Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Advisory Committee on Reactor Safeguards
Docket Number:	(n/a)
Location:	Rockville, Maryland
Date:	Thursday, September 7, 2017

Work Order No.: NRC-3254 Pages 1-105

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

646TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

THURSDAY

SEPTEMBER 7, 2017

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., Dennis C. Bley, Chairman, presiding.

COMMITTEE MEMBERS:

DENNIS C. BLEY, Chairman

PETER RICCARDELLA, Member-at-Large

RONALD G. BALLINGER, Member

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR., Member

MARGARET CHU, Member

WALTER L. KIRCHNER, Member

JOSE MARCH-LEUBA, Member
DANA A. POWERS, Member
HAROLD B. RAY, Member
JOY REMPE, Member
GORDON R. SKILLMAN, Member
JOHN W. STETKAR, Member
MATTHEW W. SUNSERI, Member

DESIGNATED FEDERAL OFFICIAL:
CHRISTINA ANTONESCU
CHRISTOPHER BROWN

ALSO PRESENT:
TONY AHN, KHNP
JOSEPH ASHCRAFT, NRO
LUIS BETANCOURT, NRO
KEVIN COYNE, NRO
ISMAEL GARCIA, NRO
IAN JUNG, NRO
DAWNMATHEWS KALATHIVEETTIL, NRO
LAUREN KENT, NRO
HANGRAE KIM, KHNP
JINKU KIM, KHNP
TANGHO KIM, KHNP
YOUNGKI KIM, KHNP

DAEHEON LIM, KHNP
MIKE MCCOPPIN, NRO
WENDELL MORTON, NRO
KENNETH MOTT, NRO
EUGSE OH, KHNP
JIYONG OH, KHNP
JAE HYUK PARK, KHNP
CAYETANO SANTOS, NRO
KEN SCAROLA, Nuclear Automation Engineering
ROB SISK, Westinghouse
ROBERT SWEENEY, KHNP
DINESH TANEJA, NRO
ANDREA D. VEIL, Executive Director, ACRS
DAVE WAGNER, AECOM
WILLIAM WARD, NRO
DEANNA ZHANG, NRO
JACK ZHAO, NRO

*Present via telephone

A-G-E-N-D-A

P R O C E E D I N G S

8:30 a.m.

CHAIRMAN BLEY: The meeting will now come to order. This is the first day of the 646th meeting of the Advisory Committee on Reactor Safeguards.

During today's meeting the committee will consider the following. Advanced Power Reactor 1400, preparation for ACRS meetings with the Commission and preparation of ACRS reports.

The ACRS was established by statute and is governed by the Federal Advisory Committee Act.

As such this meeting is being conducted in accordance with the provisions of FACA. That means that the committee can only speak through its published letter reports.

We hold meetings to gather information and support our deliberations.

Interested parties who wish to provide comments can contact our offices requesting time after the Federal Register notice describing the meeting is published.

That said we also set aside 10 minutes for spur of the moment comments from members of the public attending or listening to our meetings. Written comments are also welcome.

Ms. Christina Antonescu is the designated federal officer for the initial portion of this meeting.

Portions of the session on the APR1400 may be closed in order to discuss and protect information designated as proprietary.

The ACRS section of the U.S. NRC public website provides our charter, bylaws, letter reports and transcripts of all full and subcommittee meetings including the slides presented at the meetings.

We have received no written comments or requests to make oral statements from members of the public regarding today's sessions.

There is a telephone bridge line to preclude interruption of the meeting. The phone will be placed in listen-in mode during presentations and committee discussions.

There's also a webcast that's being done through a different mechanism because of technical problems so it should be working.

And usually the audio is better on the webcast than on the listen-in phone line.

A transcript of portions of the meeting is being kept and it is requested that speakers use one of the microphones, identify themselves, and speak with sufficient clarity and volume so as they can be readily heard.

I will begin with an item of current interest to us. It's my pleasure to announce that Alesha Bellinger, chief program management development and analysis branch, has been awarded the Meritorious Award for 2017.

This is a very prestigious award which covers her 20-year federal career. The Meritorious Civilian Service Award is the second highest award provided to civilian employees within agencies of the federal government.

I don't think Alesha is here this morning. She can't be here, but we offer her our congratulations.

The ceremony will be today but it's during our meetings and it's closed to the staff due to space. It will be televised around the campus. Even though she's not here let's congratulate her.

(Applause)

CHAIRMAN BLEY: At this time I will turn the meeting over to Professor Ballinger to conduct today's session.

MEMBER BALLINGER: Thank you, Mr. Chairman.

Today we will achieve a milestone in the APR1400 review. This will be the last of phase 2 SER with open items.

We'll be reviewing chapter 7 and 18. Chapter 7 is instrumentation and control. Chapter 18 is human factors.

And Bill, would you like to say anything?

MR. WARD: Yes, thank you. Just wanted to say we're happy to reach this milestone and completion of the first round of ACRS subcommittee and full committee meetings.

We have presentations to make which we think are going to provide enough information. We know that the heart of the meeting today is going to be the questions you have and we look forward to those. Thank you.

MEMBER BALLINGER: Thank you.

CHAIRMAN BLEY: For the record Bill is William Ward, NRC staff.

MEMBER BALLINGER: I stand corrected. So I guess the floor is yours.

MR. SISK: I'll take just a minute to again thank the committee. We look forward to having this completion of phase 3 and the ACRS review of chapter 7 and 18.

Just for clarity for this morning we're going to be covering chapter 7 and 18, and then turning over to NRC. Are we going to do 7 and then 18? Or 7 and 18 together, Bill?

MR. WARD: Yes, I think that's how it's on the schedule.

MEMBER BALLINGER: That would be William.

MR. WARD: So without further delay on my part let me introduce Mr. Eugse Oh to lead us through chapter 7.

MR. E. OH: Good morning, gentlemen. My name is Eugse Oh from KHNP and I am chapter 7 and chapter 18. So from now I will start my presentation of chapter 7 first.

Here is the contents of this presentation. Okay, next slide.

Chapter 7 consists of eight sections and each section describes the system description and the design basis and analysis.

I will continue each section for next slide.

This slide shows technical reports which we submitted for this application.

Section 7.1 is introductory section and it describes the design features.

And APR1400 I&C system used fully digitalized with proven technology. And I&C system consists of three major diverse platforms.

One is programmable logic controller which is for safety system. And the other one is distributed control system for non-safety control system.

And FPGA-based logic controllers which is for diverse actuation system.

And we use data computation system widely between safety system and non-safety system for between each division of safety systems.

And we also analyzed the common cause failures for safety systems and non-safety control system whether it impacts safety systems or not.

So, our design will comply with 10 CFR 50 and the reg guidance and IEEE standard, and INTRP step guidance.

This picture shows some overview of APR1400 I&C system architectures.

The pink color box is a safety system platform which is platforms here.

And this blue box use non-safety control system which use distributed control systems.

And the left side of the brown color box which is diverse actuation system that use FPGA-based platforms.

And these yellow boxes are for human system interface devices.

And here are the external linkers for plant data network to external of the other linkers. For example, UFY NIC connections.

Okay, this table shows system computation of the I&C system.

For human system interface we used minimum event research and ESF subcontrol module for safety systems.

And for non-safety human system interface we used information flat panel displays.

And the diverse human system interface consists of diverse indication systems and diverse ESF manual actuation switches.

And the safety system processing system we used qualified indication and alarm system P for safety and information processing system for non-safety data processing system.

And we also used qualified indication and alarm system non-safety.

And the safety control system consists of a plant protection system and the core protection calculator system and ESF which is ESF component control system.

Also we have non-safety control system, process component control system and plant power control system.

It also has diverse protection systems.

For safety data communication we used safety data network and the serial data link.

And for non-safety data communication we used data communication network for information which use ethernet.

Next slide is for section 7.2 reactor trip system. Reactor trip system has these kind of auxiliary supporting features for operating bypass and the setpoint reset, trip channel bypass, and surveillance test.

And last July Westinghouse issued nuclear safety advisory letter 17-2. The title is the AC160 Processor Module Stall Timers is not Activated as Described in Licensing Basis.

AC160 processor module is one of the current platform modules, processing module.

This start time provides a diverse functions for some subtier part.

Despite this part Westinghouse concluded that this part does not impact the safety-related function or operability of affected safety system.

MEMBER MARCH-LEUBA: Mr. Oh? I think we're going to talk about the same thing.

This was a failure that was identified in July on existing reactors. Are you trying to license a future reactor with a failure built in?

I mean, are you saying that we are not going to bother to fix it when we build a new one?

MR. E. OH: As the last said, this is our current position. The APR1400 design is based on currently licensed Common Q platform.

MEMBER MARCH-LEUBA: Which has been found to be defective.

MR. E. OH: Yes. But Westinghouse concluded this function, even though it fails, this function is for diagnostic proposed. So it does not impact safety functions.

MR. SISK: This is Rob Sisk. Maybe I can provide a little bit of clarity on this.

The NSAO identified that the stall timer was not activated. Which was required as a part of the Common Q, original Common Q licensing basis.

The current approach to APR1400 is that they will use the license-based approved Common Q system at this time.

If in the future Westinghouse revises that report and makes a change to either remove or activate, or I should say deactivate the stall timer that would be addressed at the future either through the COL or a change as any change would be evaluated from the vendor.

Right now APR1400 is going to use the approved licensing based Common Q system which at this point would require that the stall timer be activated.

MEMBER MARCH-LEUBA: Right. It's kind of a difficult -- I realize we're in a difficult position. It's caught at the very end of the design.

But I will reserve my questions for the staff if they found that acceptable. Because I was not part of the review of the Common Q system. Charlie was and I'm sure that the fact that it was defense-in-depth watchdog timer in there was a big part of the proof.

Even though it's not part of the licensing basis it really was considered as a feature.

MR. SISK: Yes, understand. But the position at this time for APR1400 is to use the Common Q platform as licensed.

MEMBER MARCH-LEUBA: Okay. I will reserve my comments for the staff and give my microphone to the next member.

MEMBER BROWN: When you say it's the currently licensed design, or Common Q, whatever the design is, whatever exists today.

As presently designed -- we talked about the fact that I saw the new paperwork that you all put out with the five timers and two of the stall timers.

Well, this, the other paper Westinghouse put out, there's five if you look at the pictures.

And the software timer was the one that was not activated. And that software timer activated the hardware timer, the hardware stall timer, not the window watchdog timers of which there are two, one in each of the processing module and the communication module.

