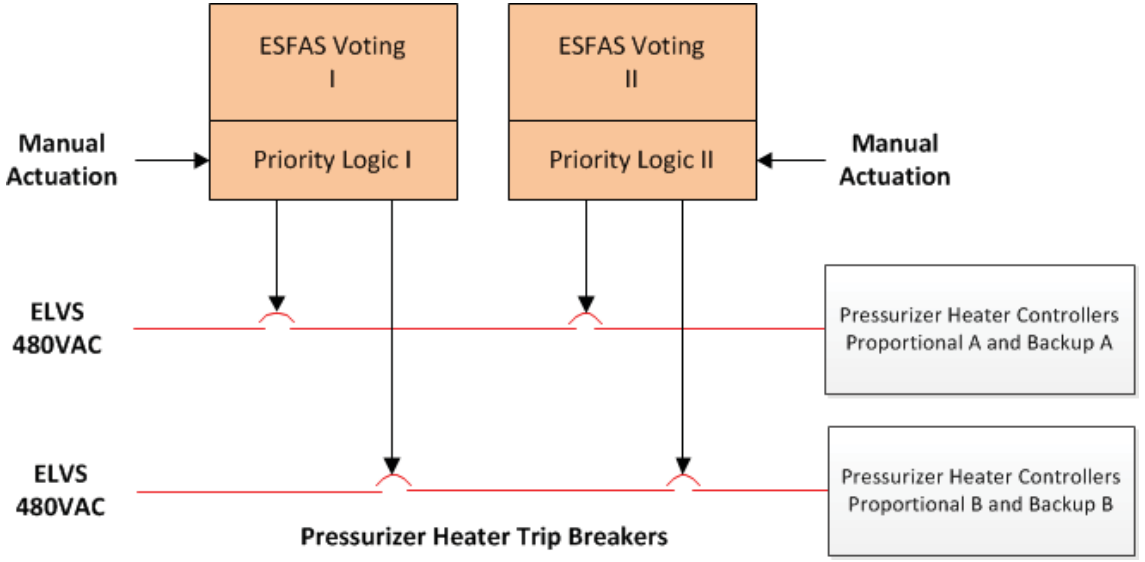


MPS Breaker Configuration

- Four reactor trip breakers, two per division



- Four pressurizer heater trip breakers, two per division



Each breaker opens upon loss of power to the under voltage coil.
A shunt trip coil is provided as a nonsafety-related diverse means to open the breakers

Nonsafety System Segmentation

- Segmentation is used as a defensive and preventative measure in the MCS architecture. Segmentation provides functional independence between major control functions preventing against a failure in one controller group from causing an undesirable condition in another controller group.
- Preventive and limiting measures are determined by a susceptibility analysis that considered malfunctions and spurious actuations, as set forth in NRC DI&C-ISG-04, Section 3.1, staff position 5.
- Control groups were evaluated for effect on:
  - reactivity addition to the reactor coolant system
  - primary coolant pressure increase or decrease
  - primary coolant temperature increase or decrease
  - primary coolant level increase or decrease
  - radioactive material release to the environment

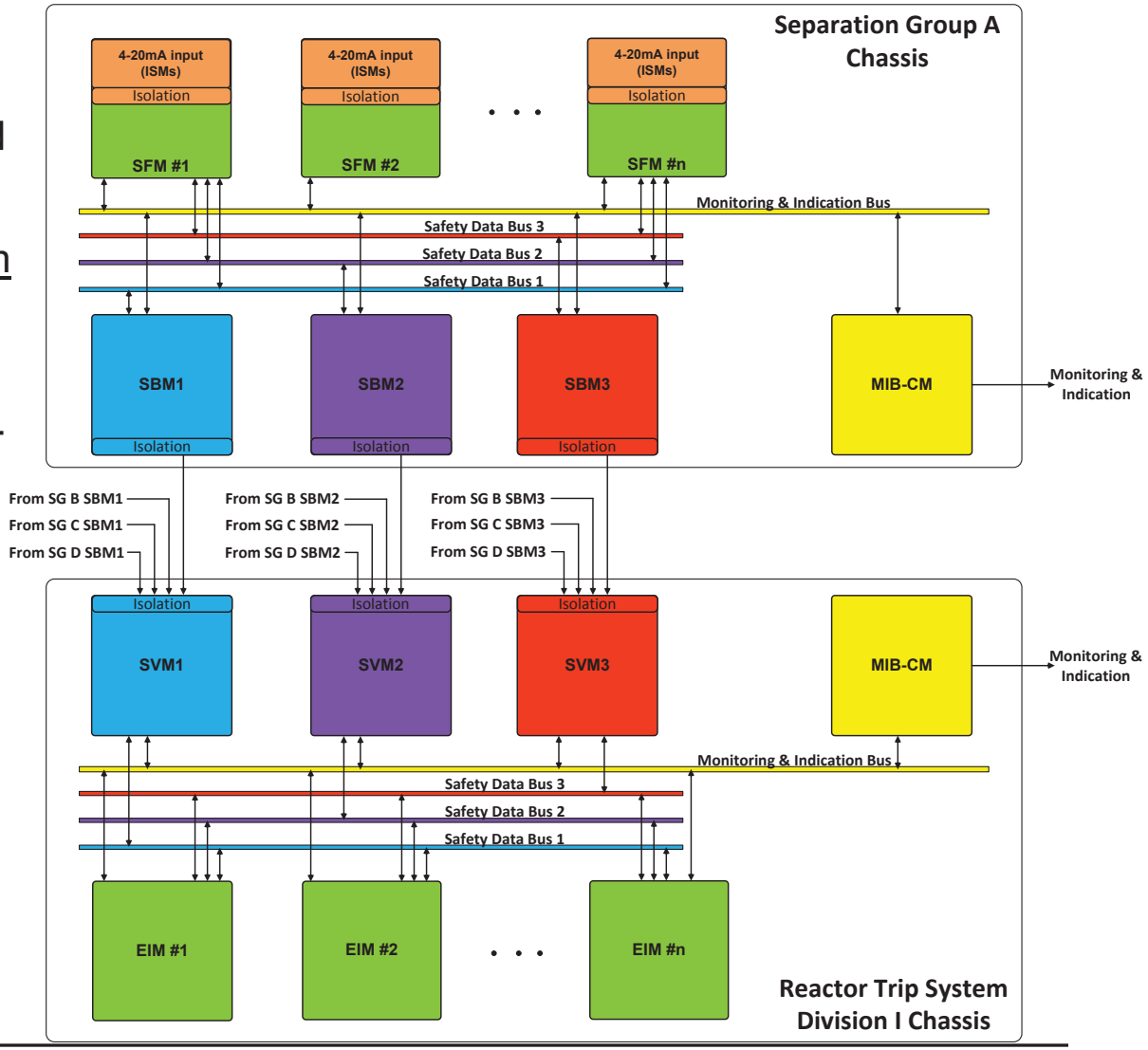
Section 7.1 Fundamental Design Principles

Fundamental Design Principles

- Independence
- Redundancy
- Predictability and Repeatability
- Diversity and Defense-in-Depth
- Simplicity

Independence

- The MPS and NMS are designed with physical, electrical, communication and functional independence.
- One-way communication from safety to nonsafety systems through isolated data paths.
- Separation of safety and non-safety communications on different communication busses.
- MCS control of safety-related components via hard-wired isolated inputs from MCS (no digital signals)



Safety Data Paths (1, 2, 3)
Safety Data Path 1
Safety Data Path 2
Safety Data Path 3
Monitoring and Indication Path

PM-0618-60212
Revision: 0

Template #: 0000-21727-F01 R4

Redundancy

- FSAR Section 7.1.3
- Four separation groups, two divisions of MPS
- Four channels of safety-related NMS
  - MPS and NMS meet single failure criterion
- Post-accident monitoring channels
  - No PAM Type A variables
  - PAM Type B and C variables meet single failure criterion
- Nonsafety I&C Systems incorporate redundancy principles for high reliability, asset protection

Predictability and Repeatability

- FSAR Section 7.1.4
- The MPS applies the deterministic features of the HIPS platform.
- The MPS response time is accounted for in the plant safety analysis actuation delays.

