Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards SHINE Subcommittee

Docket Number: (n/a)

Location: teleconference

Date: Tuesday, July 19, 2022

Work Order No.: NRC-2041 Pages 1-226

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

+ + + + +

SHINE SUBCOMMITTEE

+ + + + +

TUESDAY

JULY 19, 2022

+ + + + +

The Subcommittee met via Teleconference, at 9:30 a.m. EDT, Ronald G. Ballinger, Chairman, presiding.

COMMITTEE MEMBERS:

RONALD G. BALLINGER, Chairman

VICKI M. BIER, Member

CHARLES H. BROWN, JR. Member

VESNA B. DIMITRIJEVIC, Member

GREGORY H. HALNON, Member

JOSE MARCH-LEUBA, Chairman

DAVID A. PETTI, Member

JOY L. REMPE, Member

MATTHEW W. SUNSERI, Member

ACRS CONSULTANTS:

DENNIS BLEY

MYRON HECHT

STEPHEN SCHULTZ

DESIGNATED FEDERAL OFFICIAL:

CHRISTOPHER BROWN

C-O-N-T-E-N-T-S

P R O C E E D I N G S

9:30 a.m.

CHAIRMAN BALLINGER: Good morning. The meeting will now come to order. This is a two-day meeting of the SHINE Subcommittee of the Advisory Committee on Reactor Safeguards. I'm Ron Ballinger, Chairman of today's Subcommittee meeting.

ACRS members in attendance are Vicki Bier, Charlie Brown, Greg Halnon, Jose March-Leuba, our consultant Stephen Schultz, Matt Sunseri, Vesna Dimitrijevic, and I'm sure there will be others that will come on little bit later. Chairman Rempe will be joining us in the afternoon.

During this meeting, the Subcommittee will have a discussion with the NRC staff and SHINE Medical Isotopes concerning the staff's evaluation report of the following chapters: Chapter 3, Section 3.1, Design Criteria; Chapter 9, Section 9a.3, Fire Protection; Chapter 7, Instrumentation and Control, Safety-Related Systems; Chapter 12, Section 12.10, Operator Training, Requalification; Chapter 12, Section 7.9, Human Factors Engineering; Chapter 12, Conduct of Operations, Organization, Review and Audit Activities, Procedures, Required Actions, Reports, Records, Etc.; and Chapter 12, Section 12.11, Startup Plan.

It's a lot of ground to cover. A part of the presentations by the Applicant and the NRC may be closed in order to discuss information that is proprietary to the Licensee and its contractors pursuant to 5 U.S.C. 552(d)(c)(4). Attendants at the meeting that deals with such information will be limited to the NRC staff and its consultants, SHINE, and those individuals and organizations who have entered into an appropriate confidentiality agreement with them. Consequently, we need to confirm that we have only eligible observers and participants in the closed part of the meeting.

The rules for participating in all ACRS meetings, including today's, were announced in the Federal Register on June 13th, 2019. The ACRS section of the U.S. NRC public website provides our charter, bylaws, agendas, letter reports, and full transcripts of all full and Subcommittee meetings, including slides presented there. The meeting notice and agenda for this meeting were posted there. We have received no written statements.

There is an extremely loud background noise, like somebody is vacuuming their couch. So, whoever it is, can you -- good. You've finished vacuuming.

The meeting notice and agenda for this meeting were posted there. We have received no written statements or requests to make oral statement from the public. The Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions as appropriate for deliberation by the full Committee. The rules for participation in today's meeting have been announced as part of the notice of this meeting previously published in the Federal Register.

Today's meeting is being held over Microsoft Teams. A telephone bridge line allowing participation of the public using their computer using Teams or by phone was made available. Additionally, we have made a MS Teams link available on the published agenda. This will be the same link for tomorrow's meeting.

A transcript of today's meeting is being kept. Therefore, we request that meeting participants on Teams and on the Teams call-in line identify themselves when they speak and to speak with sufficient clarity and volume that they can be readily heard. Also, as the example just showed us, if you've got loud background noise and things like that, it hinders our operation. So, if you're not speaking, please mute yourself. The chat feature in Teams should not be used for any technical exchanges.

At this time -- okay. I've already covered that. Now I'll proceed with calling on Josh Borromeo for opening remarks. Are you available? Yep. He's there.

MR. BORROMEO: Yeah. Thank you, Professor Ballinger.

My name is Josh Borromeo. I'm Chief of the Nonpower Production and Utilization Facility Licensing Branch. I first want to thank the ACRS and the ACRS staff for their continued support on this review. Professor Ballinger highlighted some of the -- I'll call it the most anticipated sections of this review, and today we'll be talking about the design criteria, fire protection, and digital I&C related to the safety-related systems. And tomorrow we'll be talking about operator training and requalification, human factors, conduct of operations, and the startup plan.

Within these presentations, we'll be addressing some of the follow-ups we had from last meeting. In particular, there was some discussion about the timing of certain components at the accident analyses, and we'll be addressing those during the digital I&C review.

I think I said this at previous Subcommittee meetings, but I do want to highlight again the staff's support of the ACRS's process for documenting concerns as we go through these Subcommittees. We're finding that that's an efficient way for us to understand what the concerns are and address them in an efficient way at their Subcommittee meetings.

I also want to emphasize that we appreciate ACRS's timely review and insights during this review, and we also appreciate the flexibility ACRS is having with, in particular, me, but the NRC staff as well, to get through this thing. I also want to thank SHINE and the NRC staff for their preparations in the development for slides and the SE and the review for this meeting, and we look forward to a good conversation with the ACRS today.

So, with that, I believe we're turning it over to SHINE to discuss the design criteria.

CHAIRMAN BALLINGER: Thank you.

So, Tracy, are you all set to go?

MS. RADEL: Yeah.

MR. BROWN: Hey, Professor Ballinger?

CHAIRMAN BALLINGER: Yeah?

(Simultaneous speaking.)

MS. RADEL: Yes. Ready to go here. Can you hear me?

CHAIRMAN BALLINGER: Somebody else is asking for -- we can hear you fine, Tracy, but there was another comment.

MR. BROWN: Yeah. This is Chris Brown, just letting you know that Member Petti has joined, and I will be the DFO for this meeting.

CHAIRMAN BALLINGER: Oh. I'm sorry. Okay. Good. I'm trying to keep an eye on this list to see who joins and not. But that's great. Thanks.

Okay, Tracy.

MS. RADEL: Thanks.

Tracey Radel, SHINE's Vice President of Engineering. I'm going to cover the design criteria today. First, we're going to look at the development of the SHINE safety criteria and what the SHINE safety criteria is, and then go into the development of the SHINE design criteria and cover the different design criteria in the areas listed.

So the SHINE safety criteria is determined for a definition and classification of safety -related structure systems and components, which are those physical SSCs whose intended functions are to prevent accidents that could cause undue risk to the health and safety of workers and the public, and to control or mitigate consequences of such accidents.

We have defined acceptable risk as an event being highly unlikely, less than or equal to ten to the minus five per event per year, or having consequences less severe than the SHINE safety criteria. The SHINE safety criteria were developed using NUREG-1537 and the ISG augmenting NUREG-1537, 10 CFR 70.61, 10 CFR 50.2, and the NRC proposed accident dose criterion.

The SHINE safety criteria are listed here, and as stated on the previous slide, acceptable risk would be defined as highly unlikely or having a less severe consequence than the items listed here. First, we have an acute worker dose of five rem or greater total effective dose equivalent, an acute dose of one rem or greater TEDE to any individual located outside the owner-controlled area, an intake of 30 milligrams or greater of uranium in soluble form to an individual located outside the owner-controlled area, an acute chemical exposure to an individual from licensed material or hazardous chemicals produced from licensed material that could lead to irreversible or other serious long-lasting health effects to the worker or cause mild transient health effects to any individual located outside the owner-controlled area. Criticality, where fissionable material is used, handled, or stored with the exception of the target solution vessel or loss of capability to reach safe shutdown conditions.

Are there any questions on the SHINE safety criteria or its development before we move into the design criteria?

Okay. Sorry about that. So, moving on to the development of the SHINE design criteria, the SHINE design criteria was developed based on 10 CFR 50, Appendix A, and 10 CFR 70.64(a), Design Criteria.

It's selected to cover the complete range of facility operating conditions, responses to anticipated transient and potential accidents, cover safety-related SSCs, including redundancy, environmental qualification, and seismic qualification, inspection testing and maintenance of safety-related SSCs, quality standards, and then design features that prevent or mitigate consequences for fire, explosion, meteorological, hydrological, and seismic events.

As we go through the design criteria here, the format I have is if our design criteria does not differ from those listed in 10 CFR 50, Appendix A, or the 10 CFR 70.64 in any way, I have not listed those design criteria out explicitly. The design criteria where there are slight differences between the SHINE design criteria and those design criteria listed -- those are listed out, and I'll highlight just the differences as we go through. Feel free to stop me at any point if you have specific questions about the differences that I highlight.

So, in Design Criterion 2, the difference here is really in our facility structure is protecting against tornadoes, hurricanes, floods, tsunamis, and seiches. And so we distinguished that the facility structure protects all of the safety-related components from those events. And then the facility structure, along with the safety-related SSCs, are designed to withstand earthquakes. So we just simplified that in our design criteria.

On the Criterion 4, the power plant criteria focus on loss of cooling and ruptures of systems containing high pressure and temperature. With the SHINE systems at low temperature, pressure with minimal stored energy, and no forced cooling for safety, these do not pose a substantial risk. And so the differences are reflected in our design criteria.

For Criterion 5, again, the power plant criterion is focused on cooldown, which is not significant risk with the low decay heat and passive light-water pool cooling in the SHINE systems. So there's a simplification in our Design Criterion 5.

On Criterion 6, because no operator actions are required in response to an accident, the control room does not need to be occupied during accident conditions, and that leads to a simplification of Design Criterion 6.

Moving on to the subcritical assembly design criteria, there are some substitutions that are made for equivalent structures in the SHINE system, SHINE design versus the power plant. And so I want to highlight those replacement phrases.

For the 10 CFR 50, the reactor core and associated coolant control and protection systems is generally replaced with subcritical assembly system, target solution vessel, offgas system, and primary closed-loop cooling system. Fuel design limits are replaced by target solution design limits, and operational occurrences are replaced by anticipated transients.

MEMBER HALNON: Hey, Tracy? Tracy, this is Greg Halnon. Just real quick on the previous slide, on number 6, I just wanted to make sure I heard you right. There's no operator actions required for accident response, but under 6, you do have the control room -- last statement is perform required actions under postulated accident conditions. Help me just reconcile those statements.

MS. RADEL: Yeah. So the design criteria were set prior to all the design and hazard analysis being performed for the facility, and we did determine that no operator actions were required to respond to an event that does occur. And so -- you know.

MEMBER HALNON: Okay. Is it still, then, part of the design criteria -- should something down the road come up, like say a new accident situation or some other transient that was not anticipated, is it still part of the design criteria, or are you just ignoring it at this point?

MS. RADEL: It is still part of the design criteria. So, if something were determined to be required in immediate response, we would make sure that conditions are suitable for that. But at this time, there are not any required to mitigate the accident scenarios.

MEMBER HALNON: Thanks.

CHAIRMAN BALLINGER: This is Ron

Ballinger. I was going to wait until the end of your presentation to ask this question, but this is a good point, I guess. We have been reviewing chapters before this for which there were oftentimes reference to design criteria. But we hadn't reviewed the design criteria at the time.

My question to you is, now that we have the design criteria that we are reviewing, has the connection between these design criteria in the chapters that we previously reviewed where they referenced the design criteria -- has that connection changed in any way?

MS. RADEL: No. The connection has not changed at all. The design there hasn't changed. So just covering the design criteria in more detail based on your requests to go into more detail on how they are developed and what the details of them are.

CHAIRMAN BALLINGER: Okay. So we're internally consistent?

MS. RADEL: Yes.

CHAIRMAN BALLINGER: Thank you.

MS. RADEL: Okay. On Criterion 10, the reactor core and associated cooling systems has been replaced by a subcritical assembly system. And on Criterion 11, the phrasing is just slightly different, simplified because in the 10 CFR 50 language, it talks about which can result in conditions, and then uses the language of, are not possible. And so we simplified that to, they can result, because we felt if things are not possible, they don't fit into can resolve. So just simplification of language there.

Okay. Criterion 12, the reactivity control systems were replaced by target solution vessel, offgas system, primary closed-loop cooling system, and the TSV cell subsystem. The reactor coolant pressure boundary was replaced by the primary system boundary. The core was replaced by the TSV. The capability to cool the core was replaced by capability to drain the TSV.

And then the considerations, reactivity accident considerations, were adjusted. So, in reactor space, they listed rod ejection, rod dropout, steam-line rupture, changes in reactor coolant temperature and pressure, and cold water addition. For our design criteria, based on our system design, we listed excess target solution addition, changes in primary cooling temperature, changes in primary system pressure, and deflagration in the primary system boundary.

I do want to point out for this design

criterion that earlier conversations related to detonation being listed in our design criterion and a question whether there would be a change to the criterion, but the language here is that the accidents would include consideration of detonation, and we have considered detonation, although it's not possible in the system, not credible.

On the instrumentation control and protection system design criteria, there were no changes beyond kind of minor wording changes that were not of substance.

Moving into the primary system boundary design criteria, the reactor coolant pressure boundary, again, was replaced by primary system boundary in Criterion 20. In Criterion 21, the reactor coolant system and associated auxiliary control and protection systems was replaced by the primary closed-loop cooling system. And reactor coolant pressure boundary, again, was replaced by primary system pressure boundary.

On Criterion 25, the system to remove residual heat was replaced by the light-water pool, fuel design limits replaced by target solution design limits. Reactor core was replaced by target solution vessel dump tank, and the reactor coolant pressure boundary replaced by primary system boundary.

Also note that the second paragraph in the Criterion 34 from 10 CFR 50, Appendix A, was not applicable to our system. It goes into the reliability of electric power systems related to maintaining active forced cooling requirements assuming single failures.

Criterion 26, a system to transfer heat from structured systems components as an ultimate heat sink was replaced by the radioisotope process facility cooling system and process chilled water system. Note that in Criterion 44 in 10 CFR 50, Appendix A, it lists the safety functions related to active heat removal, whereas our secondary and tertiary cooling systems do not provide any safety functions. So our criterion just says they are provided to transfer heat to the environment, which serves as the ultimate heat sink.

Criterion 27 -- so, here, the criterion 17 within 10 CFR 50 is a very large -- I could not fit on one slide. So the paragraphs that begin -- where the beginning portion of the paragraph is listed and kind of dot-dot-dot there, those are reflected in the SHINE design criteria without any substantial changes.

The paragraphs that I have listed out

there in its entirety is a paragraph that is not included in the SHINE design criteria and is related to the transmission network, distribution system failure, off-site power effects. And this is really focused on loss-of-coolant accident, as you can see by the final sentence in that paragraph. So we do not feel that was applicable to the SHINE systems.

Criterion 29, getting into the confinement and control of the radioactivity design criteria, the reactor containment and associated systems was replaced by confinement boundaries. Essentially, leak-tight barrier was replaced by low-leakage barrier. And containment design was replaced by confinement design. In addition, we listed the four classes of confinement boundaries in our design criteria.

Criterion 30, the simplification here really is related to the reactor criterion focusing on the loss-of-coolant accident. So this goes into detail about the different considerations for the loss-of-coolant accident. Given that our forced cooling system performs no safety function, and we have passive cooling for the lower level of decay heat within our systems, this is not applicable.

For Criterion 31, the portion of Criterion

51 from 10 CFR 50, Appendix A, that was included directly is the surface temperature and other conditions of containment boundary material during operation maintenance, testing, and postulated accidents. To ensure that there is not fracture was included explicitly. The other ones were included in the fact that you are ensuring that there is not a fracture in that the postulated accident conditions.

MEMBER PETTI: So, Tracy, this is Dave Petti. Could you go back? I'm just looking at those two and wondering, which one is harder to meet in practice in terms of the confinement boundaries? I'm not too worried about fracture of some things, but like leakages that end up being more excessive than you think because of the accident condition would be covered in 30, right?

MS. RADEL: Yes. Yeah. So the leakage at the highest pressure scenario for accident conditions is what our confinement safety function is based off of.

MEMBER PETTI: All right. Okay. Thanks. That helps.

MS. RADEL: Okay. Criterion 33 really is a summary of multiple criteria listed in 10 CFR 50, Appendix A, so piping systems penetrating containment, reactor coolant pressure boundary penetrating containment, primary containment isolation, and closed system isolation valves, the portions of which are applicable to SHINE are included in our Design Criterion 33, which states that piping systems penetrating confinement boundaries that have the potential for excessive leakage are provided with isolation capabilities appropriate to the potential for excessive leakage.

Piping systems that pass between confinement boundaries are equipped with either a locked closed manual isolation valve or an automatic isolation valve that takes the position that provides greater safety upon loss of actuating power. Manual isolation valves are maintained locked shut for any conditions requiring confinement boundary integrity.

This criterion really works in conjunction with Criterion 34 as well. So this states that lines from outside confinement that penetrate the primary system boundary and are connected directly to the primary system boundary are provided with redundant isolation capabilities, ventilation monitoring, and other systems that penetrate the primary process glove box or hot cell confinement boundaries, are connected directly to the confinement atmosphere and are not normally locked closed, have redundant isolation capabilities, or are otherwise directed to structures, systems, and components capable of handling any leakage.

Isolation valves outside confinement boundaries are located as close to the confinement as practical, and upon loss of actuating power, automatic isolation valves are designed to take the position that provides greater safety. Manual isolation valves are maintained locked shut for any conditions requiring confinement boundary integrity. And all electrical connections from equipment external to the confinement boundaries are sealed to minimize air leakage. So, together, those two design criteria really ensure that we maintain that low leakage.

Criterion 37 is related to criticality control. Criticality in the facility is prevented by physical systems or processes and the use of administrative controls. Use of geometrically safe configurations is preferred. Control of criticality adheres to the double contingency principle, and a criticality accident alarm system to detect and alert facility personnel of an inadvertent criticality is provided.

And finally, Design Criterion 39, which is a unique SHINE design criterion due to the risk of hydrogen within the facility -- systems to control the buildup of hydrogen that is released into the primary system boundary and tanks or other volumes that contain fission products and produce significant quantities of hydrogen are provided to ensure that the integrity of the system and confinement boundaries are maintained.

Any questions on the SHINE design criteria? All right. Thank you.

CHAIRMAN BALLINGER: Does that cover it, Tracy?

MS. RADEL: Yep. That's the end of my presentation.

CHAIRMAN BALLINGER: Okay. Questions from the members? Let's see. I think we have new members that are participating, Matt Sunseri and Dave Petti. If I've missed somebody, please let me know.

Okay. So next up is the staff presentations. I'm not -- oh, good. They're up. Okay. So let's move forward. Thanks.

MR. HARDESTY: Can you see my slides and hear me okay?

CHAIRMAN BALLINGER: I was about to panic. No, you're right. We got them.

MR. HARDESTY: All right. Great.

Good morning. It's a pleasure to speak with all of you today. I am Duane Hardesty, a Senior Project Manager in the Nonpower Production and Utilization Facility Licensing Branch and the Office of Nuclear Reactor Regulation. My presentation this morning is on Chapter 3, SHINE Design Criteria.

Okay. The design criteria for a facility establishes the criteria to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public. The design criteria should be specified for each structure system and component and establish design, fabrication, construction, testing, and performance requirements for each SSC that is assumed in the FSAR to perform an operational or safety function and should also include references to applicable standards, guides, and codes to support the design functions as required by the safety analysis.

Section 50.34(b)(2) of the Code of Federal Regulations requires a description and analysis of the structures, systems, and components of the facility with emphasis upon performance requirements, with technical justification upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. The regulation requires that the description be sufficient to understanding of the system design and the relationship to the safety evaluation.

Subparagraph Section 50.34(b)(4) of 10 CFR requires a final analysis and evaluation design and performance of the SCC with the objective of assessing the risk to the public health and safety resulting from the operation of the facility and including determination of the margin of safety during normal operation and transient conditions anticipated during the life of the facility, and the adequacy of the SSCs provided for the prevention of the accidents and mitigation of the consequence of the accidents, including consideration for any pertinent information that has developed since the submittal of the preliminary safety analysis.

Section 70.61 of 10 CFR provides performance criteria related to the risk credible events evaluated in the integrated safety analysis, and the engineering controls, administrative controls, or both that are applied to reduce the likelihood of occurrence of the event. The additional Part 50 regulations require reasonable assurance that the activities authorized by the operating license can be conducted without endangering the health and safety of the public and that the activities will be conducted in compliance with the regulations and not be inimical to the common defense and security.

The acceptance criteria used by the staff to evaluate SHINE's design criteria is contained in Part 1 and 2 of NUREG-1537 and the interim staff guidance augmenting NUREG-1537 for licensing radioisotope production facilities. In addition to the base NUREG-1537 guidance, the ISG states that the design must incorporate, to the extent practicable, a preference for the selection of engineer controls over administrative controls to increase overall system reliability and features that enhance safety by reducing challenges to the items relied on for safety.

The ISG also contains guidance that addressing the radioisotope production facility design criteria and defense-in-depth practices in 10 CFR 70.64 is an acceptable way of demonstrating adequate safety of SSCs in the design of a facility. SHINE based their chosen design criteria on Appendix A to Part 50 and on 10 CFR 70.64(a) baseline design criteria.

The NRC staff performed a review of the technical information for the safety-related SSCs presented in the SHINE FSAR to assess the sufficiency of the design criteria as described in FSAR Section 3.1 to conduct the activities authorized by the operating license. The NRC staff evaluated the sufficiency of the design criteria using the guidance and acceptance criteria from Section 3.1 of the design criteria of NUREG-1537, Parts 1 and 2, and the ISG.

The NRC staff evaluated whether the design criteria for the SHINE systems and subsystems are met and if the FSAR describes how the principal design criteria for the facility are achieved. The staff's findings with regard to sufficiency of the SHINE design criteria are documented in Chapter 3 of the safety evaluation.

For each SSC, FSAR Table 3.11 and safety-related structure system components and Table 3.12, non-safety-related structure system components, identify the applicable FSAR section or sections that describe each SSC. SHINE discusses the design criteria for the individual SSCs and the applicable FSAR section describing those SSCs. Similarly, the NRC staff evaluation as applicable to those specific design criteria is also included within a chapter of the SE where the staff evaluated those SSCs.

The SHINE design criteria generally follow

Appendix A to Part 50, General Design Criteria for Nuclear Power Plants, and 10 CFR 70.64(a), Design Criteria, as Tracy just discussed. However, Appendix A provides guidance in establishing design criteria, but not all the design criteria apply directly to the SHINE design.

Additionally, as discussed in Chapter 7 of the staff's SE -- and you'll hear more about later -- the application-specific action items in the NRC topical report on the highly integrated protection system platform are intended for a power reactor application, and not all ASAIs are critical for ensuring safety in SHINE's application of the HIPS platform for the target solution vessel reactivity protection system and the engineering safety features actuation system.

SHINE's safety-related SSCs are intended to prevent, control, or mitigate the consequences of accidents that could cause undue risk to the health and safety of the workers and the public to an acceptable level. The SHINE nuclear safety criteria are based on 10 CFR 70.61 performance requirements. SHINE states that an acceptable level of risk is achieved by ensuring that events are highly unlikely or by reducing the consequences to less than the SHINE safety design criteria -- or sorry, safety criteria.

The SHINE nuclear safety criteria requires that each engineer or administrative control be applied to the extent needed to reduce the likelihood of a high or intermediate consequence event, such that upon implementation of such controls, the event is highly unlikely or its consequences are less severe than the SHINE safety criteria. Also, the risk of nuclear criticality accidents must be limited by assuring that under normal and credible abnormal conditions, all nuclear processes are subcritical.

Each engineer or administrative control necessary to comply with those requirements must be designated as an item relied on for safety, IROFS, and the safety program must ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the SHINE performance requirements.

SHINE selected radiological safety criteria and consequence limits with dose limit values that are lower than those specified in 10 CFR 70.61. The SHINE total effective dose equivalent limits are five rem for the workers and one rem for the public. The NRC staff notes that the 10 CFR 70.61(c) doesn't include a soluble uranium intake limit for intermediate consequences. The limit is actually in 10 CFR 70.61(b), which means that the event leading to an intake an excessive amount would actually be a high consequence event. However, with SHINE's approach of reducing the likelihood of both high and intermediate consequence events to highly unlikely, the staff found SHINE's use of soluble uranium intake limit to be acceptable.

SHINE requires that criticality of safety events be highly unlikely to have an acceptable risk. To achieve this, SHINE requires that an item relied on for safety must meet the double contingency principle or be safe by design. Consistent with NUREG-1520, the standard review plan for fuel cycle facilities, a system of safety-related controls having the appropriate reliability and availability qualities -- example described in sufficient detail so that their effect on the overall likelihood can be evaluated -- will possess the double contingency protection and meet the definition of highly unlikely.

SHINE also applies the safe-by-design approach to passive design components. These include items with the dimensions calculated to have a favorable subcritical geometry with margin that have no credible failure mechanism that could alter the design (audio interference) management program. The SHINE shutdown safety criteria ensures that the facility is designed to automatically shut down the irradiation process, place the target solution into a safe condition, and stabilize accident conditions without immediate operator action. The safety criteria was reviewed and found acceptable by the NRC staff in Chapter 13 of the staff's SE.

So SHINE talked about the 39 design criteria that are listed in the FSAR for the main production facility. Most of the design criteria have specific application to individual SSCs, which are listed in Table 311 and 312 in the FSAR. The NRC staff's evaluation of the design criteria are provided in the corresponding sections of its SE.

Eight of the criteria, however, are stated to be generally applicable to the entire facility. The staff evaluated the general design criteria as applicable, and as an example, the adequacy for Design Criterion 1 of the SHINE Quality Assurance Program was reviewed and found acceptable in Section 7.4 and 12.9 of the SE. The NRC staff found that the SHINE QA program is comprehensive and meets the regulatory requirements of a QA program.

Another example, Design Criteria Number 5, the NRC staff evaluation found that the SSCs are shared by both the irradiation facility and the radiation production facility -- for example, all the IUs share the ESFAS and the control room, but this does not impair the ability to perform any safety functions. The sharing of the SSCs was found acceptable in Section 1.4 and in Section 7.4421 and 7.4521 of the staff's SE.

Finally, my last example is Design Criteria 8. The NRC staff evaluated SHINE's emergency plan and found SHINE emergency capability acceptable in Section 12.47 of the SE. So, as was stated earlier, the remaining 31 SHINE design criteria are specifically assigned to systems and subsystems detailed in the tables of the FSAR, and the NRC staff's evaluations of those design criteria are provided in the corresponding sections of the SE, many of which will be discussed in presentations later today.

The NRC staff finds that the application of SHINE's design criteria discussed in the SHINE FSAR Chapter 3 reflects the design features of the safety-related SSCs, which include redundancy, environmental qualification, seismic qualification, and procedures for inspection, testing, and maintenance that are required to ensure and maintain safe facility shutdown and prevent or mitigate the consequences of design-basis events.

The NRC staff reviewed the SHINE tech specs and find that they provide appropriate safety limits limiting safety system settings and limiting conditions for operation of the facility pursuant to 10 CFR 50.36 technical specifications. Consistent with NUREG-1537 Part 2 and the ISG to NUREG-1537 Part 2, the staff confirmed that the SCCs credited in the accident analysis are designated as safety-related and included within the tech specs.

Additionally, the NRC staff finds that the tech specs include the necessary surveillance requirements with the appropriate frequency and scope to demonstrate the performance and operability of the required systems. In the presentations that follow today, the staff will discuss examples such as instrumentation controls, fire protection, and startup plans -- some of them will be tomorrow; I understand that -- that show application of the design criteria to the safe operation of the site facility.

In its evaluation, the NRC staff finds that the SHINE design philosophy applied from the outset and through completion of the design is based on providing successive levels of protection such that health and safety are not wholly dependent upon any single element of the design, construction, maintenance, or operation of the facility.

SHINE's incorporation of defense-in-depth practices results in a conservatively designed facility and a system that will exhibit greater tolerance to failures and (audio interference) final design by focusing attention on the prevention and mitigation of high-risk potential accidents to decrease the likelihood of occurrence to highly unlikely and/or reduce consequences to low.

Based on its evaluation, the NRC staff concludes that the descriptions and discussions of SHINE design criteria are sufficient and meet the applicable regulatory requirements, guidance, and acceptance criteria for the issuance of an operating license. And that is the end of my presentation.

CHAIRMAN BALLINGER: Thank you.

Questions from the members?

MEMBER HALNON: Duane, this is Greg Halnon. Criterion 5 on the sharing of systems -- we had a comment earlier on about the tech spec system, nitrogen gas. Do you have any comment on the sharing of that system given the potential margin issues that we talked about earlier?

CHAIRMAN BALLINGER: Are you talking about the nitrogen purge system?

MEMBER HALNON: Yes. I think there was 12 bottles, and 11 are required, or something to that effect.

MR. HARDESTY: Right. So we evaluated that in the tech specs. It's not a proprietary number to say that they require 16 standard cubic feet per minute of flow for the nitrogen purge system. I actually have a backup slide on hydrogen mitigation if you'd like me to discuss it.

MEMBER HALNON: Yeah, just briefly. I mean, we made a comment on it, and we wanted to make sure that we understood the uses because I believe that's shared across other systems as well, the gas system.

MR. HARDESTY: It is. I'm sorry. I went too far and lost the presentation. Okay. There we go. So you should be able to see my hydrogen mitigation slide.

MEMBER HALNON: Yes.

MR. HARDESTY: All right. So the TSV offgas system maintains the TSV head space below the lower flammability limit by using air sweep gas and via recombination. And that's the normal method. And TOGS is purged to the process vessel vent system via the vacuum transfer system. And so the process vessel vent system has blowers that maintain a slight vacuum across those RPF tanks to maintain hydrogen less than the lower flammability limit.

The N2PS system, nitrogen purge system, is a backup sweep gas flow from the nitrogen flasks. So that only initiates upon a loss of power or a loss of sweep gas flow that's sensed by the TRPS. The solenoid valves, which de-energize to open, will release the nitrogen purge gas to flow to the TSV dump tank and the TOGS equipment, which is subsequently discharged to the process vessel vent system. And upon a loss of power or loss of a sweep gas flow to the process vessel vent system, which would be sensed by ESFAS, the radiological vent zone 2 is isolated, and that nitrogen sweep gas flows through the process vessel vent system piping.

So the normal system, TOGS, is part of the pressure system boundary, and there's tech spec limiting safety system setting and the required tech spec 3.1.1, which is monitored by a tech spec required a 3.2.3 TRPS set point. And the low process vessel vent flow rate is also an LSSS with a tech spec 3.51 required system monitored by, again, a textbook 3.24 required ESFAS set point.

And the hydrate control in an operational N2PS and nitrogen purge system are part of the tech spec required definition for safe shutdown. And then, of course, tech spec 3.8 requires that the system be able to develop and deliver that 16 cf, standard cubic feet per minute, flow rate in order to meet the design criteria for the system.

MEMBER HALNON: Okay. So, given the volume flow rate required, which was very small, and then the volume of storage fill, there's adequate margin for the sharing of the system.

MR. HARDESTY: Yes. That was the staff's evaluation.

MEMBER HALNON: Thank you.

MR. HARDESTY: No problem.

CHAIRMAN BALLINGER: Other questions? Okay. I'm trying to juggle two things here. We're ahead of schedule. It's about 9:20. Fire protection was next -- was supposed to be after break. I think SHINE has -- well, the staff or SHINE; I forget which -- has 11 slides, and I'm wondering whether we shouldn't just keep on going. So I think that's what

I'll propose unless there's an objection from the members.

So, if we're ready, can the SHINE folks put up their fire protection slides?

MR. BARTELME: This is Jeff Bartelme from SHINE. We've got some additional personnel coming down to support, so we'll just need a minute or two. We'll get the slides pulled up, and we should be ready to present quickly.

CHAIRMAN BALLINGER: Okay. So should we take a break, or should we wait just a minute or so?

MEMBER DIMITRIJEVIC: I say let's take a break, Ron.

(Simultaneous speaking.)

MEMBER DIMITRIJEVIC: -- ten-minute break.

CHAIRMAN BALLINGER: Okay. Well, that being the vote, we'll take a break. It's 10:22. Let's come back at 10:30. How's that? So we'll break until 10:30.

(Whereupon, the above-entitled matter went off the record at 10:22 a.m. and resumed at 10:30 a.m.)

CHAIRMAN BALLINGER: Okay, it's 10:30, we'll go back in session.

So, the SHINE presentation is up, so let's pick it up and start.

MR. MEYER: Hello, this is Andrew Meyer. I'm the Safety Analysis Manager.

Next slide, please.

So, this is an outline of a presentation regarding the fire protection program.

The objective of the fire protection program is to minimize the probability and consequences of fires in the SHINE facility.

Elements of the fire protection program, work together to satisfy the requirements of 10 CFR 50.48 alpha.

The fire protection program takes a defense-in-depth approach to prevent fires from starting, including limiting combustible materials; detect, control; and, extinguish fires which do occur, to limit consequences.

Provide protection for systems, structures, and components important to safety so that a fire will not prevent the safe shut down of the irradiation units, or cause an uncontrolled release of radioactive material to the environment.

The diagram to the right shows how the fire protection program and structure, relate to the fire protection plan provided for in the FSAR.

It includes the overall SHINE fire protection program and the individual program elements, including the lower tier documents such as the fire hazard analysis; safe shut down analysis; pre-fire plans; and, implementing procedures.

Specific details are provided in the lower tier documents.

The fire hazard analysis establishes and describes individual facility fire areas, which are unique areas separated by fire radiant construction, or administrative controls to prevent the spread of fire between adjacent fire areas.

It determines the fire hazards posed by operations and contents of each fire area. Hazards included are combustible materials, and ignition sources.

Along with the safe shutdown analysis, it determines the worst case fire effects on safe shutdown capability, and the potential for uncontrolled release of radioactive materials.

It evaluates the efficacy of fire protection features, such as fire prevention, barriers, detection, suppression, and any need for additional protection.

The analysis is supported by a combustible loading calculation quantifying the heat load and BTUs per square foot; combustibles installed or stored in each area; and, the radioactively controlled area.

Safe shutdown analysis demonstrates a means of safe shutdown of the IUs to ensure they can be placed and maintained in a safe and stable condition, following a safe shutdown fire at any facility fire area.

Also demonstrates the capability of safety related equipment to prevent uncontrolled releases of radioactive material, as a result of fire.

The performance goals of the safe shutdown analysis are: radioactivity shall be maintained sub-critical in the event of a fire.

Combustible gas controls shall be capable of performing their necessary functions in the event of a fire.

Target solution cooling shall be capable of removing heat, such that the target solution boiling does not occur.

Uncontrolled release of radioactive material shall be prevented. Equipment credited with a safe shutdown function.

Moving components designed and credited to isolate areas containing radioactive materials, are identified as part of the analysis.

The analysis is performed on a per fire area basis. Redundant trains of safety related equipment are demonstrated to be separated, such that a single fire cannot impair safe shutdown function.

Primary separation criteria is fire resistant barriers between the redundant trains. This is redundant equipment located in different fire areas.

Where redundant equipment is located in the same fire area, the following separation criteria are used in a fulmitative analysis.

Spatial separation distance of at least 20 feet where automatic fire suppression is provided, and at least 40 feet where automatic fire suppression is not provided.

Embedment of cable conduit and structural concrete. Fixed wares suppression and/or detection in the fire area.

Areas which have restricted access and/or are sealed. Areas which are continuously occupied. Administrative controls, and combustible loading.

Where these separation criteria cannot be met by analysis, our modeling is performed to determine if both trains of equipment can be damaged by a single fire.

Our fire modeling is a quantitative fire modeling performed using the Consolidated Model of Fire and Smoke Transport codes, to support the fire hazard and analysis, and safe shutdown analysis.

Two scenarios of concern are modeled. Fire involving a neutron driver high-voltage power supply and nearby cables, and fire involving the target solution vessel off-gas system motor control centers.

With a high-voltage power supply fire scenario, the objective was to determine if a fire involving the HVPS could impact the structural members of the building. Specifically the steel roof trusses, and the steel bridge crane rails.

CFAST used to determine the hot layer gas temperature, and temperatures of targets used to represent the structural elements.

The sources of combustibles were dielectric oil in the transformer, and cables in the nearby cable trays.

The damage criteria was 593 degrees Celsius. This is the critical temperature of steel.

The conclusion of the analysis was that

hot gas layer temperature at the target areas, is less than the damage criteria. Specifically, less than the critical temperature of steel.

CHAIRMAN BALLINGER: Now this is Ron Ballinger. I have a question about that.

When you evaluated the high-voltage power supply, did you folks evaluate what I would call arc faults, that could, that may or may not happen that would be source of a fire?

MS. RADEL: This is Tracy.

The source of the fire, I don't think was evaluated in detail within the modeling. It was assumed that it started on fire and the source of combustibles was the oil within the transformer, and the cable trays.

CHAIRMAN BALLINGER: I've see what can happen when you're operating an accelerator and you get an arc fault, and it's not a very pleasant experience. So, it's something you might think about.

Maybe it's impossible with your (audio interference.)

MS. RADEL: I think for the analysis it is just assuming that it does start on fire. So, I don't think it necessarily represents a more, you know, more bonding case.

But we will go to the team and talk to them about the likelihood of, of that event.

CHAIRMAN BALLINGER: Thank you. Sometimes these power supplies have a mind of their own.

MR. MEYER: For the TOGS MCC fire scenario, the objective was to determine the distance, both vertical and lateral, where critical temperatures are exceeded to determine whether a single fire can impact both TOGS MCCs.

The CFAST model was used to determine the zone of influence for the TOGS MCC fire, and the transient fires in the TOGS MCC hallway.

The sources of the combustibles in this area were cables from the MCC and transient fires. The damage criteria was 205 degrees Celsius, which is based on the thermal damage criteria for thermoplastic cables.

This bounds damage criteria for the bulk cables, which critical temperature of 500 degrees Celsius.

The completion of the analysis with the critical temperatures of both division A MCC were not reached by the fire, and division B MCC, and vice versa.

And the cables in the raceways above the

MCCs were not ignited.

The fire plans are developed for areas of the main production facility to provide information for trained facility personnel, and responding professional fire fighters.

Plans include the following information as appropriate. The area identification; forensic contact information; the occupancy and processes; fire hazards; radiation hazards; electrical information including electrical disconnects; hazardous substances; physical hazards; exposure protection guidance; communications; access and egress routes; ventilation; fixed fire systems; portable fire fighting equipment.

(Pause.)

MR. BARTELME: This is Jeff Bartelme. Any additional questions on the fire protection?