It's going to continue to be deactivated? Is that what you're saying? Because that's the way it is now.

MR. E. OH: The letter describes the kind of information. The window watchdog timer is the external to CPU timers but it still activates.

MEMBER BROWN: I understand all that argument. What I got down to was historically when we first approved this or agreed with this approach seven years ago we went through rev zero of the Common Q platform.

And there was supposed to be an external hardware-based watchdog timer that was in the original rev zero approved back in 2000, roughly 2000 I think.

Then subsequently and it was identified Westinghouse decided not to include an external hardware timer for this processing, for the PM646. And they would use the onboard module hardware timer, focused on the word hardware timer.

And then we went through a long -- there was a daisy chain. We went through and it was evaluated there was a second review done with a second topical report with a bunch of changes made in 2003 or so.

And the staff, at least I have an SER that says the staff reviewed that and concluded the substitution of the hardware timer onboard was okay.

So the window timers were never mentioned in all those discussions. And the window watchdog timers were only briefly touched on with a few phrases or a sentence or so under a couple of parts of the original Common Q rev zero which were system diagnostics, task scheduler, and there was another, I've forgotten, configuration management or something like that. There were three different parts of the software that addressed this, or the platform that addressed that.

With almost zero description of what they did, or what their function was, or that they did anything at all. It was very vague.

Rev 3 expanded that to discuss it more, but still didn't seem to indicate that the window timer was the primary one as opposed to what was advertised as the hardware timer.

And so I guess my concern or my questions are is I'm not quite sure what the configurations are now.

Because the software is intertwined on both of these with the hardware timer that was now not activated because the software timer didn't work.

And then if you look at the pictures that were provided in the subsequent documents to NRC there's some little dotted lines that show command signals and things like that which are not described at all other than as what's their character, what do they consist of, how are they generated, how are they independent of software, why are we not going to see the same problem with software in the advertised window timer operation.

The other thing that's interesting is that those window timers have these small windows that you go, it looks like it's tested constantly throughout the entire sample period.

I mean, you're talking -- if I divert into something that's proprietary please raise your hand and flag me, but there was relatively narrow windows without saying what the times were that if you're too early or too late then it triggers, but it's roughly testing it all the time.

So something has got to be controlling all this. So right now it seems like it's intertwined with stuff. It's not very well characterized. And I just have some reservations right now that the window timers are really as it was referred to.

That's what was used to clear the open item back in 2003 and why that's really satisfactory.

There's really been no explanation, pictures, or anything else to show us why that is okay.

I know it's an open session and I didn't want to get into any more detail that's why I'm trying to be a little bit -- and that was the basis back in 2003 for the following closing out of the open item was the fact the onboard hardware timer would now become the timer that looked at the entire cycle of processing.

If you didn't get to the end within a certain time you triggered it and you'd produce a reaction. That's not the case anymore. It doesn't even do anything. Other than reset a CPU.

MR. SISK: This is Rob Sisk. Thank you, Charlie.

Rather than getting into the technical discussion because I don't think we need to at this stage.

The position of the APR1400 design right now is we will use the NRC approved Common Q system.

Now if that requires the stall timer be activated when the time comes that the Common Q system would require a stall timer, if in the interim the vendor revises the topic report and revises the design in some manner the COL applicant or the new revision would have to be evaluated and incorporated into a COL or into a design at that time.

But at this stage of the design certification application APR1400 is using the NRC approved Common Q system as licensed.

Now, if like I say, in the future if the license changes or the design changes those will have to be reconciled at that time.

But it's premature to know what the final change might be, where the vendor will go with regard to the update to Common Q.

And if the staff position is that the stall timers must be activated to maintain its current license that's where we are today.

MEMBER BROWN: Right now it's not activated.

MR. SISK: Understand. We're not buying it today.

MEMBER BROWN: You're not buying it. What does that mean?

MR. SISK: What that means is when the COL applicant goes to procure it they have to make sure that they meet the licensing basis of the design certification.

MEMBER BROWN: Okay, let me walk back. If we talk stall timers. The argument used by Westinghouse in their paper was that the window watchdog timers were now -- were what was the basis of the 2003 clearing, although that was hardly obvious to anybody that was reviewing the paperwork. Or at least not to me. I'm not steeped in all the arcane details since we don't have enough detail in that to know.

So it's not just activating the stall timer. The stall timer's function is based on software right now. So just activating -- I'm just having difficulty as how we can walk through and say that the -- using the existing whatever you called it, licensed or approved version is satisfactory. How we can be expected to say it's okay as is without having some additional information provided to show.

Because the argument from Westinghouse is forget the hardware stall timer. Forget the software-based stall timer which activates the hardware timer. We're only depending upon the window watchdog timers.

And there's no real clear understanding of how -- or characterization of how those window watchdog timers are totally independent of the software.

It talks about them being diverse and I've forgotten -- the words are in my little write-up here somewhere, diverse and something else, and independent. But that's not obvious when you look at it in the way the task scheduler, system diagnostics, and everything else discuss it. Just not obvious.

I'm just trying to get to a point where we actually come up with a discussion that shows why -- and I'm open to it, it's just why in a closed session if we have to.

CHAIRMAN BLEY: It seems to me we're going to need to talk to the staff.

MEMBER BROWN: Right now Westinghouse, I don't know what -- they gave a presentation and I have no idea what the staff intends to do with the presentation.

I'm perfectly satisfied to wait and have the staff tell us what they think and why they think. And that's okay with me, it's just that we'll have to reflect that in our report. That's all. That we're on hold until that's completed.

MR. SCAROLA: This is Ken Scarola from Nuclear Automation Engineering. I'm supporting KHNP and KEPCO.

I think maybe I can shed some light on this.

The licensing basis that has been approved by the NRC for Common Q requires the activation of both timers, a software timer and a hardware timer.

Both reside on the CPU module, what's called the PM646 module.

Both are required by the existing topical report.

Why Westinghouse did not activate both

should not be the subject of this meeting.

What is the subject is that APR1400 will comply with the topical report. The topical report requires activation of both timers.

Should Westinghouse make a change and somehow get the staff to approve that only one timer would be activated --

MEMBER BROWN: Which one are you talking about?

MR. SCAROLA: -- then APR1400 will follow that basis for Common Q.

MEMBER BROWN: Okay, let me interrupt. If it's supposed to be activated, that's fine. By activating the two stall timers, if that's required right now, that's what you're talking about, those are the two timers you're talking about.

That depends on software. That's no longer a hardware-only based timer.

MR. SCAROLA: Can I interrupt because that's not exactly correct.

The stall timer is a software timer. On that same module there's a hardware timer that is not dependent upon software.

The hardware timer can be activated by two means, by its own timeout, or by the software timer timing out and telling the hardware timer to time out.

Either one can activate the hardware timer.

The hardware timer can activate completely independent of software.

MEMBER MARCH-LEUBA: It is my hope, Charlie, that we will have a subcommittee meeting where we will discuss these things in detail, prioritization, which is not APR1400 related.

(Simultaneous speaking)

MR. SCAROLA: This is a Common Q issue. It's really not an APR1400 issue.

MEMBER BROWN: Okay, let me interrupt this time.

If I look at the figure provided by Westinghouse, and I'm not going to say what it looks like, the hardware watchdog does not have an independent trigger on it. It's strictly triggered off the software-based timer.

And I'm not going to argue about that anymore, but that's what the figure shows and that's what's stated in the write-up.

So I think we can terminate the discussion and go on with it because it's not going to be resolved at this time.

MR. SISK: Charlie, I don't think we're -- Rob Sisk -- we're not looking to resolve the technical issue here.

What we're wanting to assure the committee is that we are going to use the licensed approved Common Q.

MEMBER MARCH-LEUBA: And we the committee want to follow up with the staff how that report will be licensed.

MEMBER BROWN: That's fine. I just wanted to make sure I got on the record a discussion of how -- a little bit of who shot John and how we walked down this path to where we got.

CHAIRMAN BLEY: Not to beat a dead horse, but that Westinghouse memo you're referring to isn't part of anything official as of right now.

MEMBER BROWN: Exactly. It's not. It was simply identifying a problem and then they had a public -- not a public, they discussed this in a presentation with a bunch of slides.

And then going through those slides it becomes very clear why the inactivation of the software timer does not activate -- why just activating it doesn't solve the problem.

Now, maybe the window ones do, but it's

not -- based on the information provided that's not clear. And that will have to be resolved by the staff, NRC, with how they handle this.

MR. SISK: And I'm sure there will be future discussions with Westinghouse. But for the APR1400 we're using the Common Q approved platform.

MEMBER BROWN: My concern right now, Dennis and Ron, is that we'll just have to reflect that in our report that we're on hold relative to how that's applied.

And if that's satisfactory with you then I will de-energize my mike.

It's not software-based, it's hardware-based. I'll use my finger.

Okay, thank you very much for letting me expound here for clarifying what your intentions are. It's really out of your ballpark right now.

MR. E. OH: Okay, I will go on next slide. Next slide for core protection calculator system.

This system has CPU loading test issues and an ITAAC will be included to provide the commitment to satisfy CPU loading restrictions.

The CPCS is designed to meet the 75 percent CPU load restriction by the vendor, i.e., ABB.

The APR1400 CPCS is identical to the

Barakah nuclear power plant CPCS. And the recent Barakah nuclear power plant CPU loading test demonstrated that CPCS CPU shows deterministic behavior when CPU load is increased to 75 percent.

The RAI 7887-7.1-25 response was revised to include the results of the BNPP CPU load test.

Section 7.3 is engineered safety features systems.

This system consists of group controllers and loop controllers and safety data communication network and safety-grade soft control modules. And the gateways for the soft control modules.

And the ESCM system has independent divisions which are physically separated and electrically isolated. Using fiber optic connections.

Next section is systems required for safe shutdown.

This system consists of the main control room and the remote shutdown rooms. This picture shows -- the pictorial shows the APR1400 main control rooms.

In front of the operator consoles there is large display panels which is in the center of the area is fixed displays and left and right wing display area is variables. Depends on operator's choice.

And we have five consoles for five operators. And the left side there is a safety console for these consoles failures which can be some dedicated hardware switches and displays.

As I said before, main control room is composed of operator consoles and large display panels and safety consoles.

And the remote shutdown room has a remote shutdown console which is identical with operator console of the MCRs.

And the top of the remote shutdown console, there is a small shutdown overview display panel which is similar system unit displays of large display panel of the main control rooms.

Next section, 7.5 is information systems important to safety.