Diversity and Defense-in-Depth

- FSAR Section 7.1.5
- D3 strategy relies on platform/technology diversity for defense against common-cause failures
  - diversity for the platform technology is achieved through different FPGA chip technologies and their associated development tool sets
- Approach simplifies the D3 Diversity Assessment and narrows scope of coping analysis required for digital-based sensors.

Sensor Diversity

- Coping Analysis performed (summarized in FSAR Table 7.1-18) to address potential digital-based CCF vulnerabilities associated with digital-based sensors for pressure, level and flow measurements.
- Coping analysis included a full evaluation of all design basis events analyzed using best-estimate methods to analyze a postulated digital-based sensor CCF.
  - In some cases, the event never progressed to a trip condition using best-estimate analytical methods.
  - In other cases, diverse, non-digital sensors initiated the trip condition.

Result → D3 coping analysis acceptance criteria met

Section 7.2 - System Features

Control of Access

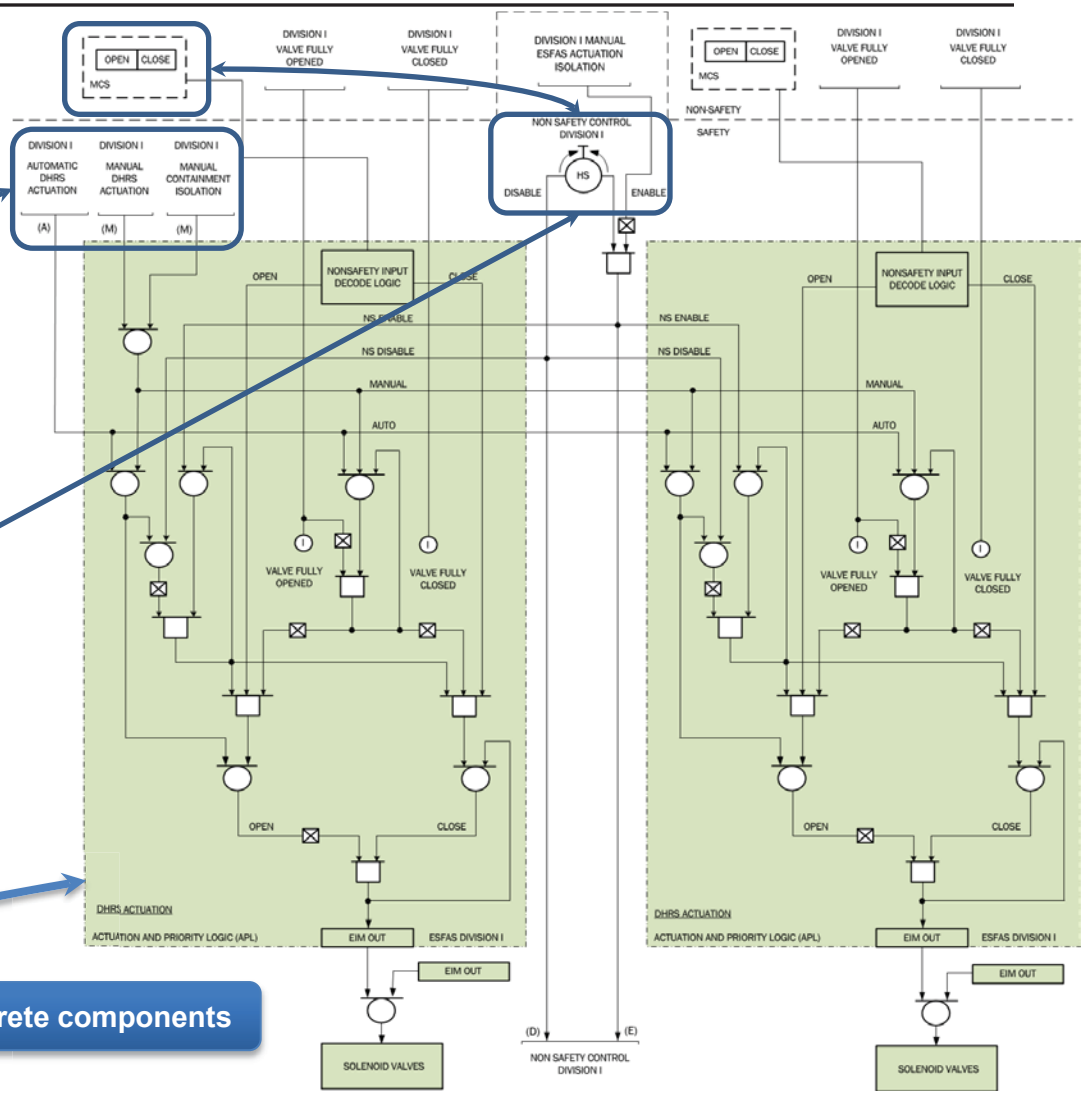
- MPS design conforms to IEEE 603-1991, Section 5.9, “Control of Access” and Secure Development and Operational Environment requirements of Regulatory Guide 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Revision 3.
  - Physical protection: locked cabinets/rooms.
  - MPS design does not provide for remote access capability.
  - Physical and logical controls prevent modification of MPS FPGA Logic while in service.
  - Limited set of MPS tunable parameters (i.e., setpoints) can be modified when SFM is bypassed and special equipment is used.

Automatic and Manual Controls

- All MPS RTS/ESFAS functions occur automatically.
- MPS provides for manual actuation via hard-wired switches in main control room as backup to automatic functions:
  - reactor trip
  - ECCS actuation
  - decay heat removal actuation
  - containment isolation
  - demineralized water system isolation
  - chemical and volume control system isolation
  - pressurizer heater trip
  - low temperature over pressure protection

Actuation Priority Logic

- APL circuit provides for prioritization of safety-related signals
  - Automatic/Manual RTS/ESFAS actuation commands have highest priority.
  - Enable control of safety-related components from nonsafety-related MCS via Enable Nonsafety Control Switch MCS hard-wired interfaces