MEMBER HALNON: Yes, this is Greg Halnon. I got a list of just kind of miscellaneous questions I'd just like to have a conversation about, and work through it.

It's not necessarily specific to your presentation, but fire plan and a fire hazards analysis.

First one, I realize, you know, we've

talked about this a little bit in the past where large area fires were not required to be evaluated for the regulation.

But you do have a aircraft impact in your design basis, and you do a good job of establishing the impact perspective, whether or not there's a problem or not.

However, the ensuing consequences of potential fire, given the fact that your structural steel is not thermally protected, or fire protected. And, that was part of the concern in the HVPS fire.

Have you thought through what that looks like from a external perspective, with the potential fuel catching on fire from an impact?

MS. RADEL: So, this is Tracy.

So the fire as a result of any aircraft fuel on the exterior of the building, was not specifically evaluated.

The SHINE structure, external structure, is concrete with embedded rebar. There's not exposed structural steel on the exterior of the safety related portion of the building.

But it was not evaluated in detail on any, any kind of effects on the concrete structure, other than the, the impact itself.

MEMBER HALNON: Okay. All right, that may be something we can talk about a little bit more.

But we need to just kind of click down, Tracy, through my questions and it's you or Andrew probably can answer.

Is there going to be a dedicated fire marshal either part-time, full-time or part-time?

MS. RADEL: No, there will not be.

MEMBER HALNON: Okay, so who's responsible for maintaining the efficacy of the fire program?

MS. RADEL: Sorry, can you restate that a little bit louder?

MEMBER HALNON: Yes. Who's responsible for the fire program? Who's the assigned person who makes sure that the fire program continues to be complied with?

MS. RADEL: For the fire protection program, that's owned by the safety analysis team.

MEMBER HALNON: Okay.

And, is there any, any fire specialist in that team?

MS. RADEL: We --

(Simultaneous speaking.)

MEMBER HALNON: This is a big deal. Fire is one of the things that, you know, can drive radiation outside any facility.

So I'm really curious about how the fire program is going to be maintained.

MS. RADEL: We utilize an outside contracting group that has been involved throughout the project on the development of the program, and performance of the analyses.

We have been working to grow the SHINE staff development in this area, through supporting ongoing educational training in that area.

So, we feel that we, with the contract firm, the vendor that has been involved throughout the project and the effort to grow this capability, that we have sufficient coverage.

MEMBER HALNON: Okay, well I think I hold the opinion that if nobody is specifically assigned on the staff, then nobody's going to specifically be that concerned about it.

So, you might consider having at least a part-time person that, just like a safety person, just like you have a corrective action person, might consider that.

The second, next question is, you do a pretty decent job throughout the hazards analysis to discuss how fire is confined to the cubicles. You know, ventilation shuts down the, the dampers shut, and that sort of stuff.

But how about re-entry. What are your plans, and maybe this is a pre-fire plan issue, or maybe it's just something you have to do ad hoc.

But what are the plans for re-entry? How do you eject that smoke, and sample it, and make sure that it's not radioactive, and passthrough filters and what not? Especially in the RCA.

MS. KOLB: Yes, this is Catherine Kolb.

The recovery actions for fire is similar to recovery actions for any emergencies, are covered by our emergency plan.

We have not pre-prepared specific recovery actions for that, but we have the capability in the emergency plan, you know, dedicated people and a process for developing recovery plans, and re-entry provisions.

But we don't have anything specifically prepared.

MEMBER HALNON: Okay. That might be again, something you think through in the pre-fire plans because eventually, you got to get back into these places and, you know, assess the damage and what else, so.

All right, the next question is, has to do with training. You pass along, I mean you have an incipient fire brigade, or fire response, and then you pass on to any fire fighting professional fire fighters.

Given the hazards that are very unique at this facility, how are you making sure that the professional fire fighters from outside are protected, one?

Two, are able to fight fires in radiological areas; and, three, don't do the wrong thing from the standpoint of putting water where it shouldn't be, especially from a moderation perspective?

MS. KOLB: Yes, this is Catherine again.

So we have been in discussions with the Janesville fire departments in relation to the, our emergency planning.

Per our plans, they will be offered periodic tours, and orientation information, to allow them to be familiar with the facility.

And, to have any kind of familiarization orientation training on the various hazards of the facility.

The pre-fire plans, as well as the

emergency plan, will be provided to the fire departments for their use, similar to other industrial facilities in the city.

MEMBER HALNON: Okay, do you plan any real time drills, or other types of things in your facility, before you actually bring in radioactive materials so that they can be familiar with the actual cubicles, and ingress and egress passes, paths?

MS. KOLB: We are not required to have a drill prior to receipt of the OL, but our emergency plan has provisions, not just for fire but for all emergencies, for drills and exercises.

Exercises to be conducted every two years with invitation to the local emergency responders, including the Janesville fire departments.

MEMBER HALNON: Okay, but there's no plan on prior to the operation, to allow the, at least the leadership of the fire department to walk through the facility to be familiar with the, with the cubicles?

MS. KOLB: We don't have plans to do a full blown exercise currently, but we do intend to, you know, give them a tour, and offer information and familiarization about the facility prior to the OL.

MEMBER HALNON: Okay. But it makes sense. I mean certainly before you can, you know you have to put the symmetry on, it would be good to get them through the facility.

Fire water storage. I know you used the Janesville water system, and there's no fire water storage on site.

Could you explain your reasoning for not having at least the minimal amount of fire water storage for potential outages, or freeze ups of the water mains?

MS. RADEL: This is Tracy. In the testing of that fire supply system, in the water supply system, we ensured that there was sufficient flow and pressure, for the duration needed.

I would need to go back and look at the exact, exact detailed numbers on, on what was required and demonstrated during that testing, for the fire loop.

MEMBER HALNON: Okay, well yes, I didn't have any question. I think I read through that and saw that there was sufficient capacity. I'm just consider the reliability of the water system.

I couldn't find any information online about reliability, so I'm assuming that it's got a high level reliability.

But it does get cold up there and I've

just, at least in my area, in Cleveland we seem to have water main breaks all the time, which it may be a much older system.

But I was just wondering if there was any discussion relative to reliability of the water system. I realize that when it's working, it's fine. But what about when it's not working?

MS. RADEL: Yes, I would, we would need to go back and check for reliability numbers on that.

MEMBER HALNON: Okay. At least we should factor that into the analysis of summary.

I think this is the last question. It talks about, and this may be a pre-fire plan and part of that familiarization training.

But since you don't have any drains in the RCA and you try to limit water in there, you talk in the plan about having operations available to the professional fire fighters to advise for when that water could go in, and what not.

The professional fire fighters will probably be in Scott Air-Paks, fully decked out. Will you have the ability, how, explain to me how the operations folks will communicate with the fire team leaders, or fire brigade leaders, from the external folks, to ensure that there's no water put one, in the

RCA, or where it shouldn't go from a moderation perspective.

MS. KOLB: This is Catherine. Are you commenting on the fact that they'll be in Scott Air-Paks and hard to talk to? Or I guess --

(Simultaneous speaking.)

MEMBER HALNON: Well --

MS. KOLB: -- could you elaborate a little bit on the question?

MEMBER HALNON: -- that just makes the communication more difficult.

I'm wondering how the operations folks will communicate with the professional fire fighters fighting a fire in the RCA on use of water, or use of agents that might be inappropriate for, from a radioactive perspective.

Or in the, I know that with no fire, with no floor drains, that the use of water in there is not expected.

But there is the statement in the fire plan that says, operations will advise the professional fire fighters about use of water to ensure that the moderation, no moderation will occur for, for fissile materials.

MS. KOLB: Okay, I understand. So the

primary means of communication to the fire fighters will be via the pre-fire plans, which they will have access to and we will have available onsite.

I guess we don't expect them, fire fighters, to come into the facility, you know, without the knowledge of the operations team.

It is a, we have site security and they would need to open the fence. So people would be escorted at least up to the, up to the building and be able to communicate with them prior to entering.

MEMBER HALNON: That's really --

(Simultaneous speaking.)

MS. RADEL: This is Tracy --

MEMBER HALNON: -- that's doesn't --

MS. RADEL: -- and in addition, the area that is restricted from a fire spray perspective, is a very small area of the facility.

And, we would ensure that that is very clear to, to the fire department as far as that, that.

MEMBER HALNON: Okay.

I think you're making the case why the professional fire fighters need to be very familiar with the facility.

People at the facility, they need to be drilled once in a while to make sure that those types of communications occur. Because that's, as an ex-fire fighter myself, water is our primary agent.

But when we're going to do that, so we need to make sure that those lines of communication. And it's a crazy time when the, when a fire is occurring. And, there's a lot of people descending on it.

There's a lot of people chasing the soccer ball, and just got to make sure that the team leaders and the operations folks are connected up.

I think that is my last question so I'm done.

Thanks.

CHAIRMAN BALLINGER: Steve Schultz, you had your hand raised. Did you get your question answered? I had mine answered by, by Greg, so --

(Simultaneous speaking.)

DR. SCHULTZ: Yes --

CHAIRMAN BALLINGER: -- do you still have a question?

DR. SCHULTZ: No. The questions that Greg asked were on my list, as well, especially associated with the training, and the familiarization of the professional fire fighters.

I don't think once every two years is

going to be sufficient, to provide them with sufficient information in case something does occur.

For all those reasons that Greg had mentioned, that communication is very important and the pre-fire, the pre-fire plans really have to be taken very seriously with regard, with regard to that, that piece.

CHAIRMAN BALLINGER: Good ideas. Are you ready?

MEMBER DIMITRIJEVIC: Yes, this is Vesna Dimitrijevic.

I have a couple questions about your safe shutdown analysis.

So the bottom of the, my first question is, what did your entering assumptions when you analyzing the, you know, you are looking at the for 70 function activity combustible gas controlled cooling, and preventing releases?

What are your entering assumptions? Do you assume the operator will initiate the IU cell safety actuation?

Is that your first assumption?

MS. RADEL: This is Tracy. We don't assume that an IU safety cell actuation was initiated, prior to the event occurring.

You know, the safety system redundancy provides protection such that if there is an outside condition during that fire event, that the safety system can sense it and take appropriate action.

So there's not operator action assumed at the, at the onset of the event.

MEMBER DIMITRIJEVIC: So, how are you going to dump the, the solution, you know? What would actuate the valves?

MS. RADEL: So if the safety system senses an unsafe condition, it will actuate the, the valves and initiate shutdown of the unit.

MEMBER DIMITRIJEVIC: Wait, wait, wait. What does it mean, if what non-safe conditions?

MS. RADEL: So the sensors within the, all of the sensors and safety functions that we'll talk about within the TSC reactivity protection system, and the engineered safety feature actuation system, have sufficient redundancy and separation such that at least one train of instrumentation and control function, safety functions, would be available to take action automatically if there was an unsafe condition.

That is not to say that if there's a fire in the facility, that we would not have operators initiate shutdown to the units.

It's just it's not relied on to, relied on to mitigate the event.

MEMBER DIMITRIJEVIC: So it's not that clear. What are the input for your activity controller, that you assume that that will be actuated?

MS. RADEL: If --

MEMBER DIMITRIJEVIC: I mean and also for cooling, right? Your cooling relies on light water pool, right?

(No audible response.)

MS. DIMITRIJEVIC: I mean that is why function of the cooling, assume that the target solution is dumped into the pool.

MS. RADEL: The target solution would be dumped into the pool if one of the, one of the limits was exceeded within the safety systems.

We do not have I guess, a system that would be based on fire, automatically dump all of the units.

It's looking at these, the safety significant parameters within all of the systems and taking the, the safety actuations if those unsafe conditions do arise, concurrent with the fire.

So, in the safe shutdown analysis, we're ensuring that with a fire in any part of the facility, we have sufficient redundancy, and passive safety within the systems, that we don't have an unsafe condition that would violate one of those performance goals that's listed on the screen.

MEMBER DIMITRIJEVIC: So basically what you're telling me, and you can have a fire in any facility, and as long as you have a cooling system working, and you have, you know, so therefore, you have offsite power, that, you know, the target solution will be in the vessel?

MS. RADEL: So to clarify, offsite power is not required. The units fail to a safe state, so on any kind of power interruption, they will dump the solution into the TSV dump tank, and it will be passively cooled by the light water pool.

MEMBER DIMITRIJEVIC: Right, right, but I'm interested the case you didn't lose the power by fire.

MS. RADEL: Okay, yes. If you do not lose power and you've lost cooling flow, then the loss --

(Simultaneous speaking.)

MEMBER DIMITRIJEVIC: But you haven't lost cooling and power, but you have a fire in some area which may damage your, you know, the combustible gas systems, things like that.

What's happening the, but you have a power in cooling, do you still have the, your target solution --

(Simultaneous speaking.)

MS. RADEL: Yes, so --

MEMBER DIMITRIJEVIC: -- in the vessel.

MS. RADEL: -- so no matter what system the fire is impacting, function of, if that, if it's a system that's going to impact the safety of the unit, it would, the impacts of that would be detected within the IU cell, within the system itself.

It's looking at, as we'll discuss later, it's looking at temperature of cooling waters, flow of off-gas, you know, ability to recombine the hydrogen. You know, all the neutron clocks.

If there are any unsafe conditions that result from the fire, those will be detected, and the appropriate safety actuation will occur due to the redundancy in the system design, and the separation between the redundant safety trains.

MEMBER DIMITRIJEVIC: Okay. I mean I have to think now about the same scenario, just because I was almost sure that you assume the operator would initiate, the, the, you know, basically what is your shutdown in this case.

So, now I have to rethink all my, you know, analyze it of this.

Let me ask you the other questions. You didn't really do that, the (unintelligible) analysis for like a spurious actuation?

MS. RADEL: Sorry, can you repeat the question?

MEMBER DIMITRIJEVIC: You didn't do (unintelligible) analysis, right? The analysis for the spurious operation of the, you know, like --

(Simultaneous speaking.)

MS. RADEL: No, the analysis doesn't go into spurious actuation, although it does assume a single, single failure in addition to the fire event.

So, that could have been a spurious actuation. But doesn't go beyond that, so we don't evaluate multiple spurious actuations.

MEMBER DIMITRIJEVIC: So for example, the one of your functions, you know, the prevent releases, requires multiple components to move, right.

The dampers, the ventilation dampers, it would make a (unintelligible) to move it a certain position.

But you did not really analyze after they move in that position, they can be spuriously open or close, or whatever the safety position is by the fire.

MS. RADEL: To clarify, we did evaluate a single failure in addition to the fire, which could have been a spurious actuation.

So essentially, a damper or an isolation valve failing to go to it's safe state. Due to the redundancy in the system, however, there is always the, the dual isolation, dual dampers.

You know, for, for the hydrogen mitigation, it is parallel paths so that a single failure would not result in an unsafe condition.

MEMBER DIMITRIJEVIC: All right, thanks.

CHAIRMAN BALLINGER: Other questions from members? Or consultants, excuse me.

(No audible response.)

CHAIRMAN BALLINGER: Okay, hearing none, can we shift over to the staff?

MR. BARTELME: Yes, good morning, this is Jay Robinson, I'll be presenting. We'll give it a second to get the slides up.

CHAIRMAN BALLINGER: I can see them fine.

MR. BARTELME: Okay, great. Good morning, my name is Jay Robinson. I am one of the fire protection reviewers, who conducted review of the SHINE facility.

The fire protection review was conducted by the office of Nuclear Reactor Regulation, Division of Risk Assessment, in the PRA licensing branch B.

Next slide, please.

Fire protection systems and programs. Fire protection for nuclear facilities uses defense-in-depth, as SHINE talked about, to achieve the required degree of safety by using administrative controls, fire protection systems and features, and post-fire safe shutdown capability.

Defense-in-depth is designed to present fires from starting, detect, control, and extinguish those fires that do occur.

And, to provide protection of SSC's important safety, so that a continuing fire will not prevent the safe shutdown of the plant.

Next slide.

The regulatory basis that's included in 10 CFR 50.48(a), fire protection. That requires a fire protection plan that describes the fire protection program, identifies positions responsible for the program, and authorities delegated to those positions.

It outlines plans for fire protection, fire detection and suppression capability, and limitation of fire damage.

Describes the administrative controls and personnel requirements, for fire prevention and manual fire suppression activities.

It describes automatic and manually operated fire detection and suppression systems; and, it describes the means to limit fire damage to SSCs important to safety, to ensure safe shutdown.

Next slide, please.

Your regulatory basis also includes criterion three of appendix A, to 10 CFR Part 50, in that SSCs important to safety shall be designed and located to minimize the probability and effects of fire and explosions.

Non-combustible and heat resistant materials shall be used whenever practical. Fire detection and fighting systems of appropriate capacity and capability, shall be provided and designed to minimize adverse effects of fires on SSCs important to safety.

And, fire fighting systems shall be designed to ensure that there their rupture or inadvertent operation, does not significantly impair the safety capability of those SSCs.

Next slide.

The acceptance criteria we used was in

NUREG-1537 Parts 1 and 2. There is the ISG also for NUREG-1537, but the ISG did not have any applicable parts related to fire protection.

The NUREG has to, states that the fire protection plan needs to discuss the prevention of fires, including limiting the types of, and types and quantities of combustible materials, and needs to discuss the methods to detect, control, and extinguish fires.

And, it needs to discuss that the facility should be designed, and protective systems should exist, to ensure a safe shutdown and prevent the uncontrolled release of radioactive material, if a fire should occur.

Next slide, please.

Acceptance criteria also includes that the SAR should contain sufficient information to support the following, the conclusions listed below.

That the facility meets local and national fire and building codes; the fire protection systems can function as described; and, limit drainage and consequences at any time.

That there is reasonable assurance that training for fire protection is adequately planned; that the potential radiological consequences of a fire will not prevent safe shutdown.

And, any fire related release of radioactive material to the unrestricted environment has been adequately addressed.

That release of radioactive material from fire would not cause radiation exposures that exceed 10 CFR Part 20.

And, that fire protection technical specialists have been developed, if that's applicable.

Next slide, please.

Our review process and evaluation included review of the preliminary safety analysis report, and also the safety evaluation for the construction permit.

We also looked at the final safety analysis report, that was submitted with the application. We also looked at additional licensee supporting documents. They're listed below. I think you all familiar with them.

The fire protection program; the fire hazard analysis; safe shutdown analysis; combustible loading calculation; fire modeling.

Draft procedures for combustible controls, et cetera. The pre-fire plans, and radiological dose consequences.

Next slide, please.

During our review we developed about I think 10 requests for additional information. Ten, they all had some sub-parts to them.

The licensee responded to those requests and provided additional information. Some of the notable clarifications included fire brigade, and manual fire fighting capability.

Operator actions, the fire protection change control process; construction elements; safe shutdown analysis.

The administrative controls; the codes of record; code deviations; and, also radiological consequences.

Next slide, please.

Our evaluation findings. We found that fire protection related SSCs and defense-in-depth controls are designed, construction, and used consistent with good engineering practice.

Which dictates that certain minimum requirements be applied as designed and safety considerations for any new nuclear material, process, or facility.

We found that there's reasonable assurance that the fire protection systems and programs are in conformance with NUREG-1537 Parts 1 and 2.

Next slide, please.

(Audio interference) found that there's reasonable assurance that the facility meets the requirements of 10 CFR 50.48, Part A, and criterion three of Appendix A, to 10 CFR Part 50.

And, we also found there's reasonable assurance that a fire in any plant area, during any operational mode in plant configuration, will not prevent the plant from achieving safe shutdown and maintaining a safe and stable condition.

And, will also not cause radiation exposures that exceed the requirements of 10 CFR Part 20.

And, that concludes my presentation. If anyone has any questions, please feel free to ask.

CHAIRMAN BALLINGER: This is Ron Ballinger. Can you go back to slide number what is it, 4?

And, I'd like to pull, oops, did I blow that regulatory basis? I'm looking at the presentation that I had before.

It's the slide titled Regulatory Basis. Okay, I'm going to pull the string a little bit more, that Member Halnon was pulling.

It says that, boy, I'm, my presentation

that I'm looking at is pretty tough compared to the one that I've seen.

It says, but anyway, 10 CFR 50.48 da da da identifies positions responsible for the program, and authorities delegated to those positions.

Member Halnon was asking questions related to who's in charge of the fire protection program. Basically, is there a fire marshal.

So from what we heard in response to his questions, it's not clear to me that that criteria is satisfied. But I'm probably misinterpreting something.

So can you elaborate a little bit? Maybe Member Halnon can enlighten me.

MR. BARTELME: Oh no, yes, I can, yes I can.

So we asked a question about that. Just bear with me for one second, I just, I had it right here. I want to make sure I'm in the right.

They responded to that in a request for additional information, where you describe the fire protection organization and its responsibilities.

And, they outlined the responsibilities for the safety analysis manager, the operations manager, the maintenance manager, and fire protection staff. And, also the fire response team.

So, in that response, they satisfied the answer to our question to describe the organization and how it functions, and the authorities, as well.

MEMBER HALNON: We were just told that there is no fire protection staff, dedicated staff though, so how did they respond to, to that?

MR. BARTELME: Hang on one second. This is in a RAI response we got in December of 2020.

(Pause.)

MR. BARTELME: Okay, the fire, this is what SHINE has stated. The fire protection staff is comprised of engineering and operations personnel, responsible, I'll slow down, responsible for the performance of inspection, surveillance, accepting and, acceptance and periodic testing, and implementation of design changes as necessary, of fire protection systems.

Specific responsibilities of the fire protection staff include resolution of day-to-day fire protection issues.

Periodic update to the fire protection plan and sub-tier documents; conduct of fire protection engineering analysis.

Conduct of fire related training;

performance of liaison activities with an offsite fire fighting organizations.

Performance of period facility walk downs to assess the compliance with housekeeping, combustible loading, ignition control, and design requirements regarding fire prevention.

Ensure facility compliance with fire protection design and licensing commitments, regulations, committed codes and standards, building code requirements, and insurance requirements.

Review of plant design changes to provide concurrence on fire protection aspects; and, reporting and investigation of fire occurrence and fire related losses.

CHAIRMAN BALLINGER: Yes, this is Ron again. I mean what you're describing is the functions of what amounts to a committee.

I'm ex-Navy, and I'm interested in if I want to pick up the phone and call somebody who's responsible, who do I call?

So, it's not a committee that I want to call, it's a person that I want to call.

Am I stating this right, Greg?

MEMBER HALNON: Well, that's the concern. I mean, the amount of things he just read off were, you know, it's a full-time job almost.

But a lot of that can be spread amongst the engineering processes and work control processes, and people would affect it.

It really comes down to the importance that we place on, on some of the programmatic aspects of it, including the training, and pre-fire plans, and what not.

It just feels uncentralized, or disbursed to the point where it could possibly be an issue, at least in my mind.

MS. RADEL: So this is Tracy. I do want to clarify, you know, we had a engineer dedicated to fire protection who recently left SHINE. We have a posting currently up for fire protection engineer.

And, the safety analysis manager is ultimately responsible for the fire protection program.

But our intent is to hire a dedicated fire protection engineer, to have their primary focus be on the fire protection aspects.

But with recent staffing challenges, we don't have that person currently on staff.

MEMBER HALNON: So Tracy, would that fire protection engineer be the liaison with the offsite folks as well, relative to the training and, and maintaining pre-fire plans, and liaison with operations, and making sure that the pre-fire plans are appropriately up to date?

MS. RADEL: Yes, and that is the function that the engineer that, that recently left SHINE did perform, so.

MEMBER BIER: Can I have a quick follow up? This is Vicki Bier.

I guess this is probably for Tracy, but maybe also for staff. One other comment with regard to fire protection responsibilities.

I think Tracy, you had mentioned that it, the primary responsible person is the quote/unquote, safety analysis manager.

But I'm also a little concerned that safety analysis is very different from day-to-day operational responsibilities, of making sure that fire suppression equipment is operational and tested, and all that kind of thing.

And, so, you know, there's, they obviously both have safety in common, but I'm not sure that safety analysis is, has the same operational focus.

MS. RADEL: Yes, as noted, the fire protection engineer would have primary focus on it, you know, safety analysis manager, you know, being that person's direct line manager.

But, you know, additionally, the people within the operations team, as well as other people within the engineering team, would also be involved and aware, you know, made aware and trained, based on what they need to know for performance of their functions.

And, that fire protection engineer would, would be, rely on to help ensure that appropriate training is developed and I know some of that has already, was already drafted by the previous fire protection engineer.

CHAIRMAN BALLINGER: Yes, this is Ron Ballinger again. I mean I think that what we're trying to convey, at least what I'm trying to convey, is that you know, fire protection, you better, you hope you never have a fire and maybe you never do, or that the frequency is so, so infrequent, that you get to the point where you don't really think you need one.

And, so things sort of decrease in importance. Let's put it that way. But when you actually have a fire, things change very radically, all at once.

So being conscious of maintaining vigilance if you will, is important here.

MEMBER HALNON: So, yes, Tracy, this is Greg.

I need to go back to the previous question I asked. I asked if there is a full-time or a part-time fire marshal, and it was stated that there was a contract out for contract staff, or contract work.

Now you're saying that there is going to be a dedicated fire protection engineer, which by default I guess the way you described it, has fire marshal responsibilities.

So, could you go back and circle back and make the record clear. Is there going to be a full-time or part-time fire, dedicated fire staff at, at SHINE?

MS. RADEL: Yes. So the intent is to hire a dedicated fire protection engineer that would, would work within the safety analysis team.

The coverage that we have through our contractors, who have been involved throughout the entirety of the process, who have been the certified fire protection engineer signing off on the program and the calculations, and documents, will remain engaged as well, to provide what we consider sufficient coverage prior to us finding that staff member.

And, longer term we intend to keep them engaged.

The as far as fire marshal duties, a power plant, having not worked at a power plant myself, I don't know the exact duties and expectations of the fire marshal.

On our, for our facility as I discussed the, you know, the redundancy and isolation between trains, as well as the failsafe states of the systems, really, you know, ensures that the fire doesn't result in exceeding the SHINE safety criteria.

So potentially, there's a difference in level of risk between our facility, and a power plant. And, Catherine, if you have other items having worked at a power plant can speak to.

MS. KOLB: Sure. So some of the other responsibilities of a fire marshal including, you know, controlling transient combustibles, and housekeeping walk downs, and making sure the, you know, systems are functioning appropriately.

You know, depending on whether it is a pre-planning kind of thing, we would expect that to be assigned to the fire protection engineer.

Or if it is, you know, a housekeeping walk downs, and, you know, minimizing transient combustibles, that would be the responsibility of the operations.

The shift supervisor, and the people that worked for them, you know, who do those kinds of walk downs of grounds as part of their normal duties.

So I should note that the SHINE facility is physically much smaller than a typical power reactor.

So it's not inconceivable that, that, you know, these duties, it's not, we don't see it as two or three full-time people to be able to do this.

That if the fire protection engineer has the primary responsibility for ensuring that the program is met, that the in-plants and surrounded by other duties, can just be accomplished by the regular operating staff.

MEMBER HALNON: Thanks, I appreciate that. I think that's appropriate. And, I don't think we were pushing for a huge staff.

I think it's mainly is there going to be an accountable person for the fire program as a whole, beyond just a management person who's got plenty of responsibilities already.

So I think it's, you know, your discussion about a dedicated fire protection engineer is appropriate.

The fires in big facilities are usually caused by welding work, or transformer failures, or motor failures to that effect, and you're not exempt from that there as well as the facility ages, and as you do other work in the facility.

So, the size of the facility doesn't matter, it just limits the amount of maybe potential equipment that could fail. Or work that you might be doing.

So, I think, you know, we probably talked about this enough. I think you get our point. I think you've satisfied at least myself, that there will be a dedicated owner for the fire plans, and fire programs.

I think that's just a real important aspect of ongoing communications with the management staff.

DR. SCHULTZ: Tracy, this is Steve Schultz.

I'll just take one more chance to having my experience with emergency planning development for nuclear power plants.

The emergency plan and the fire protection plan, is probably the most important connection you're going to have with the community.

And, to the extent you create a very firm relationship with the fire department, to make sure that they are really comfortable regarding the operation and safety of the facility.

To the extent you do that, you will find it extremely valuable in the future, in terms of your facility operation.

If there is an incident at the facility and the fire department is called, and whether it's a big fire or just an emergency of even a medical emergency, it's very important that when they get back to the community, they will be able to let the community know that they're very familiar with the facility. They know how it operates, and so on and so forth.

It's don't minimize the benefit you can create if you do those things that Greg was talking about.

Getting the fire department and individuals in the facility early. Training them so that they're very familiar with the operations so that there's no question that when they need to come to the facility, they'll have if you will, a good experience and be able to help.

MS. RADEL: That's, thank you. I think that's a very good point.

CHAIRMAN BALLINGER: Okay, other questions by the members, or consultants?

(No audible response.)

CHAIRMAN BALLINGER: Okay, we're finishing about a half an hour early. We're ready, chapter 7 is next.

And, one of our members, we have arranged this schedule so that we can accommodate the schedule of all of our members. And, one of our members will not be available until after lunch.

And, so what we're going to do is to recess the meeting until 1:00 o'clock. So we'll just have a bit longer, longer lunch.

So unless there are objections or proposals for another way to do things, that's what we'll do.

(No audible response.)

CHAIRMAN BALLINGER: Hearing none, we will recess until 1:00 o'clock.

Thank you.

(Whereupon, the above-entitled matter went off the record at 11:29 a.m. and resumed at 1:00 p.m.)

CHAIRMAN BALLINGER: Okay. It's 1:00 p.m., time to start up again. We have been joined, and I'll probably miss somebody, by Member Rempe, Chairman Rempe, and our consultant Dennis Bley.

If I have missed somebody I am sure I will get reminded of it. In any case, we're going to do pretty much Chapter 7 the rest of, most of the afternoon anyway.

So we're all set. Is it Jason that's going to do this?

MR. POTTORF: Yes. This is Jason Pottorf.

CHAIRMAN BALLINGER: Okay. All right, we're ready to go, let's go.

MR. POTTORF: All right. Thank you. Yes, again, this is Jason Pottorf, Director of Engineering with Rock Creek Innovations.

Today I am going to do a quick presentation about HIPS implementation for the TRPS and the ESFAS.

I should point out that this presentation is essentially the same as what was presented back in February with some very minor modifications intended to address some of the questions that were brought up by Member Brown.

So I am going to quickly just skim through most of the slides here and when I get to a section where we made some changes I'll make sure and point them out, but, yes, definitely stop me if you have any questions anywhere.

MEMBER BROWN: Okay, I'll stop you now. This is Charlie Brown. Please remind me of what stuff you added based on my questions, if you would, if you know what they are.

MR. POTTORF: If you go to I believe it's Slide 4 or 5.

MEMBER BROWN: You don't have to go there now. I'm just saying as you go through the presentation you can tell me at that time.

MR. POTTORF: Okay. Okay, sounds good.

MEMBER BROWN: Do this in order.

MR. POTTORF: Yes. So we really have two major sections of this presentation, those related to the high-level architecture that was implemented for the TRPS and ESFAS and then the specific platform changes that were used in the implementation.

If you go to the next slide. One more. And so really the main change here that was made is these last three bullets on this slide here, and that is to point out, you know, how we are implementing diversity within the architecture.

If you remember in the HIPS platform topical we presented the representative architecture which was essentially what is being implemented for NuScale.

That architecture has four separation groups or divisions of input to the system with two divisions of actuation, and so the use of two diverse FPGA types was sufficient to mitigate common cause concerns in those four divisions.

But with the TRPS and ESFAS only having three divisions that does not work and so we have added a third FPGA type, and I've pointed out here exactly what we are using there.

Two of those FPGAs are flash types, as shown Division A has a Microsemi flash-type FPGA and Division C also has a flash type but it is of a different manufacturer.

So we do use the separate tools, the tool suites that are used to perform the programming of the device there. And then Division B uses the Xilinx brand SRAM FPGA.

So that is really the main change that I have made here to really point out how we are addressing diversity for these systems with three divisions. Any questions on that? If not, we can move on.

DR. BLEY: Yes, I'm sorry, this is Dennis Bley.

MR. POTTORF: Mm-hmm.

DR. BLEY: At some level you have defined the logic that the rays have to carry out and at whatever level that is, and you have used this special language for it, that's a level at which you don't have diversity, diversity comes after that.

And how have you ensured I'll call it the perfection of that specification of the logic?

MR. POTTORF: I'm not sure I understand the question. Could you repeat it?

DR. BLEY: You've given each of the vendors something to build into their FPGA, a logic structure, right?

MR. POTTORF: Yes. We use a model based approach to develop the logic from which we will generate hardware description language.

DR. BLEY: Stop. Stop right there.

MR. POTTORF: Mm-hmm.

DR. BLEY: At that point it's a common specification before it becomes machine specific or vendor specific. That's the point at which we don't have diversity and my question was what techniques do you use to make sure that that logic specification is essentially perfect?

MR. POTTORF: So we do do simulation testing of that logic prior to implementation into the FPGA and the hardware and then we will also do similar testing after implementation on the FPGA.

DR. BLEY: So a simulation testing for you means giving a set of inputs like those that would come from the plant to the logic and making sure it generates what you want?

MR. POTTORF: Yes.

DR. BLEY: What process gives us very good confidence that the set of simulations you have decided to run is complete, that there is not a somewhat different specification that will not make it properly through the logic?

MR. POTTORF: We do look at coverage of the logic in that testing to ensure that, you know, we cover all of the logic that we have designed and also that there is no, you know, test error logic in the design that does not get exercised.

Then we will, you know, we use our development life cycle that meets IEEE-7432 standard guidance as well, so --

DR. BLEY: I am somehow not quite getting there. I think we're close. When you did NuScale?

MR. POTTORF: So, yes, we have not developed the logic for the specific NuScale application yet.

DR. BLEY: Okay. But you have -- Okay, let's talk about SHINE.

MR. POTTORF: Yes. We are working through that process currently for SHINE.

DR. BLEY: They have given you a set of inputs that you would simulate to cover all of the accidents they are worried about as well as normal operations?

MR. POTTORF: So SHINE provides us higher level system requirements and we capture those in our own system requirements spec that we can trace up to SHINE's requirements for the system design and system functions.

From there we will then, you know, architect the system and allocate those requirements, functional requirements, to the individual HIPS components and then for each of those HIPS components that do utilize an FPGA we will develop a separate programmable logic requirement specification that gets linked up to the higher level system requirements.

From there our development life cycle

includes generating a logic design model to implement those individual programmable logic requirements and from that model we will generate a programmable logic design specification that, you know, captures a description of that logic model and associated with that logic model we will generate specific test plans, test cases, and test procedures that will be implemented for each FPGA separately.

So we essentially implement what would look like your typical software development life cycle. We do that for every individual FPGA. So we'll do all the integration testing for the logic components and then finish up the testing for that.

We do separate sets of testing prior to implementation of that logic in the hardware and then we'll do post-implementation testing of the hardware as well.

DR. BLEY: Well I think this is coming close. For the members on the Committee, you know, we worry a lot about were there any gaps in the safety analyses and risk assessments.

But that's assuming all this stuff works right and down at the definition of logic stage I'm not sure the Committee has ever taken a good look at that.

We might have some time ago on some older projects. Charlie, I think we did a little bit of that, but being comfortable with that seems like something we ought to touch on.

MR. POTTORF: Yes. I will point out we kind of split our life cycle out. You know, we go down for each FPGA and we go through, you know, kind of that full typical software development life cycle at the FPGA level where we will, you know, identify requirements, document the design, testing.

But then once we get through FPGA development and implementation on each specific module then we'll start to, we'll come back out to that higher system level where we integrate each module into separate chassis and cabinets and there we'll do what would be your typical system integration type testing that gets tied back up to the system level requirements that come from SHINE.

DR. BLEY: Okay. Thank you.

MR. POTTORF: Mm-hmm.

MR. HECHT: This is Myron Hecht. Can I follow up with a couple of questions?

MR. POTTORF: Sure.

MR. HECHT: Okay. So the 7432 standards and the NRC standards, of course, they'll send you to the IEEE software development standards for the software requirement spec and the design document and the test and the requirements verification.

Is that I'll call it HDL development plan described anywhere and has that been provided to the Staff?

MR. POTTORF: Jeff, do you want to respond on the status of providing that? Yes, we do document our life cycle that we use.

We do have a programmable logic development plan that we provide for each project as well as a verification validation plan, configuration management plan, all those things that you would typically see required for the IEEE standards for software development.

MR. BARTELME: So this Jeff Bartelme, Director of Licensing at SHINE. Programmable logic life cycle description is provided in the FSAR and we are currently, we have provided a number, all but one of the planning phase documents to the NRC Staff right now via the NRC reading room as we prepare for an upcoming NRC audit of the requirements phase for the HIPS core logic.

So we've made a number, there is still one outstanding document that we need to, we have to make available, but we have made a number of the planning phase documents available to the NRC Staff.

MR. HECHT: Oh, so that's in Chapter 7 or is that elsewhere? You said the FSAR.

MR. BARTELME: The description of the programmable logic life cycle in subsection 745 of the FSAR, yes.

MR. HECHT: That's the description, but I was asking more about the development plans and standards.

MR. BARTELME: The documentation that has been provided to support the upcoming audit is not part of the licensing basis and we haven't made it a part of the licensing basis nor docketed that.

MR. HECHT: Okay. So it sounds like it's not clear as to whether the programmable logic development plan and the associated standards have been submitted or not.

MR. BARTELME: Yes. The programmable logic development plan was part of that set of planning phase documents that have been made available to the NRC Staff.

MR. HECHT: Okay. But not part of the FSAR, because I thought I read it and I didn't see it. So that's fine. Do you know if there is anybody on the NRC Staff who is capable of understanding whatever hardware development by in which you are using?

MR. BALAZIK: This is Mike Balazik, NRC Staff, the Project Manager for SHINE. Yes, at this point we haven't completed our life cycle review of, you know, this is in a future ACRS meeting where we plan to discuss this.

So, you know, I guess I'd prefer not to get too deep in the life cycle here. Like I said we can address this at a later subcommittee meeting.

MR. HECHT: Okay. Thank you.

MEMBER BROWN: Are you finished Myron?

MR. HECHT: Well it was just pointing out what, following up on what Dennis said. I would agree with him that this is something that at the appropriate time the DINC, the Subcommittee should be looking into.

MEMBER BROWN: Okay. Yes, I think you got that. I think Mike said we would be addressing this later. I just wanted to know if you had anything else. I had a question I wanted to ask also. You done?

MR. HECHT: No, I'm done. I'm done.

MEMBER BROWN: Okay. Yes, this is Charlie Brown again. I noticed when you all did NuScale you had two volatile FPGA, a volatile FPGA and a non-volatile FPGA in the process, you know, two in each, one in each I guess, two in two channels, two in the other channels.