We have qualified indication and alarm system-P which displays accident monitoring instrumentation type A, B, C variables for reg guide 1.97 and indication of approaching and recovery from inadequate core cooling requirement.

Qualified indication and alarm system-P displays two channels of AMI variables and the 4 channel of containment isolation valve status.

The QIAS-P provides continuous realtime

display for AMI type A and B variables.

And also, information processing system displays inadequate core cooling variables as primary display on the LDP and the QIAS-P displays the variables as a backup displays.

Next section, 7.6 is interlock system important to safety.

APR1400 has five kinds of interlock system important for safety.

One is the shutdown cooling system suction line isolation valve interlock and a shutdown cooling system suction line relief valve interlocks.

And the safety injection tank isolation valve interlocks. And the component cooling water supply and return header tie line isolation valve interlocks.

And the component cooling water cross connection line isolation valve interlocks. The description is under 7.6.

And 7.7 is control systems not required for safety.

The control system is physically separated and electrically isolated from safety systems.

And we do control system common cause failure analysis to confirm that the event consequences of chapter 15 are still effective and meet the acceptance criteria of chapter 15.

We have the following major control systems, power control system and process component control system which is implemented using distributed control system, ECS.

7.8 is diverse instrumentation and control systems.

We have three kinds of diverse I&C systems which are composed -- consist of diverse protection system and diverse indication system and diverse ESF manual actuation switches.

This system provides ATWS mitigation means and -- to cover the safety systems common cause failures.

And the diverse protection system provides diverse reactor trip function and turbine trip, and auxiliary actuation, and the safety injection actuation functions.

The DPS consists of four channels and diverse from sensor output to shunt trip coils of reactor trip CTBS system trip circuit breakers for reactor trip.

And diverse process output to control interface module of the ESF actuation of auxiliary feedwater and the safety injection actuations.

The last section is 7.9 data communication systems.

We use three major data communication. The first one is safety data, signal data link, and the safety data network, and the data communication network for information which use -- each one use different protocols.

And especially safety system has deterministic behaviors.

And the communication independence is analyzed in the safety I&C system technical report as per interim step guidance 04.

And we have external data links which provides plant data to externally for EOF, NERC, or NRC operations centers via unidirectional hardware-based firewall implemented by fiber optic link.

A virtual LAN switch provides a link interface for each external location.

MEMBER BROWN: I do have a comment on this relative to the external data communication.

I think we brought this up in a subcommittee meeting in that the VLAN switches are just shown on a figure. There is absolutely no discussion of what their characteristics are either in the safety I&C system, topical report, or in the DCD chapter 7.

Implementing via fiber optic link does not make it unidirectional. It's what the fiber optic cable is connected to which makes it unidirectional.

And the way that firewall is configured is critical. Whether it's a design-based, in other words it's literally hardware one-way only, or whether it has a software feature that can configure it and you can configure it to be one-way via software, or is it a hardware-based where you actually have to clip a wire or disconnect a connector or whatever it is.

There's no description of how that's accomplished in order to ensure it is one-way and one-way only.

VLANs I'm not -- my memory is a little bit short on the VLAN type switches, but they're loaded with software.

You're connected to an ethernet so obviously the VLAN switches have software capability in order to -- that's the output of the VLAN to the ethernet before you go to these other locations.

And therefore there's obviously software in there which is hackable and you want to prevent that from happening.

So anyway, it just needs to be described somewhat more in either the safety I&C topical report or in the DCD in order to make sure we understand that it is, in fact, one-way only and hardware-based one-way only.

Okay, I'm finished.

MR. E. OH: Can you describe?

MR. J. KIM: This is Jinku speaking, the KEPCO E&C.

And so our last technical report, we added more detailed design descriptions so you have a concern about that. We already added that information into the device I&C technical report.

MEMBER BROWN: That's a revision? I haven't seen it. The only revision I've got is the one I've got.

MR. J. KIM: And also we will provide our DCS reports -- with the RAI.

MEMBER BROWN: All right. Thank you.

MS. ZHANG: So it's not in any of the submitted -- this is Deanna Zhang.

It's not in any of the submitted technical report revisions. So this will have to be revision 2.

But in response to your RAI 7883 question number 79-2 there has been a proposed revision to the safety I&C system technical report.

Included was a description of how it is hardware one-way, that it is through the fiber optic link was only -- okay, anyway this is non-proprietary.

MEMBER BROWN: The wire is a wire.

(Simultaneous speaking)

MEMBER BROWN: The fiber optic link is not one-way. It can go both ways.

MS. ZHANG: It's one way out because of the transmitter. There's no receiver connection.

MEMBER STETKAR: We'll receive that revised technical report long before our phase 4 meeting.

MS. ZHANG: Hopefully.

MEMBER STETKAR: No, no, not hopefully. We will.

MS. ZHANG: The proposed response has the markups in it.

MEMBER STETKAR: We will receive the revised technical report long before our phase 4 meeting because we need that to support our final decision.

MS. ZHANG: Okay. Yes.

MR. E. OH: Okay, I will go on. The last slide.

MEMBER BROWN: Okay, this is -- there's still another layer of this. We've got phase 4 to go through.

And I guess is relative to the licensing basis if I'm going backwards now. Sorry for that. To the Common Q platform.

Is that issue going to be resolved at the time we do the phase 4, when we finish up the phase 4?

MR. WARD: Yes, I think it will be.

MEMBER BROWN: Okay. So the staff will be able to have a handle on that and one way or the other we'll get that cleared up.

MR. WARD: We have a lot of confirmatory actions to receive from KHNP. It should be in that.

MEMBER BROWN: Okay, thank you.

MR. E. OH: Okay, I will continue. In chapter 7 the design features of instrumentation and control system of the APR1400 are described.

And the functions and the design features are briefly presented today.

And the key features, for example, watchdog timer, CPU loading test, and continuous display and external communications are explained.

And we think our design complies with 10 CFR 50 and reg guides and the related IEEE standard and interim step guidance.

This is the end of my presentations.

MR. SISK: So this is Rob Sisk. If there are no additional questions on chapter 7 we'll move on to chapter 18.

MEMBER BALLINGER: Yes.

MR. E. OH: Okay, I will continue my presentation of chapter 18.

This page shows the contents of my presentation as follows. An overview of chapter 18 and treatment of important human actions and human factor engineering ITAAC, additional factors program milestones and procedures for integrated system validations and operating experience review and site specific information. I will cover these topics.

Chapter 18 consists of 12 sections which is same as NUREG-0711 human factor engineering review model elements.

This slide shows technical documents for the -- we submit for these applications.

Overview of chapter 18. The goal of HFE program is to ensure that HSI design is properly developed and effectively implemented.

And the program criteria is the same as in NUREG-0711 revision 3.

And the HFE program duration is following. The APR1400 HFE program has been in effect from the start of APR1400 design.

And it will continue through the completion of initial plant startup.

And the licensee will continue the HFE program in accordance with NUREG-0711 human performance monitoring programs.

This slide shows an overview of chapter 18. For these applications KHNP prepared all these elements implementation plans.

And the COL applicant generated a results summary report for implementation plan in sequence review.

And in this point of time frame integrated system validation start and which integrated all the results of previous program elements.

And the integrated system validations plans, the other program element is the design implementation verifications.

This last one is completed before fuel loading.

And the human performance monitoring starts at the fuel loading and it will continue during operations.

And currently we identified human factor when we end the design implementation as ITAAC closed package.

And one issue of treatment of important human action is some aspect of site-specific PRA will likely not be determined until fuel load which occurs after the control room has been constructed.

And the applicant does not address how the risk important human actions are identified from the site-specific PRA. For example, seismic PRAs are implemented in the HFE program.

Our preliminary observations is like this.

Design changes, including new risk important human actions which is identified at the HFE verification and validation is completed and are implemented using HED human engineering discrepancy resolution process of the human factors engineering program plan.

The human engineering discrepancy resolution will be verified in the design implementation program element.

Design changes after design implementation will be resolved using COLAs corrective action programs.

And we are working with NRC staff to

resolve this issue.

Another one is human factor engineering ITAAC.

One issue is human factor engineering ITAAC is limited to only integrated system validation and the design implementation.

And there are no other HFE ITAACs in the application to verify the completion of the other HFE activities.

MEMBER STETKAR: I'd like to discuss this a little bit. I was waiting till this slide.

Because this is an open session I do not want to discuss details of any of the implementation plans.

However, when I read chapter 18, the summary information about each plan as you noted here there are no specific COL information items called out that says the COL applicant must actually implement this plan, except for as you've noted here the integrated system validation and the design implementation.

I find that misleading. So, I want to -- on the public record I want you to confirm that a COL applicant must actually perform each task in every implementation plan. Is that correct? It is the COL applicant's responsibility to perform each task in every implementation plan. None of those tasks are completed as part of the design certification. Is that correct?

MR. SISK: This is Rob Sisk on behalf of APR1400. I think the best way to answer that question right now. This is an open item and we are working with the staff in how best to address your comment.

We understand the comment, but we have not finalized it with the staff.

MEMBER STETKAR: We need to get clear resolution on this soon because in my opinion it significantly affects how the certified design will be interpreted by a particular applicant.

And perhaps more importantly it affects the way that some of the implementation plans are written.

The way that they're written right now one could on the one hand assume that it's done as part of the design certification because they refer to things like making assumptions about information that will be available to a COL applicant well before the fuel load PRA, for example.

They're written in that nature as if the tasks are performed during the design certification.

Whereas if the expectation is that a COL applicant will perform those tasks then the information will be available.

There's no need to make assumptions. There's no need to provide guidance about what kind of assumptions might be made. The COL applicant will have that information. Whether it's site-specific design information, or whether it's information from the COL applicant PRA after including site-specific design features.

And I'm not talking about seismic analyses here. I'm talking about electric power supplies and cooling water systems and those types of things.

So, I think it's necessary to be very, very clear about what of those elements is part of the certified design and the expectations, and make it very clear to a COL applicant what they need to do. And it's not clear right now.

Not in chapter 18 even because it's -- and I hear what you're saying, that you're working with the staff to get this resolved.

MR. SISK: APR1400 has received an RAI from the staff that includes a discussion --

(Simultaneous speaking)

MR. SISK: And we're working with the

staff toward a resolution to that issue.

MR. SCAROLA: This is Ken Scarola. I'd like to add to the discussion here. Maybe I can add some insight.

The IPs, the implementation plans, were written to identify the qualifications of the people, subject matter experts in human factors engineering, subject matter experts in I&C, et cetera.