Non-digital (no software) circuit -- comprised of discrete components

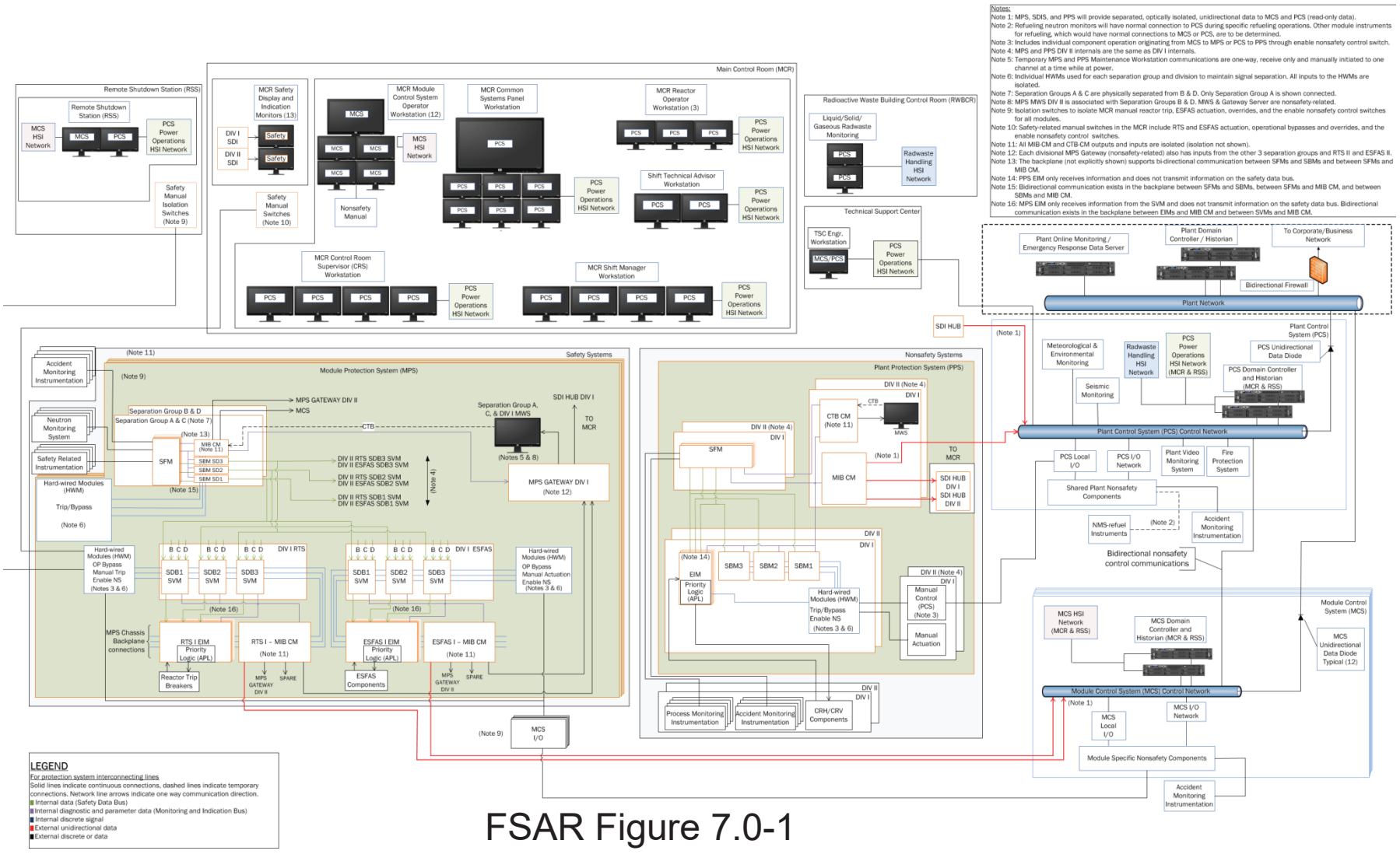
Conclusion

- NuScale FSAR follows the new Chapter 7 DSRS structure
  - Overall resulted in more streamlined, efficient review.
- The NuScale I&C design meets regulatory requirements contained in IEEE 603-1991, IEEE 7-4.3.2-2003 and SRM to SECY-93-087.
- The I&C architecture and systems incorporate the fundamental design principles with an overall focus on simplicity.
- NuScale passively safe design results in a simple I&C design solution – no complicated functions
  - Simple RTS/ESFAS functions (simple comparators, simple functions)
  - No closed/open loop control – all safety-related functions are “de-energize to actuate”
  - Safety function is accomplished by the removal of electrical power (e.g., reactor trip breakers open on loss of power)

Appendix:

FSAR Figure 7.0-1, I&C Architecture Diagram

NuScale I&C Architecture



FSAR Figure 7.0-1

Portland Office
6650 SW Redwood Lane,
Suite 210
Portland, OR 97224
971.371.1592

Corvallis Office
1100 NE Circle Blvd., Suite 200
Corvallis, OR 97330
541.360.0500

Rockville Office
11333 Woodglen Ave., Suite 205
Rockville, MD 20852
301.770.0472

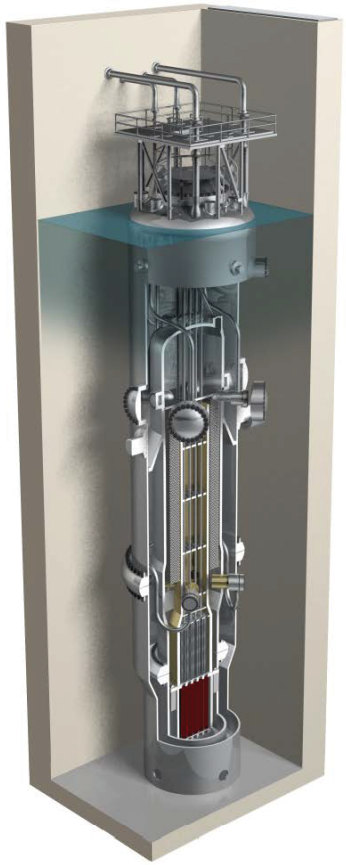
Charlotte Office
2815 Coliseum Centre Drive,
Suite 230
Charlotte, NC 28217
980.349.4804

Richland Office
1933 Jadwin Ave., Suite 130
Richland, WA 99354
541.360.0500

Arlington Office
2300 Clarendon Blvd., Suite 1110
Arlington, VA 22201

London Office
1st Floor Portland House
Bressenden Place
London SW1E 5BH
United Kingdom
+44 (0) 2079 321700

http://www.nuscalepower.com
Twitter: @NuScale_Power



NUSCALE™
Power for all humankind

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Safety Evaluation with Open Items: Chapter 7, Instrumentation and Controls

NuScale Design Certification Application Review

ACRS Subcommittee Meeting
August 23, 2018

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

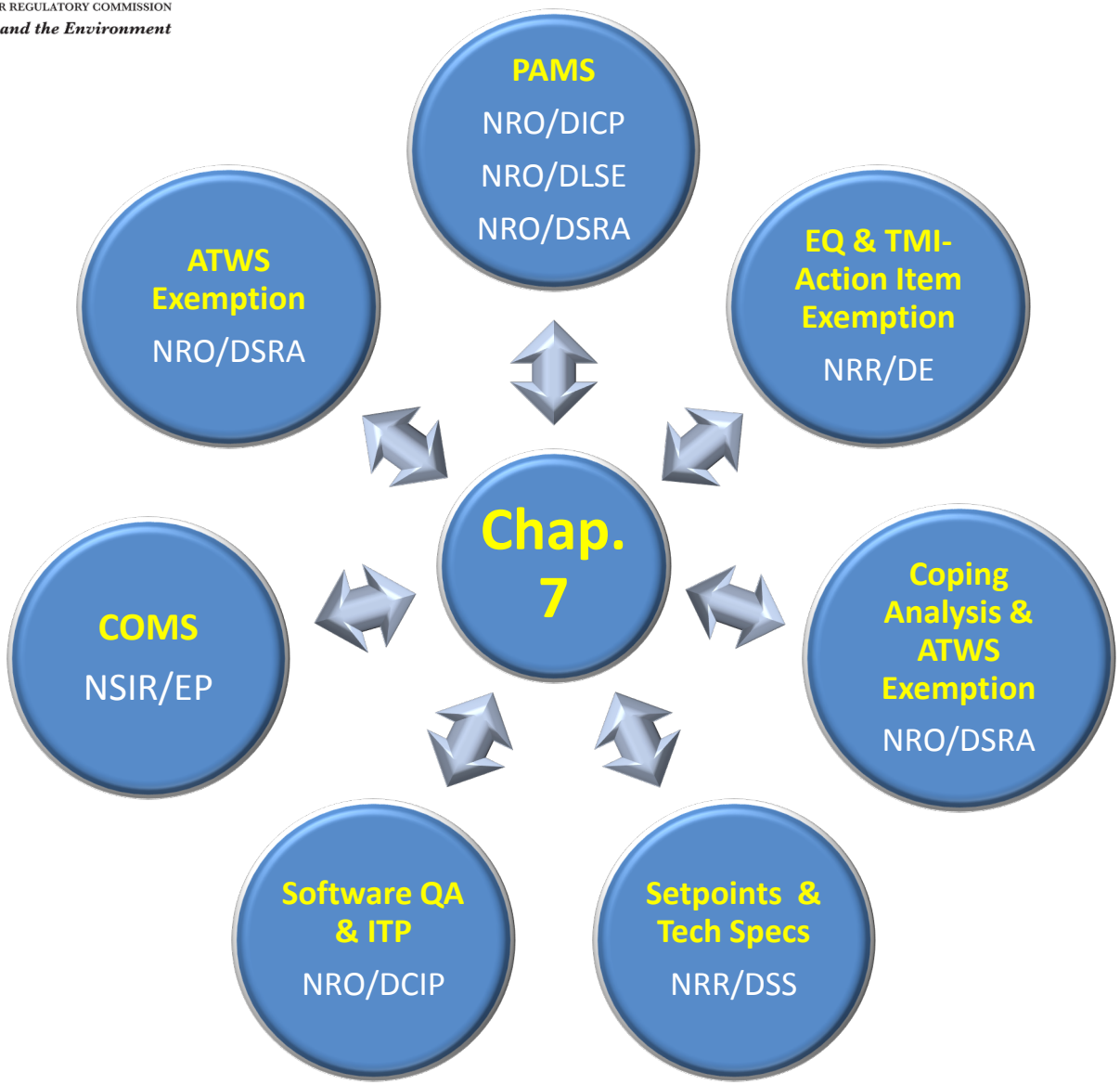
Agenda

- Background
  - NRC Staff Review Team
  - NRC Staff Interfaces
  - Timeline
- Safety Evaluation
  - Safety-Focused Review
  - Instrumentation and Controls Overview
  - Fundamental Design Principles
  - Non-safety-related Systems Segmentations
  - Exemption Request to 10 CFR 50.62(c)(1)
- ACRS Comments on Chapter 8 Subcommittee Meeting
- Conclusions