In this case because you didn't meet the standards that you needed to meet you now have gone to three separate ones, which is fine, is there a reason you picked two flash type as opposed to, which were non-volatile, and only one of them volatile, is it just easier to deal with or was there any thought at all given to that or just picked one?

I personally don't like volatile information being reprogrammed, but I like the choice. I just wondered if you had a thought on it.

MR. POTTORF: Yes, Gregg, if you are on you can probably address this better than I can.

MR. CLARKSON: Yes, certainly. Yes, this is Gregg Clarkson with Rock Creek Innovations. Yes, that's a good question.

On that third, that Division C, that Intel flash type FPGA, we definitely chose that because we like the behavior of the non-volatile FPGA.

Now I will note though that that Intel flash type is really sort of a hybrid. It's got non-volatile attributes with flash memory aspects, but it also has some of the volatile behaviors.

So it's really at the root of hybrid architecture between the two, and that was another reason we chose it, because that way, you know, it really represents more of a third type, if you will, than an all-volatile or an all-non-volatile for the third type. Did that answer your question, Charlie?

MR. POTTORF: Did we lose him?

MR. CLARKSON: Yes, did I lose -- Okay, you can hear me, Jason, okay.

MEMBER BROWN: No, I'm sorry, I turned my mic off while you were talking.

MR. CLARKSON: Oh, okay.

MEMBER BROWN: I apologize for that. I still haven't learned how to do this very well. I am not computer literate according to some people, so -- Don't take that the wrong way.

Let me rephrase my question relative -- In the NuScale as well as what you've got here you've got volatile memory such that when you lose power you obviously lose the programming of the FPGA and you have to redo it when the power comes back. It's got to reload.

I am only asking this question, I really like the diversity of the non-volatile ones that you are using here as opposed to the volatile. I didn't even think about it at the time and that what is the probability that, you know, you lose power you have to program, you lose power it re-programs.

You've got to have some confidence that you are going to get re-programmed correctly every time, you know, there is no glitches.

MR. CLARKSON: Right.

MEMBER BROWN: Did you all give that any thought at the time or --

MR. CLARKSON: Yes.

MEMBER BROWN: -- is there any hint that that is a long term, longer term problem or am I just blowing smoke?

MR. CLARKSON: No, I think that's a great point to make and certainly we looked at that. So let's just talk that through with the Division Alpha, the Microsemi Flash, are non-volatile.

So the way that works, you lose power, the power comes back up, there is no re-programming. So the configuration of the FPGA is retained, you know, exactly with the gates interconnected in absence of power because of the flash so they are maintaining that inter-connectivity.

With the Division Bravo, the Xilinx, which is the volatile type, what happens there is if you lose power that FPGA completely loses its configuration and upon power up it's going to get that configuration from an adjacent integrated circuit, an adjacent IC, that's a non-volatile memory that provides, it sends the configuration over to the FPGA and the FPGA, you know, the FPGA then powers up into that configuration.

Now this third one, this Division Charlie, this Intel, as I mentioned more of the hybrid, so what it does is it has configured, it has the non-volatile memory cells on the FPGA.

So it does not depend on an external IC like the pure, you know, the pure volatile style. But it also has some circuits that when you power up it needs to configure itself, if you well, but it does it on the same IC.

So, you know, what I did was I really studied that and, you know, wanted to basically account for -- You wouldn't have the same failure mechanism I guess is what I am trying to say.

The three are different in how they work, fundamentally work on the power up, so you wouldn't have a common failure mechanism across the three. So if your SRAM, for example, like you said, did not get the configuration information correctly, okay, it's not going to operate properly but the other two would not have failed in the same way so they are going to recognize that.

Your other two divisions are going to recognize you got Division Bravo not agreeing. You know, so that's why we, that's why that Intel hybrid flash based won out in our book, you know, to be that third type.

MEMBER BROWN: Okay, interesting. On the NuScale approach with the four channels, recognizing the same question, I walked away from that with the thought well, gee, I've got two that are non-volatile, therefore, if I come back and I lose something, but that's kind of a single failure approach.

If something happened while we were powering back up and we needed a response I had two channels that were working and would provide the two out of four that you need.

MR. CLARKSON: Right.

MEMBER BROWN: So, you know, I walked away from what we did on NuScale with that thought process, but it's just been nagging behind me. I like your explanation and I appreciate the insight you just gave me.

I am not a designer, so that's why I wanted to ask the question.

MR. CLARKSON: No, that's a great question, and like I said it was very -- You know, so it's really important when you are designed these, what we call the power-on reset circuit --

MEMBER BROWN: Yes.

MR. CLARKSON: -- is really critical here because as voltage is coming up, you know, it comes up over a period of time, it's a short period of time, but what you do not want to do is you do not want that FPGA to be released to reset prior to the voltage being stable.

So you want to give everything the proper voltage, all of circuitry the proper voltage, and then, you know, you want to make sure that in the SRAM case that it's had a chance to get its configuration over and everything is proper and then, you know, then you are allowed to release reset and let the circuit do what it's doing.

So a lot of care is taken on that, and I'll just say in simple terms how each of these three handle power on reset they are different from one another in that very minute detail of design.

MEMBER BROWN: Okay. All right. I have

seen circumstances in a couple applications I dealt with in my old, old where we had a rapid cycling of power, you know, power was restored and all of a sudden something else tripped off and it was then seconds it came back so that, so it cycled a couple of times.

So you are telling me that you don't like that to happen with the non-volatile types particularly?

MR. CLARKSON: Correct.

MEMBER BROWN: Okay.

MR. CLARKSON: Yes, you don't want to be caught in that indeterminate state.

MEMBER BROWN: Yes.

MR. CLARKSON: And that power on reset circuit is really there to make sure you don't -- You know, no matter what, even like you said in like a power glitch scenario, multiple glitches together --

MEMBER BROWN: Yes.

MR. CLARKSON: -- you don't want to ever be at an indeterminate state. And so, yes, you want to be very careful with that power on reset circuit design.

MEMBER BROWN: Well we are more stable in this because we do have battery backups that are sitting there, so you shouldn't run into that particular scenario.

All right. Well, thank you. I appreciate the -- Thank you for the discussion on that and I appreciate it.

MR. CLARKSON: Yes. Yes, you're welcome.

MEMBER BROWN: You can proceed whoever was on Slide 4.

MR. POTTORF: Okay, yes. Sorry, I was on mute as well there. Yes, if there is no more questions on this, that was the major change to the slides, so if we want to kind of walk through the rest of them.

There were no changes here on the architecture. If you keep going forward, I know the other topic, Charlie, that you had was with respect to a cybersecurity one-way flow of data from the system.

I would just point out that we have no data connections for inputs of any kind into the system from PICS. Everything interfaces with PICS from this system are discreet inputs or outputs.

MEMBER BROWN: While you are mentioning that, you don't happen to have a picture of 7.1-1, do you, in your slide pac?

MR. POTTORF: No, I do not have it in this slide pac.

MEMBER BROWN: Oh, okay. Okay, that's too bad. I understand and I got that out of reading the chapter. You've got more words -- You've probably mentioned the words "one-way," "not unit directional," et cetera, at least 22 times throughout the -- I'm pulling your -- That's a little bit of an exaggeration, but you are very emphatic on that.

The reason I ask the question about the 7.1-1 is that that's the complete picture of how both the ESFAS and the TRPS connect in and it's not clear from looking at the picture that that's what you've got relative to it.

But there is six red lines that go up out of the system out of the MICM from I guess both the two divisions of the TRPS and the two divisions of ESFAS plus another spare one coming up from something else.

So there are six inputs into the process configuration and it would just be nice if those were annotated as to being unit directional type connections.

That makes it clear and you don't have to search, word search the text, if you had a note with that. You did that on the NuScale drawing, by the way, which was useful.

That's just a suggestion for clarity. That's all. You are not required to do anything with that unless you feel that it would be a good idea to appease me, okay.

MR. POTTORF: Yes.

MEMBER BROWN: That was my only question there, just the clarity on that. So I understand that point. I do have a question later but I'll wait till the end of all this so you get through everything.

It's semi-related, but it's not exactly the same.

MR. POTTORF: Okay.

MEMBER BROWN: But you can proceed.

MR. POTTORF: All right, sounds good. Next slide, please, Jeff. Okay, so there is where we get into looking at specific changes to the HIPS platform.

Next slide. This is kind of the outline of those differences for the HIPS platform. No change to this slide from before. Next slide. Again, no changes here for this slide.

Also no changes here. This is where kind of touching on, Charlie, what you were just talking about there. That figure in the FSAR doesn't show the full details of the design implementation but we do have that one-way flow of data that starts from each of the MICMs in each division of the TRPS and the ESFAS and we're actually aggregating all of those one-way outputs from the system into a set of redundant chassis where we aggregate that information up and then provide it over to the PICS system.

MEMBER BROWN: Can I ask, let me ask one question relative to the one-way stuff. You use almost four terms within the document, the FSAR. You used the term "one-way," you use another term "one-way data diode," another term "unit directional alone," and another term "one-way isolated." Are those all the same?

MR. POTTORF: Yes.

MEMBER BROWN: Can you --

MR. POTTORF: Yes, all of those things are implemented at the MICM when we provide that data out, one-way via hardware data diode and it is isolated.

MEMBER BROWN: Okay. It just was the four different terminologies, I wanted to make sure there wasn't a nuance that I was missing somewhere.

MR. POTTORF: No. Yes, they are all referring to the same equipment there.

MEMBER BROWN: Okay. Thank you. I'll ask

a question about gateway stuff later if that's okay.

MR. POTTORF: Okay.

MEMBER BROWN: So we can get through the slides.

MR. POTTORF: Yes, go ahead, next slide. Yes, I don't believe there are any changes to the remainder of the slides here, so I think we can click through them and stop if you have any specific questions related to this.

This is covering the SBVM, which is a combination of the SBM and the SVM that were described in the HIPS platform topical that essentially all of the logic functions are the same as they were as described in the topical report.

Next slide. Just a figure to kind of show how we have combined the two functions that were described in the topical report into a single module of the SBVM.

MEMBER BROWN: Is that now a single module or I mean is it a re-designed single module concept as opposed to now two separate modules?

MR. POTTORF: That's correct.

MEMBER BROWN: Okay.

MR. POTTORF: Instead of, yes, a separate module in your signal conditioning and trip determination chassis and in a separate module of the SBM in the boating and actuation chassis.

Everything for signal conditioning and trip determination may be, for sure in TRPS it's all in one chassis whereas in ESFAS there are multiple chassis for ESFAS, but those functions are all really on the same module here.

I should point out that the logic that is implemented for say the SBM is independent on the FPGA from that logic that is used to implement the SVM. Even though they are on the same FPGA they function exactly as described in the topical report, which would have been on two separate modules.

We're just doing everything on the same module here.

MEMBER BROWN: Okay.

MR. POTTORF: Next slide. This is on the remote input submodule. This is just a new module that is essentially a mini safety function module that we're putting out in the field that is associated with a specific SFM in each division.

MEMBER BROWN: That's internal to the -- Yes, that's new.

MR. POTTORF: Yes, it --

MEMBER BROWN: I don't remember --

MR. POTTORF: But the way it functions is no different as that described for an input submodule. It's just simply we've pushed some of the communication logic out into the field on a small module.

I guess you could look at it as we have taken an SFM and kind of split off a chunk of it and put it out in the field.

MEMBER BROWN: What do you mean by "out in the field?"

MR. POTTORF: So this is specific to neutron instrumentation.

MEMBER BROWN: Oh.

MR. POTTORF: So rather than bringing those signals with the very small voltages on them all the way back to the control room we're digitizing that out next to the IU cells right next to the amplifier circuits and providing that via RS-485 connection back to its respective safety function module that's in the control room.

MEMBER BROWN: So that's the neutron flux detection system you're talking about then is where you are using them?

MR. POTTORF: Yes. We have a small module that is out in the plant right next to the neutron instrumentation equipment.

MEMBER BROWN: There is no -- That's strictly an analog function until you get to the transmitting, the RS-485?

MR. POTTORF: That's right.

MEMBER BROWN: Okay. And the RS-485 can be bidirectional, but it's a hardware configured communication device, isn't it? I have forgotten some of that.

MR. POTTORF: It is one-directional, you know, and that meets the way we have described the up to four RS-485 channels that are available on each of the HIPS modules. So we are using one of those channels to provide that one-way flow of data to its respective safety function module in the control room.

There is a second RS-485 connection that would be used for configuring the configurable parameters that are out on that module.

MEMBER BROWN: Are you -- In one of your -- Back in the, what is it, the TECRPT, section on gateway communications one of the ports in there was bidirectional intentionally.

But the way that gateway is utilized it's isolated so it didn't make it, but you're telling me that -- Where is the bidirectional use and why is safe again? You had a reason for why that was okay.

MR. POTTORF: So, yes, the gateway functionality is not related to this remote input submodule. I'll just point that out.

MEMBER BROWN: Okay, all right. Okay, all right.

MR. POTTORF: But as far was that gateway, we typically have for each MICM in each division that's where we are providing that one-way flow of data out from the TRPS and ESFAS.

That transmission of data goes to a set of redundant gateway chassis where we have multiple communications modules that are essentially collecting all of the data from both the TRPS and the ESFAS, all divisions, and then there is a set of communications modules in those two chassis, redundant modules that will then use MODBUS communications to PICS.

So that last chain in getting data out to the PICS is your typically MODBUS bidirectional communication. But all of the data that gets provided to those modules originates from those one-way connections from the MICMS to those gateway modules.

MEMBER BROWN: Yes, I saw that array, the picture, it looks like about 20 or 30 of these different little sub-ports if you want to call them that.

MR. POTTORF: Mm-hmm.

MEMBER BROWN: But the gateways are up in the, are they located up in the PICS? I don't want to get into the PICS. Is that where they are physically located?

MR. POTTORF: We put those two chassis in the Division C, ESFAS Division C cabinet, because there was room there.

MEMBER BROWN: Just a physical location, not a architectural location though, operational wise?

MR. POTTORF: That's right, yes. So we consider the modules in those two chassis that communicate with the TRPS, those are a part of the TRPS system scope.

The modules that receive the data from each of the three ESFAS divisions are part of the ESFAS scope and then we have the remainder of the communications modules that actually communicate bidirectionally all of that data.

So on the back plane of those chassis those final modules are gathering up everything from each of those TRPS and ESFAS gateway modules and providing that over to PICS.

All non-safety functions going on in those redundant chassis, but, yes, they are located in the Division C ESFAS cabinet.

MEMBER BROWN: If the indication and monitoring data from the TRPS it goes up to these gateways you said that's all sent up into the PICS and the same way with the ESFAS, do you maintain separation of that data?

It's not mixed in the same gateways? I mean in other words there is gateways dedicated to the TRPS and to gateways dedicated to the ESFAS?

MR. POTTORF: Yes. They are maintained separate into their respective modules in those two gateway chassis and then once they get brought into those modules in those two chassis they are provided over to separate modules on the back plane in those chassis so that they can be provided over to PICS via a separate set of modules.

MEMBER BROWN: Okay. But the circuits are separate, you're not mixing data?

MR. POTTORF: That's correct.

MEMBER BROWN: That answers that. That's all. That's what I was looking for.

MR. POTTORF: The very last module that provides the data to PICS we do provide everything, but everything is maintained independent and separate over into separate modules in those chassis as well.

MEMBER BROWN: When you get that last module do you lose all indication and monitoring off into PICS?

MR. POTTORF: We have redundancy so there are the two chassis, so they essentially have an identical set of modules in each of the chassis there so that if we were to lose one of those final modules we would still have that redundant module in the other chassis providing all data over to PICS.

MEMBER BROWN: How does PICS determine which module to take data from then when you are in operation if it's the same data?

MR. POTTORF: I would not be the best one to answer that question.

MEMBER BROWN: Okay. Well we'll save that for the PICS discussion. Just put that as a note for something for SHINE to tell us about -- I don't know whether that's your responsibility or not, so that would be a question that was -- There is very little detail.

I've got a number of questions that I am concerned about on the PICS because of the level of detail, but we can save that for the PICS subcommittee meeting.

So whoever hears this in the transcript can remember that I've got some other questions on that later.

MR. POTTORF: Sure.

MR. BARTELME: Yes, we've got that here, John.

MEMBER BROWN: Okay. Yes, who is that just spoke?

MR. BARTELME: This is Jeff Bartelme from SHINE.

MEMBER BROWN: Okay. Well Staff ought to pay attention that also I hope. Okay, thank you.

MR. POTTORF: Yes. Okay, Jeff, if you want to go to the next slide, please. Yes, this slide is really what we were just talking about there with the gateway communications modules.

Next slide. I think we should be close to the end. No changes on this slide covering self-testing. Next slide. Yes, no changes here on the LEDs on the front panels of the HIPS modules. Next slide.

MEMBER BROWN: Don't backtrack the slides, just does the use of gateways now complicate your self-test in terms of verifying what's coming from what place that goes to another and that the monitoring and indicating is going to be accurate?

That's a complicated setup with the gateways. That's my only thought.

MR. POTTORF: Yes, I don't think there is any impact as far as self-testing that is performed. We are still doing the self-testing on each module as described in the topical report.

MEMBER BROWN: Okay. Okay, so that shows up on LED active lights or something like that on the modules themselves?

MR. POTTORF: Yes, that's correct. You know, and that would be specific to the self-testing that is implemented on each individual module.

MEMBER BROWN: Okay. All right, okay. Thank you.

MR. POTTORF: Yes.

MR. CLARKSON: Yes, this is Gregg Clarkson. I will just add to that, Charlie, that your question there with the addition of the gateways, actually I would say that it helped our self-testing because the gateway if you think about it is a place that is aggregating that the monitoring and indication data to ultimately send to PICS, but because you have all of it there together you can do channel checks.

So it's a nice place to do, you know, an

Alpha, Bravo, Charlie division channel check, you know. So I think it actually helped our testing and gave us a little bit more visibility, you know, for that automated channel check.

MEMBER BROWN: Well the word "aggregate" just makes it sound like all the data is jumbled up and then spit out somewhere, you know, based on field data and what assigns what to what.

So that was one of my thoughts when I saw the word "aggregate." So you're telling --

(Simultaneous speaking.)

MR. CLARKSON: Well like Jason said though we were very careful to maintain that data stream is independent, you know, from each division, TRPS and ESFAS, and the independent modules to basically make sure we weren't sacrificing the protection system.

And then once we get that data over independently then, you know, on that final module is where you put it together. And it's not aggregated, it's very thoughtfully packaged up and then it's provided to the PICS.

But it's at that point there we can do an Alpha, Bravo, Charlie comparison, you know, and say, okay, these two are really close to the same but this third one is way out, something is going on there, let's throw an alarm for that.

MEMBER BROWN: Yes, that's what I was looking for, the ability to compare the various divisions to make sure you are okay, but if you aggregate it -- Identifying data and making sure you are consistent becomes a consistency issue but you are saying you are separate from your ability to compare the data coming in from each division?

MR. CLARKSON: Yes. And keep in mind that gateway, you know it's also implemented on all FPGAs, so all of that logic, you know, is finite-sate machines, completely deterministic.

It has to function the same very time, so there is really no jumbling, first come, you know, first serve type of thing. It works the same always, so the structure is very rigid.

You always know what data is what and where it came from because it's the same every time as far as the structure of how the data is packaged.

MEMBER BROWN: Okay. Thank you.

MR. CLARKSON: Mm-hmm.

MR. POTTORF: All right. Next slide.

MR. BARTELME: Jason, I believe that's the last of the slides here.

MR. POTTORF: That should be it, yes.

MEMBER BROWN: Okay. You're finished with that package slides on the HIPS then?

MR. POTTORF: Yes.

MEMBER BROWN: Does anybody else have any other questions? Dennis, do you have anything else?

DR. BLEY: No, Charlie, thanks.

MEMBER BROWN: Okay. Okay, I guess we're ready to switch over to whatever is next on the schedule. There is three different sets of slides if I remember, is that correct?

MR. BARTELME: Yes. We'll move over to TRPS/ESFAS slides now. I'll get those pulled up.

MEMBER BROWN: Okay. Is this the open set?

MR. BARTELME: That's correct, yes.

MEMBER BROWN: Okay.

CHAIRMAN BALLINGER: Who's got the slides?

MR. BARTELME: Can you guys see it? Can everyone see the slides now?

CHAIRMAN BALLINGER: I can. Thank you.

MR. BARTELME: Okay.

MS. RADEL: Okay. This is Tracy Radel. I am going to cover the Target Solution Vessel Reactivity Protection System, or TRPS, and the Engineered Safety Features Actuation System, or ESFAS.

Outline for the presentation, first we will cover an overview of TRPS and then move into the functions and monitored variables and then the mode transitions permissives and bypasses.

For ESFAS we will provide an overview along with the functions and monitored variables and then we'll touch on the priority logic and then the TRPS/ESFAS interfaces with the Process Integrated Control system, or PICS.

The TRPS is designed using the HIPS platform. It monitors variables important to safety functions of the irradiation process and performs safety functions required by the SHINE safety analysis.

It consists of eight independent instances of TRPS, each one dedicated to an individual irradiation unit. There are three divisions of monitoring equipment with two out of three coincident logic votes and there are nine total cabinets for the facility.

The first three cabinets cover IU cells 1 and 2 with Divisions A, B, and C, and then there are three cabinets, Division, A, B, and C, to cover IU cells 3 through 5, and then an additional three cabinets for cells 6 through 8.

You will notice that that division of cabinets aligns with the phased approach that will covered in a future ACRS meeting.

Moving into the TRPS functions, the safety functions are listed here in the IU cell safety actuation, IU cell nitrogen purge, IU cell tritium purification system, or TPS actuation, driver dropout, and then there is one non-safety function within the TRPS, which is the fill/stop function.

The IU cell safety actuation is initiated based on process variables that would indicate an insertion of access reactivity, a loss of cooling events, overcooling, loss of hydrogen re-combination capability, or breach of the primary system boundary.

The IU cell safety actuation transitions the unit to Mode 3 shutting down the irradiation process by opening the TSV dump valves and opening the breakers to the high voltage power supply for the neutron drivers assembly system.

It also isolates the primary system boundary as well as the primary confinement boundary. The IU cell nitrogen purge is initiated based on process variables indicating a loss of hydrogen re-combination capability and isolates the radioisotope process facility cooling system, or RPCS, to limit water intrusion.

This is for a very specific accident scenario which is related to flooding of the primary system boundary which would prevent offgas system flow, and so in response to an event we do isolate that source of water.

MEMBER BROWN: Can I interrupt you for just a second?

MS. RADEL: Yes.

MEMBER BROWN: This is just a calibration question. I just want to make sure that everybody from the Committee that is participating that the TRPS, the target solution vessel reactivity protection system, there is one of those for each of the eight IU cells.

The ESFAS is a facility protection system and there is only one of those for the whole facility. So I am just trying to make sure you understand what the configuration is for how the systems are applied.

So sorry to interrupt you. Just a little bit of a pictorial thought process, that's all. So thanks for holding up for a minute.

MS. RADEL: Yes. Appreciate the clarification. The IU cell nitrogen purge provides a purge of the primary system boundary for the affected irradiation unit with nitrogen.

So note that an individual unit could undergo a nitrogen purge while other units continue to operate. It does this by opening the nitrogen purge and vent isolation valves.

It also, as you'll see as we get into ESFAS, does send a signal to ESFAS to open the IU and TPS header valves as well.

The IU cell TPS actuation is initiated based on process variables indicating a breach of the tritium boundary within the IU cell or supply return lines or a breach of the tritium boundary in the TPS glovebox.

It isolates the TPS lines into an out of the IU cell and isolates the radiological ventilation zone one exhaust, RVZ1 exhaust, out of the IU cell. This signal comes from the ESFAS which also isolates the glovebox confinement and tritium room dampers.

Driver dropout is initiated based on process variables indicating a loss of neutron driver output or loss of cooling. These are really two separate functions of the driver dropout.

On the loss of driver output it opens the NDAS high voltage power supply breakers to terminate the irradiation process after a time delay. On

Function 2 where have lost cooling either through high temperature or through cooling flow it opens the NDAS high voltage power supply breakers without a delay. It also initiates an IU cell safety actuation after the 180-second delay.

Moving into the TRPS monitored variables and response, this slide covers those related to neutron flux. The high source range neutron flux protects against an insertion of excess reactivity during the filling process.

It initiates an IU cell safety actuation when two out of three or more signals are active. The low power range neutron flux protects against loss of the neutron beam followed by a restart of the neutron beam outside of analyzed conditions.

The driver dropout is initiated when two out of three or more signals are active for a predetermined amount of time.

High time average neutron flux protects against exceeding analyzed TSV power levels during Mode 1 and 2 and it initiates an IU cell safety actuation when two out of three or more signals are active.

The high/wide range neutron flux protects against exceeding target solution, power density, and temperature limits during Mode 1 and 2 and it initiates an IU cell safety actuation when two out of three or more signals are active.

Moving into the cooling systems, we have a high primary closed loop cooling system, or PCLS, temperature, which protects against a loss of cooling that could cause target solution heat up.

It initiates an IU cell safety actuation when two out of three or more signals are active for three minutes or 180 seconds.

Low PCLS temperature protects against an overcooling of the target solution that could cause an excess reactivity insertion. It initiates an IU cell safety actuation when two out of three or more signals are active.

Low PCLS flow protects against a loss of cooling that could cause target solution bulk boiling and initiates an IU cell safety actuation when two out of three signals are active for three minutes or 180 seconds.

In the TSV dump tank we have two level instruments. We have the low-high and the high-high. So the low-high protects about in-leakage into the primary system boundaries during Mode 1 and 2 that could result in loss of the TSV offgas system, or

TOGS, flow to the TSV dump tank headspace.

It initiates an IU cell safety actuation and an IU cell nitrogen purge when two out of three or more signals are active.

The high-high TSV dump tank level is protecting against a similar in-leakage event. During Mode 3 primarily is when this is relied on, when the low-high is bypassed because we have the target solution or TSV dump tank.

The high-high protects us on the water ingress event. It initiates an IU cell safety actuation and IU cell nitrogen purge when two out of three signals are active.

In the offgas system these are focused on detecting the loss of hydrogen recombination capability. We have the low TOGS oxygen concentration.

So this protects against deflagration in the primary system boundary caused by the inability to recombine hydrogen with oxygen. Really in operation we do expect oxygen to come out of the solution at a slower rate than the hydrogen.

So oxygen is injected into the system and we also monitor for oxygen concentration and initiate an IU cell safety actuation and an IU cell nitrogen purge if two out of three or more signals are active.

For flow we monitor the TOGS mainstream flow which protects against deflagration caused by an inability to sweep accumulated hydrogen through the TOGS hydrogen recombiners.

On low flow an IU cell safety actuation and an IU cell nitrogen purge would be initiated when two out of three or more signals are active.

We also monitor flow, directly monitor flow, to the dump tank. This protects against deflagration in the TSV dump tank caused by an inability to remove the accumulated hydrogen and also initiates an IU cell safety actuation and IU cell nitrogen purge.

High TOGS condenser to mister outlet temperature, this protects against failure of the condenser to mister which could cause adverse effects on hydrogen recombination, TOGS instrumentation, or the TOGS zeolite bed.

An IU cell safety actuation and IU cell nitrogen purge would be initiated when two out of three or more signals are active.

Additional monitor and variables within TRPS are the ESFAS loss of external power. This is a signal coming from the ESFAS indicating that power has been lost for (audio interference) three minutes or 180 seconds.

This will open the TSV dump valves and initiate the IU cell nitrogen purge of the system. Note that the TOGS blowers continue to operate for five minutes, so we start the nitrogen purge prior to losing the TOGS blowers.

The high RVZ1, the IU cell exhaust radiation, protects against a breach in the primary system boundary limiting the radiological release. So upon detection of radiation in the exhaust pathway it would initiate an IU cell safety actuation when two out of three or more signals are active.

TSV fill isolation valve position indication not closed protects against inadvertent addition of target solution to the TSV and initiates an IU cell safety actuation when one out of two or more signal is active.

ESFAS IU cell TPS actuation protects against tritium release events in the TPS and initiates an IU cell TPS actuation upon receipt of a discreet signal from ESFAS.

MEMBER BROWN: Just a momentary -- Your slides by the way are the cutting off the last line or two sometimes the way they are positioned, just letting you know that.

The IU cell line, bullet, is not there, at least it's not on my computer, I'll put it that way.

MEMBER HALNON: Charlie, I'm good. Check your screen. Maybe you need to maximize it or something.

MEMBER BROWN: I just clicked it. I just went off to something else and started clicking things and now it popped up, so thank you. I'm glad I said something.

MEMBER DIMITRIJEVIC: Charlie, this is Vesna. Can I take a little diversion in connection with my previous question in fire protection?

MEMBER BROWN: Yes, go ahead.

MEMBER DIMITRIJEVIC: So when we discussed fire protection you said that safe shutdown analysis that human actions were not credited and it was assumed the fire in the analyzed area will generate signal.

So did you trace what type of signal was analyzed for the, was generated in different fire areas, the one which will cause the trip?

MS. RADEL: To clarify, it's not assumed that the fire will cause a signal and a trip. It is that we continue to monitor all of these variables and if there is an upset condition if we do lose flow, we do have high or low temperature, we have high neutron flux, or we lose, you know, the neutron driver, the safety system will take the proper action to perform its safety function.

It's due to that redundancy and routing through separate fire areas and make sure the separation that is what is credited there for -- Essentially the system continues to monitor and actuate as needed.

MEMBER DIMITRIJEVIC: I think this is, I feel actually, really, to understand that when we are discussing but now when I am looking through your signals and trying -- So let's say that you are having some, you know, the MCC room fire, what would -- Okay, first, your definition of safe shutdown is the plant is tripped and the solution is done, right, that's a general definition of safe shutdown.

So let's say that you have a fire in, that you lose the hydrogen, you know, the combustible which is one of your signals, or whatever, how do you assume you are achieving safe shutdown given, for example, fire in that SOC (phonetic) MCC room?

MS. RADEL: The MCC fire is specifically analyzed to ensure that we would not lose both the

Division A and the Division B MCCs because those are for the TOGS blowers and heaters because those are relied on for five minutes following shutdown.

And so that is specifically analyzed in the fire modeling to ensure that we would maintain at least one division of that equipment, you know. Within the emergency procedures there will be, there is a definition of when the operators will shut down the facility based on the size of the fire, and Catherine can speak to that.

I was speaking to the kind of safety aspect of it that the systems are independent enough to take their own action and still maintain their safety functions during a fire event --

(Simultaneous speaking.)

MEMBER DIMITRIJEVIC: Okay, so now I sort of understand that, because as I understood you this morning that you said you cannot safe shutdown without tripping and damping the vessel, right, that's your definition of safe shutdown, right.

So, okay, I said the something, you said that it's not, but it's actual, in general you do credit these operator actions for those fires in these areas, right?

MS. RADEL: We don't credit operator

action for safety, but to reach our safe shutdown definition there would be an operator action taken.

MEMBER DIMITRIJEVIC: All right. So that's where we had the misunderstanding, all right. Now I understand, thanks.

MS. RADEL: Yes. Moving into the mode transitions and permissives. So the mode transitions and permissives are really to prevent the unit from tripping immediately after a mode transition, you know, when things are inactive in one mode and then active in the next.

So it's looking to make sure that, you know, the system is set up for operation in the next mode, so, you know, Mode 0 to Mode 1, ensuring that all TSV dump valve position indication (audio interference) isolation valve position indications indicate fully closed.

TOGS mainstream flow is above the minimum flow rate. Mode 1 to Mode 2, that the TSV fill isolation valve position indications indicate both valves fully closed.

Mode 2 to 3, all high voltage power supply breaker position indications indicate the breakers are open. Mode 3 to 4, IU cell safety actuation is not present, and then Mode 4 to Mode 0, that the TSV dump tank level is below the low-high TSV dump tank level.

Moving into bypasses, for Mode 0 the list of signals listed there are bypassed. Mode 0 again is when there is no target solution in the primary system boundary sources when the unit does not contain target solution.

In Mode 1, this is the filling mode, we have bypasses on the lower power range neutron flux, such as which is for driver dropout. It's not necessary in Mode 1.

TSV fill isolation valve position indication not closed. We do expect to open the fill valves during the filling mode and then low PCLS flow and high PCLS temperature.

I do want to note that these signals are not bypassed for the IU cell safety actuation function, but they are bypassed for driver dropout. So these signals feed into two separate actuations and it is only the driver dropout portion that is bypassed in Mode 1.

Mode 2, high source range neutron flux. Mode 3 and 4 have the same list of items here, and this is when the target solution has been dumped to the TSV dump dank.

We have our neutron flux input and then

PCLS because PCLS is not needed at that point when the light water pool is providing cooling and then low-high TSV dump tank level and TSV fill isolation valve position indication not closed.

The reason that that is bypassed in Mode 3 is that there is solution within the TSV hold tank that we may want to add to the dump tank prior to transfer through the hot cell, so that gives us the ability to do that.

MEMBER BROWN: Can I ask a question relative to Mode 3? This is Charlie.

MS. RADEL: Yes.

MEMBER BROWN: Mode 3 is post-irradiation and then you move it off to the production facility. Is there a resting period or some period that you have to hold it in Mode 3 for a while before you do anything after the irradiation?

MS. RADEL: Yes, there is, but it's a proprietary number and I'd be happy to cover that in the closed session.

MEMBER BROWN: Okay. I just wanted to know if there was a resting period, that's all.

MS. RADEL: Yes.

MEMBER BROWN: I don't need to know the number, okay. I was just trying to understand the wiring diagram you had in one of your figures plus the discussions and I was curious as to whether that was necessary. So that's good enough for me. Thank you.

MS. RADEL: Yes. Okay, any questions on TRPS before we move into ESFAS?

(No audible response.)

MS. RADEL: Okay. So the ESFAS is also designed using the HIPS platform. As indicated earlier there is one ESFAS system for the facility. It monitors the variables that are important to safety functions in the radioisotope production facility, or RPF, as well as the tritium systems.

It performs safety functions required by the SHINE safety analyses and there are three divisions of monitoring equipment with one out of two or two out of three coincident logic vote, depending on the operability considerations.

MEMBER BROWN: That's -- I had a question here. Excuse me. When you talk about two out of three or one out of two, that's definitely a change from the TRPS approach.

There you are two out of three and always two out of three and why the differentiation for it's okay to be one out of two, you're allowing as operation with one of the channels out of service (audio interference).

MS. RADEL: So it's completely and operability consideration on the need for reliability of different systems and different functions and the ability to, you know, adjust the production with the different functions so we can discuss based on the different functions why we chose the way we did.

MS. KOLB: And this is Catherine Kolb. Just to be clear, some of the SS channels only have, or some of the SS variables only have two channels.

So, it's not that we're designing differently, and neglecting one of the three channels. Some of the variables only have two channels.

MEMBER BROWN: That wasn't obvious from looking at the pictures, and the words I read. The first time I came across this was when I read Section 7.5.1, paragraph six. Okay?

So, it certainly wasn't obvious that there was only channels of ESFAS at any time. I thought it was a total three-channel operating system, and that the only reason for going to the one-out-of-two was because you're not in a fission-type reactor operation-type setup that, for reliability on the production front, if you lost a channel, you wanted to be able to continue with the production aspects.

So, I guess, my thought process was not correct. It certainly wasn't obvious where there were only two channels required for any particular -- the 29 safety functions that are performed in the ESFAS.

MS. KOLB: This is Catherine again. If you look at the logic diagrams, that's more clear on which variables have two channels versus three, because two inputs are shown into the logics versus three.

MEMBER BROWN: Okay. Well, talking about that fourteen or fifteen pages of fine print that you need a magnifying glass to read. Correct?

MS. KOLB: It's also identified in the technical specifications, where it says, required channels, in the various --

MEMBER BROWN: Which is not part of this discussion.

MS. KOLB: Understand. Understand.

MEMBER BROWN: I made the comment earlier, that the tech specs is at not a very good place for identifying these particular variations of operability conditions. It really ought to be in the check.

MS. KOLB: No, I apologize. It's also in table 7.4.1. and 7.5.1. It distinguishes which variables have two channels versus three.

MS. RADEL: If I understand correctly, some of the confusion is, whenever it is a one-out-of-two, if you have a Division A and a Division B in there, there is no Division C of the instrumentation there.

When it says two-out-of-three within those tables, they are the A, B and C Divisions of input.

MEMBER BROWN: So, you've really got both the protection divisions still available.

MS. RADEL: Correct. There is always a Division A and a Division B.

MEMBER BROWN: Okay. So, all you're missing is the third data channel, where you're showing the actuations required.

MS. RADEL: Correct.

MEMBER BROWN: Okay, very difficult in the limited amount of time we had to go through those logic diagrams and the tables, and put all those little things together. So, all right, that's good. You explained it to me. I appreciate that.

MS. RADEL: We appreciate the question. There are three cabinets for the ESFAS, the Division A cabinet, Division B cabinet and the Division C cabinet.

The safety functions within the ESFAS are the RCA Isolation, Super Cell Isolation, Carbon Delay Bed Isolation, Vacuum Transfer System, or VTS, Safety Actuation, TPS Train Isolation, TPS Process Bent Actuation, IU Cell Nitrogen Purge, RPF Nitrogen Purge, Moly Extraction and Purification System, or MEPS, Heating Loop Isolation, Extraction Column, and Iodine and Xeonon Purification and Packaging, or IXP, Alignment Isolation, and the Dissolution Tank Isolation.

The RCA Isolation is initiated based on process variables indicating efficient product release into RVZ-1 or RVZ-2 areas of the facility, or a breach to the tritium boundary within an IU cell, supply return lines, or a TPS glove box.

The RCA isolation closes the RVZ dampers, and turns off blowers for the RVZ-1 and RVZ-2, and initiates a super cell area isolation, VTS safety actuation, TPS train isolations, and TPS process vent actuations.

Supercell isolation. Note that there are isolations for each of the ten areas of the supercell. And so, initiated based on process variables indicating fission product released into a supercell area of confinement.

It closes the inlet and outlet dampers for the supercell area that is affected. It initiates a VTS safety actuation if the release occurs in the process special vent system, PVVS, or extraction areas of the hot cells. It initiates a MEPS Heating Loop Isolation if the release occurs in an extraction area.

MEMBER BROWN: Can you back up to the supercell again for me for a minute? This is an off-the-wall question.

The supercell is another -- I'm trying to figure out the right word for it. We've got it covered with ESFAS, but there's a lot of control functions associated with supercell operation. At least that's what I kind of gathered out of reading the supercell stuff.

MS. RADEL: Yeah, so the supercell is a bank of ten hot cells. It's where our processing occurs where we extract and purify isotopes. There's also the PVVS cell is where a lot of the equipment for the vent system is located, such as we can do maintenance and replacement of components.