Those qualifications of the people that needed to execute that particular program element.

It is silent as to who does that. It can be done by the COL applicant. It can be done by KHNP. It can be done by a subcontractor.

What is important is that the completion of all of these program elements are in fact prerequisites to the integrated system validation.

So you cannot close the ITAAC for the integrated system validation until all of those program elements are completed by those subject matter experts.

So, APR1400 is purposely silent on who does these things, but very explicit on the qualifications of the people that need to do them.

And that is purposely the intent. And that's why there are statements about site-specific assumptions, because some of these program elements, for example, task analysis verification cannot be done unless we know what the switchyard looks like, unless we know what the cooling water towers look like.

Therefore if you're going to do those activities without a COL applicant you need to make assumptions about those.

Then you execute the program element. Now it -- and you do the integrated system validation if you want.

The integrated system validation does not require a COL applicant. It can be closed without one.

However, when there is a COL applicant the COL applicant must verify that all those assumptions remain valid. That's part of what's called the design implementation program element. That final validation is the responsibility of the COL applicant.

CHAIRMAN BLEY: Ken, thanks. And I've been listening to what John brought up and your discussion.

It sort of fits together for me, but I guess the things I have to go back and double-check is to make sure it's perfectly clear in that ITAAC you referred to that in fact that's where it will all be brought together.

And I have to look at that ITAAC because I don't remember it in detail.

MEMBER STETKAR: In one way of looking at it you can interpret it that way.

In other ways of looking at it you can say I throw the switch to start a nuclear power plant and I have to have a good design by the time I throw the switch.

There are many parts of that design that have to be verified I would say as you build the machine.

And that it's not simply the sum of the total that you base your overall conclusion on.

Now, what Ken said is accurate in the sense that each of the program plan implementation plans specify the requirements for the people who will actually do -- who will actually implement those elements.

However, my larger concern is that several of those implementation plans do provide guidance, technical guidance if I can characterize it that way about assumptions that can or should be made.

And those assumptions will be different as Ken noted if that part of the implementation plan is executed as part of the certified design, or if it's executed by a COL applicant.

And there should not be that level of vagueness in something that gets certified. It should be very clear that this part of the human factors engineering design and implementation is part of the certified design, leaving the remaining tasks.

Some of those might be verification of assumptions. Some of them might be execution of each element of an implementation plan. Those are left to the COL applicant.

Or, is what's in the certified design simply the implementation plan itself without necessarily vague qualifications about assumptions, technical assumptions now.

And the COL applicant is expected to implement, execute -- I have to be careful about terminology -- execute all of the elements of each of those implementation plans.

If I were going to be a COL applicant buying this plant I certainly would want to know what I'm on the hook for very clearly.

And right now it's not clear, and it's not -- I don't think Ken's answer helped us a lot.

I'll just leave it there.

MR. SCAROLA: Can I give you one more point of clarification, John?

There is no intent in these implementation plans to say that any of these program elements would be completed as part of the certified design.

It is expected that the design would be certified based on the IPs and that the implementation of the IPs would take place sometime subsequent to the design certification.

The implementation of the IPs can be by the COL applicant, they could be by KHNP. They could be a subcontractor arrangement. There's many ways to do that.

The important point is they take place subsequent to the certified design.

MEMBER STETKAR: And that's what I'm trying to get clarity on.

Because right now if you read chapter 18 and if you read several of the implementation plans they are written as if the elements of those implementation plans can be completed and by this it's inferred that they would be completed as part of the certified design.

At least that's my interpretation of it.

We've discussed it enough. I'm happy to

hear you say that there is an expectation that they will be done.

I don't care whose letterhead is on the paycheck of the person who does the work. That's irrelevant to me.

It's that the work is done and that a COL applicant clearly knows the expectations of what they need to do and what elements -- the tasks that they need to do to implement the design and the validation verification of design and so forth.

CHAIRMAN BLEY: I had another question.

I guess for me if I were buying I would assume I'm on the hook for all of this.

MEMBER STETKAR: Well, you would except for the fact in most places in the DCD when there is a section that has a COL information item.

It calls out something that says COL applicant is on the hook for this basically.

In the HFE section in particular most of the discussions about the implementation plans don't have that hook at the end.

So when I first read chapter 18 I said oh well, because this is a design that is actually being built in Korea we know a lot about the hardware, we know a lot about the human-machine interface at least from the Korean implementation of the design.

Perhaps the proposal is that as part of the certified design several of those implementation programs, or at least as much as you can do on them would be part of the certified design.

And indeed when you read the implementation plans a lot of them read that way because they say, well, because the information about the switchyard will not be available you make assumptions about the switchyard.

Well, okay. I would do that if I were doing it as part of the certified design. I would need to verify that assumption if I were a COL applicant.

And they're written that way. If there were hooks in each of them saying COL applicant must, you know, execute this implementation plan I think it would be clearer.

MR. SISK: Thank you, John. Rob Sisk. We've captured the note.

But I do just want to repeat we are working with the staff to resolve this. And this helps inform but we are looking to get this cleared up and you'll hear more about this in phase 4.

CHAIRMAN BLEY: My question kind of

started two slides ago on 7. Went through eight and got to this one. It's kind of --

MEMBER STETKAR: That's why I waited till this one because it has --

CHAIRMAN BLEY: Yes, but there are some specifics on the other one that I wanted to go back to.

And they're related in that they all have to do with what belongs to the COL guy and what belongs here.

Seven since you brought it up says some aspects of the site-specific PRA will likely not be determined until a fuel load.

Well, it has to be done by fuel load. Most everybody doing this wants to have it done substantially before fuel load so they can do the associated things.

One of the associated things is these risk important human actions that are flagged here.

And then on the next slide we seem to be saying we're not going to get that done in time to have that done. And that's going to have to belong to the COLA. And we'll throw it into the COLA's corrective action program.

These seem like things that need to be in place for that prior to fuel load PRA to be reasonably reflective of the actual design.

And throwing it into the corrective action program smells like it might be done after fuel load which seems inconsistent with having the PRA done by fuel load.

So I'm confused about that. And you say you're still working to resolve this and I don't know where the status is.

But if you can comment on how you see that working out and we'll follow this as we go into the next phases of this design cert.

Try to take a shot at it.

MR. SCAROLA: This is Ken Scarola. The DI program element, design implementation, must be completed before fuel load.

In that program element the COL applicant must verify all of the assumptions that were made for the integrated system validation.

They must verify that the integrated system validation remains valid for their plant.

So nothing remains open for the corrective action program. All of these integrated system validation assumptions must have been verified in the DI program element.

What this says is anything that happens subsequent to the DI program element which would be subsequent to fuel load now become part of the COLAs corrective action program.

So I think we need to make it clear.

CHAIRMAN BLEY: If that's what it means that's okay.

Hooking it up with the previous slide seemed to create confusion.

MR. SCAROLA: I understand.

MR. SISK: Rob Sisk. You made note on the graphic that was up previously.

There's a monitoring section after fuel load. So there's anything that takes place after the DI there's a mechanism to provide feedback into the program is all that really is saying. And it's identified through the corrective action program.

CHAIRMAN BLEY: Okay. Go ahead.

MR. E. OH: Okay. I will continue page 10.

And for HFE ITAAC our preliminary observation is in accordance with human factors V&V implementation plan completion of HFE analysis and designs are prerequisites for the integrated system validation start.

These are inherently encompassed by ISV ITAAC.

And design implementation verifies any design changes that occur after the integrated system validation and remaining as-built HSI design issues that cannot be verified during the integrated system validation.

For example, main control room noise level and lighting level, et cetera.

MEMBER STETKAR: I'd just like to make a comment I think more than a question.

The reliance on this slide of the integrated system verification ITAAC sounds as if it is a very complete and encompassing activity. Because it's got the words integrated in it.

It's actually focused on a rather small number of specific scenarios that are selected to test parts of the human system interface design.

There's a list someplace and I can't remember whether it's probably in one of the implementation plans right now so it's proprietary, but it's not tens of scenarios, it's less than that.

So it's not this notion of a fully integrated evaluation of the entire design. Which is part of my concern about -- there are other elements of the implementation plan that are somewhat more comprehensive within the scope of those elements.

So that if you will some of the piece parts you get a little bit more comprehensive.

And then when you put the piece parts together and do the integrated system verification validation, especially the validation, it eventually funnels down into a set of distinct scenarios.

So saying that everything in that whole human system interface design, all the procedures, all of the hardware task analyses and so forth ultimately will be tested if you will as part of the ISV is a bit -- not quite accurate.

It is true that it's intended to test the important parts of the design.

MR. E. OH: This picture repeats again. And it shows the ITAAC close, the time frames here, show loading. Here show loading all HFE elements except human components monitoring should be closed. Especially this human factors implementations and design implementation program element should be closed.

And at design implementations the remaining programs, remaining design changes are following COLAs corrective action programs.

Next slide. One issue for procedures for integrated system validation.

The scope of human system interface design computer-based procedure, we call it CBP, conversion is limited to the procedures used during the ISV.

All other procedures should be converted to CBP within the human system interface design program element.

Our preliminary observation is the operating procedures and converted to CBPs for the ISV include procedures directly used in the ISV scenarios.

The other procedures specifically included to ensure CBP inventory does not influence operator decisions.

These procedures will be converted to CBP for applicant's procedure development programs.

Any comments or question?

MEMBER STETKAR: This illustrates one of my concerns from my previous comment about the scope of the ISV versus the scope of the design.

MR. E. OH: Next slide, operating experience reviews.

There is two issues. One is operating experience with dates before Shin-Kori 3 and 4 constructions are assumed to be included in the

APR1400 design and are not screened again.

Another issue is NUREG/CR-6400 operating experience criteria helps how these category grouping helps to understand the similarities and differences between operating experience lessons learned. There is two issues.

Our preliminary observation is like this. Shin-Kori 3 and 4 operating experience is reviewed up to the date 1996 and considered using the criteria of NUREG-0711 revision zero.

And current OER IP include INPO and WANO operating experience database.

And for another issues, NUREG/CR-6400 provides expanded human factor engineering design issue categories and proposed candidate resolutions.

And these OE grouping follows the issue category helps designers to clarify the OE-related design issues and to decide their design resolutions.

MEMBER BALLINGER: I have -- is the first statement correct, Shin-Kori 3 and 4 OE up to 1996? Shin-Kori 3 and 4 just started operating, right?

MR. E. OH: Last year, yes.