NRC Staff Review Team

- Technical Staff
  - Joseph Ashcraft, NRO
  - Sergiu Basturescu, NRO
  - Luis Betancourt, NRO
  - Derek Halverson, RES
  - Dawnmathews Kalathiveettil, NRO
  - Dinesh Taneja, NRO
  - Yaguang Yang, RES
- Project Manager
  - Gregory Cranston, Lead Project Manager
  - Omid Tabatabai, Chapter Project Manager

NRC Staff Interfaces



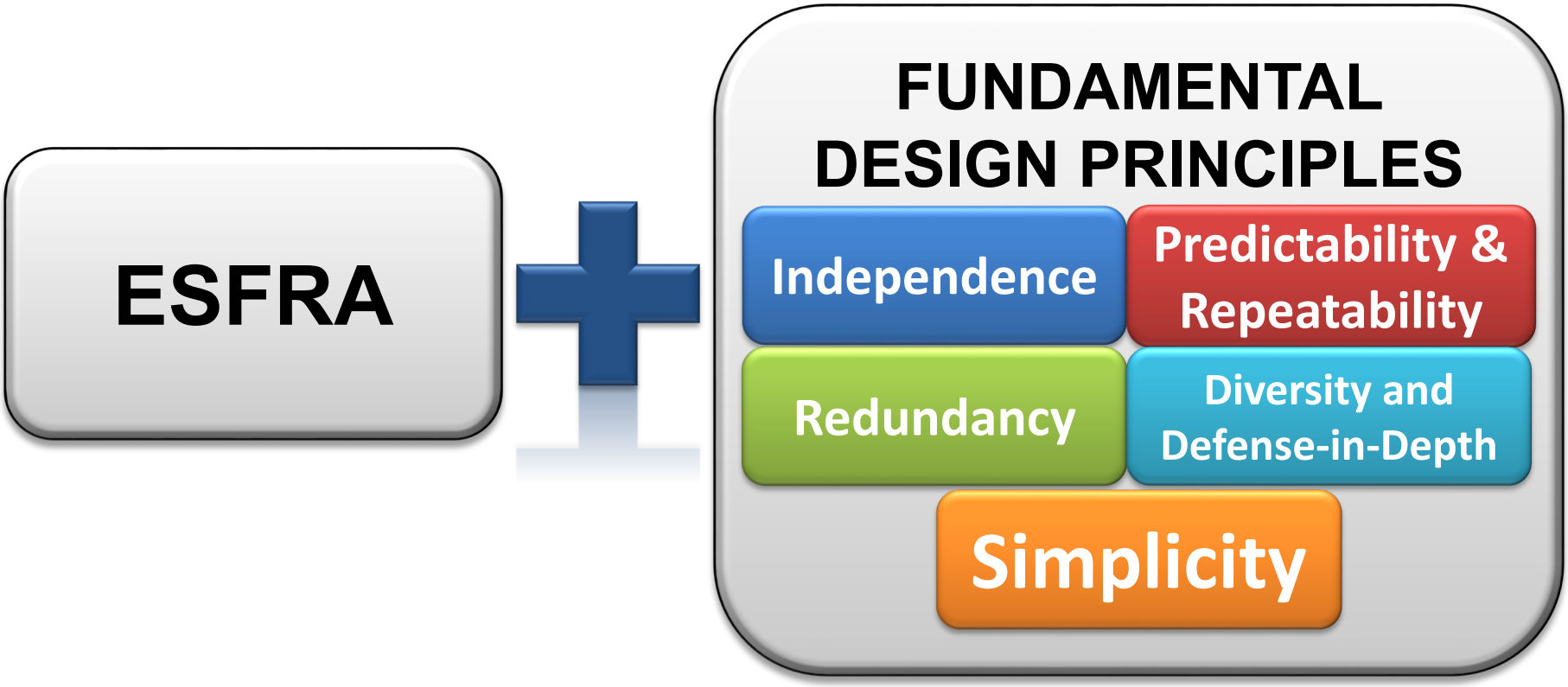
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Timeline

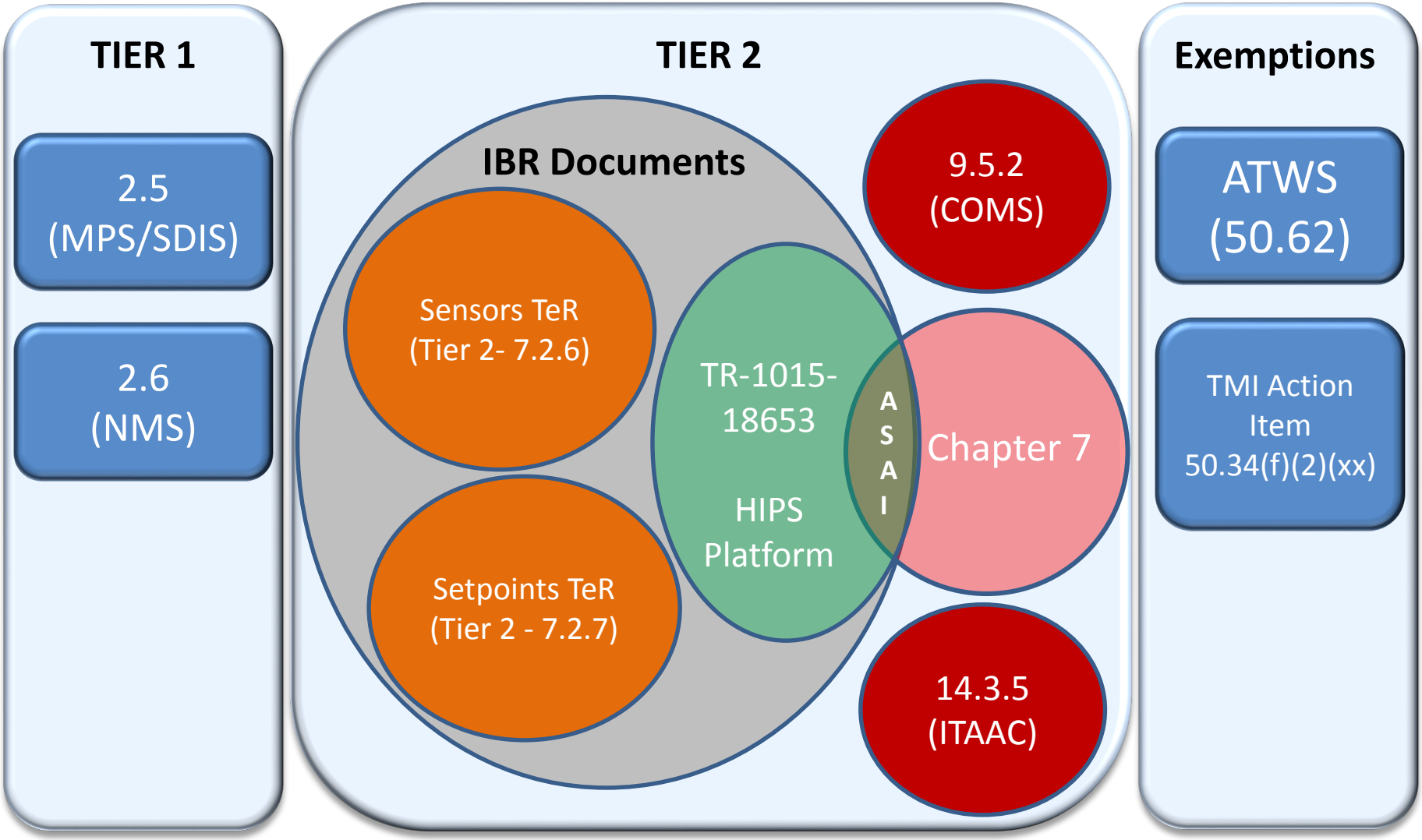
Date	Activity
2014 – 2016	Pre-application Activities
September 2016	Readiness Review
March 2017	Accepted Revision 0 of the DCD for Review
April 2017	ACRS Full Committee Meeting on HIPS Platform Topical Report
March 2017 – December 2017	Held 5 Public Meetings / Issued 9 RAIs / Completed 1 Audit
January 2018	Draft SE with Open Items Completed
March 2018	Applicant Submitted Revision 1 of the DCD
April 2018	All Confirmatory Items Incorporated into Revision 1 of the DCD
August 2018	ACRS Subcommittee Meeting
September 2018	ACRS Full Committee Meeting