So, those hot cells each have their own confinement. So, there's ten individual confinements with inlet and outlet dampers, and isolation valves for process lines going into and out of the cells. And we can isolate each area individually.

MEMBER BROWN: The reason I ask the question is that it's also covered, what I recall, under the -- one of the boxes on the control system for the supercell is covered under the PICS.

And the PICS has an ethernet external connection, based on the 7.1-1, and it's also mentioned in the text.

So, I guess whenever we get around to that at some point, I'd like to hear how we maintain our no-external-connections to the Internet for, particularly, the supercell, but probably everything else that's covered under the PICS area. That's later for another discussion. That's just something to lay on the table.

I'm obviously bothered by what they call vendor-provided control systems, non-safety-related, but the supercell has got to have control systems somewhere. And if it's computer-based, then you want to make sure it's not connected to anything. You certainly can't put virus software into the supercell control systems.

(Simultaneous speaking.)

MS. KOLB: Hopefully, I can address this quickly. This is Catherine Kolb. The vendor-provided control systems are physically in the facility.

Maybe that was confusing there, but we're not connecting to a cloud-based thing or at a vendor facility. The vendor provided the control system, but it's physically in our facility.

MEMBER BROWN: Well, it says this has an ethernet connection in the text. That's why I ask the question.

MR. WATTSON: Yeah, this is Bill Wattson. I'm the INC manager. It is an ethernet connection, but it's internal ethernet, and it's only connected within the layer-four of our cybersecurity model --

(Simultaneous speaking.)

MEMBER BROWN: Oh, okay. All right, it's not external-external then. It's internal-external. Or external-internal. It's internal to the facility. It's an ethernet around the facility.

MS. RADEL: Correct.

MEMBER BROWN: Okay, thank you. That's good. Wasn't clear from the reading. That's all.

MS. RADEL: Good. The next function is the carbon delay bed isolation. This is initiated based on process variables indicating a fire in the PVVS carbon delay bed-one, -two, or -three, and isolates and bypasses the impacted beds, suppressing for fire while maintaining flow through the other seven beds.

I do want to note that this is different from the off-star version that you likely saw, so we are no longer isolating CO, carbon monoxide, for the PVVS fire scenario. We are isolating based on temperature.

And rather than a delay bed group isolation, it is a isolation of the individual carbon delay beds for beds one, two and three. And then, there is no safety-related isolation provided for beds four through eight.

This change was initiated based on the analysis that showed that full release of maximum inventory off of beds four through eight would not exceed the SHINE safety criteria.

And so, we can cover more on that kind of change and design at the next ACRS meeting.

MEMBER HALNON: Tracy, this is Greg. What are the size of these carbon beds? Just approximately.

MS. RADEL: They're very large. They just appeared onsite last week. I don't know the exact size, but we can get that for you though.

MEMBER HALNON: Okay. My thought was that when a fire heats some combustion in a bed, it's very localized. And I'm sure they're largely dependent on whether the sensors are.

So, where are the sensors, relative to the carbon? And how do you answer the question about a gray, localized fire starting, or combustion?

MS. RADEL: The sensors are located on the out-limit line at the exit of the carbon delay beds, each carbon delay bed.

Our analysis for this event is assuming that the entirety of the affected delay bed, all of the radionuclides on that affected bed are released prior to isolation. And the set point for the temperature sensors is based on the requirement that the next bed not start on fire due to the temperature exiting the delay bed.

MEMBER HALNON: Okay, so just running it through the isolation will cause the bed to suffocate basically, and the next bed will not catch because of the heat. Is that restating correctly?

MS. RADEL: Correct. The isolation will isolate the bed that is affected by fire, suppressing the fire. And then, bypass that bed such that flow will still pass through the other seven carbon delay beds.

MEMBER HALNON: Okay, is that through a

failure of one of the dampers to isolate?

MS. RADEL: Yes. The valves -- yes. It includes a single failure of valves. Yes.

MEMBER HALNON: Okay. All right, thanks.

MS. RADEL: The VTS safety actuation is initiated based on process variables indicating that a break in the process boundary has occurred in either the subgrade or the hot cells, and this actuation is provided to limit the radiological release in that event.

It terminates the vacuum-lifting operations by opening the breakers to the vacuuming pumps, and also opening vacuum relief valves. It also isolates the chemical reagent lines that penetrate the confinement boundary.

The TPS train isolation is initiated based on process variables indicating a breach of the tritium boundary within an IU cell, the supply return lines, or the TPS glove box.

It isolates the TPS glove box, closes the tritium room dampers, and initiates the IU cell TPS actuation, which isolates the TPS lines into and out of the IU cell.

The TPS process vent actuation is initiated based on process variables indicating high tritium in the process exhaust out of the tritium systems, encloses the tritium process exhaust valves from all trains, and initiates an IU cell TPS actuation, which isolates the TPS lines into and out of the IU cell.

The IU cell nitrogen purge is initiated based on the discrete signal from TRPS, indicating loss of hydrogen recombination capability in one or more of the IU cells, or indication of loss of external power following three-minute time delay.

It opens the nitrogen purge system, or N2PS, IU cell header valves, and the N2PS valves to the individual IU cells are actually opened by the TRPS. So, these functions work together.

The RTS nitrogen purge is initiated based on process variables indicating loss of flow in the process vessel vent system.

It opens the N2PS RPF header valves, and opens the PVVS carbon guard bed bypass valves. This is done in case the loss of flow was due to a plug or obstruction in that guard bed system.

The MEPS heating with isolation is initiated based on process variables indicating a leak of target solution into the MEPS heating route or a break in the process boundary, either in the subgrade or in the hot cells.

It closes the isolation valves for the MEPS heating loop and opens breakers for the MEPS extraction column feed pump.

The extraction column and IXP alignment actuation is initiated based on process variables indicating a valve alignment that could lead to fissile material in a non-favorable geometry tank. It aligns the valves to a safe position and is a criticality safety control.

The dissolution tank isolation is also a criticality safety control that is initiated based on process variables indicating an overflow of the target solution preparation system dissolution tanks, potentially leading to fissile material in a non-favorable geometry location.

It isolates the tank inlets and outlets, and isolates the cooling waters up high and return to prevent additional water intrusion.

Moving to the monitoring variables in response, on the exhaust radiation we have a High RVZ1 and High RVZ2 RCA exhaust radiation, which protects against contaminant leakage, or accidents that could potentially result in excess radiation dosage to the workers or to the public. It's initiated when two out of three or more signals are active.

The High RVZ1 supercell exhaust ventilation radiation on the PVVS hot cell protects against hot call equipment leakage or an accident that could potentially result in excess radiation doses to workers or the public.

Supercell isolation Area One is initiated off of the signal, as well as the VTS safety actuation, when two out of three or more signals are active.

The High RVZ1 supercell exhaust ventilation radiation for the MEP's extraction hot cells again protects against hot cell equipment leakage, or an accident that could potentially result in excess radiation doses.

It initiates supercell isolations to the affected area, the affected extraction cells, MEPS Heating Loop Isolation and VTS safety actuation, when one out of two or signals are active.

Continuing with exhaust radiation, there's High RVZ1 supercell exhaust ventilation radiation on the IXP hot cell, again protecting against excess radiation doses.

The supercell isolation area ten, which is an IXP cell, and the VTS safety actuation, are initiated when one out of two or more signals are active.

High RVZ1 supercell exhaust on the purification and packaging hot cells again protects against excess radiation doses, and will isolate the affected area of the supercell on a one-out-of-two or more signals being active.

MEPS and IXP, High MEPS Heating Loop Isolation protects against leakage of high radiation solutions and to the heating water loop, which is partially located outside the supercell shielding and could potentially result in excess dose to workers.

It initiates a MEPS Heating Loop Isolation of the affected loop when one out of two or more signals are active.

MEPS Area A, B and C three-way valve position indication protects against the misalignment of the extraction column upper and lower three-way valves, which is criticality safety control and initiates an extraction column alignment actuation when two out of two signals are active.

The IXP three-way valve position indication protects against a misalignment of the upper and lower three-way valves, which would degrade barrier of the preventing misdirection, similar to the

MEPS, and it initiates an IXP alignment actuation when two out of two signals are active.

Okay, the PVVS, VTS and RDS variables. We have the high PVVS carbon delay bed exhaust temperature, which protects against fire in the PVVS delay beds. It initiates a carbon delay bed isolation of the affected bed when one out of two or more signals are active.

Well PVVS flow protects against loss of hydrogen mitigation capabilities in the RPF and initiates an RPF nitrogen purge when two out of three or more signals are active.

The VTS vacuum header liquid detection protects against an overflow of the vacuum lift tanks, to prevent a potential criticality event. The VTS safety actuation is initiated when one out of two or more signals are active.

And then, the RDS liquid detection detects leakage or overflow from other tanks and piping, and initiates a VTS safety actuation when one out of two or more signals are active.

For the tritium systems, we monitor for high TPS IU cell target chamber exhaust pressure or supply pressure, and this is individually monitored on each of the eight IU cells.

This protects against a break in the tritium exhaust for supply lines, as well as if there were a breach in the neutron driver pressure boundary that would release tritium into the IU cell or the transfer area between the tritium system and the IU cell. This would initiate a TPS train isolation for the affected train and an RCA isolation, when one out of two or more signals are active.

High TPS exhaust to facility stacked tritium protects against the release of tritium from the TPS glove box pressure control exhaust and back ITS process, vent exhaust into the facility ventilation systems, it initiates a TPS process vent actuation when two out of three or more signals are active.

High TPS confinement tritium, and this is provided on each train of the tritium equipment, protects against a release of tritium from TPS equipment and its associated TPS glove box.

It initiates a TPS train isolation for the affected train and an RCA isolation when one out of two or more signals are active.

And one more slide, monitor variables. Lots of monitor variables in slide.

So, we have the TRPS IU cell nitrogen

purge. This is a discrete signal coming from the TRPS for each individual IU cell. It protects against the loss of nitrogen mitigation capabilities in the irradiation units, and initiates a IU cell nitrogen purge.

The TSPS target fission preparation system dissolution tank level -- and there's two different dissolution tanks with level instrumentation, where it protects against a criticality event, leaving access for cell material and non-capable geometry system, and initiates a dissolution tank isolation when one out of two or more signals are active.

The UPSS loss of external power protects against an anticipatory loss of hydrogen mitigation capability in the IU cell, loss of the TOGS blowers and heaters after the UPSS runtime of this equipment is exceeded.

It initiates an IU cell nitrogen purge when one out of two or more signals are active for the 180 seconds.

Any questions on the ESFAS safety functions or monitor variables, before I turn to priority logic? Okay.

Priority logic. The actuation priority logic, or APL, is designed to provide priority of safety-related signals over non-safety-related signals.

Division A and Division B of TRPS ESFAS priority logic prioritizes the automatic safety actuation and APL safety actuation over any signals coming from the PICS on safety-related controls system.

When the enabled non-safety control is not active, the non-safety-related control signals are ignored by the TRPS and ESFAS. If the enabled non-safety control is active and no automatic safety actuation or manual safety actuation command is present, the non-safety control signal can control the component.

MEMBER MARCH-LEUBA: Hey Tracy, this is Jose. So, it's a little unusual to have signals that ignore the control or non-control of safety and non-safety. You guys have reviewed that the safety signals are never filtered. Correct?

MS. RADEL: Correct. The safety signals are never ignored. This is just those PICS signals coming in to reset the component. If there are no safety actuations present, either automatic or manual, then it allows PICS to reset the component for --

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: This is kind of equivalent to what we would call a hold, or a lock. So, once you take, you're not allowed to reset the breakers automatically. Yeah, this priority logic is a little too complicated.

On reactors, what we've been doing in the past, if you open a breaker and you let the control rods in, the control system cannot possibly close it, because it's locked.

MS. RADEL: Right. And that is true for our system as well. You would need an operator action then to reset that, and you would only be allowed to perform that action if the system was no longer in a trip condition, and that enabled non-safety switch was turned.

MEMBER MARCH-LEUBA: And this logic is equivalent to that. A little more sophisticated maybe. Okay, that's fine. Thank you.

MS. RADEL: Okay. Communication between TRPS ESFAS and PICS. This site covers the types of information that is communicated. So, each division of TRPS and ESFAS trains MEPS monitoring indication and diagnostic information to PICS for display to the operators.

PICS provides mode transition signals to

TRPS when manually initiated by the operator. PICS provides valve and damper position indication to the TRPS and ESFAS for verification of completion of protective function, and PICS provides signals to TRPS ESFAS, to reposition components when they're manually initiated by operators, and the enabled non-safety switch is in the enabled position.

The ways that this communication occurs are noted on the last slide here. Communication from the TRPS ESFAS to the PICS is via serial connection, via MODBUS RTU protocol.

Communication from the PICS to the TRPS ESFAS is via a series of discrete contacts which communicate a series of addresses that are correlated to inputs and non-safety control signals, and all interfacing between TRPS ESFAS and the PICS is by the gateway communication module, which Jason touched on earlier.

That's the last slide. Are there any additional questions on TRPS or ESFAS? Thank you.

CHAIRMAN BALLINGER: Okay, that concludes the SHINE presentations for today, is that correct? Except for the closed session.

MR. BARTELME: No. This is Jeff Bartelme. We still have a session on safety-related radiation monitoring and --

(Simultaneous speaking.)

CHAIRMAN BALLINGER: Ahh. Sorry, sorry.

MR. BARTELME: We're bringing those slides up now.

CHAIRMAN BALLINGER: Got it.

MEMBER BROWN: Ron, this is Charlie.

CHAIRMAN BALLINGER: Yes, sir?

MEMBER BROWN: Let me get back to what I can see here. SHINE. The closed-session slides are just pictures of the detailed, eyeball-piercing logic diagrams.

CHAIRMAN BALLINGER: Okay, yeah.

MEMBER BROWN: You can take a look at that. I'm just giving you a heads, I'm not sure this is going to add much value for the members, unless they want to see it.

CHAIRMAN BALLINGER: All right. Well, we'll get a chance to ask that question.

MEMBER BROWN: Yeah, I'm just bringing it up to you so you have it ahead of time. That's all.

CHAIRMAN BALLINGER: Yeah, I was looking at them also.

MR. BARTELME: This is Jeff Bartelme from SHINE. We have not prepared any presentation material for closed session. But because so much of that content did contain proprietary and export-controlled information, we just wanted to put them into a slide deck that if we had any sort of specific information to share to them, or any questions which we need to refer to them, we wanted to have them available in a presentation for closed session.

CHAIRMAN BALLINGER: Got it. Thank you. Thank you. Okay, onward and upward.

MR. WATTSON: Sure. Okay, this is Bill Wattson, the INC manager. Because of the earlier problems. Can everybody hear me okay now?

CHAIRMAN BALLINGER: Yeah, whatever you're saying, about half of your sentence sounded like you were far away, and the rest of it sounded like you were close and very good. So, I don't know what you're doing.

MR. WATTSON: Okay, does it sound okay now, Carl?

CHAIRMAN BALLINGER: Sounds okay to me. It depends on the reporter. Okay, good.

MR. WATTSON: Okay, good deal. Great. Well, I'm here to present on the safety-related radiation monitoring and the neutron flux detection system.

The rad monitors are for fission products and tritium, and are both inputs to the ESFAS and TRPS system. The fission product monitors are comprised of beta particle gas-use monitors, and gamma monitors for the MEPS water overloads.

The beta simulators provide their inputs to both TRPS and ESFAS, whereas the gamma monitors are to ESFAS only.

Tritium monitors monitor the various points in the tritium processing system, providing their inputs to ESFAS, and the rad monitor information is displayed in the control room on the operator workstations via the PICS system. Next.

Fission product radiation monitors. The RVZ1 supercell PVVS exhaust monitors, comprised of three channels, A, B and C, provided to ESFAS, the RVZ1 supercell extraction, purification and packaging exhaust ventilation monitors are to ESFAS channels per each area, and the RVZ1 and RVZ2 RCA exhaust monitors are comprised of three channels for each to the ESFAS system.

The fission product-produced monitors continue in the RVZ1 exhaust subsystem, or RVZ1E. PCLS expansion tank exhaust vent monitors detect elevated levels of radiation from the IU PCLS expansion tank exhaust, and they are comprised of three channels each provided to TRPS per expansion tank. And then, the MEPS hot water loop monitors, or gamma monitors, with two ESFAS channels provided for each of the water loops.

Tritium monitors, or TPS tritium confinement atmosphere monitors, are provided with two channels per glove box, signaling to ESFAS.

TPS exhaust to facility-stacked tritium monitors detect tritium in the RVZ1E exhaust, and that's comprised of three channels. And they're also signaling to ESFAS.

And in conclusion, and interfacing with TRPS and ESFAS, there are analog inputs to both systems. The safety actuations occur when the input value exceeds the predetermined set point, the point being is that the set point determination is done by the safety system.

And that concludes the brief presentation on safety-related radiation monitoring. Do you have any questions before I proceed?

Okay, Neutron Flux Detection System, or NFDS. The NFDS monitors an (unintelligible) neutron flux, determined multiplication factor and power level during the filling in the TSV and the irradiating and the target solution.

The NFDS monitors variables and important safety functions of the irradiation units, provide input to the TRPS performance safety functions. The signals provided the PICS for main control room indication, to cover the entire range of neutron flux levels in three different ranges, the source range, the wide range, and the power range.

The NFDS is a three-division system, with six detectors positioned around the subcritical assembly support structure, at approximately 120-degree intervals to the TSV.

MEMBER BROWN: Before you switch slides?

MR. WATTSON: Sure.

MEMBER BROWN: I'm looking at the diagram. Does this provide its data and information to the PICS via the same path that TRS -- come on, I'm going to get it right here -- TSRP system does? TRPS, rather?

The data shows like it goes into the various -- for the TRPS system it goes into the various SFMs. And does that then goes out via the MSEM and the other gateways and everything else? Is that how it goes into the PICS? It doesn't go directly --

MR. WATTSON: Yes, it is. The signal

comes in to TRPS, and then it's related to PICS for display.

MEMBER BROWN: Okay. All right, that's all I needed to know. Make sure it's got the same isolation. That's all, thank you.

MR. WATTSON: Sure.

MEMBER MARCH-LEUBA: This is Jose. I do have a question about, apparently there is only one detector for the power and wide, and it's shared? Is it the same head unit but two different electronics?

MR. WATTSON: Yeah, it's a compensated ion chamber. It actually covers both the power range and the narrower band and the wide range to give it the overlap with the source range detector.

MEMBER MARCH-LEUBA: But it is the same ion chamber for both power and wide?

MR. WATTSON: Yeah, the same CIC. That's correct.

MEMBER MARCH-LEUBA: So, you're only changing the electronics?

MR. WATTSON: Yes.

MEMBER MARCH-LEUBA: So, I'm assuming the wide range is pulse counting and the power is what they call current?

MR. WATTSON: No. Actually wide and power range are current. Only the source range uses pulse counting.

MEMBER MARCH-LEUBA: So, you're using just a different scale, but same detector, same counting method? I mean, I don't see the different between power and wide, from what you're telling me.

MR. WATTSON: Sure. I think it's more a matter of resolution. The wide range is -- I guess maybe a construct way to think about it, yeah, it's almost more like a long-scale -- well, actually, I think about like control on panels on like trigger reactors.

You have the long-scale pen, which covers the entire range of power, and then the linear scale for basically power range operation in finer increments.

MEMBER MARCH-LEUBA: So, the sensitivity of the detector, because the next question I want to ask you, see do you know what the dead time, pulse pileup issues. If you are including the pulse pileup, probably will make a difference. But dead time is probably either.

When you have a detector that has more sensitivity to cover a wide range, you end up always having problems with dead time and pulse pile-up, and all that stuff.

MR. WATTSON: Yeah, dead time and pulse pile-up isn't a fact of a pulse rate-type detector. These are ionization chambers. So, they're measuring current.

MEMBER MARCH-LEUBA: (Unintelligible) pulses. They just pile them up and create a current. You can count the pulses in an ion chamber. Okay, I still don't understand how out of the same physical sensor here, you get two different ranges. But I guess you guys know how to do it. I'm surprised.

MR. WATTSON: Actually, the detector design that's pretty established -- well, I have my SRO and trigger reactor 40-something years ago, and basically, exactly the same detector configuration. It effectively used a fission chamber of the source range detector.

Now, that is also an ion chamber, but it generates pulses because the fission event is so significant to the current output in chamber, it's effectively a pulse.

But the normal operation of the even the source range is to put out a constant current associated with leakage current in operating in the ionization range, and the compensated ion chamber is essentially always an ion chamber. It's basically compensating for the gamma contribution from secondary chamber.

MS. RADEL: This is Tracy. I do want to clarify that we did discuss how the design changed to move this sort of strange detector from the BF3 detector to a fission chamber recently, after the BF3 detectors failed some of their testing, and it was due to gamma pileup issues, as the phase discussing that can be an issue.

So, we are making the switch within the licensing documentation and with the vendor, so that'll be coming across in the Joy submittal.

MEMBER MARCH-LEUBA: So, this whole advantage went to the fission detector?

MS. RADEL: Correct.

MR. JARROUJE: Which, that one is completely independent from gamma. That's pretty good. Okay, go ahead.

MEMBER BROWN: I'm surprised. You said you had a problem with your gamma pileup with the BF3s?

MR. WATTSON: Yeah, absolutely.

MEMBER BROWN: Geez. That's all I ever used.

MR. WATTSON: Yeah, I think part this --

MEMBER BROWN: Fission chamber is just horrible to deal with. That's all.

MR. WATTSON: Yeah, of course. And, yeah, if you want to get more into that --

(Simultaneous speaking.)

MEMBER BROWN: Well, it's your decision. It's your decision.

MR. WATTSON: Okay. Are we done with this slide?

MEMBER MARCH-LEUBA: Yes. Yes, we are.

MR. WATTSON: Okay, moving on. Okay, let's talk about the source range detector. Source range detectors with fissure low-flex levels common to what would be expected during the filling of the TSV, the NFDS provides TRPS with a count rate signal for TRPS to perform its trip determination, and then the TRPS initiates the IU cells, safety actuation, when two out of three or more source range, or high source range neutron flex signals, occur. Next slide.

The power wide-range detector. The power wide-range measures, the flex levels and the ranges that are expected when the neutron driver is operating.

The power range neutron flex signal is

input into the safety-related trip determination for TRPS, and the TRPS initiates the driver dropout on either a low power-range neutron flux, and initiates IU cell safety actuation on high power range time-average neutron flux.

Wide-range neutron flux connects the gap between the source range and the power range with overlap, and is useful during both source and power range levels.

The NFDS wide-range neutron flux signal is input to the safety-related trip determination by a TRPS, and the TRPS initiates IU cell safety actuation on high wide-range neutron flux.

To cover the gap between source and power ranges, the wide-range -- oh, you know, I've got to repeat my slide, never mind, I'm sorry -- monitors the flux levels between the source range and the power range with the minimum of one decade of overlap, and with a high end of the source range in two decades of overlap, at the low end of the power range.

Detector calibration. The normal startup count rate, or what we call NSCR here, is determined by filling the TSV to approximately 95 percent of critical-by-volume, with optimal concentration solution at a stable temperature.

The source range set point is then set relevant to NSCR per technical specifications. The drift allowance relied on by the source range set point calculations is periodically checked using empty TSV count rate. Final slide.

Detector calibration of the power wide-range detectors. Prior to filling a TSV for radiation, a sample is taken from the associated target solution, and the sample is analyzed for activity to determine the volumetric activity of the selector isotopes.

The TSV is then pulled using standard startup procedure, and the TSV level is recorded to determine the volume of irradiated solution.

Target solution's irradiated for sufficient time to create activity levels of selected isotopes sufficient for calibration.

Then, a sample of the target solution is analyzed post-irradiation, to determine the volumetric activity levels of the selected isotopes, post-radiation.

And finally, power level during the irradiation is calculated based on the initial and final volumetric activity levels of the selected isotopes, indicated power history, and the TSV volume.

This value is then used to calibrate the NFDS power range and wide-range detectors. Are there any questions on that?

MEMBER REMPE: So, this is Joy. And I don't really have a question about that particular slide, but I guess I want to explore a little bit more. Didn't I hear someone say that, yes, we're going to be modifying something with a submittal that's coming in? And what exactly will be changed? Will all of these changes to Section 7 coming up?

MR. BARTELME: This is Jeff, pardon me. So, to account for the source range detector, detecting only a fission chamber, there will be modifications to Section 78 of the FSAR, to remove that reference to the BF3 detector and provide reference to the fission chambers.

MEMBER REMPE: So, when that revised section comes in -- we saw a table, I probably have the wrong digits on it if I tried to cite the number right now, but I look it up before the staff come up, but beside percentage of table -- and actually, part of that table was even presented in the open section, where they included the delays and some information and references to other sections in the FSAR -- will that table be included in the updated submittal on

Section 7? I can look up the table number while you're trying to answer that's puzzling you, what I'm trying to talk about here.

MR. BARTELME: No, the timing table, that sort of compilation of information, is not something we'll be incorporating into the licensing basis, and it won't change with the change in the detector type.

MEMBER REMPE: Okay. So, I guess then, the next question I have, and I'll be asking the staff about it, is the audit and the progress that's going on.

Because the backup slides indicate that the audit still isn't done, with respect to some of the timing and the delays, or whatever. There seems to be some outstanding issues. But again, I'll wait for the staff.

CHAIRMAN BALLINGER: Okay.

MR. WATTSON: Yeah, and that's the last slide, so that concludes my presentation on rad monitoring.

CHAIRMAN BALLINGER: Ah. Okay, thank you. So, that is the last set of slides for this section. Am I correct?

MR. BARTELME: It is, yes.

CHAIRMAN BALLINGER: Okay. The next

presentation is from the staff. We're not scheduled for -- well, actually, we're scheduled for a break at 3:30, but we've been going at it for two hours, and that presentation was pretty detailed.

So, I'm going to propose that we take a break now. It sounds to me -- at least I'm getting the impression that the closed sessions will be shorter than listed.

So, let's take a break until -- now, let's do it until 3:30. So, unless there are objections from anybody, we'll recess until 3:30. Thank you.

(Whereupon, the above-entitled matter went off the record at 3:09 p.m. and resumed at 3:30 p.m.)

CHAIRMAN BALLINGER: Okay, speaking of going two hours straight, we're about to go another straight. We're back in session and we're ready for the staff's presentation.

And I've discovered why it was so hard for me to read chapter seven. The staff has six pages of acronyms in the back of their slides. Anyway, okay.

MEMBER BROWN: I told them to put them there because then you don't have to try to get back to the chapter seven to find out what acronyms mean. There's only about 22 acronyms. I forgot how many.

There's just a ton of them. I can't even keep them straight.

CHAIRMAN BALLINGER: Six pages.

MEMBER BROWN: Yes, the chapter itself.

MR. BALAZIK: This is Mike Balazik. Can you see the slides?

CHAIRMAN BALLINGER: Yeah, we're fine.

MR. BALAZIK: Okay, got you.

CHAIRMAN BALLINGER: We'll have to get rid of the -- we'll stop the levity. Okay, let's go.

MR. WATERS: All right, this is Mike Waters. I'll start off. And don't fear, we're only going to go through five of the six slides of acronyms. I'm kidding.

My name is Mike Waters. I'm Chief, Instrumentation and Controls Branch, NRC, and I'm happy to be here today to introduce the review team this hour which will brief you on the chapter seven safety evaluation report.

So, the staff evaluations primarily focused on electronic design of the SHINE I&C systems in terms of its ability to achieve its intended design functions for detecting potential upset conditions and, of course, actuating safety system components to put the facility into a safe configuration and mitigate consequences as credited in the safety analysis.

This slide shows the primary reviewers that contributed to chapter seven SE. I'd also like to note that the reviewers that have greatly contributed to the I&C review. Those include Michael Caul and Joe Staudenmeier among them.

The I&C team has coordinated closely with them on the interface between the intended functions of the I&C with ensuring safety features limits that protect the facility against postulated events which you've been briefed upon in previous events.

So, as you know, we're here today to highlight aspects of our technical review, and given the comprehensive discussion and the time, please feel free to tell us where to fast forward or focus our presentation here. Slide five, please, Michael?

Yeah, I just want to reiterate the scope of the SE before you. We have completed our review of the primary safety systems, TRPS and ESFAS, with the exception of a few open items related to life cycle development and technical specifications, and the fixed design is currently under review, and, of course, we'd be happy to engage later on these issues as needed. Next slide, please?

Yeah, this is for reference that may come up in further discussion. This is a diagram from the safety analysis report that provides an overview of the overall I&C architecture for the facility.

It includes a TRPS and neutron flux detection system for each iteration unit, the ESFAS for the entire facility, and those associated modules that operate on the HIPS platform.

Basically, the area is encompassed by the green on these pictorials that are the focus of our safety evaluation report and discussion today. Slide seven, please?

And finally, before I hand it over to Dinesh, at the highest level, a major focus of our safety evaluation was independently confirming that the I&C system satisfies those applicable facility design criteria that are listed here.

As you heard this morning, the criteria for I&C is the same or closely tracks to the general design criteria in Part 50. Obviously, multiple facility systems, structures, and components contribute to satisfying each facility design criterion, and, of course, chapter seven focused on those I&C-related portions for those criteria.

And as you would guess, we had a higher

focus on certain criteria for our reasonable assurance determination. Those include such things as criterion 13 for appropriate controls, criterion 15 for reliability and testing, and criterion 16 for independence, and well as criterion 18 for separation of protection controls, as well as all the ones listed here.

And just to close it out, the (unintelligible) described how we applied the five I&C fundamental design principles which extracted these, including independence, redundancy, predictability, diversity, and simplicity within our confirmatory view.

MEMBER BROWN: Okay, don't go yet. If you're ready to switch slides, let me ask a question.

MR. WATERS: I was about to turn it over to Dinesh, but please go ahead.

MEMBER BROWN: This is Charlie. I forgot to ask SHINE, if they're still on the line. I presume they're still listening. When they were doing their ESFAS part, I had tracked the design criteria between TRPS and ESFAS and I found that the ESFAS has a design criteria 18 which is not present for the TRPS.

And it was related to the no single failure within the instrumentation or power concurrent with failure as a result of design basis event. That criteria is not in TRPS and I was wondering why, from the power supply standpoint as it's explained down below.

MR. BARTELME: We're still here. We'll look into that. We can follow up.

MEMBER BROWN: Okay, I was just going through the TRPS one, the one, two, three, four. I got to 18 and 18 is now 19 in the ESFAS and there's a new 18 in the ESFAS part. That's what triggered my thoughts. So, anyway, put that on the plate. Go ahead, Mike.

MR. WATERS: With that, I'll hand it over to Dinesh to start out with the HIPS review.

MR. TANEJA: I hope you can hear me. Good afternoon.

MEMBER BROWN: You're fine.

MR. TANEJA: Good afternoon, Professor Ballinger, and all of the members of the subcommittee. My name is Dinesh Taneja. I am the I&C technical reviewer in NRR, the Division of Engineering and External Hazards, ELTB branch, and I am responsible for evaluating the SHINE implementation of the HIPS platform and the ESFAS design.

So, you know, the TRPS and the ESFAS are designed using the HIPS platform, and in the SHINE's FSAR, they have incorporated the HIPS topical report that we reviewed prior to looking at the NuScale design, and we came in front of you with our topical report prior to reviewing the NuScale.

And the 65 application-specific items, the ASAIs that are identified in this topical report, they were developed for the power reactors, and some of those ASAIs do not apply to the SHINE facility, but SHINE prepared this technical report, tech report 2018-0028, that provides dispositions to all of the applicable ASAIs and also provided the explanation of the architecture differences between what was in the topical report, you know, which had the representative four-channel system with, you know, diversity with two different FPGA technologies, and some of the changes that they've made to the modules, they are described in this technical report.

So, as part of my review, I evaluated that report and basically my conclusion was that the SHINE architecture and the implementation still conforms with the fundamental design principles that we evaluated as part of its topical report, so it's pretty consistent with what we have in the topical report.

So, it continues to meet the fundamental principles of independence, redundancies, predictability and repeatability, and the diversity and defense-in-depth. Next slide, please?

So, you know, I guess SHINE covered the key modification this morning. If you want, I can go through them again, but basically, you know, we reviewed them and we found them acceptable.

So, it's just a remote input submodule which basically takes one of the ISMs for the SFM, you know, module. You know, these are the four submodules on the safety function module and they remodeled it for the neutron flux detection.

And, you know, combining the ESP (phonetic), the voting module and the scheduling bypass module on one module, and they created these gateway modules, you know, for doing the communication with the HIPS platform.

And the other changes are, I think they were described earlier this morning as well, so in the topical report, the hardwire input module signals were directed to certain modules and the SHINE application, they made those signals available on the back frame of the chassis, so any logic that needs that input, it can utilize that.

And also, the EIM outputs, you know, now it drives eight components, so the way it's grouped in now, you know. In the topical report, we were driving four components off of each EIM module, this one because all of the components are really not -- you know, they are small-sized sunlight valves and all of that, so they were able to drive, you know, eight components off of one EIM module.

So, those are the key differences. Now, if there are any questions, I can, you know, answer those right now or I can move onto the next slide.

MEMBER BROWN: Move on.

MR. TANEJA: All right, next slide, please? So, this figure comes out of the FSAR. It just kind of shows the -- you know, this morning, they were saying that there are nine cabinets with TRPS, so this is your cabinet number one that has the IU cell one and two chasses and then the maintenance workstation in the middle of that.

So, this is just representing, you know, one of the cabinets of the nine TRPS cabinets. I just wanted to provide a pictorial view of that. Next slide, please?

So, one thing that we did not have in the topical report, I guess we had that as an ASAI, was the environmental qualification of the actual, you know, equipment, so we evaluated the report, EQ report.

So, that EQ report basically demonstrated that the seismic qualification meets the requirements. It was tested for EMI/RFI qualification in accordance with Reg Guide 1.180, and it was subjected to, you know, these environmental conditions which is classified as a mild environment in accordance with the IEEE standard 623-2003 version, which basically verified that these equipment can work continuously at 140 degrees Fahrenheit and there is no -- you know, it's a passive cooling, so there is no forced cooling in the cabinets, and it has limited operational capability at an exterior temperature of 158 degrees Fahrenheit. So, we did review that, you know, and I guess it was an audit of the EQ documents for this equipment. Next slide, please?

So, it's just, I think, in words I'm saying basically the makeup of the TRPS and ESFAS architecture. You know, even though it's using feed channels, the basic architecture is essentially the same. That is that, you know, each channel is triple module redundant.

It has three safety buses and, you know, it has three, the SBMs and three voting modules. So, each of these receive a voted input and then three signals go out to the EIMs, which again get voted, so it's the same concept that's in the topical report.

So, there is only one-way interdivisional communication and there's a one-way data communication going out to PICS while the M&I communication module. So, this one is, you know, I think, Charlie, you were mentioning those red lines.

So, the red lines, you know, are the communication from the M&I CB, you know, communication module, the monitoring and indication, maintenance and indication communication module buses that goes out --

(Audio interference.)

MR. TANEJA: Slide, please? The next? Go to the one over? I can talk about that and we can come back to that. So, Charlie, this figure we received as part of the RAI response. Now, this figure shows the gateway modules and how they are actually, you know, implemented in the TRPS and ESFAS design.

So, each of the TRPS, you know, channels, and each of the ESFAS channels provides input to these specific modules, and then they are combined together before they go out to the PICS.

So, it's all one-way communication, so basically each of the RS-485 modules, they have three ports configured as input only and then one port is configured that's talking to the PICS as a two-way, so it really does provide us the isolated output coming out of the, you know, TRPS and ESFAS cabinets into that, and it has --

You know, this was one of the questions that we were asking. What happens if I lose this interface and if I lose the indication in the PICS? So, their implementation is doing the redundance out of inputs to provide reliability of PICS displays of all the information that's available in the TRPS and ESFAS. So, if we can go back to the slide, please? We were on, I think, the one before, let's see. Yeah, this is it.

MEMBER BROWN: Thirteen.

MR. TANEJA: Yeah, so slide 14, please? All right, so, you know, the fundamental design principle of independence, and so here, I think we -- we received this thing, you know, pretty thoroughly, and there were the independence single failure criteria.

So, we audited a couple of the documents and they were the ESFAS TRPS single failure analysis report and the failure most in effect analysis report to basically confirm the single failure criteria and redundancy arguments and the independence arguments of this whole design.

And then we looked at the T3 assessment of the TRPS and ESFAS, diversity and defense-in-depth assessment technical report, and we audited that report to basically confirm that this report verified that there is adequate diversity in the system.

And this assessment was performed using the, you know, our NUREG, what is that, 93-0? We kind of mixed up that number, let's see. Yeah, it's the NUREG CR that we have on T3 assessment is what they used to really model this diversity analysis and assessment on.

So, we evaluated that and we came to a conclusion that it had adequate diversity and, you know, and it basically met the SHINE design criteria 19 which talks about the high probability of accomplishing their safety function in the event of anticipated transients, and the protection system independence requirements and the single failure criteria, you know, they meet the SHINE design criteria 15.

So, on the access control element, you

know, the interfaces that we have from the TRPS or the ESFAS, so all of the access control features that are discussed in the topical report are being implemented here.

That is that you cannot change any logics on any of the cards unless you pull them out of the circuit, and also to changing any set points, you have to take the card, you know, and put it in a bypass. Take it out of service and then you have to physically enable an input before a maintenance workstation can make a change to a set point. So, those features are identical to what we reviewed as part of the topical report.

And so, they actually do not have any -- the only other communication that's coming into the TRPS and ESFAS is the hardwired inputs from the PICS. So, those are -- there are no data communication happening. They are coming through the isolated contacts on the hardwired input modules.

And then the priority scheme that they talked about this morning which is, you know, the APL logic, which is implemented in the equipment interface module using discrete components, and there is no FPGA or any of that used in there.

So, those inputs handle the manual system level actuations, and that provides another diversity element. So, you can provide manual actuations in the case and that basically protects us against the potential common cause failures on the software side.

And any inputs coming in from the non-safety, which is PICS, you have to actually, you know, enable that input before you could actually take access of any of the components, so that's like a component-level control from PICS that is done, you know, administratively using the enable feature, which is also identical to what we reviewed in the topical report.

Completion of protective actions, so all of the designs, all of the logic diagrams we looked at, all of these safety functions, once initiated, they basically go to completed, you know, completed action and they are sealed in, and everything is a failsafe design, so they go to a safe state on loss of power or on fault, any given fault.

You know, if it is a fatal fault detected, it would put the output in a safe state. If it is a fault where the safety function is not impacted, then it would just simply alarm that there is a fault that needs attention, so the same design principles that were discussed in the topical report, you know, the different levels of faults, and how they are identified, and how they are treated.