MEMBER BALLINGER: So I guess I'm not clear about up to 1996. I mean it can't be Shin-Kori 3 and 4 operating experience up to 1996. It has to be the previous design up to 1996.

CHAIRMAN BLEY: Whatever Shin-Kori considered perhaps is what they meant.

MEMBER BALLINGER: I don't know. What does that mean, Shin-Kori 3 and 4 operating experience up to 1996.

MR. E. OH: After the 3 and 4 construction permissions we submit operating experience review record. After that time the cutoff date is 1996.

MEMBER BALLINGER: Oh, okay, so it's not Shin-Kori 3 and 4 operating experience.

CHAIRMAN BLEY: I couldn't follow the response. You sounded convinced but I don't know what he said.

MEMBER BALLINGER: Shin-Kori 3 and 4, construction began at point X, sometime ago.

The operating experience that they considered was --

CHAIRMAN BLEY: That they considered.

MEMBER BALLINGER: -- up to that point. Not Shin-Kori 3 and 4 operating experience up to 1996. That would be a Star Wars kind of thing. Okay, I understand.

MR. E. OH: Okay. And next slide the issue is why it should be necessary to make generic assumptions during these activities. I mean function requirement analysis and function locations.

And COL applicant will be able to use site-specific information to develop the control room design at the site.

Our preliminary observation is like this. The generic function requirement analysis and the function location assumption provide the basis for the human system interface design and supports an iterative process includes site-specific information as design develops.

The design implementation program element requires confirming the application of the site-specific assumption or regression analysis to address any plant-specific differences.

This is the last slide. In chapter 18 the APR1400 human factor engineering program has been established to satisfy the review criteria in NUREG-0711 revision 3.

KHNP has concluded that this will result in an acceptable HSI design.

CHAIRMAN BLEY: I didn't attend this subcommittee meeting. And if you discussed this please tell me you've already talked about it.

In the development of the panel displays and the operating procedures and the computer-based procedures did you work from the Korean design and the Korean procedures and just kind of translate things?

Or did you go through with U.S. operators and develop a new confirmed set of displays and procedures?

MR. E. OH: APR1400 was referenced design is a System 80+. In Korea we used the CBP procedures. So we convert that procedures to computer-based procedures. It's very similar in U.S.

MR. SISK: Did that answer your question?

CHAIRMAN BLEY: Well, the last phrase. I'm sorry, John, what.

MEMBER STETKAR: This comes back to kind of my confusion because I have gotten to the point where I believe, and I may be wrong, that the human factors engineering and the human system interface design for APR1400 is all -- it is not yet final. They haven't made those translations yet.

CHAIRMAN BLEY: But my question is really are you thinking of translations, or are you thinking of what you have to do.

In at least one other design that came from another country and was brought here the first approach was to essentially translate everything and put it into English.

And operators here couldn't work with that because the whole philosophy was different.

And it took at least three different stages to work to the point that we had displays and procedures that were workable with the kinds of requirements and training we have for operators in this country. That's where I was headed.

And if this is all to be done later and it's DAC sort of like John says that's one thing.

If you haven't even thought about that process it might not be as easy as you think.

MR. SCAROLA: This is Ken Scarola. This gets back to the point that I made earlier about subject matter experts.

The individual IPs, for example the procedure IP, the IP on designing displays defines the qualifications of the people that must be involved.

U.S. licensed reactor operators or senior reactor operators are required for each of these program elements.

So none of these will be a simple translation of a Korean procedure into a U.S. -- an English procedure.

They will be certainly manipulated so that

U.S. licensed reactor operators can fully understand them and execute them.

(Simultaneous speaking)

MR. SCAROLA: And it's after the design certification.

CHAIRMAN BLEY: That's where I was -- both aspects I was interested in.

Okay, so one was John raised earlier, but the other was have you thought about that process.

MEMBER STETKAR: And my spin a bit because, again, I don't want to get into the proprietary stuff.

There are many references to the original combustion engineering procedures.

So my spin on it is your concern actually was more for Shin-Kori which was taking the English stuff and translating it into something that could be implemented in Korea rather than bringing it back here.

But it depends on what that starting point will be for an APR1400 in this country.

CHAIRMAN BLEY: In any case it sounds like it's put off on the COLA.

MEMBER REMPE: This point you raised yesterday in another meeting.

And just to make it more concrete could you give an example where the logic would be different?

CHAIRMAN BLEY: No, I can't. I'd have to go back through the details.

MEMBER REMPE: I'd be interested.

CHAIRMAN BLEY: I'll be happy to give you those papers.

(Simultaneous speaking)

CHAIRMAN BLEY: I can send you the papers.

MEMBER STETKAR: There are -- I hate to use the term cultural differences, but I don't know how other to characterize it.

There are differences in the ways that different countries organize their responses to events.

A good example, one that came out after Chernobyl was that the Russians did not use many procedures. They relied on the knowledge of their individual operators. They very heavily thought that their individual operators were very highly trained and could sort out any problems.

That's much different, for example, for even through the United States the paradigm that we at least have emergency operating procedures, we have function restoration guidelines and stuff like that, things that are written down that people are trained on that a scenario might depart somewhat from that, but at least there's something to anchor you.

And different people have done different ways of interpreting a range of things.

MEMBER REMPE: That helps me understand, but I would be interested in seeing those papers. Thanks.

MR. SISK: I think that concludes chapter 18 unless there's any further questions and I'll turn it back to Mr. Ballinger.

MEMBER BALLINGER: Okay, thank you very much. I think this is -- we're going to have to change people out so I think this is a convenient point for a break until 10:15, Mr. Chairman?

CHAIRMAN BLEY: We'll recess till 10:15.

(Whereupon, the above-entitled matter went off the record at 10:00 a.m. and resumed at 10:16 a.m.)

CHAIRMAN BLEY: Meeting will come to order. Back to you, Ron. Use your microphone, sir.

MEMBER BALLINGER: This is Roland. We now have a staff presentations and two sets of slides. And I don't know who is going to do the presenting --

Mr. Ward.

MR. WARD: Thank you. My name is William Ward. I am the lead project manager for the APR 1400 review for NRC. Thank you, again, for the meeting now. We are looking forward to getting through this and through Phase 3. As you will see in the slide presentation that the staff has today, it is very minimalist.

We feel like we provided slides earlier and we provide a lot of information. There's a lot of discussion in the subcommittee. And we know you have a lot of questions, so we wanted to keep this to a minimum -- just give you a quick update on where we -- where we are and then let you ask the questions. So, next slide.

This slide shows what staff is focused on. This -- the details were provided in the subcommittee discussions, but these are the major points of the Instrumentation and Controls Review. As we identified during that subcommittee presentation, we had a total of 33 open items and 109 confirmatory items at the end of the group. Sorry. Next slide.

At this time we have only five open items. We do have 63 confirmatory actions. And there was a question earlier about when are we going to see revisions to reports and things like that. I will say that we have been talking with KHNP about possibly locking down revisions for the DCD Rev. 2 by the end of September. And that would include technical reports at that point, and hopefully we would see the revisions by early 2018. So that would be before the next meeting with you.

So, anyway, hopefully those confirmatory actions that we do have left will be closed out at that point. As I said, we have five open items. We have five RAIs that are waiting for supplemental responses. And we also have a new REI that is just being generated at this time.

The key remaining issues that are left are subpoint methodology, restrictive subpoints, the secure development operational environment, vulnerability analysis and post-actionate monitoring variables -- the justification for the selection of those variables. There were two other issues on data communications and control system failure analysis that have been resolved. So we are down to these concerns.

As you have already discussed, we do have sort of a new issue in the NSAL letter which was submitted. At this point, you know, the letter wasn't addressed to us. We don't really have any new information. As was clearly stated, we are working towards the existing licensing basis. However, we are curious and we are working on REI to ask for some more information because we don't have anything to work on at this time. So --

MEMBER BROWN: Can I make one observation? Are you finished with that?

MR. WARD: Yes, I was just going to say, that completes my presentation, so --

MEMBER BROWN: I guess right now you say you are still working to the current licensing basis and I -- I think that is what you just said. Maybe I didn't say that actually correctly.

MR. WARD: Yes. I did. The topical report that's been submitted --

MEMBER BROWN: Yes. As specified -- or, as we previously -- as I discussed earlier, there is -- in my mind, based on earlier understandings when we first reviewed the difference between the utilization of a hardware -- external hardware timer and these things called window watchdog timers, which were literally discussed only under and with respect to triggering and figuring out whether it was tested or not to see if it responded, there was no information in -- that they were actually the application code. The whole sampling period monitor was not identified in the topical reports.

So when we left our previous design approvals for the earlier designs as well as the earlier discussion -- Chapter 7 here on APR 1400, my perspective was it was the hardware timer on the PM646 that had no connection to a software stall timer and it was not referred to as a hardware stall timer in the earlier documents, either. It was a hardware built into the -- I had no problem with using that hardware timer that is on the module. But it was a hardware timer. It monitored the entire cycle and that was my understanding. And then that is what triggered the reactor trip if it locked up, per se.

That was not covered. That application was not discussed in either Rev. 0 or it was not clear relative to Rev. 3 of the topical report. So, in my own mind, the utilization of -- even though it was -- Westinghouse states in this NSAL that it was the window timers they were talking about to resolve the open item back in 2003, that is not clear -- that those window timers are in fact independent, hardware based and provide the, you know, required overall sample time.

If you look at how they are utilized and the times that are specified for those -- and they were only discussed as being tested by the test scheduler and/or the system diagnostics, which is not related to actual protection functionality. So that, to me -- seems to me that the Common Q platform in its current configuration has an open issue relative to how the hardware timing -- hardware watchdog timer functionality is truly hardware only.

The only thing that made any indication was in the Westinghouse presentation to you all where there was something called a command -- a little dotted line with a -- and that's not even talked about in the topical report. So right now it is not clear to me that the window watchdog timers are even satisfactory for the function as presently described. So I just wanted to get that on the table. It is not an open item, but to me the Common Q platform right now is questionable.

MS. ZHANG: So just to clarify a couple items, we do understand there are some timing issues that were not well discussed in the Common Q topical report. And this was something that we did raise to Westinghouse during the meeting we had on the INSO letter. They said that one of the plans is to go back and fix some of the timing issues because some of the timing cycles that were stated in the Common Q topical report may not be correct. So that is one thing for them to go back and do a comprehensive review and look at just this overall issue of the watchdog timer.