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

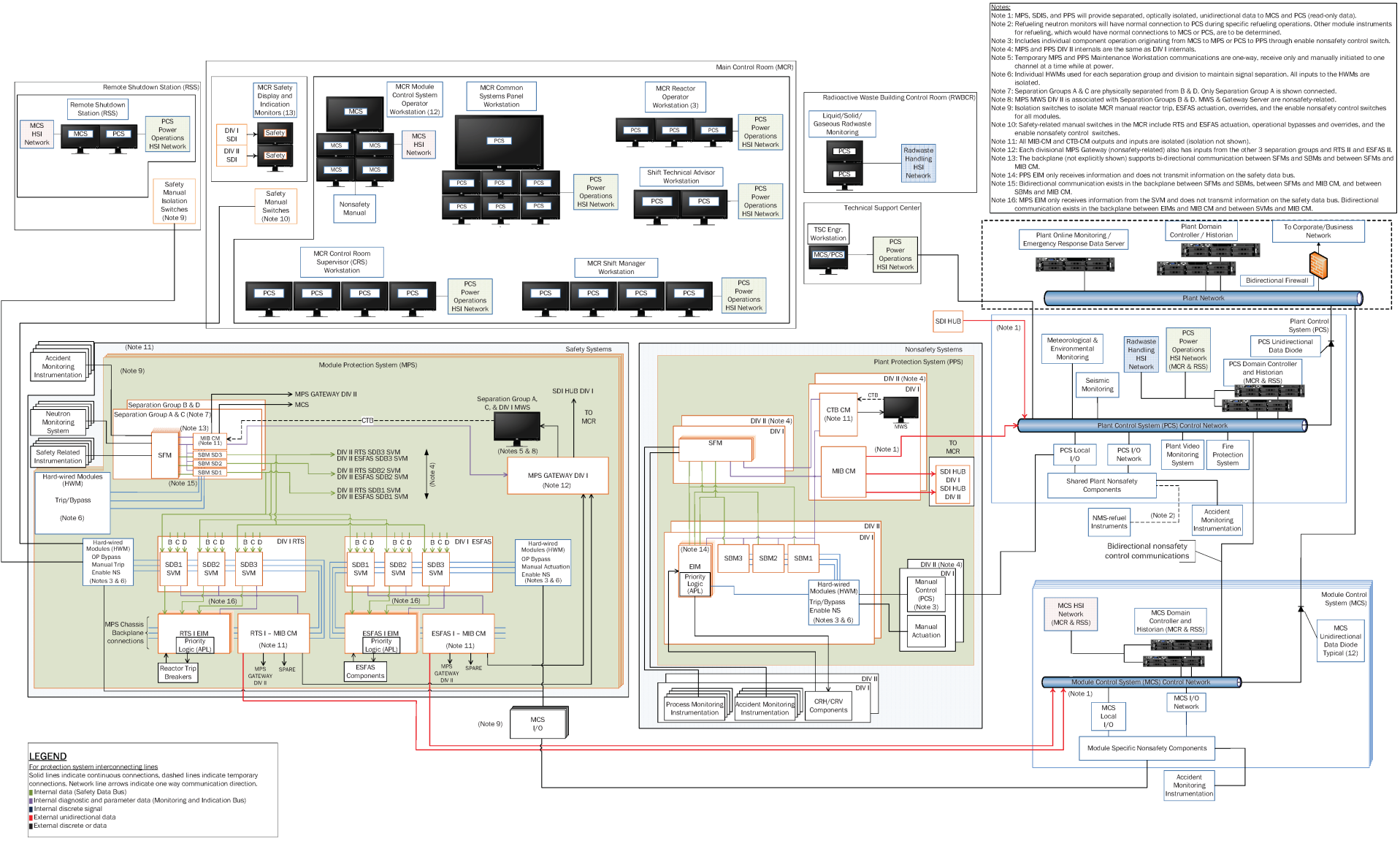
Safety-Focused Review



NuScale DCD Evaluation



NuScale I&C Architecture



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

Safety Classification

A1

MPS & NMS

A2

None

B1

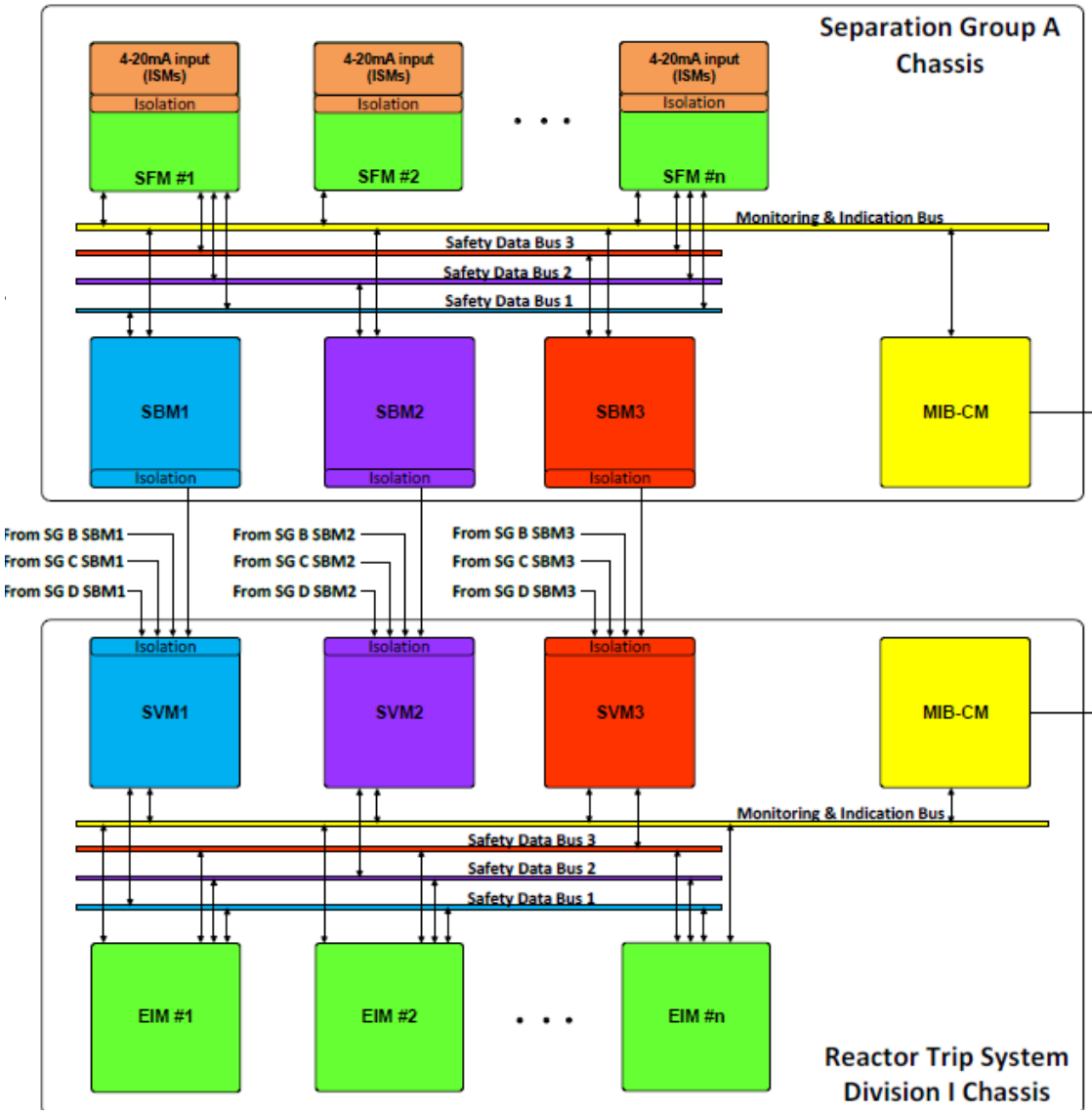
None

B2

HPN, ICIS, MCS, NMS, PCS, PPS, SDIS, RM

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

Independence



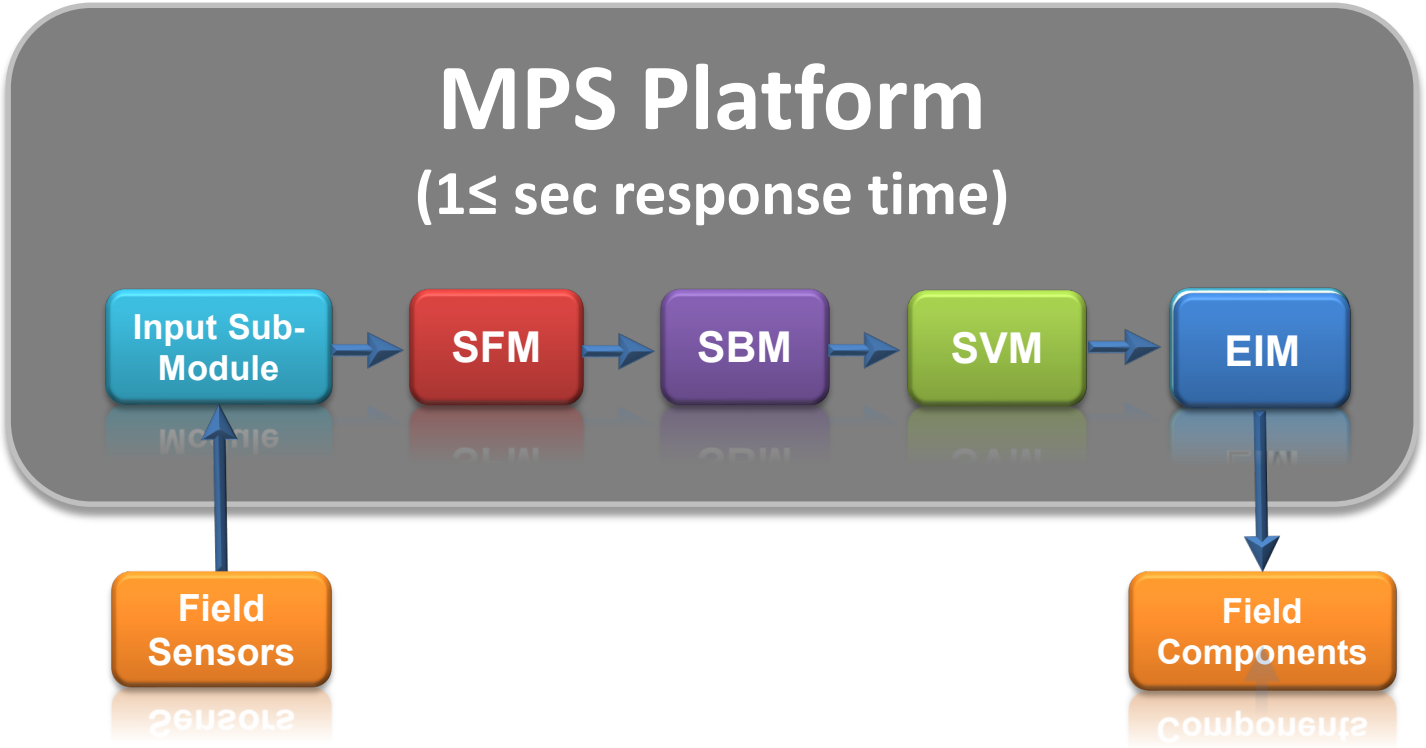