All right, next slide, please? Okay, we talked about that one. Diagnostics and self testings, they talked about that this morning.

Operational and maintenance bypasses, so all of the operational bypasses are automatic. They are in the TRPS system. There are no operational bypasses in the ESFAS.

And the maintenance bypasses are controlled via the tech specs, basically making sure that we have minimum redundancy available, so they only take out -- there's administration controls in the tech specs that only allow us to take out one safety function module in a given division at a time and not take out the redundant one on the companion division.

We talked about all of the manual actuation. So, there is a set of, you know, system-level manual actuations which are safety related, and then you have capability to actuate components using PICS via the, you know, the enable feature in the TRPS and ESFAS.

Response times, regulated limits, and set points. Now, in tables 741 and 751 of the FSAR, so what we have there is the sensor response times given and analytical limits are specified.

Now, we audited a couple of calculations, set point calculations, and the set point calculations do a pretty good job of, you know, providing the basis of the analytical limit and how they arrived at those things, and the response times are, essentially accounts for the --

You know, so the 500 millisecond response time is allocated to the HIPS equipment. That is, you know, from the sensor input to all the way to the output, going out to the output device.

So, the sensor response time is in the table, 500 milliseconds is allocated to the HIPS, and then there is the response time of the actuated component.

So, that combined total is accounted for in the set point calculations, and the set point calculations are performed using a methodology which essentially follows the ISA standards, so it's a pretty standard methodology, and these calculated calculate the total loop uncertainty and they select the set points, and those set points are used as the limiting safety system settings in the tech specs.

But we are still evaluating some of those calculations as part of the tech spec review that we are still underway, and that's being done still, continuing to be done. Next slide, please?

So, you know, so basically the conclusion is that, you know, we reviewed the HIPS platform implementation, you know, and we reviewed all of the application-specific action items, you know, how they were dispositioned, and we looked at the topical report areas and which areas specifically, like the EQ wasn't done back when we reviewed the topical report. It was just an action item, so that was definitely looked at.

The EMI/RFI testing, you know, it was an action item and we looked at that, and we looked at all of these, you know, features which are essentially providing us assurance of these, you know, fundamental principles of the I&C design, which is, you know, it continues to maintain those independence, redundancy, predictability, and repeatability, and D-3 concepts in the design, and we found that the HIPS implementation meets design criteria 15, 16, and 19.

So, those are the review of the HIPS platform. I think the next slide, we are going to talk about -- next slide, please? Yeah, it's the TRPS review, so I'm going to turn it over to Norbert Carte to take over the TRPS review, and then I'll come back and I'll talk about the ESFAS review. If there is any questions on the HIPS platform implementation, I can take those right now.

MEMBER BROWN: I guess we're good to go. Thank you, Dinesh.

MR. TANEJA: All right, Charlie. So, Norbert, it's all yours.

MR. CARTE: Thank you. Hi, my name is Norbert Carte. I'm a senior I&C technical reviewer at NRR. Next slide, please?

So, I wanted to talk a little bit about the philosophy of the review. So the design criteria in chapter three and which are translated into chapter seven are essentially the performance objectives. So, if you perform those performance objectives, then you have reasonable assurance of adequate safety. And SHINE did that or discussed that in chapter three by showing how they meet their safety criteria.

So, the next level down is -- now, with SHINE, SHINE has a lot of design criteria in the FSAR. They're not all equally important. Some are more safety significant than others and we focused our review on the safety significant ones such as independence.

Anyway, the next level down in this design hierarchy is basically the design bases, which are effectively functions and values. So, a safety analysis report has an analysis that shows that if the functions are performed at these values, then the design criteria are met.

So, what happens is what we have done or completed so far is we have looked at the design criteria, if the design basis and functions are consistent with those functions assumed in other FSAR chapters and meet the design criteria. The values essentially are set points, response times, and ranges of instruments.

Since we haven't looked at the instruments in detail, what we've seen in the set point calculations and in the FSAR -- well, the FSAR has analytic limits. The tech spec will have limiting safety system settings.

We have looked at those, but that's under review and discussion, and those numbers may or may not change based on some of the audit discussions we've had.

So, what we will eventually do in a thread, or we should eventually do in a thread audit is pull the thread all the way through. In other words, look at the values assumed in the safety analysis in chapter seven, so, I mean, 13. They're not in 13. They're in underlying calculations.

Our reviewer in that area did look at those things, but we will then trace that into the set point calc where the analytic limit is adjusted for all the uncertainties.

We should trace the uncertainty budget in the set point calculation to the actual instruments to ensure that they can reasonably assure those budgets. What we've seen in the calculations are reasonable numbers, not the necessarily actual numbers for actual pieces of equipment that we've seen.

The one number that I think is probably the most important is the set point. The response time, with 500 milliseconds on an FPGA-based system, that's actually a very, very generous response time. It's very slow.

I haven't seen the specific processors or what they're doing, but 500 milliseconds is very slow because these things can perform the calculations in parallel and can have response times on the order of two milliseconds. So, I'm not sure why it takes 500 milliseconds, but we'll look at that in detail. Next slide, please?

So, what I wanted to talk a little bit here about is some architectural things. What didn't get emphasized is if we look at these, those top green boxes, the singular ones, there's a little white box and it has an arrow out to PICS.

Well, if you get out your magnifying glass and you look at the text inside that little white box, it says TX, so that's a transmit only box and that gives us our -- it's a communication module, a communication port configured as transmit only. That gives us our one-way isolation.

In addition, you have the gateway which also has a receive only, which the transmit only port is connected to a receive only port, which is additional isolation, but this is where we achieve our isolation.

When we talk about configurable parameters, you'll see there is this white box, maintenance workstation, that has a dotted line. You turn a key and make a connection in order for the received port on the green module to be connected to the send port in the maintenance workstation, so you have to actually make a connection.

So, between those two features effectively have translated electronic control of access features into a physical control of access issue. You have to use controlling access to the key.

You have to remove the cards to reprogram them. You control access to the physical cards and that's basically how TRPS addresses digital communications.

Now, there's one other thing that comes up, what you saw on 741 that you don't see here. Actually, I'm having trouble reading it. There is an input to the gray box from the control room.

So, the manual controls do come across in a multiplex signal, but it's very discrete multiplexing, and in a sense, the signal comes across as a binary word. Part of that word is the address. It's parity checked. It's complemented and parity checked, so there's a lot of assurance on that. Shoot, I wonder if I'm going too far.

Also then there's the command to what to actuate, and again, they've talked about the priority logic a little bit. That command can only happen under two conditions. There is no either automatic safety actuation or there is no -- and the enable switch is in the correct position.

So, those gives us our control of access and independence criteria. There's also independence between the divisions, which is also done by some, I guess, pink lines on this diagram. Again, that's through send and receive ports on the SBMs or SBVMs. Next slide, please?

So, the other thing that happens is that the TRPS is mode dependent and it has a mode dependency in part to enable and disable operational bypasses automatically.

So, there is no -- so in some function, in some modes, some functions are not needed. They are automatically disabled when they are not needed and automatically enabled when they are needed, so there is no operator initiated operational bypass.

Maintenance bypass can be performed on individual modules or components and it's not disabling the whole function across all three divisions. It's disabling or being able to work on one component.

There is a maintenance bypass feature that can be either put in trip, for instance, in a two out of three system, or it can be put in a bypass state for a one out of two system. Therefore, you can perform maintenance on the sensor, NSFM function module, without actuating a protective function.

The use of that maintenance bypass is

discussed in the tech specs, but we'll look at tech specs later, but there is a very restricted and limited use on when you may bypass a signal for testing or maintenance purposes.

MEMBER MARCH-LEUBA: This is Jose. When you put a channel on bypass, what happens to the voting logic? Is it still two out of three --

MR. CARTE: Well --

MEMBER MARCH-LEUBA: -- or is it one out of two?

MR. CARTE: Effectively you're either putting the channel -- you can put it in two -- there's two switches. One --

MEMBER MARCH-LEUBA: If you put it on three, then --

(Simultaneous speaking.)

MR. CARTE: Right, right, right, one is -- there's two switches. One switch is an out of service switch and the other -- which it's in service or out of service.

And if you're in the out of service position, then the indication on the other switch matters, and that indication is either tripped or bypassed, so, and that tripped is either an open signal or a closed signal basically.

It's not really changing the voting logic. It's driving the signal to be a particular state, which effectively changes the voting logic. So, a two out of three signal with one signal in a tripped position is effectively a one out of two signal.

MEMBER MARCH-LEUBA: That's obvious, but what happens if you put it on bypass?

MR. CARTE: The --

MEMBER MARCH-LEUBA: Would you need a two out of two?

MR. CARTE: Yes, you would need a two out of two. That can be used for -- there's certain systems like ESF that is basically always required to be operable, and so you, and you will need to do some testing, and some of those functions in ESF has two inputs and it's a one out of two logic to accomplish the single failure criteria.

Therefore, in order to do maintenance or test those particular functions, you must put it in bypass. The current tech spec says two hours in order to do that testing, but --

MEMBER MARCH-LEUBA: Okay, so that's what I was going to ask you. It's limited by tech specs, the amount of time that you can be in this dangerous configuration?

MR. CARTE: Yes.

MEMBER MARCH-LEUBA: Okay, and you've looked at it and you're happy with, I mean --

MR. CARTE: We're not done with tech specs, but we're heading in the right direction.

MEMBER MARCH-LEUBA: Okay, thanks.

MEMBER BROWN: Norbert?

MR. CARTE: Yes?

MEMBER BROWN: Back at the beginning of your spiel, you mentioned that, you stated that within the mode or some circumstances, some functions aren't necessary and they are automatically disabled.

MR. CARTE: Correct.

MEMBER BROWN: Is there an indication that they've been disabled?

MR. CARTE: Right, so this is where --

MEMBER BROWN: To the operators?

MR. CARTE: Well, we haven't finished looking at PICS and the PICS doesn't have the specific information. It is all communicated to the PICS, so.

MEMBER BROWN: That's my thought. That's what I was asking about. Is it available to the operators when they -- in the PICS, fundamentally in the control room or whatever is it?

MR. CARTE: Right, so since we're not done with PICS, I hesitate, but the information is --

MEMBER BROWN: That's fine. That's okay. I just -- you're looking at it. You can let us know when we get to that point.

MR. CARTE: It's output to PICS --

MEMBER BROWN: Yeah.

MR. CARTE: -- at this point.

MEMBER BROWN: Okay --

(Simultaneous speaking.)

MR. CARTE: And the bypass is, yes, the bypass is indicated in the block diagrams, the figures that are in the proprietary section, and those figures in the proprietary material are just the FSAR figures in case we wanted to talk about them, but all of the mode enable aspects are in those logic diagrams.

MEMBER BROWN: Okay, all right, that's it. Thank you.

MR. CARTE: Next slide? So, if we talk about design criteria, basically one design criteria is that transients won't cause -- not fuel. I can't say fuel. It's not a reactor -- solution, target solution design limits to be exceeded, right?

So, we did look at those events and we believe that is the case. There was some discussion about what is a transient? The other requirement is that it initiate functions in the case of an accident.

Well, all of the functions that the system does are traced to different scenarios in chapter 13, so it meets that criteria. We didn't find any inconsistencies between the FSAR chapters and the functions described in chapter seven.

So, the other, I mean, the failsafe criteria which you mentioned is listed in the FSAR for chapter seven. So, if you lose power -- so basically it goes into the safe state by removing power to the component, and therefore if you lose power to the TRPS, you're going to lose -- it's going to go into the safe state anyway.

So, failsafe criteria is pretty easy to achieve for loss of power. That's a program feature into the HIPS equipment as well. Certain modules fail safe. We discussed control of access and we discussed independence from PICS through the one-way communication.

There's another criteria which I didn't mention here, the separation of protection and control. There are no, in a sense, shared protection and control equipment.

So, the protection and control criteria is targeted at a very specific problem, well, in general.

If you really -- let me see how much -- the basic philosophy is generally that a facility can withstand two bad things, and this is not regulatory speak, right?

The first bad thing, we call an initiating event. It can be an operator action or it can be failure, and the second bad thing is sometimes called a single failure within the protection system.

Now, in the unique case where the protection system and the control system share components, how do you deal with the two failure criteria? And that's what the separation of protection and control criteria is for.

There are no shared components, so it's kind of an irrelevant criteria for this design because they could have just said we don't share components, but they had criteria for is they do, but they don't, so it's kind of an irrelevant criteria at this point. Next slide, please?

So, we've already discussed the basic design bases functions. If you go to the FSAR, it's actually discussed at various levels. You have this level of function discussed and then the next level is sets of components actuated, like which particular valves.

The valve numbers are not provided. If you look at the diagrams in chapter four, you can't trace the specific valves described in chapter seven to the valves on the diagrams in figure four since they're not labeled, but that's something we would also do as part of an audit.

We would do a thread audit on one particular event and trace that all the way from the safety analysis assumed values to the RPS functions, the equipment specs, components actuated and diagrams, just to see that we had a feeling that their document shows that everything is addressed.

We typically do that, two or three thread audits, or for a power plant, we do two or three. I'm not quite sure how many we'll do here, and the thing that's actually most important is the analytic limits.

And we did have our fellow other chapter reviewers look at the analytic limits in chapter seven and they concurred that those are the right values since we couldn't cross-check the analytic limits through chapter 13 or because chapter 13 didn't actually have the specific analytic limits in it. It's in the underlying calcs. Next slide, please?

So, I guess I went into this a little bit. So, in terms of the design bases, what's really covered well in the TRPS, I mean in the FSAR is the design bases. So, it's telling you what the variables monitored are.

It links to specific events covered in chapter 13. Chapter 13 then references back to chapter four. It identifies the specific equipment actuated or the functions like TRPS isolation, TSV isolation, TSV dump, but not the specific valves, which we might check later.

And the analytic limits that we see in Table 741 were mapped over to the tech specs. We still need to -- we have done some thread audits on set point calculations to look at the limiting safety system setting that is actually in the LCO, some further discussions on that.

Operation site criteria, I can't remember what I was going to say on that last one. Next slide?

MEMBER BROWN: Good choice.

MR. CARTE: So basically these are the same words that is in the safety evaluation, we have concluded that the design meets the design criteria, supports the functions in the other chapters.

We still have yet some confirmatory audits to do in terms of set point calculations in the tech specs, in terms of equipment meeting the values in the set point calculations, in terms of development processes for TRPS and HIPS, and traceability of values through the design documentation is what we're going to do.

Sorry, that was a lot coming at you very quickly. Any questions?

MEMBER REMPE: So this is Joy, and I guess I'm going to follow up on my earlier question. Could you talk about where you are with this audit and report?

Is this the right place? I know there's a slide, like, 42, but I think that's a backup slide, right?

MR. CARTE: Well, so ideally, from my point of view as a regulator, I want to put the audit off as long as possible. Because that means I'm looking at things that are as complete as possible, the more draft it is the less of a litmus test I get from looking at a document.

And so I think the ball -- we're really just in the --

MR. WATERS: Norbert, this is Mike Waters, let me clarify.

So we have an open audit plan, the audit's ongoing, we are primarily focused on the sub points and, you know, we're close to core loading, as I mentioned in the beginning. But for reviewers on the panel limits and response times that's, you know, described and validated by chapter, so it's part of the open tech spec review which, you know, we're not really prepared to talk about in any detail right now.

MEMBER REMPE: Well okay, so, again, I'm not going to say anything proprietary, it's very general -- but if it needs to be in a closed session or something later, that's fine. But with the information we were provided last month, I know they cited chapters as the reference for some of the assumed times, and I mentioned, hey, you know, that's great but it's not in those other chapters, and the Applicant acknowledged, yeah, it's not. And then I turned to the staff and said, how did you guys conclude that the timing for the response of the sensors and subsequent actions was adequate without having those times?

And I was referred to the audit and the report that's not yet available as where staff gained the confidence to believe that things were adequate. And will that be documented in the audit report?

MR. WATERS: I believe so. And what you're talking about is a, you know, it's both, an I&C

issue and assistant reviewer's issue -- we're working together on that issue.

And you're right that, as the reference in SE, some of the validation is referred to the underlying documents and the basis for that, that is confidence that the analytical limit and response times are correct.

And I can assure you, you know, internally the ones we looked at had been validated for some of the more risk-significant event sequences, within the underlying documents, when you put it all together.

MEMBER REMPE: So this sounds great but I'm from Missouri, I'd like to see it. When will it be available for ACRS?

MR. BORROMEO: So this is Josh --

(Simultaneous speaking.)

MR. WATERS: I -- okay, Josh. I was going to refer to Joshua.

MR. BORROMEO: Yeah. So this is Borromeo, Chief of the NPUF Licensing Branch. So maybe I can put, maybe a little bit of a -- coming at a different angle so, you know, we tried to find the appropriate place to kind of draw the line for, you know, when we complete these audits -- and as we mentioned a couple times, like, we're still doing the tech spec review.

We're wrapping up the tech spec review right now, we're slated to come to you in the early September time frame to discuss that. But we still have some ongoing audits related to I&C so, you know, I'm hopeful, you know, in the next -- shortly after the SE is completed -- that we will be able to the issue the audit report to you as well. And I'm thinking that we will do it in a way that we completed the NuScale audit reports, that they just came just after the SE was completed.

MEMBER REMPE: Can we see a draft before? I mean, again, I mean --

(Simultaneous speaking.)

MR. BORROMEO: Yes. Yeah, so -- yes, we can --

MEMBER REMPE: Something that we know and have confidence in. Because I get it, that you have to do, like, a bunch of internal reviews. But I just would like to see a draft, even, to give -- you know, you're documenting what gave you this confidence.

MR. BORROMEO: Understood. We can certainly provide the draft prior to the ACRS meetings.

MEMBER REMPE: So sometime in August we'll see this, is that a good assumption of what you're telling me?

MR. BORROMEO: We can provide something to you in August, how about that? Can I promise something? Is something better than nothing?

MEMBER REMPE: You bet, and August sounds good. Thank you.

MR. BORROMEO: Okay.

CHAIRMAN BALLINGER: This is Ron, am I reading between the lines that chapter seven is not complete, the review?

(Simultaneous speaking.)

PARTICIPANT: Is a draft a problem in terms of --

MR. BORROMEO: Well -- someone's talking. Maybe --

MEMBER BROWN: Well, obviously it's not complete, we've only covered 7.4 and 7.5 in this meeting. There's still 7.1 through three and 7.6, seven, eight, and nine.

CHAIRMAN BALLINGER: Okay, I got it. I got it.

MR. BORROMEO: Right. So some of these sections, they do have overlap, all right? So, you know, we present today on the areas where we have, you know, come, you know, made a determination on but for the overall I&C system, that review is still ongoing.

We felt that this approach would help us, you know, continue to move the review along efficiently.

MEMBER BROWN: And this is a much easier way to do it, so this only covers 7.4 and 7.5.

MR. BORROMEO: Right, and --

MR. CARTE: Well a little bit more than that because part of the problem is, the neutron flux detection system is actually, kind of, three complicated -- it's not really a system, it's three complicated input channels, right? Two detectors in each channel, three signals in each channel -- source, power, and wide, right? But it's not really a system, it's three independent inputs.

So we're treating neutron flux detection system as sort of an input to the TRPS in our safety evaluation, and the radiation monitoring system is also not a system, so to speak. There are some inputs that have various functions, like continuous air monitoring systems, or the stack release monitoring system, or the inputs, the ESFAS or tritium.

So there are different inputs and they're lumped and described together under the one name of radiation monitoring, but the inputs to TRPS -- those that are inputs to TRPS and ESFAS were covered today.

MEMBER BROWN: Norbert, you're making this complicated. There's a Section 7.8 on the nuclear flux detection system and there's another section on the RMS. So I --

MR. CARTE: The neutron flux detection system was covered today.

MR. WATERS: Let me -- this is Mike, let me try to address the bigger question.

For the safety related I&C, our design review was essentially complete with the exception of the few things I noted up front. One being, you know, the life cycle development process of programmable logic, that's part of the statement of findings, so that's still open.

As well as the technical specification issues, as Norbert talked about, and some of the underlying audit issues, you know, related to sub point calculations, response times, and analytical limits, that's still ongoing.

And in a confirmatory sense, you know, the explanation and the FSAR on that appears to be generally sound, but part of our confirmatory view is looking at those things as part of our audit process to confirm it. And of course we have not completed a review of PICS.

So that's the current stated evaluation, you know, the safety system review is very -- in the grand scheme of things -- very close to complete with the exception of the few things that we still review and are looking at. And I'll --

(Simultaneous speaking.)

MEMBER BROWN: Well, somewhere between five and seven, you know, seven-eight are -- like, you've completed them. I mean, you've, I assume --

(Simultaneous speaking.)

MR. WATERS: Yes, RMS and NFDS is complete from a design standpoint.

MEMBER BROWN: Yeah. So the outstanding -- I mean, 7.1 for instance covers a lot of stuff relative to operators, displays, and stuff like that, but I thought you were going to be covering that in the PICS discussion since --

(Simultaneous speaking.)

MR. WATERS: Yes --

MEMBER BROWN: In the main control rooms and stuff.

MR. WATERS: Anything related to PICS and, you know, the control room displays -- we're just calling it PICS as one -- will probably be one section we'll talk about that together.

MR. CARTE: So Human Factors obviously, has the arrangement and display of information and how that relates to the operator's task. We're looking at it more from a functional, how the equipment is arranged, not how it's presented to the operator.

MR. WATERS: Right. I didn't want to imply we're doing that type of review, I think Charlie's talking about what SRP says for chapter seven.

MR. CARTE: Right, but Human Factors is doing the human part.

MEMBER BROWN: That's tomorrow.

MR. CARTE: Yeah.

MEMBER BROWN: That's tomorrow. 7.9 is tomorrow, tomorrow at 11:00 o'clock, if we're on time, as part of the presentations.

MR. WATERS: Yep.

MEMBER BROWN: And, you know, I had a bunch of questions on displays and stuff like that, I'll pass those on but I wasn't going to mouse-milk them today, other than let you know what they are.

But -- well, I was going to do that at the end. I wanted to get through this other stuff first and make sure we closed out seven-four and seven-five, and seven -- whatever, seven-eight, and whatever the RMS one is, seven-seven or something.

MR. WATERS: Well we can transition over to Dinesh, you know, ask Dinesh to expedite, get us back on schedule here. And then the ACRS can make a decision if we need any specific proprietary discussions, if that's okay with the committee.

MEMBER BROWN: The logic diagrams, my personal opinion, we don't need to go through them, okay? You've got a whole bunch of those and we ought to go through the other part, unless Ron wants to countermand me and sit through somebody explaining all those little one-line diagrams to you.

CHAIRMAN BALLINGER: You're not going to get pushback from me on that, I've look at both, the staff and the SHINE presentations, and the diagrams are, they're basically the same sets of diagrams.

MEMBER BROWN: Yes.

CHAIRMAN BALLINGER: But let's try to continue, I'm sorry I complicated things.

MEMBER BROWN: Yes.

MR. CARTE: One last point before we move on, I think what you're going to get from Human Factors tomorrow is a discussion of the -- it's a process oriented review, not -- but I think that's what you're going to get, a process, not the actual display review.

But we can move on to ESFAS.

MEMBER BROWN: Yep.

MR. CARTE: Next slide, please.

MEMBER BROWN: I don't even have a section 7.9 in my ESFAS document right now, I don't even have a copy of that so I've got to go find it somewhere. I don't know who's got that.

MR. TANEJA: All right. We're ready?

MEMBER BROWN: Yep.

MR. TANEJA: So this is Dinesh again. So the ESFAS is in section 7.5 of the FSAR and I am combining that with the RMS, that is section 7.7 of the FSAR. So primarily all the safety related process radiation monitors which are part of the RMS provide analog signals to ESFAS and the TRPS, to generate the actuation signals.

So what we are getting from these radiation monitoring systems is a analog signal that, you know, is coming into the safety function modules and then the logic in the safety function module is determining the trip state based on the set point.

And also it's processing that signal and sending it over to the monitoring and indication bus, which gets sent over to the, you know -- which is all getting sent over to PICS.

Now, like Norbert said, we are still, you know, reviewing the PICS design so all the information and what information is made available to the operators is going to be part of that discussion, but the information is being sent over there.

So primary function, the ESFAS monitors the process variables for confinement of fission products and tritium, and for criticality safety. And it also provides all the process variable values and the system status indication to PICS for viewing, recording, and trending. Next slide, please.

So this is the ESFAS architecture which is very similar to the TRPS architecture, the only differences is in the TRPS we have basically nine separate systems, each for one of the IU cells.

Here we have one ESFAS system for the entire facility, basically we have three cabinets, each cabinet just consisting of a division, A, B, and C of the ESFAS. And other than that they are very identical, the only difference being that in ESFAS we have some, you know, that are based on one-out-of-two logic. So that input, you know -- we don't have that input going to the C channel, it only goes into channel A and B.

And then we have some variables where we have only channel A inputs -- well actually the channel A actuation of the device, because there are credit being taken for some check valves to provide the redundancy and isolation function. And we have one active valve and one check valve, so we have channel A providing the actuation and then the passive valve doesn't have any input coming into it. Next slide, please.

So the ESFAS and the RMS design, you know, I think, you know, the SHINE criterias that apply to it are the, you know, the general design criterias one through six, and 13 through 19, and 37 to 39, they apply to the ESFAS. And for the RMS, the general criteria is one, two, four, and then 13 and 38 apply to the radiation monitoring system.

So the key features of the feature is, like, I guess the criteria five talks about sharing of the system between control and, you know, and the protection system. Same thing is true here in ESFAS, they do not share any component between the radiation units and the control system. So that's all -- and that's how they meet SHINE criteria five.

And then the criteria 13 talks about the

I&C, so we have seven, five, one that provides all the signals that are being monitored by the ESFAS. And, you know, and we reviewed that and we basically came to conclusion that the ESFAS has operable protection capability in all operating modes, anticipated transients, and postulated accidents. So therefore it meets the design criteria 13. Next slide, please.

Design criteria 14 talks about protective system functions, so we looked at all the protective system functions and looked at the basis (audio interference) or, you know, essentially the accidents that are credited in chapter 13, and these are the function that are required to either, you know, maintain the facility confinement strategy and provide process shutdown functions. So we reviewed that and we came to the finding that the, you know, design meets SHINE criteria 14.

We talked about the, you know, protection system failure mode. So the HIPS platform, you know, is designed to fail safe, and we looked at all the, you know, components in the ESFAS design and they are all also designed to fail in a safe state. The passive components, such as check valves as well as the, you know, active components, you know, they fail safe on loss of power or the, you know, loss of the

ESFAS component, or any adverse environmental conditions will result in a fail safe state. And we also, you know, audited the ESFAS and TRPS single failure analysis to come to the same conclusion.

Separation of protection and control system, that's SHINE criteria 18. Essentially the same thing, you know, there is, you know, no sharing of the components and there is separation maintained between PICS and the protection system by the means the interfaces are implemented.

That is, we have one-way data going out to PICS for display and, you know, out for the operators, and also doing any kind of trending and, you know, and data logging. And any inputs coming in from PICS are coming through hardwired inputs through the, you know, through the isolated contacts.

So that separation is maintained between protection and control system, so any failure that may happen in the control system would not have any adverse impact to the ESFAS performing its safety function. So from there we came to the conclusion that the design meets SHINE design criteria 18. Next slide, please.

Protection against anticipated transients. So that is the SHINE design criteria 19, and here, you know, we have the ESFAS, you know, implemented on the HIPS platform which is a deterministic functionality. And primarily because of that, you know, it's -- everything is implemented on that so there is a -- and then, you know, the way it's implemented and using the three channels, it has a high probability of achieving all of safety function under all postulated conditions. So that's how we came to the conclusion of compliance to design criteria 19.

Criteria 37 is criticality control in a radio isotope production facility. So most of the criticality controls are achieved by the -- in a passive design nature of the plant, and some administrative controls. But there are two functions that are relied upon, you know, for active engineer control to provide the double contingency principle, and these are the two safety functions, vacuum transfer actuation and the DSPS distillation tank isolation functions.

So they are, you know, providing the engineered, active engineered criticality safety to satisfy the design criteria 37.

Monitoring of radioactive releases, that's criteria 38. So there is actually a table in section 7.7 that identifies all the safety related, you know, process, radiation monitors -- we looked at that. We also looked at non-safety related area radiation monitors, and the other affluent monitors to essentially assure that there was adequate coverage of all the monitoring of the -- and as well as, I think we coordinated the review with the other chapters for looking at all the radio monitors to come to a conclusion that it meets criteria 38. So next slide, please.

Hydrogen mitigation, that's criteria 39. So ESFAS is designed to initiate hydrogen purge to control any buildup of hydrogen that releases into the primary system boundary.

And we reviewed that and essentially initiates the nitrogen purge system under certain circumstances, and, you know, and those logics, we looked at the logic diagrams, and we looked at the interfaces between the ESFAS and the TRPS to initiate the hydrogen purge for a given condition, and came to a conclusion that it complies with the SHINE design criteria 39.

And then there were some specific, you know, design specific criterias and the single failure criteria essentially that I wanted to highlight here, is that in the ESFAS design we have instances where the actuator components are only in division A and then we rely on these passive check valves for the redundancy purposes. So that's how it meets the single failure criteria and, you know, so no single failure is going to result in loss of protective action. Next slide, please.

So, you know, I think, you know, this is basically the conclusion, summary from the safety evaluation that really came to the conclusion that the ESFAS and the radiation monitoring system -- specifically the safety related process radiation monitors -- meet the specified design criterias. And the ESFAS and the RMS are capable of performing their allocated design functions under all postulated conditions.

So that is my presentation on ESFAS and RMS. Are there any questions?

(No audible response.)

CHAIRMAN BALLINGER: Okay, I think, if there aren't any questions, that concludes the staff presentation, correct?

MR. TANEJA: Correct.

CHAIRMAN BALLINGER: So what we need to do now is to ask for public comments, and then have the discussion related to the necessity of having closed session.

So if there are members of the public that would like to make a comment, please unmute yourself and state your name and make your comment please.

(No audible response.)

CHAIRMAN BALLINGER: It's hard to tell. Okay, it doesn't sound -- it doesn't appear that we have any members of the public that would like to make a comment, so now we need to have the discussion about whether or not we need a closed session.

Now, Charlie, has your opinion remained the same?

(No audible response.)

CHAIRMAN BALLINGER: Hello?

(No audible response.)

CHAIRMAN BALLINGER: Well, while we're waiting for Charlie, other members and/or the --

MEMBER BROWN: My mic was off, I'm sorry. My mic was off and it was hidden by one of the other charts I had up.

No, I haven't changed my mind at all. As far as I'm concerned those will not add, the value was added by the presentations they made. That's my opinion.

CHAIRMAN BALLINGER: Thank you.

Now I should also ask the staff, as well as SHINE, whether they feel that there is additional information that needs to be conveyed by having a closed session?

MR. BALAZIK: This is Mike Balazik with the NRC staff, we just had those in case we went into proprietary information to support our discussion, so my opinion, we don't need one for the NRC staff.

CHAIRMAN BALLINGER: Tracy? Who am I asking in the SHINE side?

MR. BARTELME: This is Jeff Bartelme from SHINE. No, agree, don't have to go into closed session but before we do wrap, there was a -- from the staff presentation, Member Brown's question on ESFAS criterion 18 and why there's not a comparable TRPS criterion, and we do want to address that before we wrap today.

CHAIRMAN BALLINGER: Okay, well why don't you give it a shot.

MS. RADEL: This is Tracy, so the ESFAS criterion in question, criterion 18, and that is a system specific design criteria versus a SHINE general design criteria, is only applied to ESFAS versus both, ESFAS and TRPS. And that is because it comes out of the draft chapter seven of the interim staff guidance, which -- it comes specifically out of the radiation monitoring section, and it is applied for systems where you're monitoring for radiological release into the facility, out of the confinements, and out of the facility. And so those monitoring systems are within the ESFAS system, not within the TRPS.

There are radiation monitors on the outlet of the IU cells but those are redundant to the RVZ1 and RVZ2 ones within ESFAS, as far as their flow paths. So we applied it only to the ESFAS system and not to both.

CHAIRMAN BALLINGER: Does that answer your question, Charlie?

MEMBER BROWN: I don't know.

(Laughter.)

MEMBER BROWN: I was trying to look for something a little bit more crisp. You said it came out of what document? You cited a document that I wasn't aware of.

MS. RADEL: It came out of the draft chapter seven interim staff guidance for NUREG 1537, which is where all the system specific I&C design criteria came from. And that particular design criterion came from the radiation monitoring section of that draft chapter seven.

MEMBER BROWN: So the words, the protection system is separated from control systems to the extent that any failure of a single control or channel, or failure or removal from the service of any protection system or component that is common to the controller protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnections of the protection system is limited to ensure that safety is not significantly impaired.

And I'm trying to figure -- you're saying there's no application in (audio interference) your all's response and it says, there are no sensor outputs that have ESFAS and a non-safety related control function, therefore we're not doing anything (audio interference) that.

Is that correct, even though you listed it?

MS. RADEL: There are separate single failure criterion that are applied to TRPS -- sorry, I'm looking. So there's still TRPS --

(Simultaneous speaking.)

MEMBER BROWN: I don't see anything to deal with radiation monitoring in there, that's all I'm saying.

MR. BARTELME: I want to be sure -- this is Jeff Bartelme, I want to be sure we're not confusing, you know, how ESFAS meets design criterion 18, and how ESFAS meets that specific ESFAS criterion 18. We've got both, SHINE general design criterion and system specific design criterion listed in both, seven-four and seven-five.

What we're describing here is how we meet ESFAS criterion 18 and why there's not a corresponding system specific criterion for TRPS.

MEMBER BROWN: Yeah. That's what I'm looking at. I'm sorry, I read from the wrong one.

But no single failure with failures result of design basis event should prevent operators from being presented information necessary to determine the safety status of the facility following the event.

So you're saying, because ESFAS is facility covered and TRPS is an individual system coverage, that that's why that applies to ESFAS. Did I phrase that properly?

MS. RADEL: Yes, that is correct.

MEMBER BROWN: Okay, I got it now. You had far more words.

Okay, so the answer is varied -- it's not varied, it's necessary to determine the safety status of the facility, following the design basis event. More specific detailed, I got it.

Okay? We're good, you're good, you don't have to do anything else. Thank you for making sure I knew what to look at.

CHAIRMAN BALLINGER: Okay. So now let's ask questions from the members or consultants, are there questions that you may have that would require us to have a closed session either, from members or consultants?

MARCH-LEUBA: This is Jose, I don't have any more questions. My concerns were addressed.

CHAIRMAN BALLINGER: Thanks.

MEMBER SUNSERI: This is Matt, I don't need a closed session.

CHAIRMAN BALLINGER: Okay. Well, I'm assuming --

MEMBER REMPE: So this --

CHAIRMAN BALLINGER: Whoop. Okay.

MEMBER REMPE: This is Joy, I don't need a closed session but I am looking forward to receiving what Josh said he'd provide in August.

CHAIRMAN BALLINGER: Yes.

MEMBER REMPE: Something is definitely better than nothing.

(Laughter)

CHAIRMAN BALLINGER: I think there's a song here somewhere.

Anyway, okay, absent any additional requirements for a closed session, then we are in -- thank you very --

MEMBER BROWN: No, don't stop. I think between us we ought to make sure of one other thing in your schedule for tomorrow, just amongst us. I mean, the staff can stay there because I'm not quite sure -- you've got a one hour session tomorrow, between 11:00 and 12:00, on Human Factors, chapter 12, section 7.9.

I went back and looked at chapter 12, couldn't find it -- at least on the version of the document I've got on my laptop, of the FSAR, and I couldn't find a section 7.9. And I think Vicki is supposedly working Human Factors, so maybe she's got something that I don't know about it.

I just want to know that we have something to talk about, or we have something to review, because I see they do have slides on it. It's 7.4.9 or something is what they're referring to on their slides.

MR. CARTE: Michael, can you clarify --

MR. BARTELME: I think the SE input

provided to you was labeled chapter seven-nine -- it's not a part of chapters 12, it's actually a separate SE section called 7.9. Do you have an SE section seven-nine?

MEMBER BROWN: I didn't look at the SE, I looked at the FSAR.

MR. BALAZIK: This is Mike Balazik, the SHINE project manager. Yeah, it's added to the end of chapter seven SE, that's where we decided that Human Factors would best fit. We were debating whether to put it in chapter 12 or chapter seven, but we concluded that it would best fit in chapter seven because in the NUREG 1537 it does talk about certain aspects of Human Factors, so that's where we plan on putting it.

MEMBER BROWN: Okay, I found it, I went off and -- I just looked up the SER, it's there.

Vicki, are you there?

MEMBER BIER: Yes, I'm on.

MEMBER BROWN: Were you aware of this?

MEMBER BIER: Yeah, I had it. Sorry.

MEMBER BROWN: Okay. All right. I apologize --

MEMBER BIER: No problem.

MEMBER BROWN: I was just trying to make

sure, my ignorance --

(Simultaneous speaking.)

MEMBER BIER: Yeah. I appreciate it.

MEMBER BROWN: All right. I'm sorry for the confusion, troops.

MEMBER BIER: No, I'm glad to get it straightened out.

CHAIRMAN BALLINGER: Okay, so I think we've concluded we do not need a closed session, and we're having discussions related to other things. Are there any other discussions that we need to have before tomorrow?

(No audible response.)

CHAIRMAN BALLINGER: Okay. Then I would -- then we thank you very much for the presentations, I'm sure we're all thankful for the presentations.

We are now adjourned until 9:30 tomorrow morning. Thank you again, folks.

(Whereupon, the above-entitled matter went off the record at 4:52 p.m.)