The other part about whether the windows watchdog timer is hardware-based, we didn't ask specifically on the windows watchdog timer -- on that terminology. But in the Safety INC System topical report it stated that it was going to use the hardware watchdog timer reference in the Common Q topical report. We did ask an RAI, RAI 7881, question 7-14 on how is that hardware? And the response we got from KHNP was that it is not programmable. There is nothing -- no FPGA, no any -- nothing that is software-based for that watchdog timer.

MEMBER BROWN: But you just used the word hardware and if you look at the little picture that was shown in that presentation there was the software stall goes to the hardware watchdog timer, which was also a stall timer. Had another picture that goes down to the window watchdog timer. What hard -- which is the hardware timer?

My understanding was the hardware timer we were talking about -- external -- turns out all that does is reset the CPU. And they -- and because it wasn't activated, CPU wouldn't have been reset. As long as it trips, I guess that would be okay, okay? But when we are talking about -- we keep throwing these words around like candy at a child's party and it doesn't seem to connect the dots in terms of what we mean. Is it truly hardware? What signal is going over there? What is the nature of the command signal that goes to it? It is not even talked about.

MS. ZHANG: Yes.

(Simultaneous speaking)

MEMBER BROWN: -- command signal, go to the window -- it is not even talked about in the topical report.

MS. ZHANG: And I think that is where there is some clarification needed in the Safety INC System topical report to go back and look at the different watchdog timers discussed in the Common Q Topical Report in order to match it better with the watchdog timers -- how they -- how KHNP plans to use the watchdog timers to cut all power to the undervoltage relays.

MEMBER BROWN: Yes, I agree -- the safety -- Safety INC Technical Report -- it is a technical report, correct? Is very -- has no discussion on that. Virtually none. So -

MS. ZHANG: Yes, it references a watchdog timer, but it's -- and, you know, in the RAI response we got that it is a hardware. I need to clarify what they mean by hardware -- watchdog timer. But it doesn't tie back to the terminology used in the Common Q.

MEMBER BROWN: In the Common Q. Exactly right. And how that command is generated, characteristic. And if it is a software signal or is it a hard, bistable high or low signal as we -- we are told? In the discussions I remember asking specifically what is the nature of the command signal? Is there some conversion on the way from the processor to the watchdog timer where that has to be accomplished or converted?

And the answer is no, it is a bistable type one-zero -- you know, 10, 12, 3 volts -- zero volts, whatever it is. I don't care. That does that with no software involved. And the answer was yes. However, now I am not even sure.

CHAIRMAN BLEY: Deanna, can we -- can you make sure we get the RAI and the response?

MS. ZHANG: Well, we are currently drafting the RAI right now.

CHAIRMAN BLEY: Oh. Well, I thought you said you got a response? Or was that just Vogtle?

MS. ZHANG: No, that was for a separate RAI.

CHAIRMAN BLEY: Oh, okay.

MS. ZHANG: That I was referring to on clarification when they said hardware watchdog timer, what do they mean by hardware? And also, when they talked about the outputs of the watchdog timer cutting the undervoltage relay, exactly how is that done? We needed better graphics. That RAI took care of that.

CHAIRMAN BLEY: Okay.

MS. ZHANG: But we are drafting a new RAI to better understand when the tie to the ENSO 1702, what -- to get an official response on what KHNP plans to do with that information. Whether it -- you know, we heard from KHNP this morning that they plan to stick with their current licensing basis, which is to activate those stall -- the different stall timers.

MEMBER BROWN: That doesn't solve the problem.

MS. ZHANG: But that doesn't -- so there are two issues that I see. One is the INSO letter which talks about the -- the inactivation. That, I think we can take care of if KHNP says we will stick with our current licensing basis. The other portion is to tie -- to understand better how the watchdog timers mentioned in the APR-1400 tie to the different Common Q Topical Report watchdog timers.

And, you know, with that tie I think would help explain everything and get a better picture of how all the watchdog timers work together with the APR-1400 application.

MEMBER MARCH-LEUBA: My hope is -- and I plan to bring it up tomorrow during our ACIS Planning Committee and with the INC Subcommittee chairman, that we will have a Subcommittee meeting, or information meeting on this topic which will close it down -- have all the proprietary information available. We can dig into the details of everything. And that's where we can solve it.

MS. ZHANG: But there are two separate issues. There's solving the issues in the ENSO on 1702 separately than there is the APR1400, which currently they're not going to stay with what the ENSO letter says, which is it's inactivated. They are going to activate it in their -- yes.

(Simultaneous speaking.)

MEMBER MARCH LEUBA: That's what I wanted to ask the staff this morning is -- what I heard KHNP say on the record this morning is that they have -- require that the Common Q LTR SER is the one they are going to follow. And that one is approved and it's good.

What we know now is that the actual implementation of the hardware doesn't really follow the SER completely. But as long as KHNP follows -- says we will build it according to the approved CR, which is now with the additional timer. Or, in the future we will get a result one way of the other.

Is that acceptable to the staff? That -- to provide KHNP with an approval for this conceptual design for our reactor based on an approved LTR and an SER with it?

MS. ZHANG: Yes, because in essence this system has not been procured. It has not been implemented. So once they procure it they can fully say where we'll only procure this system was the stall timers activated.

MEMBER MARCH-LEUBA: And that's what they're saying. They're saying ---

MEMBER BROWN: However --

MEMBER MARCH-LEUBA: We are referencing the SER that is already approved that has a hardware.

MEMBER BROWN: Okay.

MEMBER MARCH-LEUBA: Now you will have -- you, the staff, will have to make sure the thing to buy follows the SER. Right?

MEMBER BROWN: However, activating the stall timer -- hardware stall timer, does not resolve the issue because the statements are that it's the window timers. And the way they are operated and their characteristic is not described at all. Okay? They're called hardware and diverse. That's the only language used.

How they are commanded -- okay, when you look at the little diagrams and the little pulses that come in, the very short time frames that are only test pulses doesn't talk about what -- how is it monitoring the entire sample processing time such that if it doesn't process in time?

And that's well over an order of magnitude -- or two orders of magnitude -- not two orders, but some number of order of magnitude above what they are showing in terms of the time frames being sent to that -- the timing pulses being -- or the triggers being sent to that window watchdog timer. No discussion of application monitoring other than a little thing -- dotted line that calls command.

MS. ZHANG: Yes, so ---

MEMBER BROWN: So that's open as far as I'm concerned ---

MS. ZHANG: So that's the separate ---

MEMBER BROWN: That's the second issue.

MS. ZHANG: Yes, that's a separate issue. But yes.

MEMBER BROWN: If they want to run and have the hardware stall timer operate and have brief sets of CPUs, I am happy as a pig in a mud wallow. Okay? But it does not resolve the issue of the overall monitoring of the overall sample process by a hardware-based, independent, watchdog timer that is independent of the basic software -- of the operating system in the Common Q platform.

MS. ZHANG: Yes. As we understand it, you know, we need that clarification as part of the APR1400 design licensing basis, which is --

MEMBER BROWN: Exactly. I would also argue that that probably applies to the earlier designs that we have already agreed to because we did not -- this was totally -- and I am not casting -- no aspersions are being cast. I think it's just a language issue of what people understand based on saying certain words. So that is a different issue. But put that aside. I am only working on APR1400.

That is the only one I can deal with right now.

MEMBER MARCH-LEUBA: So I have two questions about process. Okay, so it's not technical. It's more for management. Okay? The fact that we are approving, generically, a reactor with an SER on a licensed topical report that we know the hardware doesn't follow -- does this raise to an ITAAC or a check item for COL that says when they buy the hardware make sure that -- how can make sure -- you will probably be working here by the time they build it, but everybody else won't be here.

(Laughter)

MEMBER MARCH-LEUBA: And I don't think it raises to an ITAAC, but certainly a checklist -- an item to make sure during the COL that this issue has been resolved.

MR. WARD: I don't think we have an exact answer how we are going to resolve that at this point. We need more information. We are going to ask for that, look through it, and we will figure out what the right approach is to ensure that we get what we need.

(Simultaneous speaking)

MEMBER MARCH-LEUBA: From my point of view, the answer for question B is good. We have an LTR, we have an approved SER which finds our LTR acceptable and we will buy that. Now, we want to make sure when they buy it that they really, truly follow the SER which not -- today they couldn't. They couldn't do it.

MEMBER REMPE: So as an add-on to your question, I heard KHNP today say, if the SER is changed by -- or this middle from the LTR is changed by Westinghouse because they know their hardware doesn't follow it and the staff approves it, there may be a different SER. And that may be fine for what Westinghouse is doing with that LTR in their plant, but how do I know that the new SER will meet what is needed for the KHNP design? I mean, there's -- is it linked too?

MS. ZHANG: Well, they can't just -- yes, they cannot just take whatever the staff wrote as an SER to any possible middle that Westinghouse does and not do something specific for any COL that uses the APR1400 designs.

MEMBER REMPE: So the --

MS. ZHANG: So they would have to do a separate action to submit whatever information they have obtained based on what Westinghouse decides to do with the design.

MEMBER REMPE: Okay.

MS. ZHANG: And then that will have to be submitted for staff approval.

MEMBER REMPE: Okay, thank you.

MEMBER MARCH-LEUBA: So the concern I have -- let me put it on the record -- is that we are approving a reactor design with a known deficiency. Right? I mean, it is a minor deficiency. It is a something that will be resolved by the time the reactor gets built for sure. But I want to be ensured that this will be taken care of. And I think we can give an admissibility that it will be taken care of, but there has to be a process to any of that.

MR. WARD: The wild car is, we don't know exactly what Westinghouse is planning at this point. So all we can do is ask KHNP how they want to resolve this. And, you know, if they know of anything that Westinghouse might be doing specifically. Because that would inform how they are going to approach the issue and we will work with that. So we can't really say at this point exactly how it is going to work out.

MEMBER MARCH-LEUBA: And let me follow up with another process since this is an session and the Subcommittee I am trying to put together on the technical will be closed. Let me ask you this question in particular. When an applicant or a vendor submit a licensee topical report, an LTR, and he has a licensing basis that you approve it on, but the LTR describes a number of defense-in-depth items.

We the staff -- or you the staff consider the defense-in-depth as part of the review. Can an applicant remove the defense-in-depth of what is described on LTR and say no, those are not important? We are only going to take item A, but B, C, and D which were defense-in-depth, we don't need to implement them.

I thought that an LTR was a complete item. If defense-in-depth methods were described in the LTR, they also have those VID methods, right? Is that correct?