- Physical
- Electrical
- Communications
- Functional

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

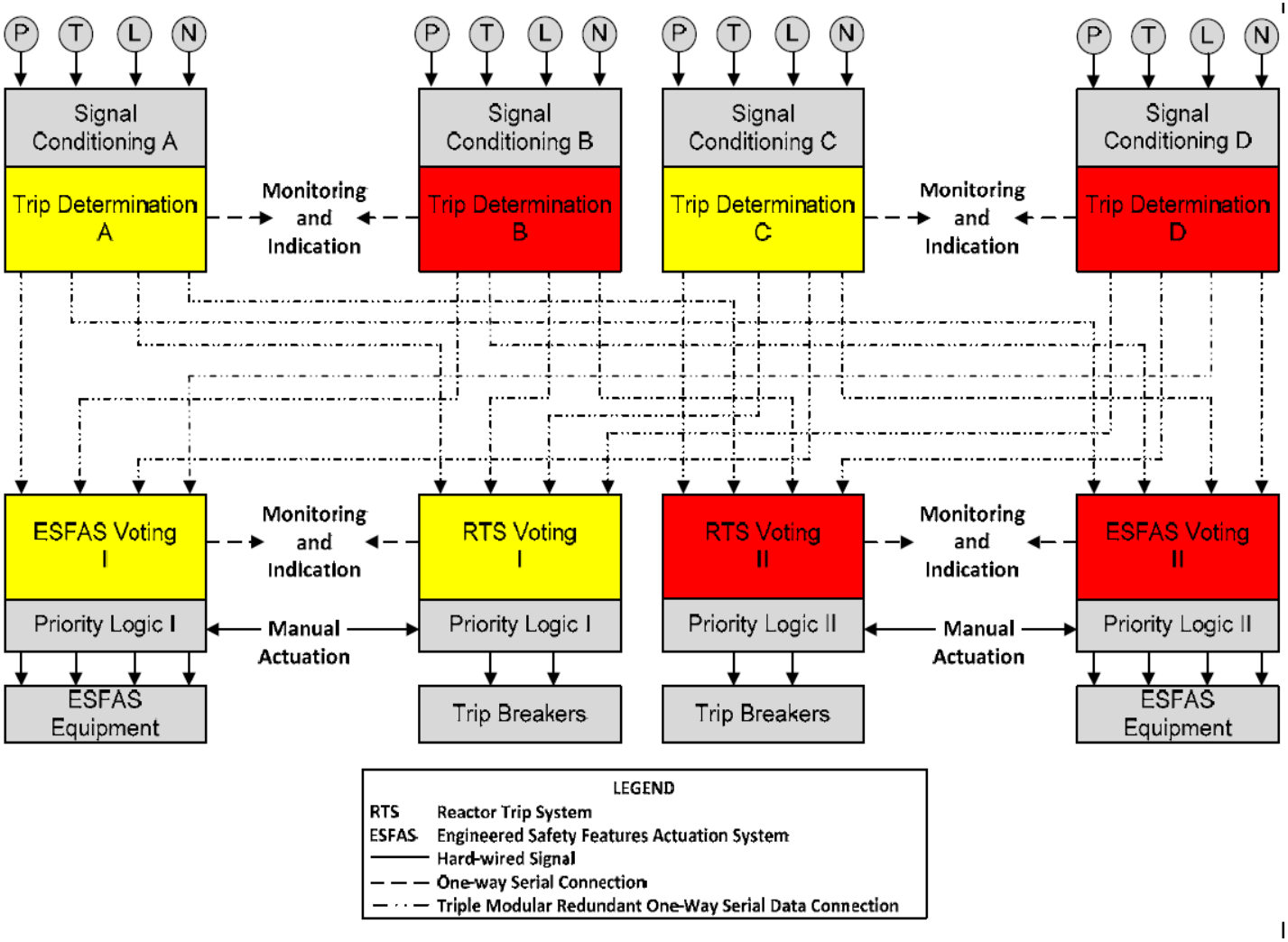
Redundancy

- MPS Redundancy
  - Four separation groups and two divisions of RTS/ESFAS
  - Internal Platform Redundancy
- NMS Redundancy
  - Four separation groups
- Post-Accident Monitoring
  - Two divisions of SDIS

Predictability and Repeatability



Diversity and Defense-in-Depth



Diversity and Defense-in-Depth (Cont.)