Design Criteria

TRACY RADEL, VICE PRESIDENT OF ENGINEERING

Outline

- Development of SHINE Safety Criteria
- SHINE Safety Criteria
- Development of SHINE Design Criteria
- SHINE Design Criteria
  - Generally-Applicable Design Criteria
  - Subcritical Assembly Design Criteria
  - Instrumentation, Control, and Protection System Design Criteria
  - Primary System Boundary Design Criteria
  - Electric Power Systems Design Criteria
  - Confinement and Control of Radioactivity Design Criteria

Development of SHINE Safety Criteria

- Safety-related structures, systems, and components (SSCs): Those physical SSCs whose intended functions are to prevent accidents that could cause undue risk to health and safety of workers and the public; and to control or mitigate the consequences of such accidents.
- Acceptable risk can be achieved by an event being highly unlikely (≤ 10^{-5} per event, per year) or having consequences less severe than the SHINE safety criteria.
- SHINE safety criteria were developed using:
  - NUREG-1537 and Interim Staff Guidance (ISG) augmenting NUREG-1537
  - 10 CFR 70.61
  - 10 CFR 50.2
  - NRC-proposed accident dose criterion (as part of proposed rulemaking related to non-power production and utilization facility license renewal)

SHINE Safety Criteria

- An acute worker dose of 5 rem or greater total effective dose equivalent (TEDE)
- An acute dose of 1 rem or greater TEDE to any individual located outside the owner controlled area
- An intake of 30 milligrams or greater of uranium in a soluble form by any individual located outside the owner controlled area
- An acute chemical exposure to an individual from licensed material or hazardous chemicals produced from licensed material that could lead to irreversible or other serious, long-lasting health effects to a worker or could cause mild transient health effects to any individual located outside the owner controlled area
- Criticality where fissionable material is used, handled, or stored (with the exception of the target solution vessel)
- Loss of capability to reach safe shutdown conditions

Development of SHINE Design Criteria

- Developed based on 10 CFR 50, Appendix A and 10 CFR 70.64(a) design criteria
- The design criteria are selected to cover:
  - The complete range of irradiation facility and radioisotope production facility operating conditions
  - The response of SSCs to anticipated transients and potential accidents
  - Design features for safety-related SSCs including redundancy, environmental qualification, and seismic qualification
  - Inspection, testing, and maintenance of safety-related SSCs
  - Design features to prevent or mitigate the consequences of fires, explosions, and other manmade or natural conditions
  - Quality standards
  - Analyses and design for meteorological, hydrological, and seismic effects
  - The bases for technical specifications necessary to ensure the availability and operability of required SSCs

Generally-Applicable Design Criteria

Criterion	SHINE Design Criteria	Basis
1	Quality standards and records	10 CFR 50 Appendix A, Criterion 1 10 CFR 70.64(a)(1)
2	Natural phenomena hazards *The facility structure supports and protects safety-related structures, systems, and components (SSCs) and is designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches as necessary to prevent the loss of capability of safety-related SSCs to perform their safety functions.* *Safety-related SSCs are designed to withstand the effects of earthquakes without loss of capability to perform their safety functions.*	10 CFR 50 Appendix A, Criterion 2 *Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed.* 10 CFR 70.64(a)(2)
3	Fire protection	10 CFR 50 Appendix A, Criterion 3 10 CFR 70.64(a)(3)

Generally-Applicable Design Criteria

Criterion	SHINE Design Criteria	Basis
4	Environmental and dynamic effects *Safety-related structures, systems, and components (SSCs) are designed to perform their functions with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents. These SSCs are appropriately protected against dynamic effects and from external events and conditions outside the facility.*	10 CFR 50 Appendix A, Criterion 4 *Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. However, dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping.* *10 CFR 70.64(a)(4)*
5	Sharing of structure, systems, and components *Safety-related structures, systems, and components (SSCs) are not shared between irradiation units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions.*	10 CFR 50 Appendix A, Criterion 5 *Structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units.*

SHINE

Generally-Applicable Design Criteria

Criterion	SHINE Design Criteria	Basis
6	Control room *A control room is provided from which actions can be taken to operate the irradiation units safely under normal conditions and to perform required operator actions under postulated accident conditions.*	10 CFR 50 Appendix A, Criterion 19 *A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.*
7	Chemical protection	10 CFR 70.64(a)(5)
8	Emergency capability	10 CFR 70.64(a)(6)

Subcritical Assembly Design Criteria

Criterion	SHINE Design Criteria	Basis
9	Subcritical assembly design *The subcritical assembly system, target solution vessel (TSV) off-gas system, and primary closed loop cooling system are designed with appropriate margins to assure that target solution design limits are not exceeded during conditions of normal operation, including the effects of anticipated transients.*	10 CFR 50 Appendix A, Criterion 10 *The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.*
10	Subcritical assembly inherent protection *The subcritical assembly system is designed so that the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity.*	10 CFR 50 Appendix A, Criterion 11 *The reactor core and associated coolant systems shall be designed so that in the power operating range the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity.*
11	Suppression of subcritical assembly power oscillations *The subcritical assembly system is designed to ensure that power oscillations that can result in conditions exceeding target solution design limits can be reliably and readily detected and suppressed.*	10 CFR 50 Appendix A, Criterion 12 *The reactor core and associated coolant, control, and protection systems shall be designed to assure that power oscillations which can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.*

SHINE

Subcritical Assembly Design Criteria

Criterion	SHINE Design Criteria	Basis
12	Reactivity limits *The target solution vessel (TSV) off-gas system, primary closed loop cooling system, and the TSV fill subsystem are designed with appropriate limits on the potential amount and rate of reactivity increase to ensure that the effects of postulated reactivity accidents can neither (1) result in damage to the primary system boundary greater than limited local yielding nor (2) sufficiently disturb the TSV, its support structures or other TSV internals to impair significantly the capability to drain the TSV. These postulated reactivity accidents include consideration of excess target solution addition, changes in primary cooling temperature, changes in primary system pressure, and deflagration or detonation in the primary system boundary.*	10 CFR 50 Appendix A, Criterion 28 *The reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures or other reactor pressure vessel internals to impair significantly the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by positive means), rod dropout, steam line rupture, changes in reactor coolant temperature and pressure, and cold water addition.*

Instrumentation, Control, and Protection Systems Design Criteria

Criterion	SHINE Design Criteria	Basis
13	Instrumentation and controls	10 CFR 50 Appendix A, Criterion 13 10 CFR 70.64(a)(10)
14	Protection system functions	10 CFR 50 Appendix A, Criterion 20
15	Protection system reliability and testability	10 CFR 50 Appendix A, Criterion 21 10 CFR 70.64(a)(8)
16	Protection system independence	10 CFR 50 Appendix A, Criterion 22
17	Protection system failure modes	10 CFR 50 Appendix A, Criterion 23
18	Separation of protection and control systems	10 CFR 50 Appendix A, Criterion 24
19	Protection against anticipated transients	10 CFR 50 Appendix A, Criterion 29

SHINE

Primary System Boundary Design Criteria

Criterion	SHINE Design Criteria	Basis
20	Primary system boundary *The primary system boundary is designed, fabricated, erected, and tested to have an extremely low probability of abnormal leakage, of rapidly propagating failure, and of gross rupture.*	10 CFR 50 Appendix A, Criterion 14 *The reactor coolant pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, and of gross rupture.*
21	Primary closed loop cooling system design *The primary closed loop cooling system is designed with sufficient margin to ensure that the design conditions of the primary system pressure boundary are not exceeded during any condition of normal operation, including anticipated transients.*	10 CFR 50 Appendix A, Criterion 15 *The reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.*
22	Quality of primary system boundary	10 CFR 50 Appendix A, Criterion 30
23	Fracture prevention of primary system boundary	10 CFR 50 Appendix A, Criterion 31
24	Inspection of primary system boundary	10 CFR 50 Appendix A, Criterion 32

SHINE

Primary System Boundary Design Criteria

Criterion	SHINE Design Criteria	Basis
25	Residual heat removal *The light water pool is provided to remove residual heat. The system safety function is to transfer fission product decay heat and other residual heat from the target solution vessel dump tank at a rate such that target solution design limits and the primary system boundary design limits are not exceeded.*	10 CFR 50 Appendix A, Criterion 34 *A system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.* *Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.*
26	Cooling water *The radioisotope process facility cooling system and process chilled water system are provided to transfer heat from safety-related SSCs to the environment, which serves as the ultimate heat sink.*	10 CFR 50 Appendix A, Criterion 44 *A system to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink shall be provided. The system safety function shall be to transfer the combined heat load of these structures, systems, and components under normal operating and accident conditions.*

Electric Power Systems Design Criteria

Criterion	SHINE Design Criteria	Basis
27	Electric power systems	10 CFR 50 Appendix A, Criterion 17 *An onsite electric power system and an offsite electric power system shall …* *The onsite electric power supplies, including the batteries, and the onsite electric distribution system, shall…* *Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to minimize to the extent practical the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of these circuits shall be designed to be available in sufficient time following a loss of all onsite alternating current power supplies and the other offsite electric power circuit, to assure that specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded. One of these circuits shall be designed to be available within a few seconds following a loss-of-coolant accident to assure that core cooling, containment integrity, and other vital safety functions are maintained.* *Provisions shall be included to…*
28	Inspection and testing of electric power systems	10 CFR 50 Appendix A, Criterion 18

Confinement and Control of Radioactivity Design Criteria

Criterion	SHINE Design Criteria	Basis
29	Confinement design *Confinement boundaries are provided to establish a low-leakage barrier against the uncontrolled release of radioactivity to the environment and to assure that confinement design leakage rates are not exceeded for as long as postulated accident conditions require. Four classes of confinement boundaries are established:* *1) the primary confinement boundary,* *2) the process confinement boundary,* *3) hot cells and gloveboxes, and* *4) radiologically-controlled area ventilation isolations*	10 CFR 50 Appendix A, Criterion 16 *Reactor containment and associated systems shall be provided to establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.*

Confinement and Control of Radioactivity Design Criteria

Criterion	SHINE Design Criteria	Basis
30	Confinement design basis *Each confinement boundary is designed to withstand the conditions generated during postulated accidents.*	10 CFR 50 Appendix A, Criterion 50 *The reactor containment structure, including access openings, penetrations, and the containment heat removal system shall be designed so that the containment structure and its internal compartments can accommodate, without exceeding the design leakage rate and with sufficient margin, the calculated pressure and temperature conditions resulting from any loss-of-coolant accident. This margin shall reflect consideration of (1) the effects of potential energy sources which have not been included in the determination of the peak conditions, such as energy in steam generators and as required by § 50.44 energy from metal-water and other chemical reactions that may result from degradation but not total failure of emergency core cooling functioning, (2) the limited experience and experimental data available for defining accident phenomena and containment responses, and (3) the conservatism of the calculational model and input parameters.*
31	Fracture prevention of confinement boundary *Each confinement boundary design reflects consideration of service temperatures and other conditions of the confinement boundary material during operation, maintenance, testing, and postulated accident conditions to prevent fracture of the confinement boundary.*	10 CFR 50 Appendix A, Criterion 51 *The reactor containment boundary shall be designed with sufficient margin to assure that under operating, maintenance, testing, and postulated accident conditions (1) its ferritic materials behave in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the containment boundary material during operation, maintenance, testing, and postulated accident conditions, and the uncertainties in determining (1) material properties, (2) residual, steady state, and transient stresses, and (3) size of flaws.*

Confinement and Control of Radioactivity Design Criteria

Criterion	SHINE Design Criteria	Basis
32	Provisions for confinement testing and inspection	10 CFR 50 Appendix A, Criteria 52 and 53
33	Piping systems penetrating confinement *Piping systems penetrating confinement boundaries that have the potential for excessive leakage are provided with isolation capabilities appropriate to the potential for excessive leakage.* *Piping systems that pass between confinement boundaries are equipped with either:* *1) a locked closed manual isolation valve, or* *2) an automatic isolation valve that takes the position that provides greater safety upon loss of actuating power.* *Manual isolation valves are maintained locked-shut for any conditions requiring confinement boundary integrity.*	10 CFR 50 Appendix A, Criterion 54 *Piping systems penetrating containment* 10 CFR 50 Appendix A, Criterion 55 *Reactor coolant pressure boundary penetrating containment* 10 CFR 50 Appendix A, Criterion 56 *Primary containment isolation* 10 CFR 50 Appendix A, Criterion 57 *Closed system isolation valves*

Confinement and Control of Radioactivity Design Criteria

Criterion	SHINE Design Criteria	Basis
34	Confinement isolation *Lines from outside confinement that penetrate the primary confinement boundary and are connected directly to the primary system boundary are provided with redundant isolation capabilities.* *Ventilation, monitoring, and other systems that penetrate the primary, process, glovebox or hot cell confinement boundaries, are connected directly to the confinement atmosphere and are not normally locked closed, have redundant isolation capabilities or are otherwise directed to structures, systems, and components capable of handling any leakage.* *Isolation valves outside confinement boundaries are located as close to the confinement as practical and upon loss of actuating power, automatic isolation valves are designed to take the position that provides greater safety. Manual isolation valves are maintained locked-shut for any conditions requiring confinement boundary integrity.* *All electrical connections from equipment external to the confinement boundaries are sealed to minimize air leakage.*	10 CFR 50 Appendix A, Criteria 55 and 56
35	Control of releases of radioactive materials to the environment	10 CFR 50 Appendix A, Criterion 60
36	Target solution storage and handling and radioactivity control	10 CFR 50 Appendix A, Criterion 61

SHINE

Confinement and Control of Radioactivity Design Criteria

Criterion	SHINE Design Criteria	Basis
37	Criticality control *Criticality in the facility is prevented by physical systems or processes and the use of administrative controls. Use of geometrically safe configurations is preferred. Control of criticality adheres to the double contingency principle. A criticality accident alarm system to detect and alert facility personnel of an inadvertent criticality is provided.*	10 CFR 50 Appendix A, Criterion 62 10 CFR 70.61(b) and (d) 10 CFR 70.64(a)(9) 10 CFR 70.24(a)
38	Monitoring radioactivity releases	10 CFR 50 Appendix A, Criterion 64
39	Hydrogen mitigation *Systems to control the buildup of hydrogen that is released into the primary system boundary and tanks or other volumes that contain fission products and produce significant quantities of hydrogen are provided to ensure that the integrity of the system and confinement boundaries are maintained.*	Unique SHINE design criterion

Advisory Committee on Reactor Safeguards

SHINE Medical Technologies, LLC Operating License Application

Chapter 3.1 - Design Criteria

Duane Hardesty
Sr. Project Manager
Office of Nuclear Reactor Regulation

July 19, 2022

Design Criteria

- The FSAR must specify the design criteria for the facility structures, systems, and components (SSCs) that are assumed in the SAR to perform an operational or safety function.
- Establish the necessary design, fabrication, construction, testing, and performance requirements for SSCs important to safety that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.
- The design criteria must include applicable standards, guides, and codes to support that the SSCs will function as designed as required by the safety analyses.

Regulatory Basis

- Regulatory Requirements
  - 10 CFR 50.34, "Contents of applications; technical information"
  - 10 CFR 50.40, "Common standards"
  - 10 CFR 50.57, "Issuance of operating license"

Acceptance Criteria

- NUREG-1537, Part 1, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Format and Content,” issued February 1996;
- NUREG-1537, Part 2, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Standard Review Plan and Acceptance Criteria,” issued February 1996;
- Final Interim Staff Guidance (ISG) Augmenting NUREG-1537, Part 1 and Part 2, for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors

Review Procedures and Technical Evaluation

- A review of the technical information presented in SHINE FSAR to assess the sufficiency of the principal design criteria for the SHINE facility and its safety-related SSCs for the protection of the public and the environment in support of the issuance of an operating license.
- The sufficiency of the design criteria is determined by ensuring that SHINE meets applicable regulatory requirements, guidance, and acceptance criteria, as discussed in Section 3.3, "Regulatory Requirements and Guidance and Acceptance Criteria," of the SER.
- The findings of the staff review are described in SER Section 3.5, "Review Findings."

SHINE's Design Criteria

- For each SSC, FSAR Tables 3.1-1 "Safety-Related Structures, Systems, and Components," and Table 3.1-2, "Nonsafety-Related Structures, Systems, and Components" identify the applicable FSAR section or sections that describe each SSC.
- SHINE discusses design criteria for individual SSCs in the applicable FSAR section describing those SSCs.
- Similarly, the NRC staff evaluation, as applicable to the specific design criteria, is included within the chapter of the SE where the staff evaluated those SSCs.
- Section 3 of the NRC staff's evaluation discusses the acceptability of SHINE's general design criteria (1-8) identified in Table 3.1-3, "SHINE Design Criteria," and of the Nuclear Safety Classification, as described in FSAR Section 3.1.

NRC Staff Observations

- The SHINE design criteria follows Appendix A to Part 50, "General Design Criteria for Nuclear Power Plants" and 10 CFR 70.64(a) "Design criteria."
  - Not all the GDC apply to SHINE's use of low enriched uranium (LEU) in the form of a uranyl sulfate target solution that is irradiated in a subcritical assembly by neutrons produced by a fusion neutron source.
  - Additionally, as discussed in Chapter 7 of the staff's SE, the application specific action items (ASAIs) in the NRC topical report on the HIPS platform are intended for power reactor applications and not all ASAIs are critical for ensuring safety in SHINE's application of the HIPS platform for the TRPS and ESFAS.
- The SHINE nuclear safety criteria are based on the 10 CFR 70.61, "Performance requirements" and the ISG to NUREG-1537.

SHINE Facility Nuclear Safety Criteria

To demonstrate that the principal design criteria are adequate, SHINE states in FSAR Section 3.1 that acceptable risk is achieved by ensuring that all postulated events are highly unlikely or by reducing the consequences to less than the SHINE safety criteria

- The SHINE safety criteria:
  - An acute worker dose of five rem or greater total effective dose equivalent (TEDE)
  - An acute dose of 1 rem or greater TEDE to any individual located outside the owner-controlled area
  - An intake of 30 milligrams or greater of uranium in a soluble form by any individual located outside the owner-controlled area
  - Criticality where fissionable material is used, handled, or stored (with the exception of the target solution vessel)
  - Loss of capability to reach safe shutdown conditions

General Design Criteria

Consistent with the guidance in NUREG-1537, the SHINE FSAR includes the following eight general design criterion:

- Criterion 1– Quality standards and records
- Criterion 2 – Natural phenomena hazards
- Criterion 3 – Fire protection
- Criterion 4 – Environmental and dynamic effects
- Criterion 5 – Sharing of structure, systems, and components
- Criterion 6 – Control room
- Criterion 7 – Chemical protection
- Criterion 8 – Emergency capability

Evaluation Findings and Conclusions

- Design criteria is provided for each SSC that is assumed in the FSAR to perform an operational or safety function.
- Design criteria includes references, as appropriate, to applicable standards, guides, and codes.
- Descriptions of the design are included in the section of the FSAR that corresponds to the specific SSC and generally include the following:
  - Design for the complete range of normal expected operating conditions.
  - Design to cope with anticipated transients and potential accidents.
  - Design redundancy, so that any single failure of any active component will not prevent safe shutdown or result in an unsafe condition.
  - Design to facilitate inspection, testing, and maintenance.

Evaluation Findings and Conclusions (cont.)

- Descriptions of the design are included in the section of the FSAR that corresponds to the specific SSC and generally include the following (continued):
  - Design provisions to avoid or mitigate fires, explosions, and potential man-made or natural conditions
  - Quality standards commensurate with the safety function and the potential risks.
  - Design requirements necessary to ensure the availability and operability of required SSCs.


thank you!

Hydrogen Mitigation

- SHINE Design Criteria No. 39 (Facility Unique)
  - Systems to control the buildup of hydrogen that is released into the primary system boundary and tanks or other volumes that contain fission products and produce significant quantities of hydrogen are provided to ensure that the integrity of the system and confinement boundaries are maintained.
    - Radiological ventilation zones 1, 2, & 3 (RVZ) [9a.2.1]
    - Subcritical assembly system (SCAS) [4a.2]
    - Target solution staging system (TSSS) [4b.1.3, 4b.4, 9b.2.4]
    - TSV off-gas system (TOGS) [4a.2]
    - TSV reactivity protection system (TRPS) [7.4]
    - Vacuum transfer system (VTS) [4b.1.3, 9b.2.5]
- Three systems are provided to mitigate hydrogen generation:
  - TOGS → SCAS gas management
  - Process vessel vent system (PVVS) → RPF Tanks
  - Nitrogen Purge system (N2PS) → RPF distribution header

Fire Protection

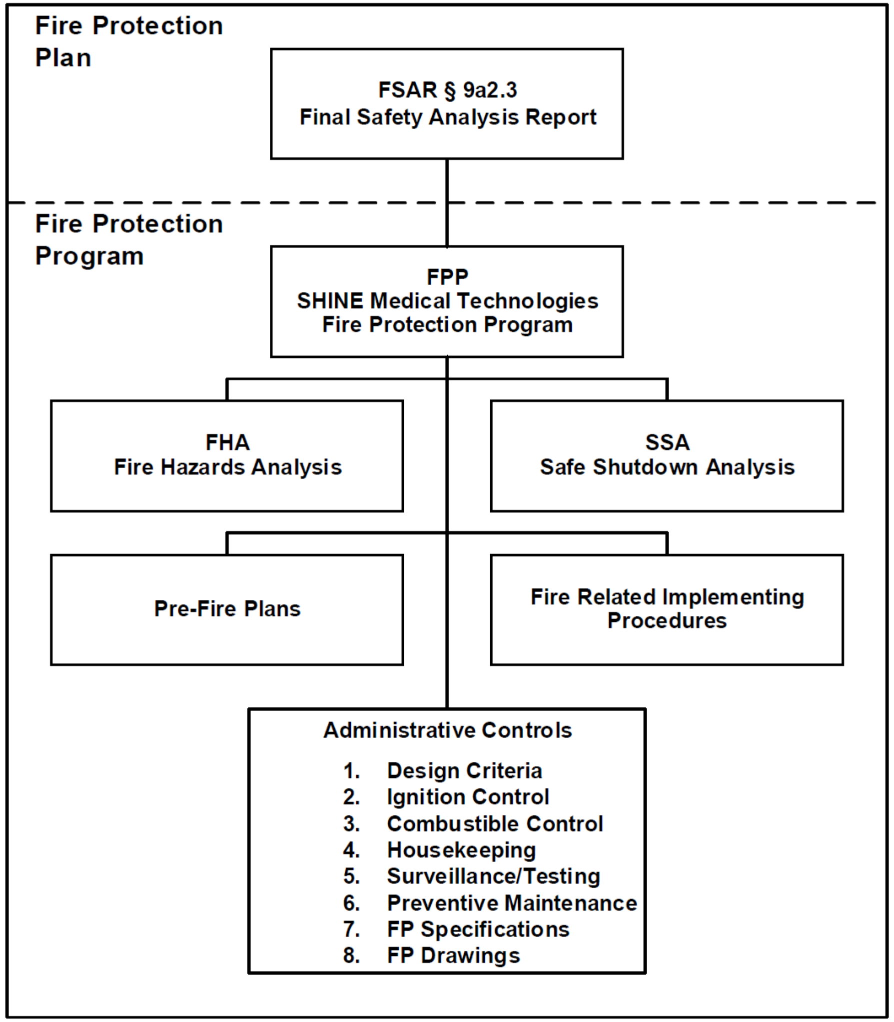
ANDREW MEYER, SAFETY ANALYSIS MANAGER

Outline

- Fire Protection Program
- Fire Hazards Analysis
- Safe Shutdown Analysis
- Fire Modeling
- Pre-Fire Plans

Fire Protection Program

- Objective of the fire protection program is to minimize the probability and consequences of fires in the SHINE facility
  - Elements of the fire protection program work together to satisfy the requirements to 10 CFR 50.48(a)
- The fire protection program takes a defense-in-depth approach
  - Prevent fires from starting, including limiting combustible materials
  - Detect, control, and extinguish fires which do occur, to limit consequences
  - Provide protection for systems, structures, and components (SSCs) important to safety so that a fire will not prevent the safe shutdown of the irradiation units (IUs) or cause an uncontrolled release of radioactive material to the environment



Fire Hazards Analysis

- Establishes and describes individual facility fire areas, which are unique areas separated by fire rated construction or administrative controls to prevent the spread of fire between adjacent fire areas
- Determines the fire hazard posed by operations and contents of each fire area
  - Hazards included combustible materials and ignition sources
- Along with the safe shutdown analysis, determines worst-case fire effects on safe shutdown capability and the potential for uncontrolled release of radioactive materials
- Evaluates the adequacy of fire protective features (e.g., fire prevention, barriers, detection, suppression) and any need for additional protection
- Analysis is supported by a combustible loading calculation, quantifying the heat load (in BTU/sq. ft.) of combustibles installed or stored in each fire area in the radiologically controlled area (RCA)

Safe Shutdown Analysis

- Demonstrates a means of safe shutdown of the IUs to ensure they can be placed and maintained in a safe and stable condition following a safe shutdown fire in any facility fire area.
  - Also demonstrates the capability of safety-related equipment to prevent uncontrolled releases of radioactive material as a result of fire
- Performance goals of the safe shutdown analysis:
  - Reactivity shall be maintained subcritical in the event of a fire
  - Combustible gas control systems shall be capable of performing their necessary functions in the event of a fire
  - Target solution cooling shall be capable of removing heat such that target solution boiling does not occur
  - Uncontrolled release of radioactive material shall be prevented
- Equipment credited with a safe shutdown function (including components designed and credited to isolate areas containing radioactive materials) are identified as part of the analysis

Safe Shutdown Analysis

- Analysis is performed on a per-fire area basis
  - Redundant trains of safety-related equipment are demonstrated to be separated such that a single fire cannot impair a safe shutdown function
- Primary separation criteria is fire-resistant barriers between redundant trains (i.e., redundant equipment located in different fire areas)
- Where redundant equipment is located in the same fire area, the following separation criteria are used in a qualitative assessment:
  - Spatial separation distance of at least 20 feet where automatic fire suppression is provided and at least 40 feet where automatic fire suppression is not provided
  - Embedment of cable conduit in structural concrete
  - Fixed fire suppression and/or detection in the fire area
  - Areas which have restricted access and/or are sealed
  - Areas which are continuously occupied
  - Administrative controls on combustible loading
- Where these separation criteria cannot be met as determined by analysis, fire modeling is performed to determine if both trains of equipment can be damaged by a single fire

Fire Modeling

- Quantitative fire modeling is performed using the Consolidated Model of Fire and Smoke Transport (CFAST) code to support the fire hazards analysis and safe shutdown analysis
- Two scenarios of concern are modeled:
  - Fire involving a neutron driver high-voltage power supply (HVPS) and nearby cables
  - Fire involving the target solution vessel (TSV) off-gas system (TOGS) motor control centers (MCCs)
- HVPS fire:
  - Objective: determine if a fire involving a HVPS could impact the structural members of the building (specifically the steel roof trusses and steel bridge crane rails)
    - CFAST used to determine the hot gas layer temperature and temperature of targets used to represent structural elements
  - Sources of combustibles: Dielectric oil in a transformer and cables in nearby cable trays
  - Damage criteria: 593°C (critical temperature of steel)
  - Conclusion: hot gas layer temperature at target areas is less than the damage criteria (i.e., less than the critical temperature of steel)

Fire Modeling

- TOGS MCC fire:
  - Objective: determine the distance (vertical and lateral) where critical temperatures are exceeded to determine whether a single fire can impact both TOGS MCCs
    - CFAST used to determine the Zone of Influence (ZOI) of TOGS MCC fire and transient fire in the TOGS MCC hallway
  - Sources of combustible: cables in an MCC and transient fires
  - Damage criteria: 205°C (based on thermal damage criteria for thermoplastic cables)
    - This bounds damage criteria for bulk cables (critical temperature of 500°C)
  - Conclusion: critical temperature at Division A MCC not reached by fire in a Division B MCC (and vice versa) and cables in raceways above MCCs are not ignited

Pre-Fire Plans

- Pre-fire plans are developed for areas of the main production facility to provide information for trained facility personnel and responding professional firefighters
- Plans include the following information, as appropriate:
  - Area identification
  - Emergency contact information
  - Occupancy/processes
  - Fire hazards
  - Radiation hazards
  - Electrical information (electrical disconnect)
  - Hazardous substances
  - Physical hazards
  - Exposure protection guidance
  - Communications
  - Access/egress routes
  - Ventilation
  - Fixed fire systems
  - Portable firefighting equipment

SHINE

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Advisory Committee on Reactor Safeguards

SHINE Medical Technologies, LLC
Operating License Application

Chapter 9a2.3 - Fire Protection Systems and Programs

Jay Robinson
Fire Protection Technical Reviewer
Office of Nuclear Reactor Regulation

July 19, 2022

Fire Protection Systems and Programs

- Fire protection for nuclear facilities uses the defense-in-depth (DID) concept to achieve the required degree of safety by using echelons of administrative controls, fire protection systems and features, and post-fire safe-shutdown capability.
- Fire Protection DID is designed to:
    - Prevent fires from starting, including limiting combustible materials;
    - Detect, control, and extinguish those fires that do occur to limit consequences; and
    - Provide protection for structures, systems, and components (SSCs) important to safety so that a continuing fire will not prevent the safe shutdown of the irradiation units (IUs) or cause an uncontrolled release of radioactive material to the environment.

Fire Protection Systems and Programs

- A fire protection plan is required. The fire protection plan:
  - Describes the overall fire protection program (FPP) for the facility.
  - Outlines the programs for fire protection, automatic fire detection and suppression capability, and limitations of fire damage.
  - Describes specific features necessary to implement the program, such as administrative controls and personnel requirements for fire prevention and manual fire suppression activities.
  - Describes the means to limit fire damage to SSCs important to safety, including those that are safety-related so that the capability to safely shutdown the plant is ensured.

Regulatory Basis

- 10 CFR 50.48(a), “fire protection.” Requires a fire protection plan that:
    - Describes the FPP.
    - Identifies positions responsible for the program and authorities delegated to those positions.
    - Outlines plans for fire protection, fire detection and suppression capability, and limitation of fire damage.
    - Describes administrative controls and personnel requirements for fire prevention and manual fire suppression activities.
    - Describes automatic and manually operated fire detection and suppression systems.
    - Describes the means to limit fire damage to SSCs important to safety to ensure safe shutdown.

Regulatory Basis

- Criterion 3, "Fire protection," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50.
  - SSCs important to safety shall be designed and located to minimize the probability and effect of fires and explosions.
  - Noncombustible and heat resistant materials shall be used wherever practical.
  - Fire detection and fighting systems of appropriate capacity and capability shall be provided and designed to minimize the adverse effects of fires on SSCs important to safety.
  - Firefighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the safety capability of these SSCs.

Acceptance Criteria

- NUREG-1537, Parts 1 and 2
- "Final Interim Staff Guidance Augmenting NUREG-1537, Parts 1 and 2

- Fire protection acceptance criteria describes:
    - The prevention of fires, including limiting the types and quantities of combustible materials.
    - Methods to detect, control, and extinguish fires.
    - That the facility should be designed and protective systems should exist to ensure a safe shutdown and prevent the uncontrolled release of radioactive material if a fire should occur.

Acceptance Criteria

- The SAR should contain sufficient information to support the following types of conclusions:
  - Facility meets local and national fire and building codes.
  - Fire protection systems can function as described and limit drainage and consequences at any time.
  - There is reasonable assurance that training for fire protection is adequately planned.
  - The potential radiological consequences of a fire will not prevent safe shutdown, and any fire-related release of radioactive material from the facility to the unrestricted environment has been adequately addressed.
  - Release of radioactive material from fire would not cause radiation exposures that exceed the requirements of 10 CFR Part 20.
  - Fire Protection technical specifications have been developed (as applicable).

Review Process and Technical Evaluation

- PSAR, SE For Construction Permit
- FSAR
- Additional Licensee Supporting Documents:
  - Fire Protection Program
  - Fire Hazards Analysis
  - Fire Detection and Suppression Design Criteria Documents
  - Safe Shutdown Analysis
  - Combustible Loading Calculation
  - Detailed Fire Modeling
  - Fire Protection Impact Review
  - Draft Procedures for Combustible Controls, Control of Ignition Sources, Housekeeping
  - Fire Protection Pre-Fire Plans
  - Radiological Dose Consequences

Review Process and Technical Evaluation

- Requests for Additional Information
- Licensee Clarified Information Regarding
  - Fire Brigade and Manual Firefighting Capability
  - Operator Actions
  - Fire Protection Change Control Process
  - Construction Elements
  - Safe Shutdown Analysis
  - Fire Protection Administrative Controls
  - Codes of Records
  - Code Deviations
  - Radiological Consequences

Evaluation Findings and Conclusions

- Fire protection-related SSCs and DID controls are designed, constructed, and used consistent with good engineering practice, which dictates that certain minimum requirements be applied as design and safety considerations for any new nuclear material process or facility.

- There is reasonable assurance that the fire protection systems and programs are in conformance with NUREG-1537, Parts 1 and 2.

Evaluation Findings and Conclusions

- There is reasonable assurance that the facility meets the requirements of 10 CFR 50.48(a) and Criterion 3 of Appendix A to 10 CFR Part 50.

- There is reasonable assurance that a fire in any plant area during any operational mode and plant configuration will not prevent the plant from achieving safe shutdown and maintaining a safe and stable condition and will also not cause radiation exposures that exceed the requirements of 10 CFR Part 20.

Implementation of the Highly Integrated Protection System

JASON POTTORF, DIRECTOR OF ENGINEERING, ROCK CREEK INNOVATIONS

Outline

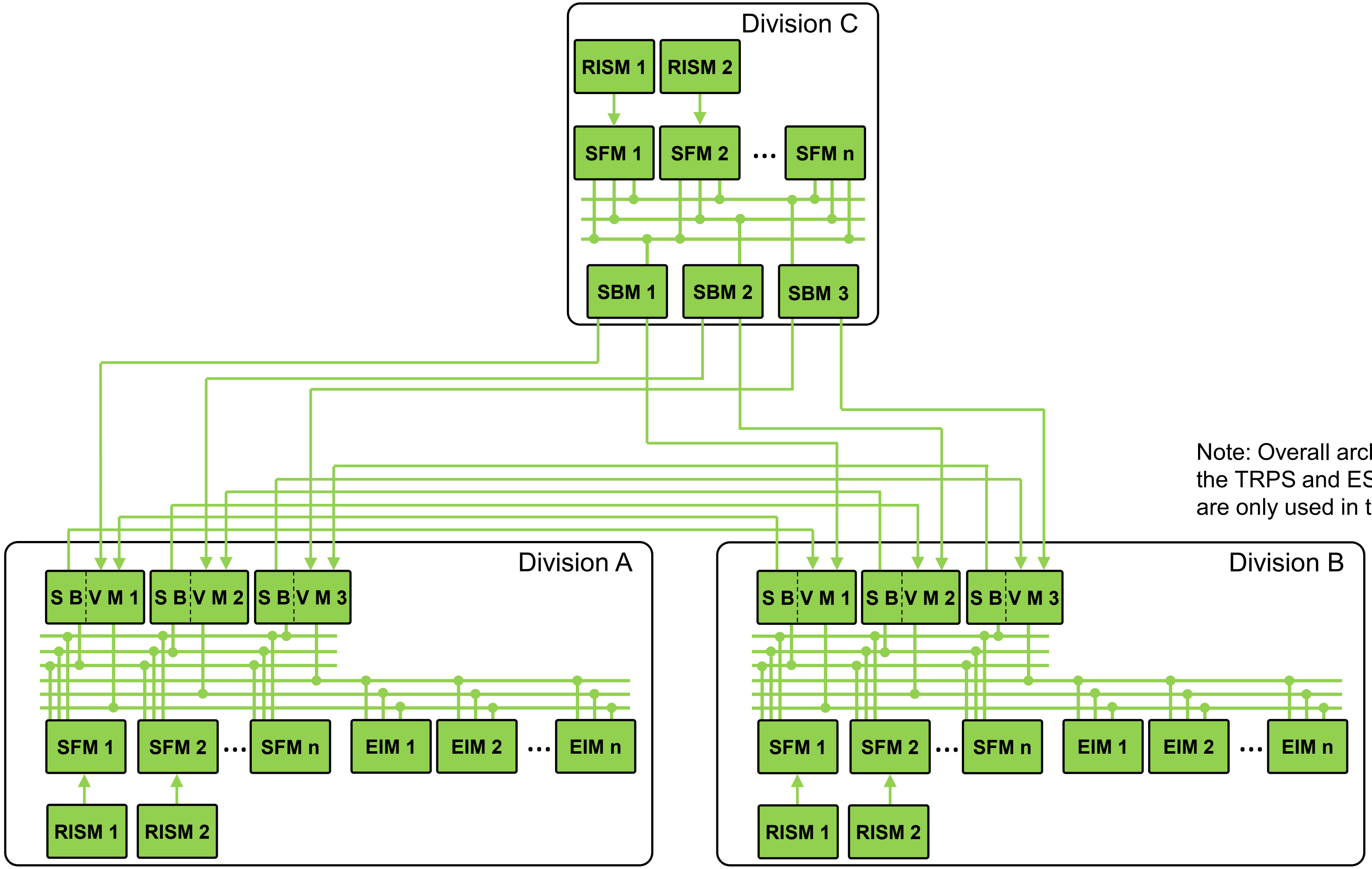
- Target Solution Vessel Reactivity Protection System (TRPS) and Engineered Safety Features Actuation System (ESFAS) Architecture
- Highly Integrated Protection System (HIPS) Platform Changes

TRPS and ESFAS Architecture

TRPS and ESFAS Architecture

- Architectual Differences compared to NuScale:
  - Function of Scheduling and Bypass Modules (SBMs) and Scheduling and Voting Modules (SVMs) is performed by a single module (Scheduling, Bypass, and Voting Modules [SBVM]) within Divisions A and B
  - Created two new modules which are simple variants of existing HIPS platform modules (Remote Input Submodules [RISMs] and Gateway Communication Modules [GWCMs])
    - RISM used to provide neutron flux input to a respective Safety Function Module (SFM)
    - GWCM used to aggregate multiple divisions of monitoring and indications information and provide it to the nonsafety-related control system
  - Three divisions of input signal conditioning and trip determination (A, B, C) with two divisions of voting and actuation (A and B)
  - Three different field programmable gate arrays (FPGAs) used – one for each of Divisions A, B, and C
    - Division A - Microsemi Flash type FPGA
    - Division B - Xilinx SRAM type FPGA
    - Division C - Intel Flash type FPGA

TRPS and ESFAS Architecture



Note: Overall architecture applies to both the TRPS and ESFAS, however the RISMs are only used in the TRPS.