MS. ZHANG: Well, for a COL that uses the APR1400 once it gets the design certification, if they were to take any departures from what is the certified design, they will have to specify. And that will have to be part of their COL application. The staff will have to review that separately.

MEMBER MARCH-LEUBA: Good. It is on the record and it is in the open session. Excellent.

MR. JUNG: Hello. Can you hear me? Okay. My name is Ian Jung, Chief of the Instrumentation Controls and Electronics Engineering and Division of

Engineering. I think the question that the member asked about this whole change of process for Part 52 licensing -- it is -- there -- we do have a process and -- right? And so and Part 52 requirements has an element where once design certification is approved, or COLs are approved, the follow up changes to the licensing basis. There are several -- there are requirements on it.

And licensing basis changes after design certification and things of that nature. There are 50-59 like process that -- which requires training and evaluation to see how those are really important. And some of the changes, like TO1 changes -- TO1 information changes require specific departure either through rule making or combined license amendment application -- the departure information to be reviewed by the staff.

But this type of information and some of the, you know, technical or topical reports typically would probably require some degree of staff involvement or some degree of inspection through ITAAC or sample inspection through the design development process. So there is a lot more than just saying it is going to be here or that. I just want to mention there are processes and changes to the licensing basis. There are several procedures and guidelines to use.

MEMBER BROWN: Just want to emphasize the last point. Hopefully nobody else will change or say anything else. As presently configured, just following the Topical Report and activating that software stall timer, which would then result in the hardware stall timer working, is not an answer to whether this platform is satisfactory in terms of how it monitors overall lock up of the processors. Unless we get some better clarification of the operation of the window watchdog timers.

If they separate the hardware stall timer from the software stall timer and use that hardware timer as a trigger -- which I don't think they're going to do. But that would be a solution. But if not, the only path to success in here is to provide additional information of how that window watchdog timer is activated as opposed to just tested for that little small millisecond set of windows and how it then triggers the end result.

It does trigger the relay, okay? But I mean it's still how you command it and what's its configuration? And is it totally hardware and there is no software involved in that? That's not -- there is only words and -- every time I see the word diverse, then it starts triggering, you know, defective brain waves in my old brain. So, seems to me that's got to be clarified somehow.

So right now I am hung up on the Common Q processor totally until we resolve that. Because that's what I have been saying. We are okay because we had it, and now it's not clear.

MS. ZHANG: Yes. We are preparing and RAI. So that will be presented.

MEMBER BROWN: Well that's all I am looking for. So just following the present approved thing does -- even if they activate it, does not work for the long haul.

MR. WARD: The timing of this meeting is fortunate. We can hear your concern and doctor those in. We are still early in looking at this and trying to figure out how to resolve it.

MEMBER BROWN: I can imagine that. That's why I'm -- that's why I'm trying to make sure there's plenty of discussion on this to make sure the bottom line -- it's not ITAACs or anything else to -- you know, after COL, that is an inappropriate time to try to get this resolved. We need to be able to have it covered when we issue our final Betty Crocker, Good

Housekeeping stamp of approval with our report.

MEMBER SKILLMAN: The words that I was waiting to hear have been spoken. And that is, depending on how this pans out, there could be a departure. And like the gentleman just mentioned, you get there and Part 52 through a 50.59-like process that determines that you need a change that could then lead to a departure.

What does give me a concern right now is the slide that KHNP provided and on that slide are the words the stall timer provides diagnostic functions, so on and so forth, and is not required for the system to perform its safety-related functions. And the question that I would have for the staff is, reading that statement from KHNP, how deeply have you interrogated that statement for extent of condition?

That statement stands alone as hey, this thing is okay. Don't worry about it.

MEMBER BROWN: Actually, Westinghouse said that. They took it ---

(Simultaneous speaking)

MEMBER SKILLMAN: KHNP has provided this on the record from Westinghouse. I got that.

MEMBER BROWN: Yes, okay.

MEMBER SKILLMAN: But where I am going is

-- is the NRC team looks at this. I think there needs to be an examination of the degree to which this impact on other safety functions has been exhausted. In other words, there aren't other extensive condition issues that this is emblematic of, but we really haven't discovered.

MS. ZHANG: And we do recognize that, and this is why we are continuing dialogue with Westinghouse to explore the extent of this finding because we don't know what is the extensive, you know, because we thought every requirement was traced and, you know, verified. So -

MEMBER MARCH-LEUBA: Let me ask you, I know we are running out of time, but short process also on process. You are NRO because we are reviewing APR1400, but this Common Q also applies for operating reactors. How does the Agency interact in our -- who owns this issue? NRO? NRR? Research?

MR. JUNG: This is Ian Jung again. So when this letter came in we -- the Agency took immediate notice and we have been actually discussing this issue quite a bit. The letter by Westinghouse has been sent to the applicable licensees. So those licensees themselves are -- have a process for themselves to evaluating the impact of that for their own licensing basis or safety behind it.

So that process -- we believe this process for individualized licensees to evaluate and see how their -- either through their corrective action program or in a problem identification or resolution process, we believe that is their licensee's responsibility by regulation.

MEMBER MARCH-LEUBA: Yes, but my question is more administrative.

MR. JUNG: Yes.

MEMBER MARCH-LEUBA: Who is responsible for the final product, NRR or NRO?

MR. JUNG: We all do. So me in NRO and Mike Waters and all.

MEMBER MARCH-LEUBA: So jointly -- you jointly work -

(Simultaneously speaking)

MR. JUNG: Actually, yes, we held a meeting with Westinghouse a few weeks ago to better understand what -- what they have, what their plans are. So in addition to the APR1400, for examples, Vogtle and Summer are actually -- they have procured the equipment. They are in the process of, you know, installing. And so we are working with -- we notified -- reached out to Vogtle and they are evaluating their options. One of their options would be bringing licensed amendment for staff review.

For NRR, there are equipment they are operating right now, right? S that's more of a potentially immediately safety issues. So they are working with the project managers for individual plant and -- and reaching out to the individual licensees to see what their action point for it is.

And beyond all that Westinghouse really plays a critical role. They are the ones who really knows the design and beyond it, right?

MEMBER MARCH-LEUBA: M-hm.

MR. JUNG: So their initial assessment, they explained to us if we can only sort of understands it, the key issue that we asked them was -- asking our self say, is there a really immediate safety concern that we need to worry about? So based on the information we have so far, we don't believe that there's an immediate safety concern.

Westinghouse explained some of them are proprietary. This system -- this particular feature has been -- one of them, it's been implemented for many plants the last 25 years. There was no cases where challenges were made and all that. So I think we -- we are dealing with this.

MEMBER MARCH-LEUBA: I think this resolution is we will look into this when you guys get the resolution. And we will have a subcommittee meeting and maybe a letter.

MR. JUNG: Yes, we will be glad to support. And we will coordinate with Westinghouse.

MEMBER MARCH-LEUBA: Right. But I was asking ACRS how this was supposed to look about process within the building, and I'm bringing it up because we have a different project. Completely -- nothing to do with this whatsoever, in which our vendor came with a methodology. And then restrict the methodology only to operating reactors, because they did not want to have NRO involved in the review even though it made no sense whatsoever because it was the same reactor. Okay?

But there has to be a way that -- somebody has to own the problem and one has to be the principal -- in this case NRR for example, and NRO is a supporting role -- that we don't have to issue two SERs on this.

(Simultaneous speaking)

MEMBER MARCH-LEUBA: And I am not sure that the procedures inside the building allows to have a single SER for a common problem.

MR. JUNG: Now for a topical report revision, they've -- Westinghouse comes in, we will join the review to make sure we both are, you know ---

MEMBER MARCH-LEUBA: I am not saying you guys are not involved. It's somebody has to be the lead. And one person issues an SER which applies to both operating and new reactors at the same time.

MR. JUNG: I mean, well what I can tell you is that we are fully coordinating now.

MEMBER MARCH-LEUBA: Two methodologies?

MR. JUNG: We will get the one message out there.

MEMBER MARCH-LEUBA: Yes.

MEMBER BALLINGER: Can we move this along a little bit?

MR. WARD: Is there something else?

MEMBER BALLINGER: I don't know.

(Laughter)

MR. WARD: Any other questions? Related to Chapter 7 INC?

(No response)

MR. WARD: Then Chapter 18.

MR. SANTOS: Good morning, my name is Cayetano Santos. I am the Chapter 18 project manager for the APR1400 design certification. I would also like to acknowledge Lauren Kent, the technical reviewer NRO for this chapter.

So the first thing I would like to discuss is the scope of the staff's review. So KHNP submitted an implementation plan or a COL item for each of the HFE elements identified in HFE elements identified NUREG-0711 as described earlier. And the staff uses the guidance in this NUREG to evaluate whether the control room meets the HFE-related NRC requirements.

This NUREG also provides guidance for the staff to evaluate whether an applicant's HFE-designed process will result in a design that will comply with the HFE NRC requirements. The implementation plans that KHNP submitted describe the design process and methods that will be used to develop the APR1400 HSI.

And I guess to address maybe an issue that came up earlier, I would mention it's the staff's expectation that a COL applicants would be the ones to perform all the tasks identified in these implementation plans because the staff's SERs is evaluating the process, and their conclusions are based on approval of the process that will be used to design the control room.

The starting point for the development of this APR1400 HSI design is the basic HSI conceptual design, which is described in detail in the application. The Applicant also provided a style guide that has like some design-specific HFE guidelines for this. And there was also submitted a couple of HFE ITAAC as part of the Tier 1 documentation.

So even though this is a Phase 2 SER, it currently contains no open items. There are 55 confirmatory items in the SER, which we are in the process of closing out as we review revision one, which you received in March. And as Bill mentioned earlier, we are expecting a revision two sometime early next year.

The next slide is -- so KHNP and staff met with APR1400 Subcommittee to discuss this chapter back in June. And then after considering some of the issues that were raised by members during that meeting, the staff issued some additional RAIs to KHNP last month in August. These RAIs were discussed earlier as part of the KHNP's presentation, so I won't go in a lot of detail into those two except mention one about Tier 2 Star information.

The staff requested some information related to the ITAAC issue that was described earlier. And this particular RAI I wanted to mention because of a recent SECY paper that was issued. SECY-170075 titled Planned Improvements in Design Certification Tiered Information Designations was issued in July of this year.

And this is an information paper sent to the Commission. And it communicates to the Commission the staff's intent to continue to use Tier 2 Star designation of information for both the APR1400 and the new scale design certifications. It also talks about staff's plans to try to develop improved guidance for identifying and designating Tier 2 Star information in design certification applications. And this approved guidance would reflect kind of lessons learned from the staff's review of licensed amendment requests from the Vogtle and Summer combined licenses.