Effect of Digital-Based CCF on MPS built-in Diversity

Event	Module	A	C	B	D
Transient or DBE with no DBC	SFM	✓	✓	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or DBE with DBC (modules exhibiting functional and equipment diversity)	SFM	✗	✗	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or DBE with DBC (modules exhibiting only equipment diversity)	SFM	✗	✗	✓	✓
	CM	✗	✗	✓	✓
	EIM	✗	✗	✓	✓

KEY

DBE: Design-Basis Event

SFM: Safety Function Module

CM: Communication Module
EIM: Equipment Interface Module

CCF: Common-Cause Failure
DBC: Digital-Based CCF

✓ - Available to perform function

✗ - Not available to perform function

- Division I modules

- Division II modules

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

Simplicity

- The I&C architecture and systems incorporate the fundamental design principles with an overall focus on simplicity
- NuScale passively safe I&C design results in a simple I&C design solution
  - Simple RTS/ESFAS functions
  - No closed/open loop control
  - All safety-related functions are “de-energize to actuate”

Non-Safety-Related Systems Segmentations

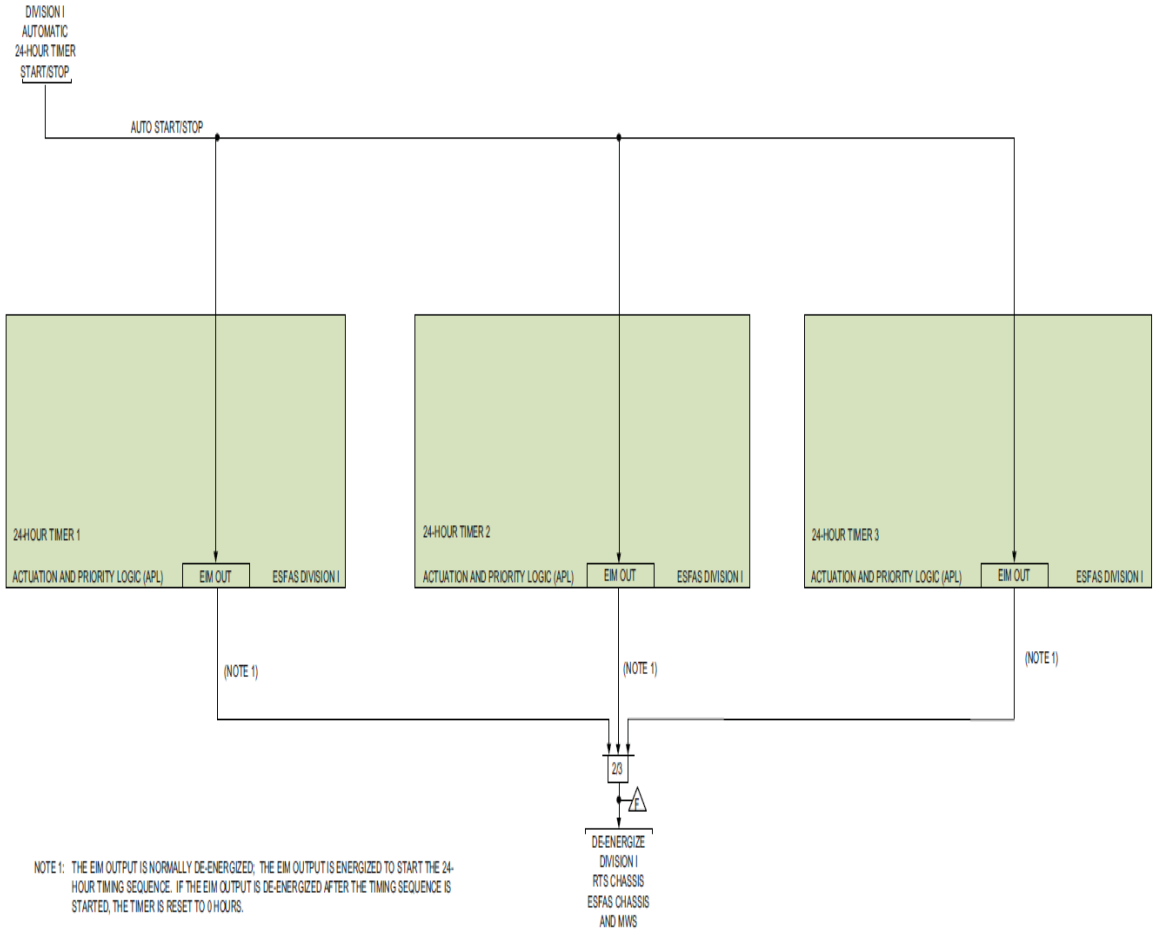
- Segmentation of the MCS and PCS ensures that a failure of these systems does not adversely affect the MPS functions
- This segmentation prevents any multiple failures resulting in spurious actuations or situations which put the plant in an unanalyzed condition
- Staff audited the technical basis of the segmentation analyses for both the MCS and the PCS

10 CFR 50.62(c)(1) Exemption

Three aspects to acceptance of exemption

- Built-in Diversity of the MPS
- ATWS Response Bounded by Plant Design and Chapter 15 analysis
- ATWS contribution to CDF is well below the target CDF $1x10^{-5}$/reactor year

ACRS Comments from NuScale Chapter 8 SC Meeting



24-hour timers

- 24-hour timers are part of the MPS boundary
- Powered by the non-safety-related EDSS

MPS Undervoltage Design Feature

- Upon voltage degradation conditions, the MPS fails into a safe state

Source: DCD Tier 2, Figure 7.1-1ai: Loss of AC Power to ELVS 24 Hour Timers Division I

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

Conclusion

- The approach of DSRS Chapter 7 resulted in:
  - A simple I&C architecture and the HIPS design, which are based on the fundamental design principles
  - A completion of safety evaluation in an efficient and effective manner (safety-focused)
- The staff finds the I&C design to be safe and that it complies with applicable regulatory requirements

Acronyms

- ACRS: Advisory Committee on Reactor Safeguards
- ASAI: application-specific action item
- ATWS: anticipated transient without scram
- CCF: common-cause failure
- CDF: core damage frequency
- CM: communications module
- COMS: communication systems
- D3: diversity and defense-in-depth
- DBC: digital-based CCF
- DCD: design control document
- DCIP: Division of Construction Inspection and Operational Programs
- DLSE: Division of Licensing, Siting and Environmental Analysis
- DSRA: Division of Safety Systems and Risk Assessment
- DSRS: design-specific review standard
- DSS: division of safety systems
- EDSS: highly reliable direct current power system
- EIM: equipment interface module
- EP: emergency preparedness
- ESFAS: engineered safety features actuation system
- ESFRA: enhanced safety-focused review
- EQ: environmental qualification
- HIPS: highly integrated protection system
- HPN: health physics network
- I&C: instrumentation and control
- ICIS: in-core instrumentation system
- ITAAC: Inspections, Tests, Analyses, and Acceptance Criteria
- MCS: module control system
- MPS: module protection system
- NRC: U.S. Nuclear Regulatory Commission