SHINE

HIPS Platform Changes

HIPS Platform Changes

- Hardwired Module (HWM) input routing
- Use of fiber optic communications
- Communications Module bi-directional communications
- Number of Equipment Interface Module (EIM) switching outputs per module
- Scheduling, Bypass, and Voting Module (SBVM)
- Remote Input Submodule (RISM)
- Gateway Communication Module (GWCM)
- Self-Testing
  - Input Submodule Analog-to-Digital Converter (ADC)
  - EIM input and output testing
  - HWM input channel test
- Module front panel light-emitting diodes (LEDs)

HIPS Platform Changes

- Hardwired Module input routing
  - Section 2.5.2 of the Topical Report (TR) states that Trip/Bypass switch inputs to the HWMs are "routed only to the SBMs where it is used."
    - For SHINE, all signals input to the HWMs are made available on the backplane to all modules within the chassis where they are used only by those modules that need the specific signals
    - This supports using some safety valve position feedback inputs for safety function actuation (in the SBVMs) and also confirmation of completion of the safety function (in the EIMs)
- Use of fiber optic communications
  - Sections 2.5.3, 4.3, and 4.6.2 of the TR describe the use of fiber optic ports for inter-divisional transmit-only or receive-only communications.
    - For SHINE, all inter-divisional communications are implemented with copper RS-485 connections

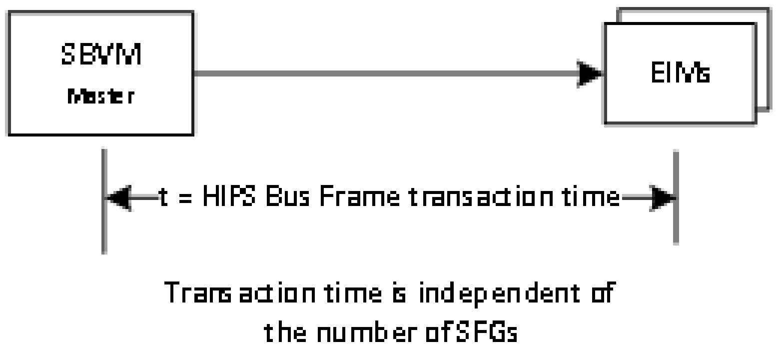
HIPS Platform Changes

- Communications Module bi-directional communications
  - Section 2.5.3 of the TR describes transmit-only or receive-only communications for a Communications Module (CM).
    - For SHINE, the GWCM implements the MODBUS communications protocol
    - Communications upstream of the GWCM are transmit-only from the Monitoring and Indication Communications Modules (MICMs) to the GWCMs
    - All communications handled by the GWCMs are nonsafety related communications
- Number of EIM switching outputs per module
  - Section 2.5.4.4 of the TR states that each EIM can control two groups of field components and each group can have up to two field devices
    - For SHINE, each EIM can control four groups of field components and each group can have up to two field devices

SHINE

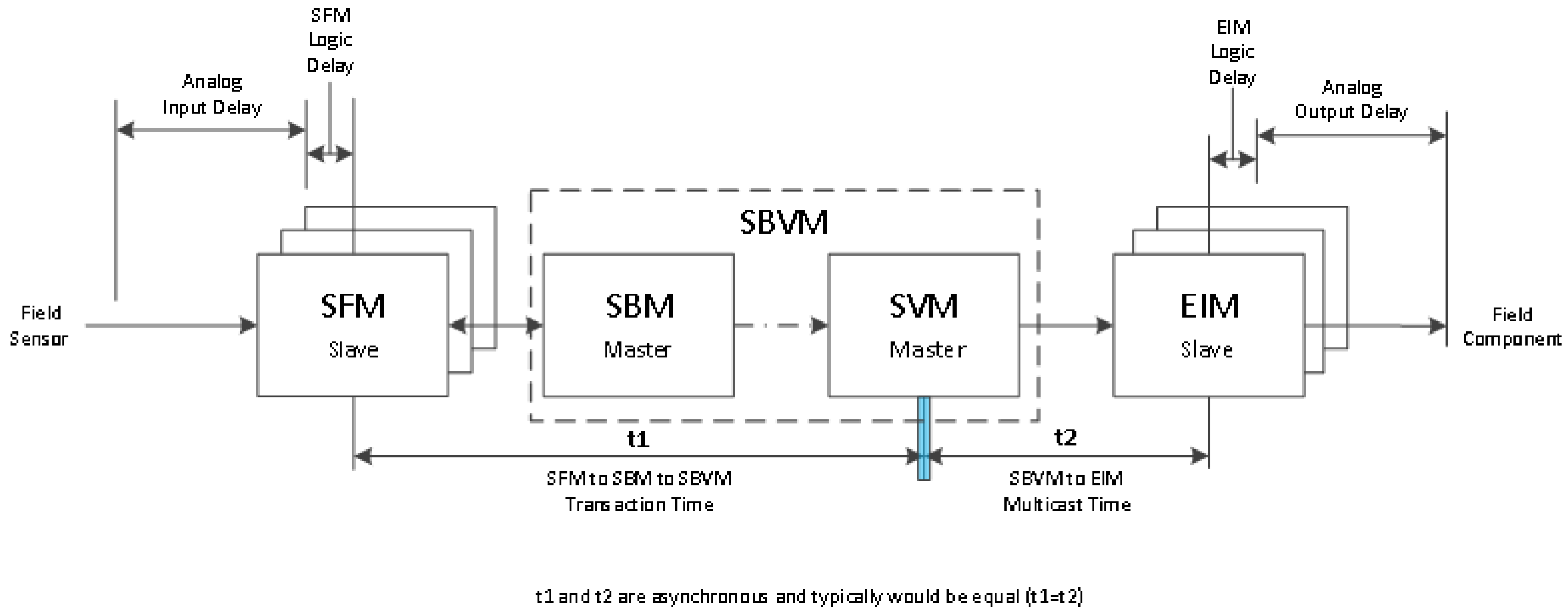
HIPS Platform Changes

- Scheduling, Bypass, and Voting Module
  - Throughout the TR, the use of SBMs and SVMs (two types of a communications module) is discussed as part of the "representative architecture."
    - For SHINE, the SBVM communications module combines all functions, capabilities, and design principles described in the TR for the SBM and SVM into a single module.
    - For SHINE, Figure 7-8 of the TR is modified to show: (1) only three divisions; (2) the "Wait for Sync" is not necessary for the SBVMs; and (3) the voting is different (not 2oo4 voting).
    - For SHINE, Figure 7-12 of the TR is modified to show that all safety function groups (SFGs) are voted on at the same time and the trip determination actuation (TDA) for all SFGs are then transferred to the EIMs at once instead of sending separate TDA information for each SFG to the EIMs.



HIPS Platform Changes

- For SHINE, Figure 7-14 of the TR is modified simply to show the SBM and SVM functionality being performed by the SBVM module (dashed box).



HIPS Platform Changes

- Remote Input Submodule
  - New module not discussed in the TR
  - Each RISM is directly associated with a single Safety Function Module (SFM) and allows for remotely locating one Input Submodule (ISM) from its associated SFM
  - The ISM on a RISM is the same as described in the TR with the self-testing/ADC modification (described on next slide)
  - The ISM on a RISM can be configured for a specific input type and calibrated as described in the TR for the SFM
  - The RISM includes communications module capabilities necessary to provide the input data via an isolated, one-way RS-485 connection to its associated SFM within the division
  - An additional RS-485 connection between the RISM and its associated SFM is provided to support modification of tunable parameters on the RISM

HIPS Platform Changes

- Gateway Communication Module (GWCM)
  - New type of communications module not discussed in the TR which utilizes two-way MODBUS communications
  - Similar to an MICM and performs only nonsafety-related monitoring and indication (M&I) functions
  - Receives M&I data via one-way isolated RS-485 connection from multiple MICMs
  - One communications port is configured for MODBUS communications with the respective PICS channel to provide aggregated M&I data

HIPS Platform Changes

- Self-Testing
  - Input Submodule Analog-to-Digital Converter
    - Sections 7.1.1 and 8.2.1 of the TR describe the self-testing features for the ADC for an analog input submodule (ISM)
    - The auto-calibration function described included the use of external passive components, whereas the TRPS and ESFAS designs will incorporate the critical passive components onto the ADC chip
    - Results in very precise values that are factory calibrated and are significantly less prone to drift over time and temperature
  - EIM input and output testing
    - The self-testing described in Sections 8.2.3.2 and 8.2.3.4 of the TR for discrete input circuitry (open/closed contact tests) and high drive output testing not being implemented for the TRPS and ESFAS designs
    - This implementation would require interaction between the FPGA logic and the analog actuation priority logic (APL) circuitry, and it was desired to keep the interface between the FPGA and APL as simple as possible
  - HWM input channel test
    - The self-testing identified in Section 8.2.7 of the TR for HWM input signals is not being implemented for the TRPS and ESFAS designs
    - This implementation would require interaction of the FPGA with the hardwired input circuitry (used for manual protection system actuation) and it was desired to not allow any interface of the FPGA with this capability

SHINE

HIPS Platform Changes

- Module front panel LEDs
  - Section 8.2.7 of the TR identifies that LED tests will be performed to identify if an incorrect LED status is being displayed
    - These tests will not be performed on a continuous basis for the TRPS and ESFAS designs for the following reasons:
      - Module front panel indication is not a safety function; and
      - Correct LED operation will be tested as part of factory and installation testing.
  - Section 8.4 of the HIPS platform topical report describes the two LEDs on the front of each HIPS module which are used to indicate the state of the module latches, the operational state of the module, and the presence of any faults for the module
  - The TRPS and ESFAS designs will include the following changes to the function of the LEDs from that presented in the TR:
    - The ACTIVE LED will turn Red on a vital fault or when the module has one latch open
    - The FAULT LED will never flash and not turn Red
    - The FAULT LED will turn Yellow for any fault (non-vital or vital)

Target Solution Vessel Reactivity Protection System and Engineered Safety Features Actuation System (Open Session)

TRACY RADEL, VICE PRESIDENT OF ENGINEERING

Outline

- Target Solution Vessel (TSV) Reactivity Protection System (TRPS)
  - Overview
  - Functions and Monitored Variables
  - Mode transitions, Permissives, and Bypasses
- Engineered Safety Features Actuation System (ESFAS)
  - Overview
  - Functions and Monitored Variables
- Priority Logic
- TRPS/ESFAS Interfaces with the Process Integrated Control System (PICS)

SHINE

Overview of the TRPS

- Designed using the highly integrated protection system (HIPS) platform
- Monitors variables important to safety functions of the irradiation process
- Performs various safety functions as required by SHINE safety analysis
- Consists of eight independent instances of TRPS, each dedicated to one irradiation unit (IU)
- Three divisions of monitoring equipment with two-out-of-three coincident logic vote
- Nine cabinets in total:
  - Three cabinets for IU Cells 1 and 2 (Division A, Division B, and Division C)
  - Three cabinets for IU Cells 3 through 5 (Division A, Division B, and Division C)
  - Three cabinets for IU Cells 6 through 8 (Division A, Division B, and Division C)

SHINE

TRPS Functions

- Safety Functions
  - IU Cell Safety Actuation
  - IU Cell Nitrogen Purge
  - IU Cell Tritium Purification System (TPS) Actuation
  - Driver Dropout
- Nonsafety Function
  - Fill Stop

IU Cell Safety Actuation

- Initiated based on process variables indicating:
  - Insertion of excess reactivity
  - Loss of cooling
  - Overcooling
  - Loss of hydrogen recombination capability
  - Breach of the primary system boundary
- Transitions the unit to Mode 3, shutting down the irradiation process
  - Opens the TSV dump valves and neutron driver assembly system (NDAS) high voltage power supply (HVPS) breakers
- Isolates the primary system boundary and primary confinement boundary

IU Cell Nitrogen Purge

- Initiated based on process variables indicating:
  - Loss of hydrogen recombination capability
- Isolates radioisotope process facility cooling system (RPCS) to limit water intrusion
- Purges the primary system boundary for the affected IU with nitrogen
  - Opens nitrogen purge and vent isolation valves

IU Cell TPS Actuation

- Initiated based on process variables indicating:
  - Breach of the tritium boundary within the IU cell or supply/return lines
  - Breach of the tritium boundary in the TPS glovebox
- Isolates the TPS lines into and out of the IU cell
- Isolates the radiological ventilation zone 1 (RVZ1) exhaust out of the IU cell

SHINE

Driver Dropout

- Initiated based on process variables indicating:
  - Loss of neutron driver output
  - Loss of cooling
- Function 1: Loss of driver output
  - Opens NDAS HVPS breakers to terminate the irradiation process after time delay
- Function 2: Loss of cooling
  - Opens the NDAS HVPS breakers to terminate the irradiation process without delay
  - Initiates IU Cell Safety Actuation after 180 second delay

TRPS Monitored Variables and Response

NEUTRON FLUX

- High source range neutron flux
  - Protects against an insertion of excess reactivity during the filling process
  - IU Cell Safety Actuation initiated when two-out-of-three or more signals active
- Low power range neutron flux
  - Protects against loss of the neutron beam followed by a restart of the neutron beam outside of analyzed conditions
  - Driver Dropout initiated when two-out-of-three or more signals active for predetermined amount of time
- High time-averaged neutron flux
  - Protects against exceeding analyzed TSV power levels during Modes 1 and 2
  - IU Cell Safety Actuation initiated when two-out-of-three or more signals active
- High wide range neutron flux
  - Protects against exceeding target solution power density and temperature limits during Modes 1 and 2
  - IU Cell Safety Actuation initiated when two-out-of-three or more signals active

TRPS Monitored Variables and Response

COOLING SYSTEM

- High primary closed loop cooling system (PCLS) temperature
  - Protects against a loss of cooling that could cause target solution heat-up
  - IU Cell Safety Actuation initiated when two-out-of-three or more signals active for three minutes
- Low PCLS temperature
  - Protects against an overcooling of the target solution that could cause an excess reactivity insertion
  - IU Cell Safety Actuation initiated when two-out-of-three or more signals active
- Low PCLS flow
  - Protects against a loss of cooling that could cause target solution bulk boiling
  - IU Cell Safety Actuation initiated when two-out-of-three or more signals active for three minutes

TRPS Monitored Variables and Response

TSV DUMP TANK

- Low-high TSV dump tank level
  - Protects against in-leakage into the primary system boundary during Mode 1 and 2 that could result in loss of TSV off-gas system (TOGS) flow to the TSV dump tank headspace
  - IU Cell Safety Actuation and IU Cell Nitrogen Purge initiated when two-out-of-three or more signals active
- High-high TSV dump tank level
  - Protects against in-leakage into the primary system boundary that could result in loss of TOGS flow to the TSV dump tank headspace
  - IU Cell Safety Actuation and IU Cell Nitrogen Purge initiated when two-out-of-three or more signals active

TRPS Monitored Variables and Response

TOGS

- Low TOGS oxygen concentration
  - Protects against a deflagration in the primary system boundary caused by the inability to recombine hydrogen with oxygen
  - IU Cell Safety Actuation and IU Cell Nitrogen Purge initiated when two-out-of-three or more signals active
- Low TOGS mainstream flow
  - Protects against a deflagration in the primary system boundary caused by the inability to sweep accumulated hydrogen through the TOGS hydrogen recombiners
  - IU Cell Safety Actuation and IU Cell Nitrogen Purge initiated when two-out-of-three or more signals active
- Low TOGS dump tank flow
  - Protects against a deflagration in the TSV dump tank caused by an inability to remove accumulated hydrogen from tank
  - IU Cell Safety Actuation and IU Cell Nitrogen Purge initiated when two-out-of-three or more signals active
- High TOGS condenser demister outlet temperature
  - Protects against failure of the condenser-demister causing adverse effects on hydrogen recombination, TOGS instrumentation, or the zeolite beds
  - IU Cell Safety Actuation and IU Cell Nitrogen Purge initiated when two-out-of-three or more signals active

TRPS Monitored Variables and Response

ADDITIONAL VARIABLES

- ESFAS loss of external power
  - Anticipatory protection against the impending loss of TOGS blowers and recombiners after the runtime of that equipment on the uninterruptible electrical power supply system (UPSS) has been exceeded
  - IU Cell Nitrogen Purge initiated upon receipt of discrete signal from ESFAS
- High RVZ1e IU cell exhaust radiation
  - Protects against a breach in the primary system boundary, limiting radiological release
  - IU Cell Safety Actuation initiated when two-out-of-three or more signals active
- TSV fill isolation valve position indication not closed
  - Protects against the inadvertent addition of target solution to the TSV
  - IU Cell Safety Actuation initiated when one-out-of-two or more signals active
- ESFAS IU cell TPS actuation
  - Protects against tritium release events in the TPS
  - IU Cell TPS Actuation initiated upon receipt of discrete signal from ESFAS

SHINE

Mode Transition Permissives

- Mode 0 to Mode 1
  - All TSV dump valve position indications and all TSV fill isolation valve position indications indicate valves are fully closed
  - TOGS mainstream flow is above the minimum flow rate
- Mode 1 to Mode 2
  - TSV fill isolation valve position indications indicate both valves are fully closed
- Mode 2 to Mode 3
  - All HVPS breaker position indications indicate the breakers are open
- Mode 3 to Mode 4
  - IU Cell Safety Actuation is not present
- Mode 4 to Mode 0
  - TSV dump tank level is below the low-high TSV dump tank level

Bypasses

- Mode 0:
  - Low power range neutron flux
  - Low PCLS temperature
  - High PCLS temperature
  - Low PCLS flow
  - Low TOGS mainstream flow (Train A) (Train B)
  - Low TOGS dump tank flow
  - High TOGS condenser demister outlet temperature (Train A) (Train B)
  - ESFAS loss of external power
- Mode 1:
  - Low power range neutron flux
  - TSV fill isolation valve position indication not closed
  - Low PCLS flow
  - High PCLS temperature
- Mode 2:
  - High source range neutron flux

Bypasses

- Mode 3:
  - High source range neutron flux
  - Low power range neutron flux
  - High PCLS temperature
  - Low PCLS temperature
  - Low PCLS flow
  - Low-high TSV dump tank level
  - TSV fill isolation valve position indication not closed

- Mode 4
  - High source range neutron flux
  - Low power range neutron flux
  - High PCLS temperature
  - Low PCLS temperature
  - Low PCLS flow
  - Low-high TSV dump tank level
  - TSV fill isolation valve position indication not closed

Overview of the ESFAS

- Designed using the HIPS platform
- Monitors variables important to safety functions in the radioisotope production facility (RPF) and tritium systems
- Performs various design basis safety functions as required by SHINE safety analysis
- Three divisions of monitoring equipment with one-out-of-two or two-out-of-three coincident logic vote depending on operability considerations
- Three cabinets in total:
  - Division A cabinet
  - Division B cabinet
  - Division C cabinet

ESFAS Safety Functions

- Radiologically Controlled Area (RCA) Isolation
- Supercell Isolation
- Carbon Delay Bed Isolation
- Vacuum Transfer System (VTS) Safety Actuation
- TPS Train Isolation
- TPS Process Vent Actuation
- IU Cell Nitrogen Purge
- RPF Nitrogen Purge
- Molybdenum Extraction and Purification System (MEPS) Heating Loop Isolation
- Extraction Column and Iodine and Xenon Purification and Packaging (IXP) Alignment Actuation
- Dissolution Tank Isolation

RCA Isolation

- Initiated based on process variables indicating:
  - Fission product release into RVZ1 or radiological ventilation zone 1 (RVZ2) areas of the facility
  - Breach of the tritium boundary within an IU cell, supply/return lines, or a TPS glovebox
- Closes RVZ dampers and turns off blowers
- Initiates Supercell Area Isolations, VTS Safety Actuation, TPS Train Isolations, and TPS Process Vent Actuation

Supercell Isolation

- Initiated based on process variables indicating:
  - Fission product release into a supercell area confinement
- Closes inlet and outlet dampers for the supercell area that is affected
- Initiates a VTS Safety Actuation if the release occurs in process vessel vent system (PVVS) or extraction areas
- Initiates a MEPS Heating Loop Isolation if the release occurs in an extraction area

Carbon Delay Bed Isolation

- Initiated based on process variables indicating:
  - Fire in a PVVS carbon delay bed 1, 2, or 3
- Isolates and bypasses impacted bed, suppressing fire while maintaining flow through other seven beds

VTS Safety Actuation

- Initiated based on process variables indicating:
  - Break in the process boundary, either in the subgrade or the hot cells, where VTS operation could lead to increased radiological release
- Terminated vacuum lifting operations by opening the breakers and vacuum valves
- Isolates chemical reagent lines that penetrate the confinement boundary

TPS Train Isolation

- Initiated based on process variables indicating:
  - Breach of the tritium boundary within an IU cell, supply/return lines, or a TPS glovebox
- Isolates the TPS glovebox
- Closes the TPS room dampers
- Initiates and IU Cell TPS Actuation, which isolates the TPS lines into and out of the IU cell

TPS Process Vent Actuation

- Initiated based on process variables indicating:
  - High tritium in the process exhaust
- Closes the tritium process exhaust valves from all trains
- Initiates and IU Cell TPS Actuation, which isolates the TPS lines into and out of the IU cell

SHINE

IU Cell Nitrogen Purge

- Initiated based on:
  - Discrete signal from TRPS indicating loss of hydrogen recombination capability in one or more IU cells
  - Indication of loss of external power, following three-minute time delay
- Opens nitrogen purge system (N2PS) IU cell header valves
- N2PS valves to individual IU cells are opened by TRPS

RPF Nitrogen Purge

- Initiated based on process variables indicating:
  - Loss of flow in PVVS
- Opens N2PS RPF header valves
- Opens PVVS carbon guard bed bypass valves

MEPS Heating Loop Isolation

- Initiated based on process variables indicating:
  - Leak of target solution into MEPS heating loop
  - Break in the process boundary, either in the subgrade or the hot cells
- Closes isolation valves for MEPS heating loop
- Opens breakers for MEPS extraction column feed pump

Extraction Column and Iodine and IXP Alignment Actuation

- Initiated based on process variables indicating:
  - Valve alignment that could lead to fissile material in a non-favorable geometry tank
- Aligns valves to safe position
- Criticality safety control

Dissolution Tank Isolation

- Initiated based on process variables indicating:
  - Overflow of target solution preparation system (TSPS) dissolution tanks, potentially leading to fissile material in non-favorable geometry location
- Isolates tank inlets and outlets
- Isolates cooling water supply and return
- Criticality safety control

ESFAS Monitored Variables and Response

EXHAUST RADIATION

- High RVZ1/2 RCA exhaust radiation
  - Protect against confinement leakage or accidents that could potentially result in excess radiation doses to the workers or to the public
  - RCA Isolation initiated when two-out-of-three or more signals active
- High RVZ1 supercell exhaust ventilation radiation (PVVS hot cell)
  - Protects against hot cell equipment leakage or an accident that could potentially result in excess radiation doses to the workers or to the public
  - Supercell Isolation (area 1) and VTS Safety Actuation initiated when two-out-of-three or more signals active
- High RVZ1 supercell exhaust ventilation radiation (MEPS extraction hot cells)
  - Protect against hot cell equipment leakage or an accident that could potentially result in excess radiation doses to the workers or to the public
  - Supercell Isolation (affected area), MEPS Heating Loop Isolation, and VTS Safety Actuation initiated when one-out-of-two or more signals active

ESFAS Monitored Variables and Response

EXHAUST RADIATION

- High RVZ1 supercell exhaust ventilation radiation (IXP hot cell)
  - Protects against hot cell equipment leakage or an accident that could potentially result in excess radiation doses to the workers or to the public
  - Supercell Isolation (area 10) and VTS Safety Actuation initiated when one-out-of-two or more signals active
- High RVZ1 supercell exhaust ventilation radiation (purification and packaging hot cells)
  - Protect against hot cell equipment leakage or an accident that could potentially result in excess radiation doses to the workers or to the public
  - Supercell Isolation (affected area) initiated when one-out-of-two or more signals active

ESFAS Monitored Variables and Response

MEPS AND IXP

- High MEPS heating loop radiation
  - Protect against leakage of high radiation solutions into the heating water loop, which is partially located outside the supercell shielding and could potentially result in an excess dose to the workers
  - MEPS Heating Loop Isolation (affected loop) initiated when one-out-of-two or more signals active
- MEPS area A/B/C three-way valve position indication
  - Protect against a misalignment of the extraction column upper and lower three-way valves, degrading one of the barriers preventing misdirection of chemical reagents or target solution
  - Extraction Column Alignment Actuation (affected area) initiated when two-out-of-two signals active
- IXP three-way valve position indication
  - Protect against a misalignment of the upper and lower three-way valves, degrading one of the barriers preventing misdirection of chemical reagents or target solution
  - IXP Alignment Actuation initiated when two-out-of-two signals active

ESFAS Monitored Variables and Response

PVVS, VTS, AND RDS

- High PVVS carbon delay bed exhaust temperature
  - Protect against a fire in the PVVS delay beds
  - Carbon Delay Bed Isolation (affected bed) initiated when one-out-of-two or more signals active
- Low PVVS flow
  - Protects against loss of hydrogen mitigation capabilities in the RPF
  - RPF Nitrogen Purge initiated when two-out-of-three or more signals active
- VTS vacuum header liquid detection
  - Protects against an overflow of the vacuum lift tanks to prevent a potential criticality event
  - VTS Safety Actuation initiated when one-out-of-two or more signals active
- RDS liquid detection
  - Detects leakage or overflow from other tanks and piping
  - VTS Safety Actuation initiated when one-out-of-two or more signals active

ESFAS Monitored Variables and Response

IU CELL AND TPS

- High TPS IU cell 1/2/3/4/5/6/7/8 target chamber exhaust pressure
  - Protects against a break in the tritium exhaust lines in the IU cell
  - TPS Train Isolation (affected train) and RCA Isolation initiated when one-out-of-two or more signals active
- High TPS IU cell 1/2/3/4/5/6/7/8 target chamber supply pressure
  - Protects against a break in the tritium supply lines in the IU cell
  - TPS Train Isolation (affected train) and RCA Isolation initiated when one-out-of-two or more signals active
- High TPS exhaust to facility stack tritium
  - Protects against a release of tritium from the TPS glovebox pressure control exhaust and VAC/ITS process vent exhaust into the facility ventilation systems
  - TPS Process Vent Actuation initiated when two-out-of-three or more signals active
- High TPS Confinement Tritium
  - Protect against a release of tritium from TPS equipment into the associated TPS glovebox
  - TPS Train Isolation (affected train) and RCA Isolation initiated when one-out-of-two or more signals active

SHINE

ESFAS Monitored Variables and Response

ADDITIONAL VARIABLES

- TRPS IU cell 1/2/3/4/5/6/7/8 nitrogen purge
  - Protects against a loss of hydrogen mitigation capabilities in the IUs
  - IU Cell Nitrogen Purge initiated upon receipt of discrete signal from TRPS
- TSPS dissolution tank 1/2 level
  - Protect against a criticality event due to excess fissile material in a non-favorable geometry system
  - Dissolution Tank Isolation initiated when one-out-of-two or more signals active
- UPSS loss of external power
  - Protects against an anticipatory loss of hydrogen mitigation in the IU cell (i.e., loss of TOGS blowers and recombiners after the UPSS runtime of that equipment has been exceeded)
  - IU Cell Nitrogen Purge initiated when one-out-of-two or more signals active for predetermined amount of time

SHINE

Priority Logic

- The actuation priority logic (APL) is designed to provide priority of safety-related signals over nonsafety-related signals
- Division A and Division B TRPS/ESFAS priority logic prioritizes inputs as follows:
  1) Automatic Safety Actuation, Manual Safety Actuation, and
  2) PICS nonsafety control signals
- When the enable nonsafety control is not active, the nonsafety-related control signals are ignored
- If the enable nonsafety control is active, and no automatic safety actuation or manual safety actuation command is present, the nonsafety control signal can control the component

Communication between TRPS/ESFAS and PICS

INFORMATION COMMUNICATED

- Each division of TRPS and ESFAS transmits monitoring, indication, and diagnostic information to the PICS for display to operators
- PICS provides mode transition signals to TRPS, when manually initiated by the operator
- PICS provides valve and damper position indication to TRPS/ESFAS for verification of completion of protective function
- PICS provides signals to TRPS/ESFAS to reposition components, when manually initiated by the operator and enable nonsafety switch is in the “enable” position

Communication between TRPS/ESFAS and PICS

METHODS OF COMMUNICATION

- Communication from the TRPS/ESFAS to the PICS is via serial connection (via MODBUS RTU protocol)
- Communication from the PICS to the TRPS/ESFAS is via a series of discrete contacts which communicate a series of addresses that are correlated to inputs and nonsafety control signals
- All interfacing between the TRPS/ESFAS and the PICS is by the gateway communication module (GWCM)

Advisory Committee on Reactor Safeguards

SHINE Medical Technologies Operating License Application

Chapter 7 – Instrumentation and Controls

July 19, 2022 – Non-Proprietary

Office of Nuclear Reactor Regulation

I&C Technical Review Team

- **Dinesh Taneja –** Senior Electronics Engineer (HIPS, ESFAS, RMS)
- **Norbert Carte –** Senior Electronics Engineer (TRPS, NFDS, PICS)
- **Duane Hardesty** - Sr. Project Manager

  (Technical Specifications)
- **Rossnyev Alvarado** – Electronics Engineer

Guidance and Acceptance Criteria

- NUREG-1537, Part 1, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Format and Content,” issued February 1996;
- NUREG-1537, Part 2, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, Standard Review Plan and Acceptance Criteria,” issued February 1996;
- Final Interim Staff Guidance (ISG) Augmenting NUREG-1537, Part 1 and Part 2, for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors

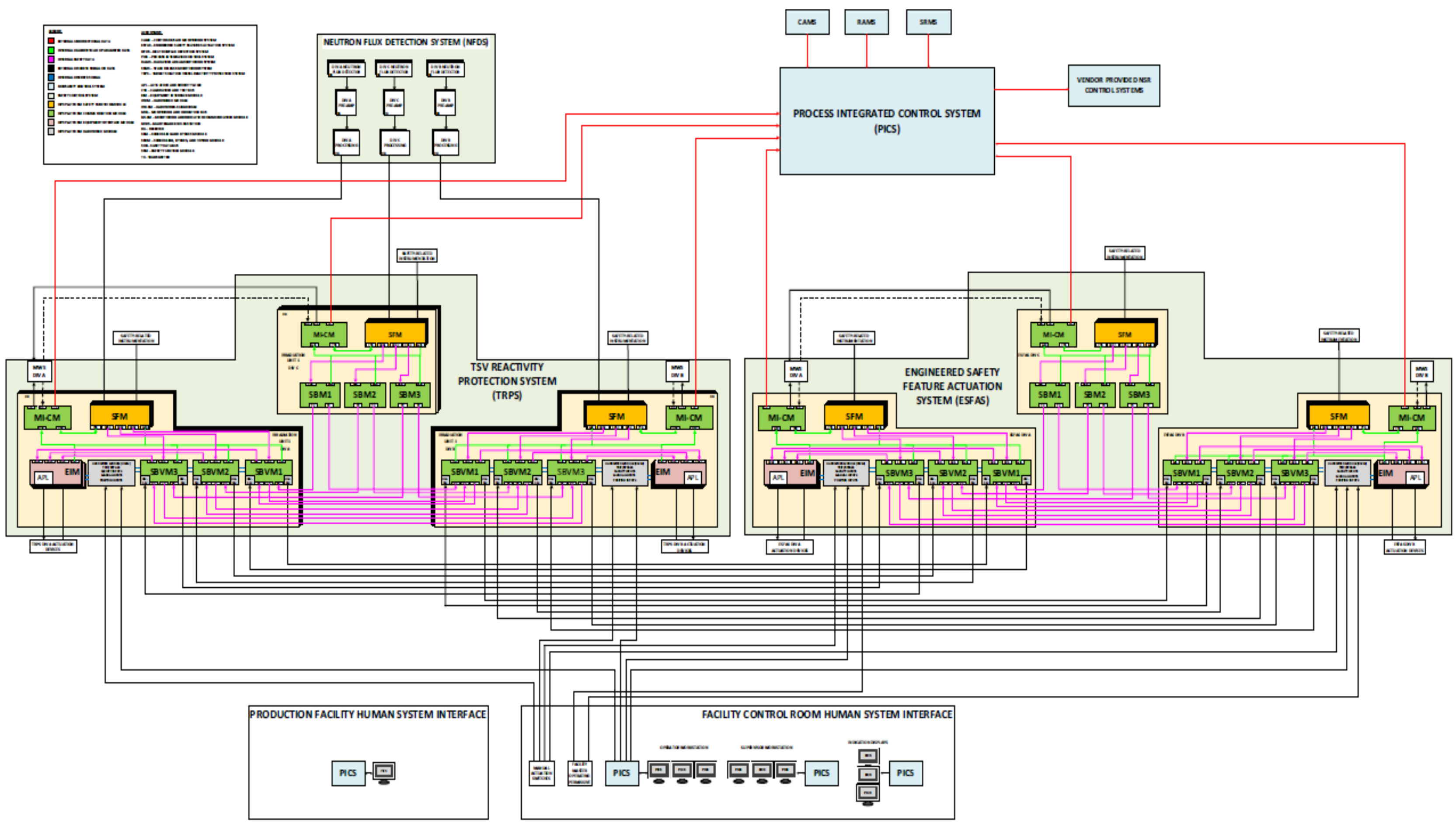
SAFETY EVALUATION OVERVIEW

Chapter 7 Safety Evaluation

- Current Scope
  - I&C Design Criteria
  - Highly integrated Protection System (HIPS)
  - Target solution vessel reactivity protection system (TRPS)
    - neutron flux detection system (NFDS)
  - Engineered safety features actuation system (ESFAS)
    - radiation area monitoring system (RMS)
- Under NRC Review
  - Lifecycle Development (HIPS, TRPS, & ESFAS)
  - Technical Specifications
  - PICS

I&C Systems

Figure 7.1-1 – Instrumentation and Control System Architecture



Applicable SHINE Facility Design Criteria

- Staff evaluated the I&C design against relevant SHINE Design Criteria
  - TRPS: Criteria 1-6, 13-19, 38, 39
  - NFDS: Criteria 13-19
  - ESFAS: Criteria 1-6, 13-19, 37-39
  - RMS: Criteria 13, 38

HIPS REVIEW

HIPS Design

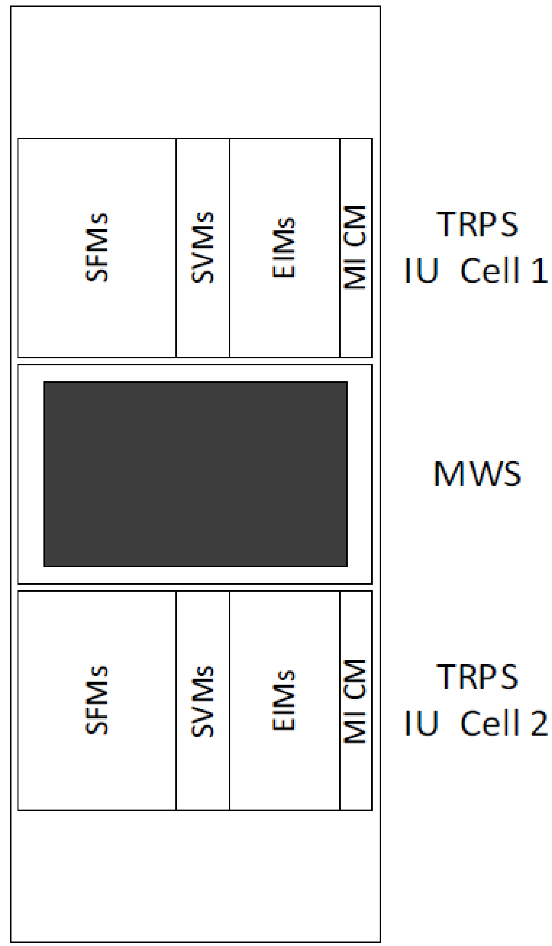
- HIPS platform is used for SHINE TRPS and ESFAS
- SHINE incorporates by reference HIPS Topical Report (TR)
- SHINE technical report TECRPT-2018-0028 dispositions the HIPS TR ASAIs and explains the TRPS & ESFAS architecture differences from TR
- Consistent with HIPS TR, TRPS & ESFAS design incorporates the fundamental design principles of independence, redundancy, predictability & repeatability, and diversity & defense-in-depth

HIPS Design

- Key modifications & additions to HIPS platform for SHINE TRPS & ESFAS applications:
  – Remote input submodule (RISM)
  – Implementation of communication modules (CM)
    - Scheduling, bypass, and voting modules (SBVM)
    - Gateway Communications modules (GWCM)
  – Hardwired module (HWM) input routing
  – Implementation of equipment interface module (EIM) outputs
  – HIPS platform Self-testing features

HIPS Design

Figure 7.6-3 – Maintenance Workstation



HIPS Design

- HIPS platform equipment qualification (EQ)
  - Mild environmental qualification performed per IEEE Std. 623-2003
    - 140°F for continuous operations
    - 158°F for limited operations
  - Seismic qualification per IEEE Std. 344-2013
  - EMI/RFI qualification per RG 1.180
    - HIPS equipment grounding per IEEE Std. 1050-2004

HIPS Operations

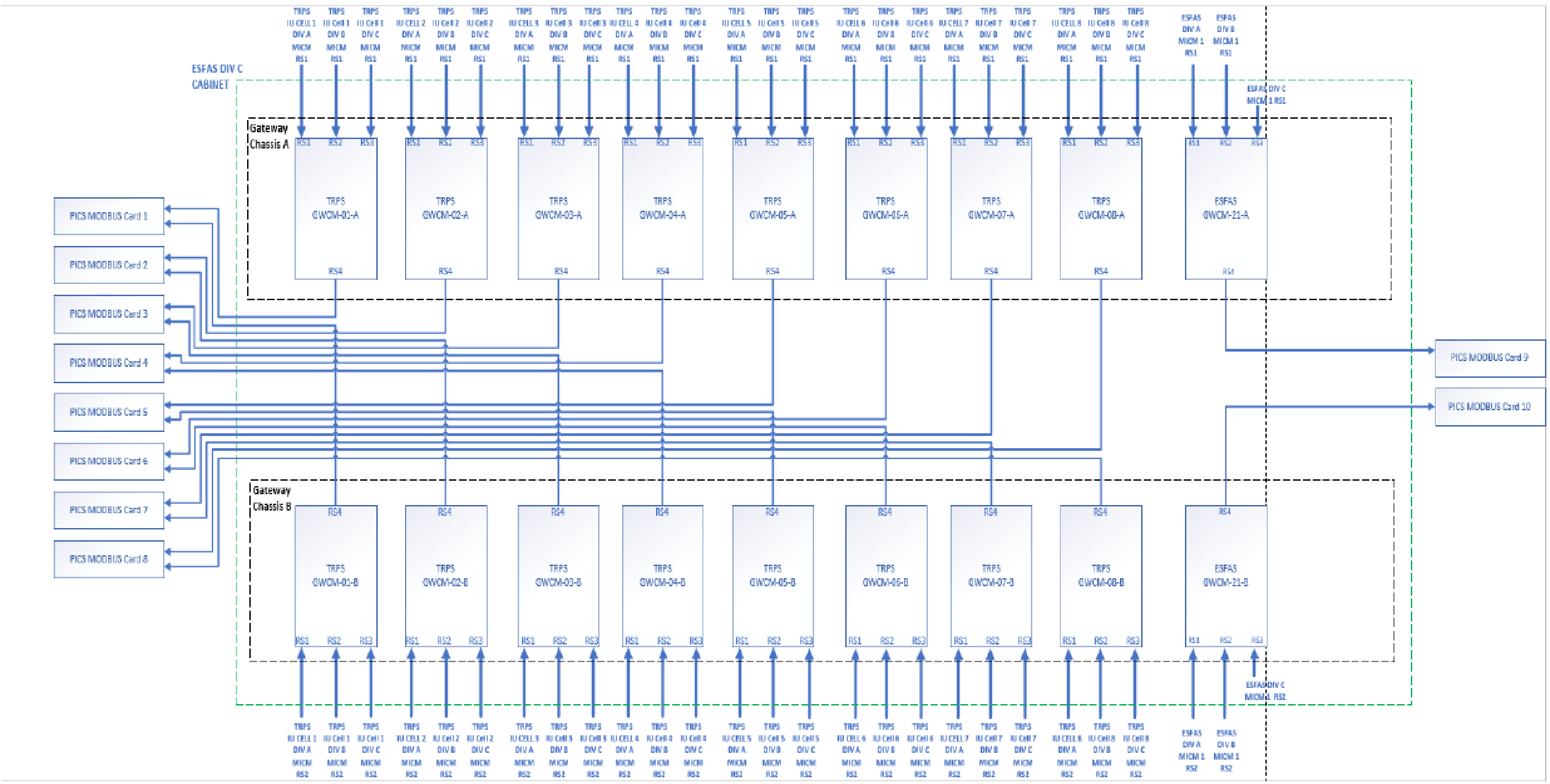
- TRPS and ESFAS architecture is consistent with HIPS TR
  - Three separate and independent divisions consisting primarily SFMs, SBMs, SBVMs, and EIMs
  - Each division based on different FPGA technology
  - Each division uses TMR architecture
    - Three Safety Data Buses (SDB1-SDB3)
    - Three SBVM or SBM
    - Each EIM receives three voted inputs
  - One-way interdivision communications
  - One-way data communication to PICS via M&I CM

HIPS Operations

- TRPS and ESFAS architecture incorporates following fundamental design principals:
  - Independence
  - Redundancy
  - Predictability and Repeatability
  - Diversity
- Additional TRPS and ESFAS design attributes:
  - Access control
  - Prioritization of functions
  - Completion of protective functions

Gateway Communications Architecture

Figure 7-15-1: TRPS and ESFAS Gateway Communications Architecture



HIPS Operations

- Diagnostics and self-testing
- Operational and maintenance bypass
- Manual Actuations
- Response Times/ Analytical Limits / Setpoints

Staff Evaluation of SHINE's HIPS Equipment

The NRC staff has reasonable assurance that the HIPS digital I&C platform used to implement TRPS and ESFAS is designed to be consistent with the approved HIPS TR and incorporates the fundamental design principals of independence, redundancy, predictably and repeatability, and diversity.