Acronyms

- NMS: neutron monitoring system
- NRO: Office of New Reactors
- NRR: Office of Nuclear Regulation
- NSIR: Office of Nuclear Security and Incident Response
- NuScale: NuScale Power, LLC
- PAMS: postaccident monitoring system
- PCS: plant control system
- PPS: plant protection system
- QA: quality assurance
- RAI: request for additional information
- RES: Office of Nuclear Regulatory Research
- RTS: reactor trip system
- RM: fixed area radiation monitoring
- SBM: scheduling and bypass module
- SC: subcommittee
- SFM: safety function module
- SDIS: safety display and indication system
- SER: safety evaluation report
- SVM: scheduling and voting module
- TeR: technical report
- TMI: Three Mile Island

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

Backup Slide

10 CFR 50.34(f)(2)(xx) Exemption

- 10 CFR 50.34(f)(2)(xx) specifies power provisions for pressurizer relief valves, block valves, and level indicators
- Staff finds pressurizer level instrumentation is not necessary to maintain natural circulation cooling

Notes:
Note 1: MPS, SDIS, and PPS will provide separated, optically isolated, unidirectional data to MCS and PCS (read-only data).
Note 2: Refueling neutron monitors will have normal connection to PCS during specific refueling operations. Other module instruments for refueling, which would have normal connections to MCS or PCS, are to be determined.
Note 3: Includes individual component operation originating from MCS to MPS or PCS to PPS through enable nonsafety control switch.
Note 4: MPS and PPS DIV II internals are the same as DIV I internals.
Note 5: Temporary MPS and PPS Maintenance Workstation communications are one-way, receive only and manually initiated to one channel at a time while at power.
Note 6: Individual HWMs used for each separation group and division to maintain signal separation. All inputs to the HWMs are isolated.
Note 7: Separation Groups A & C are physically separated from B & D. Only Separation Group A is shown connected.
Note 8: MPS MWS DIV II is associated with Separation Groups B & D. MWS & Gateway Server are nonsafety-related.
Note 9: Isolation switches to isolate MCR manual reactor trip, ESFAS actuation, overrides, and the enable nonsafety control switches for all modules.
Note 10: Safety-related manual switches in the MCR include RTS and ESFAS actuation, operational bypasses and overrides, and the enable nonsafety control switches.
Note 11: All MIB-CM and CTB-CM outputs and inputs are isolated (isolation not shown).
Note 12: Each divisional MPS Gateway (nonsafety-related) also has inputs from the other 3 separation groups and RTS II and ESFAS II.
Note 13: The backplane (not explicitly shown) supports bi-directional communication between SFMs and SBMs and between SFMs and MIB CM.
Note 14: PPS EIM only receives information and does not transmit information on the safety data bus.
Note 15: Bidirectional communication exists in the backplane between SFMs and SBMs, between SFMs and MIB CM, and between SBMs and MIB CM.
Note 16: MPS EIM only receives information from the SVM and does not transmit information on the safety data bus. Bidirectional communication exists in the backplane between EIMs and MIB CM and between SVMs and MIB CM.

Remote Shutdown Station (RSS)
Remote Shutdown Station (RSS)
MCS HSI Network
MCS
PCS
PCS Power Operations HSI Network
Safety Manual Isolation Switches (Note 9)

Main Control Room (MCR)
MCR Safety Display and Indication Monitors (13)
DIV I SDI
DIV II SDI
Safety
Safety
Safety Manual Switches (Note 10)
MCR Module Control System Operator Workstation (12)
MCS
MCS HSI Network
Nonsafety Manual
MCR Common Systems Panel Workstation
PCS
PCS Power Operations HSI Network
MCR Reactor Operator Workstation (3)
PCS
PCS Power Operations HSI Network
Shift Technical Advisor Workstation
PCS
PCS Power Operations HSI Network
MCR Control Room Supervisor (CRS) Workstation
PCS
PCS Power Operations HSI Network
MCR Shift Manager Workstation
PCS
PCS Power Operations HSI Network

Radioactive Waste Building Control Room (RWBCR)
Liquid/Solid/ Gaseous Radwaste Monitoring
PCS
Radwaste Handling HSI Network

Technical Support Center
TSC Engr. Workstation
MCS/PCS
PCS Power Operations HSI Network

SDI HUB
(Note 1)

Plant Online Monitoring / Emergency Response Data Server
Plant Domain Controller / Historian
To Corporate/Business Network
Bidirectional Firewall
Plant Network

Plant Control System (PCS)
Meteorological & Environmental Monitoring
Seismic Monitoring
Radwaste Handling HSI Network
PCS Power Operations HSI Network (MCR & RSS)
PCS Unidirectional Data Diode
PCS Domain Controller and Historian (MCR & RSS)
Plant Control System (PCS) Control Network
PCS Local I/O
PCS I/O Network
Plant Video Monitoring System
Fire Protection System
Shared Plant Nonsafety Components
NMS-refuel Instruments
(Note 2)
Accident Monitoring Instrumentation
Bidirectional nonsafety control communications

Module Control System (MCS)
MCS HSI Network (MCR & RSS)
MCS Domain Controller and Historian (MCR & RSS)
MCS Unidirectional Data Diode Typical (12)
Module Control System (MCS) Control Network
(Note 1)
MCS Local I/O
MCS I/O Network
Module Specific Nonsafety Components
Accident Monitoring Instrumentation

Safety Systems
(Note 11)
Accident Monitoring Instrumentation
(Note 9)
Module Protection System (MPS)
Neutron Monitoring System
Safety Related Instrumentation
Hard-wired Modules (HWM)
Trip/Bypass
(Note 6)
Separation Group B & D
Separation Group A & C (Note 7)
(Note 13)
SFM
MIB CM (Note 11)
SBM SD3
SBM SD2
SBM SD1
(Note 15)
MPS GATEWAY DIV II
MCS
CTB
Separation Group A, C, & DIV I MWS
(Notes 5 & 8)
SDI HUB DIV I
TO MCR
MPS GATEWAY DIV I (Note 12)
DIV II RTS SDB3 SVM
DIV II ESFAS SDB3 SVM
DIV II RTS SDB2 SVM
DIV II ESFAS SDB2 SVM
DIV II RTS SDB1 SVM
DIV II ESFAS SDB1 SVM
(Note 4)
Hard-wired Modules (HWM)
OP Bypass
Manual Trip
Enable NS
(Notes 3 & 6)
B C D
DIV I RTS
SDB1 SVM
SDB2 SVM
SDB3 SVM
(Note 16)
DIV I ESFAS
Hard-wired Modules (HWM)
OP Bypass
Manual Actuation
Enable NS
(Notes 3 & 6)
MPS Chassis Backplane connections
RTS I EIM
Priority Logic (APL)
Reactor Trip Breakers
RTS I – MIB CM
(Note 11)
MPS GATEWAY DIV II
SPARE
ESFAS I EIM
Priority Logic (APL)
ESFAS Components
ESFAS I – MIB CM
(Note 11)
MPS GATEWAY DIV II
SPARE
(Note 9)
MCS I/O

Nonsafety Systems
Plant Protection System (PPS)
DIV II (Note 4)
DIV I
CTB
CTB CM (Note 11)
MWS
MIB CM
(Note 1)
TO MCR
SDI HUB DIV I
SDI HUB DIV II
SFM
(Note 14)
EIM
Priority Logic (APL)
SBM3
SBM2
SBM1
Hard-wired Modules (HWM)
Trip/Bypass
Enable NS
(Notes 3 & 6)
Manual Control (PCS) (Note 3)
Manual Actuation
Process Monitoring Instrumentation
Accident Monitoring Instrumentation
CRH/CRV Components

LEGEND
For protection system interconnecting lines
Solid lines indicate continuous connections, dashed lines indicate temporary connections. Network line arrows indicate one way communication direction.
Internal data (Safety Data Bus)
Internal diagnostic and parameter data (Monitoring and Indication Bus)
Internal discrete signal
External unidirectional data
External discrete or data