The NRC staff also finds that the HIPS design meets the applicable portions of the SHINE Design Criteria 15, 16, and 19. Therefore, the NRC staff concludes that the HIPS platform used to implement TRPS and ESFAS is capable of performing the allocated design basis safety function under postulated conditions.

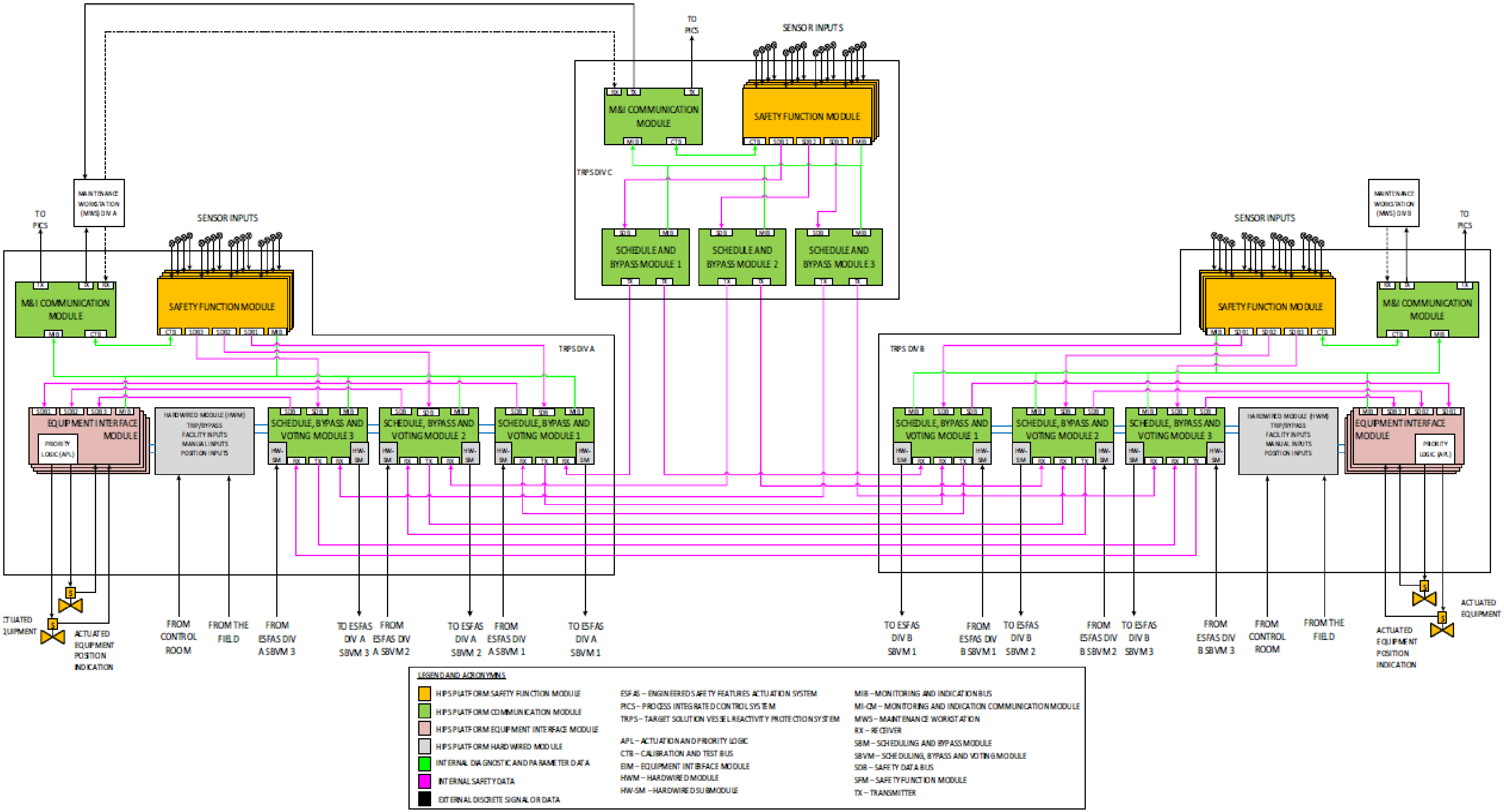
TRPS REVIEW

TRPS / NFDS Design

- Design Criteria – Performance Objectives
  - Provide criterion for achieving reasonable assurance of adequate safety
  - Some are more safety significant than others
- Design Bases – Functions and Values
  - Events Described in other FSAR Chapters
  - Analysis Demonstrates the DB achieves the DC
  - Variables Monitored & Functions Actuated
  - **Setpoints** and Response Times (Analytic Values)

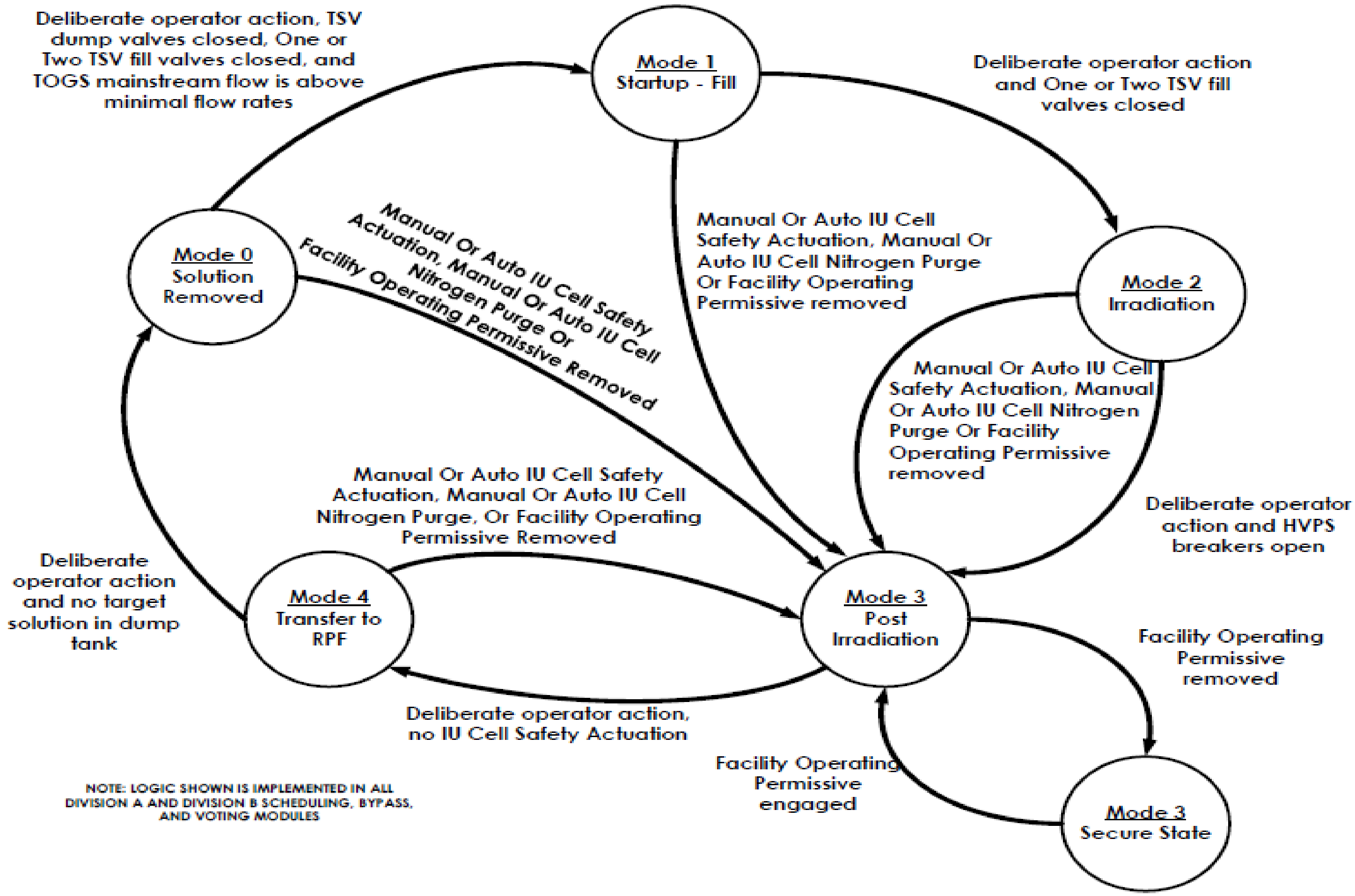
TRPS Design

Figure 7.1-2 – Target Solution Vessel Reactivity Protection System Architecture



TRPS Design

Figure 7.4-1 TRPS Logic Diagrams
(Sheet 8 of 14)



TRPS – SHINE Design Criteria

- Protect Solution Design Limits – for AOOs
- Functions Support other FSAR Chapters
- Single Failure Criteria
  - redundancy & independence
  - supports maintenance and testing
- Control of Access (HIPS Equipment Features)
- Independence from PICS

TRPS – Design Bases

- Safety Functions – FSAR 7.4.3.1 / 7.8.3.1
  - IU Cell Safety Actuation
  - IU Cell Nitrogen Purge
  - IU Cell Tritium Purification System (TPS) Actuation
  - Driver Dropout
- Analytic Values – See FSAR Table 7.4-1
  - Range, Accuracy, **Analytic Limits**, & Response Times

TRPS – Design Bases

- Safety Functions – FSAR 7.4.3.1
  - FSAR 7.4.3.1.x References Specific Ch 13 Scenarios
  - Variables Monitored: FSAR 7.4.4.1.x
    - References Specific Ch 13 Scenarios
  - Equipment Actuated: FSAR 7.4.3.1.x
- Analytic Values – See Table 7.4-1
  - Range, Accuracy, **Setpoints**, & Response Times
- Operation & Design Criteria

Staff Evaluation of SHINE's TRPS & NFDS

The NRC staff has reasonable assurance that the SHINE TRPS is designed to 1) mitigate the consequences of design basis events within the main production facility, 2) provides sense, command, and execute functions necessary to maintain the facility confinement strategy, 3) provides process actuation functions required to shut down processes and maintain processes in a safe condition, and provides system status and measured process variable values to the facility process integrated control system (PICS) for viewing, recording, and trending.

The NRC staff has reasonable assurance that the NFDS is adequately described in SHINE FSAR Section 7.8. The NFDS is adequately designed for measurement of the neutron flux signal, signal processing, indication, and interfacing with other systems, including providing analog input to the TRPS.

The NRC staff also finds that the TRPS design meets SHINE design criteria 1 through 6, 13 through 19, and 37 through 38. The staff review of the lifecycle development process for HIPS is described in Section 7.4.2 of this SER and the adequacy of HIPS and TRPS-related TS is evaluated in Section 7.4.10 of this SER. Therefore, the NRC staff concludes that the TRPS is capable of performing the allocated design basis safety function under postulated conditions.

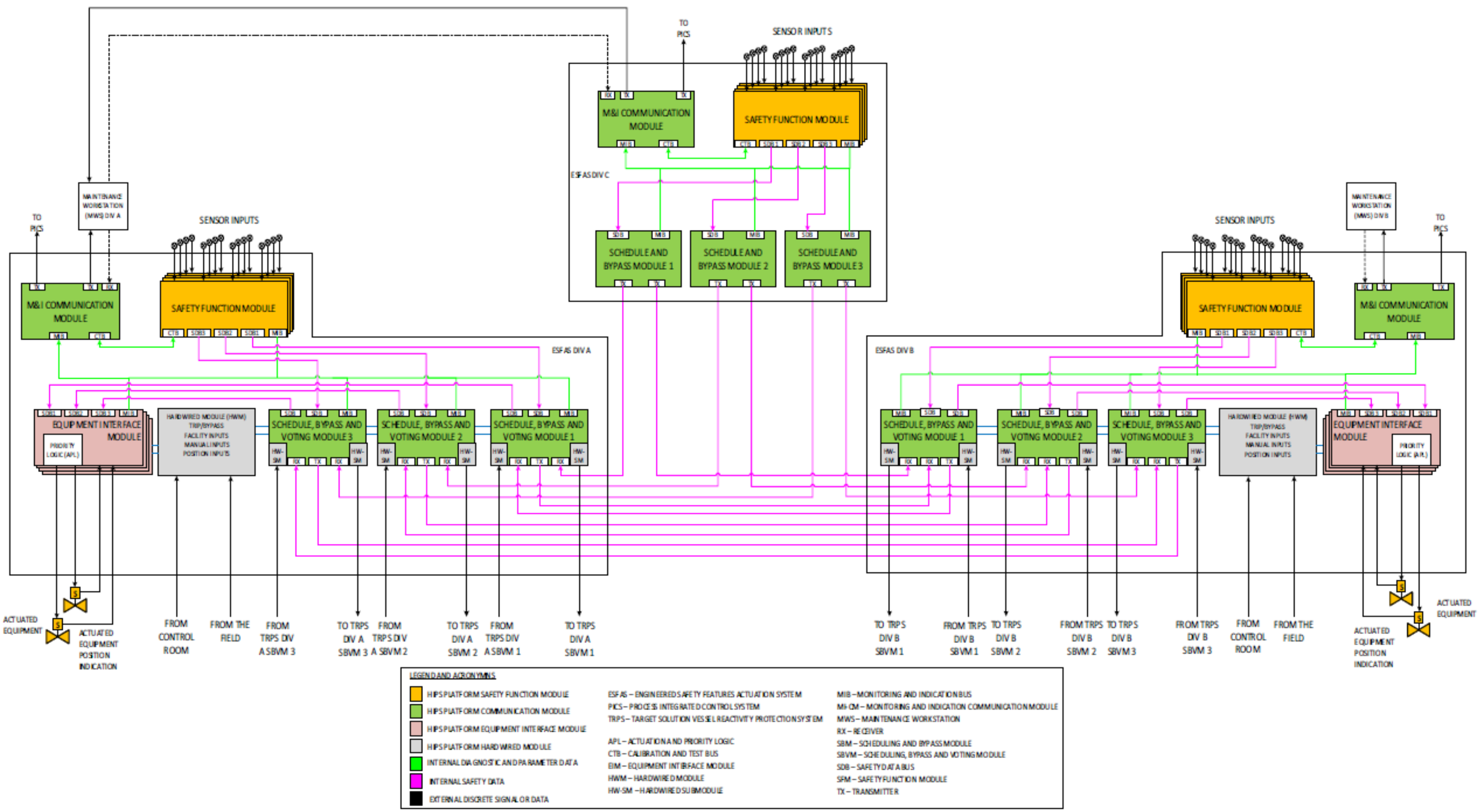
ESFAS REVIEW

ESFAS / RMS Design

- ESFAS monitors process variables for confinement of fission products and tritium, and for criticality safety
- Safety-related process radiation monitors (part of RMS) provide analog signals to the ESFAS and TRPS used to generate actuation signals
- ESFAS also provides system status and process variable values to the PICS for viewing, recording, and trending

ESFAS Architecture

Figure 7.1-3 – Engineered Safety Feature Actuation System Architecture



ESFAS / RMS Design

- SHINE Design Criteria 1 through 6, 13 through 19, and 37 through 39 apply to the ESFAS
- SHINE Design Criteria 1, 2, 4, 13 and 38 apply to safety-related process radiation monitors
- **Key ESFAS Design Features**:
  - Sharing of Structures, Systems, and Components
    - **ESFAS does not share components between irradiation units** and meets SHINE Design Criterion 5
  - Instrumentation and Controls
    - Process variables listed in FSAR Table 7.5-1 are used for display and to initiate defined actuation of the applicable engineered safety features. **ESFAS has operable protection capability in all operating modes, anticipated transients, and postulated accidents** and meets SHINE Design Criterion 13

ESFAS / RMS Design

- Protective System Functions
  - **ESFAS is designed to perform the safety functions for transients and accidents credited in FSAR Chapter 13 to maintain the facility confinement strategy, provide process shut down functions and maintain processes in a safe condition**, and meets the SHINE Design Criterion 14
- Protection System Failure Modes
  - **ESFAS is designed to fail into a safe state and perform its protective actions upon loss of power, loss of an ESFAS component, or adverse environmental conditions**, and meets the SHINE Design Criterion 17
- Separation of Protection and Control Systems
  - **ESFAS is adequately separated from the PICS such that failure of any single PICS component leaves intact a system satisfying all reliability, redundancy, and independence requirements of the ESFAS,** and meets SHINE Design Criterion 18

ESFAS / RMS Design

- Protection Against Anticipated Transients
  - **ESFAS is designed to ensure an extremely high probability of accomplishing its safety functions in the event of anticipated transients,** and meets the SHINE Design Criterion 19
- Criticality Control in the Radioisotope Production Facility
  - **To satisfy the double contingency principle (DCP) required by the SHINE criticality safety program, ESFAS is designed to provide two active engineered criticality safety controls, namely; vacuum transfer system (VTS) actuation and TSPS dissolution tank isolation,** and meets the SHINE Design Criterion 37
- Monitoring Radioactivity Releases
  - **ESFAS is designed to monitor primary confinement boundary, hot cell, and glovebox atmospheres to detect potential leakage of gaseous or other airborne radioactive material that may be released from normal operations, including anticipated transients and from postulated accidents,** and meets the SHINE Design Criterion 38

ESFAS / RMS Design

- Hydrogen Mitigation
  - **ESFAS is designed to initiate nitrogen purge to control the buildup of hydrogen that is released into the primary system boundary and tanks or other volumes that contain fission products and produce significant quantities of hydrogen to ensure that the integrity of the system and confinement boundaries is maintained,** and meets the SHINE Design Criterion 39
- Single Failure
  - ESFAS is designed to actuate only Division A component for select safety functions where a passive check valve is credited as a redundant component. **In each instance, sufficient redundancy is provided such that no single failure results in the loss of the protective function.**

Staff Evaluation of SHINE's ESFAS & RMS

- SHINE ESFAS & RMS are designed to:
  - 1) Mitigate the consequences of design basis events within the main production facility
  - 2) Provides sense, command, and execute functions necessary to maintain the facility confinement strategy
  - 3) provides process actuation functions required to shut down processes and maintain processes in a safe condition and provides system status and measured process variable values to PICS for viewing, recording, and trending.
- ESFAS design meets SHINE design criteria 1 through 6, 13 through 19, and 37 through 39
- Safety-related process radiation monitors meets SHINE Design Criteria 1, 2, 4, 13, and 38
- ESFAS & RMS are capable of performing the allocated design basis safety function under postulated conditions

Questions

Acronyms

APL	actuation and priority logic (see HIPS TR)
ASAI	application specific action item (see HIPS TR)
BF3	boron trifluoride
BIST	built-in self-test (see HIPS TR)
CAAS	criticality accident alarm system
CAMS	continuous air monitoring system
CCF	common cause failure
CDA	critical digital asset
CM	communication modules (a HIPS module)
COTS	commercial off-the-shelf
CTB	calibration and test bus (see HIPS TR)
EIM	equipment interface module (a HIPS module)
EMI	electromagnetic interference

Acronyms

ESFAS	engineered safety features actuation system
FAT	factory acceptance test
FCR	facility control room
FDCS	facility data and communications system
FPGA	field programmable gate array (see HIPS TR)
HIPS	highly integrated protection system (see HIPS TR)
HVPS	high voltage power supply
HW-SM	hardwired submodule (a HIPS module)
HWM	hardwired module (a HIPS module)
I&C	instrumentation and control
IEEE	Institute of Electrical and Electronic Engineers
IF	irradiation facility

Acronyms

ISG	interim staff guidance
ISM	input submodule (a HIPS module)
IU	irradiation unit
MI-CM	monitoring and indication communication module (see HIPS TR)
MIB	monitoring and indication bus (see HIPS TR)
MWS	maintenance workstation (see HIPS TR)
NDAS	neutron driver assembly system
NFDS	neutron flux detection system
NPSS	normal electrical power supply system
NVM	nonvolatile memory (see HIPS TR)
OOS	out of service(see HIPS TR)
PDC	Principal Design Criteria
PICS	process integrated control system

Acronyms

PLDS	programmable logic design specification
PLRS	programmable logic requirements specification
QA	quality assurance
RAMS	radiation area monitoring system
RCA	radiologically controlled area
RDS	radioactive drain system
RFI	radio-frequency interference
RISM	remote input submodule (a HIPS module)
RVZ1	radiological ventilation zone 1
RVZ1e	radiological ventilation zone 1 exhaust subsystem
RVZ1r	radiological ventilation zone 1 recirculating subsystem
RX	receiver (Figure 7.1-x)
SASS	subcritical assembly support structure
SBM	scheduling and bypass modules (a HIPS module)

Acronyms

SBVM	scheduling, bypass, and voting modules (a HIPS module)
SCAS	subcritical assembly system
SDB1	safety data bus 1 (see HIPS TR)
SDB2	safety data bus 2 (see HIPS TR)
SDB3	safety data bus 3 (see HIPS TR)
SDE	secure development environment (see HIPS TR)
SFM	safety function module (a HIPS module)
SOV	solenoid operated valve
SR	safety-related
SRM	stack release monitor
SRMS	stack release monitoring system
SVM	scheduling and voting module (a HIPS module)
SyRS	system requirements specification

Acronyms

TMR	triple modular redundant
TOGS	TSV off-gas system
TPS	tritium purification system
TR	topical report
TRPS	target solution vessel reactivity protection system
TSPS	target solution preparation system
TSSS	target solution storage system
TSV	target solution vessel
TX	transmitter (Figure 7.1-x)
UPSS	uninterruptible electrical power supply system
V&V	verification & validation
VTS	vacuum transfer system

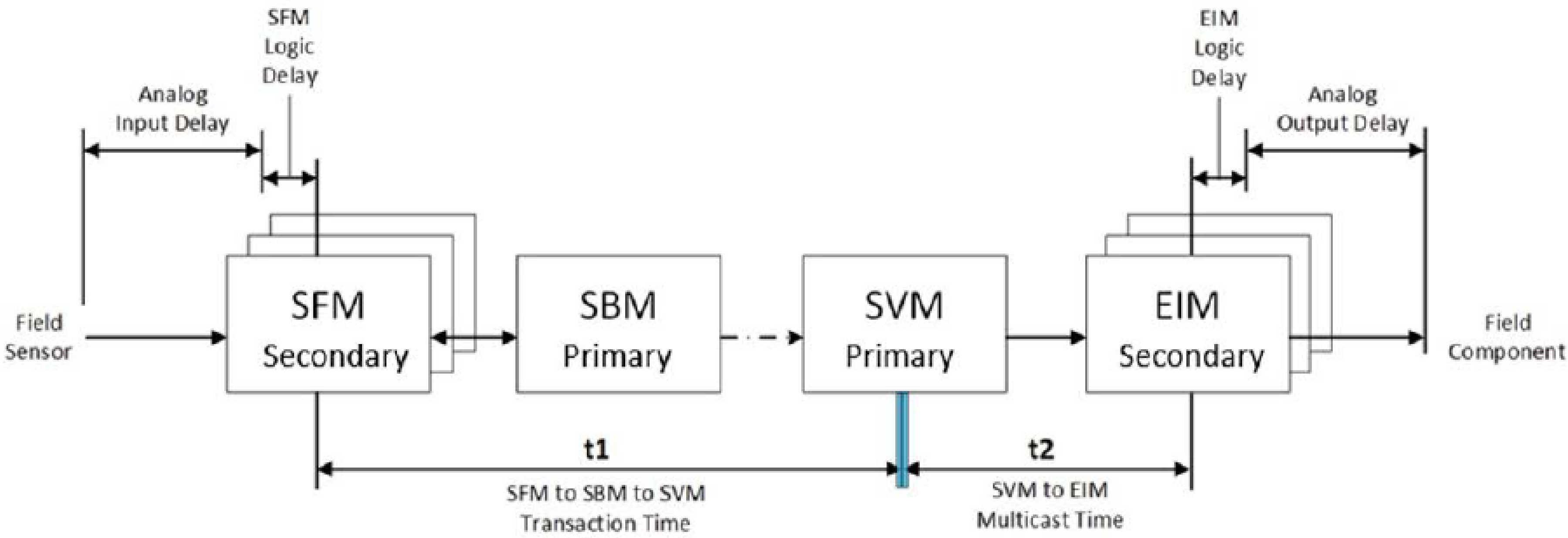
BACKGROUND

Setpoints

- Setpoints established to protect Analytical Limits
  - Derived from Analytic Limits in Safety Analysis (Tables 7.4-1 & 7.5-1)
  - Incorporates margin and assumed uncertainties in sensors & instrumentation
  - Setpoint Methodology Described in FSAR (under audit)
- Provided in Technical Specifications & LSSSs/LCOs
  - Most limiting Values in TS LCOs (under review)

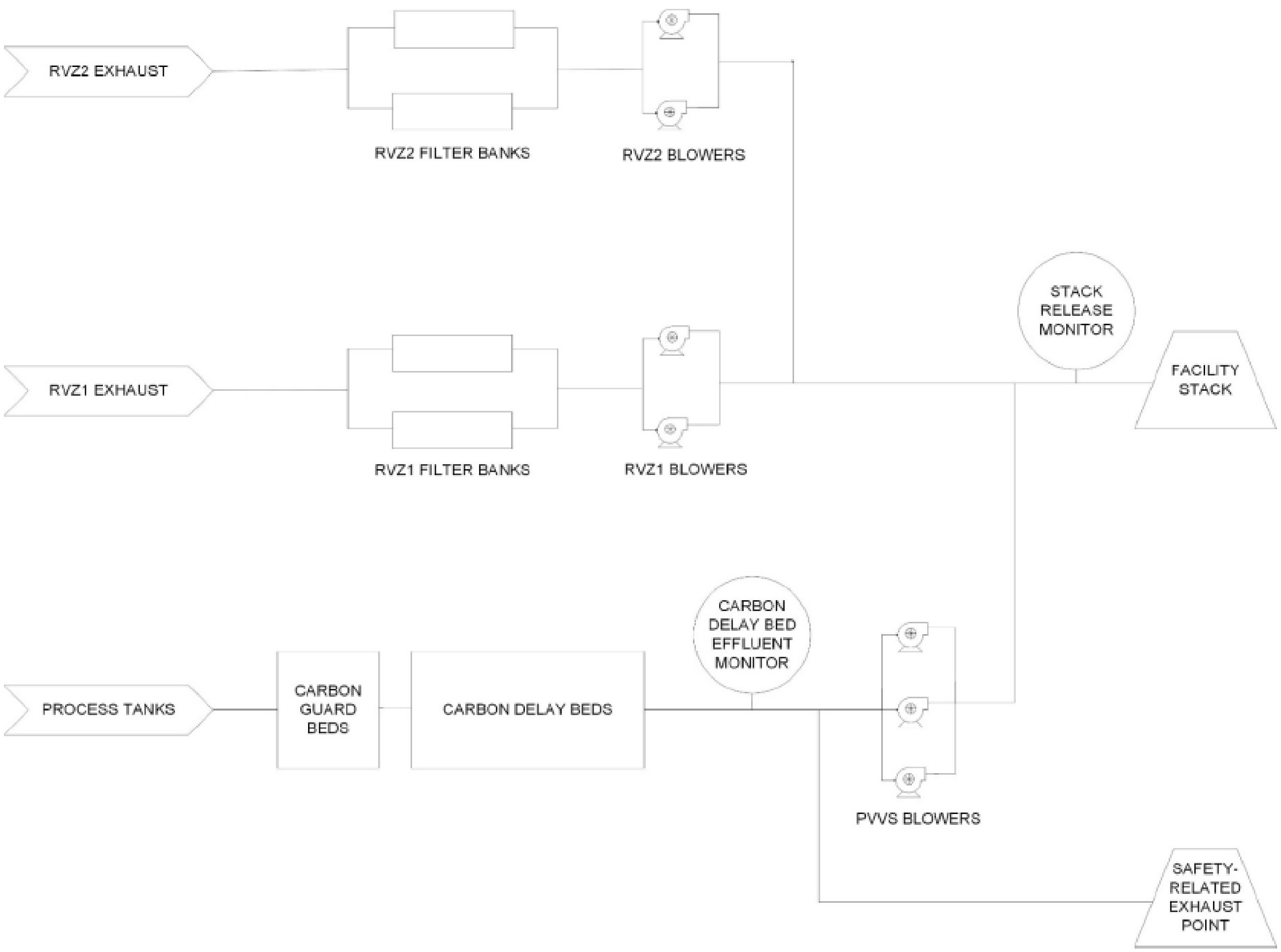
Background Information

Figure 7.4-2 – HIPS Platform Timing



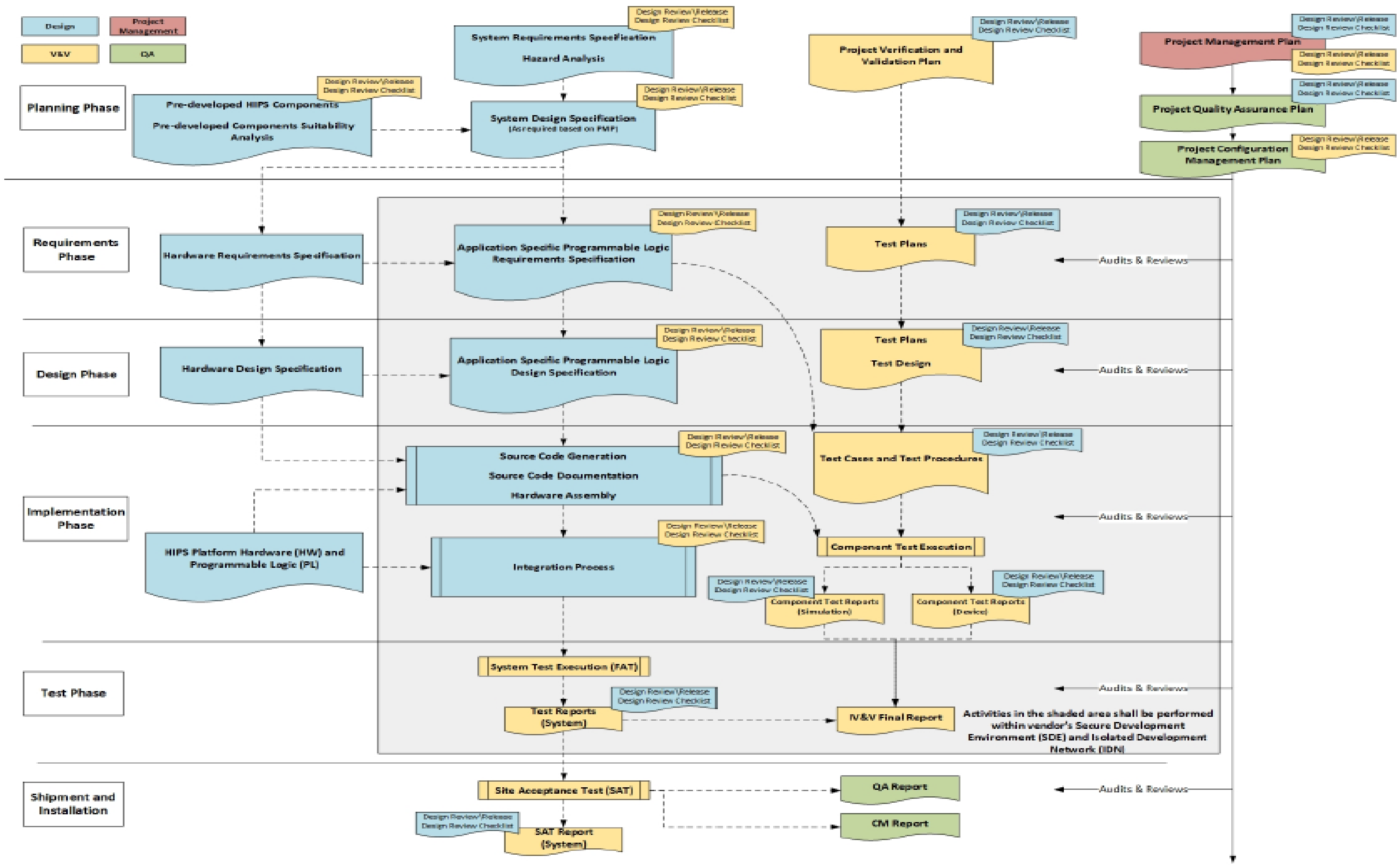
Background Information

Figure 7.7-1 – Effluent Monitor Locations



Lifecycle Process (under review)

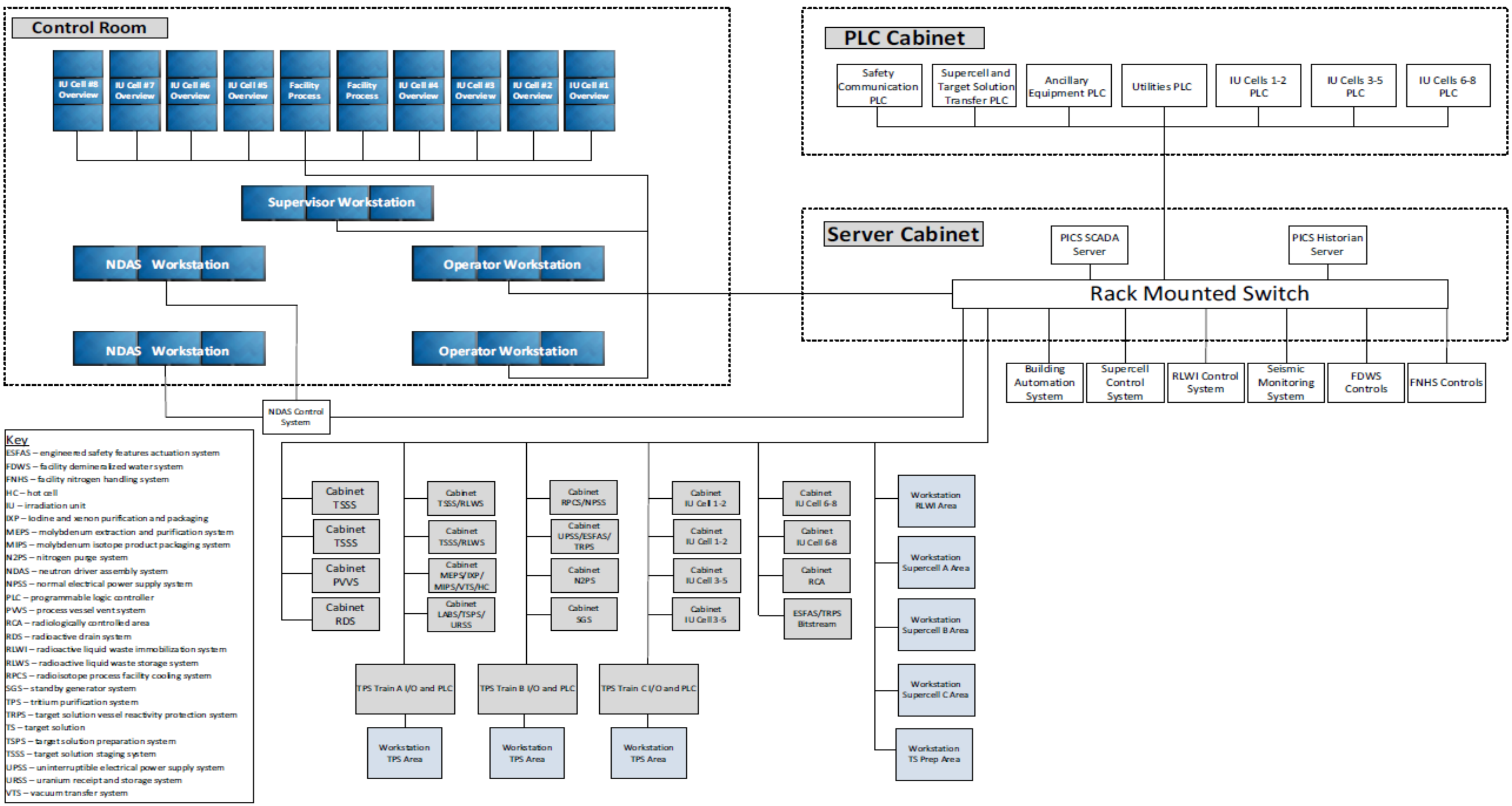
Figure 7.4-3 – TRPS and ESFAS Programmable Logic Lifecycle Process



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

PICS (Under Review)

Figure 7.3-1 – Process Integrated Control System Architecture



SHINE Medical Technologies 7.3-38 Rev. 5

Background Information - Main Control Board

Figure 7.6-2 – Main Control Board Sections