And, final, this paper tries to clarify that the intent of Tier 2 information is to identify information that has the same safety significance as Tier 1. But the NRC has approved an applicant's request to change its designation to Tier 2 Star to get approved flexibility. Okay?

And the nature of the staff's question on Tier 2 Star is consistent with the SECY paper that I just described. Lauren did you have anything to add on the -- anything about the ITAAC discussion? Or just -- no? Okay.

No other questions on that. The next slide topic I would like to cover is a question about staffing that came up during the subcommittee meeting in June. So the DCD of Tier 2 information identifies five license operator in the main control room as an initial staffing assumption. That includes the shift supervisor, senior technical adviser, reactor operator, turbine operator and electric operator.

The electric operator position is unique to this design, which kind of combines a turbine -- to existing plants, which you usually combine the turbine and electric operator position. So the initial staffing assumption is an input that the HFE-designed process described in the various implementation plans. And then the final staffing level and control room configuration is the result of a combined licensed applicant reforming all of these activities and these implementation plans.

So if a COL applicant were to change this initial staffing assumption of five, it would be identified as a departure in the DCD -- as a departure from the DCD in the combined license application. So since this information is Tier 2, it probably would not meet the criteria requiring NRC staff approval prior to making the change. But the final staffing levels are determined by performing the analyses in these implementation plans, you know, which the staff has reviewed and approved. And then they're -- the validation is done as part of the integrated systems validation that was described earlier.

And finally, this integrated systems validation is one of the ITAAC that is performed by the staff for this chapter. Yes?

MEMBER STETKAR: Any of the -- this is cast on this slide in the sense of staffing, which is human bodies.

MR. SANTOS: Yes.

MEMBER STETKAR: It also has a substantial effect on the actual hardware because the hardware design that is described in Chapter 18 includes separate consuls each of those five people.

MR. SANTOS: Right.

MEMBER STETKAR: The layout, the distribution of the main control room would change. So it's not just a number of licensed bodies staffing in the sense of how many people do I have to respond to an accident.

MR. SANTOS: Right.

MEMBER STETKAR: It's a rather significant change to the hardware. And it might be a change to things like not just the consul for that electrical operator, which is the same as the other reactor operators. But in principle, depending on how you read it -- reconfigure the control room, it can have effects design and layout of the large display panel visibility from different places -- I mean, it isn't just as simple as saying well, I only need two licensed reactor operators to cope with any accident.

MR. SANTOS: Right.

MEMBER STETKAR: Which is -- it is okay, I get it. But again, a COL applicant needs to know pretty clearly going in what their challenges will be.

MR. SANTOS: Right.

MEMBER SKILLMAN: And then let me ask this, is this change at Tier 2 for the additional operator -- the electrical operator -- related to the prior slide regarding Tier 2 Star?

MR. SANTOS: No.

MEMBER SKILLMAN: Or is this unique -- just Tier 2 information?

MR. SANTOS: No, the prior slide -- I thought -- tried to identify any Tier 2 Star information in Chapter 18, which is different from this --

MEMBER SKILLMAN: Okay.

MR. SANTOS: Tier 2 information because the number 5 is clearly Tier 2 information in the DCD.

MEMBER SKILLMAN: Okay, thank you. I understand the difference ---

MR. SANTOS: Right, right.

MEMBER SKILLMAN: I was just trying to understand whether or not the prior slide ---

MR. SANTOS: Yes, no there's no ---

MEMBER SKILLMAN: Connection and it was very subtle.

MR. SANTOS: No, no. Right, right.

MEMBER SKILLMAN: Thank you. All right.

MEMBER KIRCHNER: So how significant a departure would this be? I mean, one can make the analogy to what the air lines went through. They used to have three in the cockpit. They eliminated the engineer. They combined the functions between the pilot and the copilot. Obviously, that was aided by advances in INC and control system technology.

But given that everything we've seen to date with this INC chapter 7 indicates, you know, three operators. And as John pointed out, there is some -- just not that, it is going to impact the load on each of the operators and such. So if a COL applicant comes in and looks for a departure, what gets restarted in the system? Do you do the HIP program over again? Lauren, do you want --

MS. KENT: This is Lauren Kent sitting here, I'd like to address the topic. So if you look at the -- look here, this slide is providing some information -- follow-up to a question that was raised during the subcommittee meeting. So the information we are talking about is an assumption -- the initial staffing assumption that -- so KHNP has said based on the design that is the predecessor plant that this design concept is based on, Shin Kori 3 and 4. In Shin Kori 3 and 4 there is a desk, a consul, in the control room for an electrical operator, which is a non-licensed operator.

So the initial assumption -- and in this initial assumption is that the APR1400 will need three licensed operators. So the assumption changes a bit from what is in Shin Kori. It goes from a non-licensed operator to a licensed operator. Initial staffing assumption is an input to the process described in the staffing qualifications implementation plan, which describes in part a set of activities that are performed to determine the staffing level for the design that will be licensed through this process.

So we are talking about, first of all, a hypothetical situation where a COL wants to change the initial assumption from three licensed operators to two for their initial -- the initial assumption used for the activities that are then performed in accordance with the implementation plans. The implementation plans that -- the results of performing those activities may demonstrate that indeed you do need this number of licensed operators available in the control room. It may not.

But we are talking about changing an initial assumption or an input, not changing the staffing level for the APR1400 which has yet to be determined, and will be determined through performing the activities in the implementation plans.

MEMBER STETKAR: Walt, I think the answer to your question is if they had done any of the human factors engineering design and implementation as part of the design certification, they would need to redo it.

MEMBER KIRCHNER: Yes.

(Simultaneous speaking)

MEMBER STETKAR: Oh, yes.

MEMBER KIRCHNER: They'd have to redo the whole thing.

MS. KENT: And with respect to the scope of evaluating such a departure, departures in the COL application of this nature with Tier 2 need to be identified, but you do not need staff approval to proceed with departure of this significance.

MEMBER STETKAR: That's -- just on the record, and we are short on time -- I find that rather surprising when we are talking about main control room staffing and configuration of the hardware in the main control room. And I will just leave it there.

MS. KENT: Well let's be clear though, what we are talking about -- which is an initial staffing assumption -- it is an input to a process. The process needs to be implemented to arrive at what the APR1400 control room configuration and staffing is. So that is the difference. We are talking about an initial assumption versus what has yet to be determined, which would have a separate change process. You would have to re-perform analyses once you had already established what the configuration was. They have not established that, is my point.

(Simultaneous speaking)

MEMBER KIRCHNER: I was going to make a philosophical comment, something on the order I did during the subcommittee meeting. I will repeat it here.

What bothers me in all this is that it's like the human factors engineering program is a retroactive, retrospective implementation rather than a forward-looking design implementation. So it is coming at the end of the process basically forcing the human element to fit the as-built machine. Not thinking ahead to build the machine with the human element in mind. And something like this, where you substantially change the operating crew configuration and the display panels is, in my mind, it is a significant departure.

MS. KENT: Well, just to clarify, so Mr. Stetkar said something earlier that I would like to quote. He said he had come to the conclusion that all of Chapter 18 was DAC. And he is not wrong. So all of Chapter 18 is DAC. And the explanation for that, if you would like to hear our reasons why that is -- first of all, we are doing the design certification now. That is the process we are in.

The Applicant has chosen to provide implementation plans that contain the design acceptance criteria in lieu of providing the control room design for the APR1400. So additionally, the staff asked an RAI and asked the Applicant to state who would be completing the results summary reports?

Results summary reports are the reports that are generated that describe the results of executing the activities in the implementation plans. And the Applicant stated the COL is responsible for performing and completing the result summary reports. Thereby the staff concludes the COL is responsible for performing all of these activities.

And then Mr. Bley raised a point earlier about translation. KHNP is saying we have a predecessor design -- and I realize I sound like I am speaking for KHNP, but this my interpretation of their application as I reviewed it. They have said this is our predecessor design, however, although that predecessor design has -- certainly has a control room design because it is operating, there are aspects of that design that have not been -- were not developed in accordance with U.S. standards, which are those standards in NUREG-711.

In order to avoid simply translating what exists in Korea into English and expecting that to work for U.S. operators, they have not proposed to do that. Rather, they have proposed to take their Korean design -- certainly there will be some kind of translation such that you can go forth and execute these implementation plans. But they are going to go through all of the elements in NUREG-711, which is what is captured in those implementation plans. And when I say they, I mean the COL applicant, to be clear. Because KHNP did not provide results, they provided implementation plans. And that is what we are reviewing at this stage.

Which is also why the ITAAC are necessary because when an applicant provides design acceptance criteria, which are contained in these implementation plans, we need the ITAAC to verify the completion of the design in accordance with the approved implementation plans. So the process that we have here is a design based on a predecessor plant that a COL applicant will complete the activities in these implementation plans, which encompass all of those described in the HFE program review model in NUREG-711.

And through that process there will certainly be, as we would expect, changes to be made from the Korean design in order to facilitate safe operation in a U.S. plant. Part of their process, as described in HSI design plan, is to develop a prototype here in the United States based on the

Korean design and have U.S. licensed operators run through several scenarios using the prototype based on the Korean design.

And that allows an opportunity specifically for cultural differences to be -- to be accounted for. Those operators get to provide feedback on -- perhaps, say the way in which the alarms sound, the say in which the alarms are presented, the way in which certain information is presented or how they have to perform certain tasks. And that is used as feedback into the process.

So I hope I have clarified. The DAC is -- all of Chapter 18 is DAC.

MEMBER KIRCHNER: No, I think I understood that. I will go back to a point I raised with KHNP on other aspects of this design certification. And if that is -- and for example, if we are not looking at operating experience until after the design is complete, with cosmetics aside I -- what the sound levels are on the display panels and such to me is cosmetic.

It is important for human factors, but that, yes, can easily be adjusted later. But substantive improvements based on the operating experience of the KHNP 3 and 4 will be -- you know, where does that enter the program?

MS. KENT: That -- so ---

MEMBER KIRCHNER: It enters the program after we have evaluated the design certification. So substantive changes to the plant are not likely to happen. Likewise, there probably is, I would guess, a PRA for the KHNP rep? Sorry, Shin Kori 3 and 4, which would be very useful to data mine to look at risk-important human actions and opportunities for improvements. Btu I see this all coming downstream well after the substantial part of the hardware of the plant has been designed. Maybe with the exception of the switch yards and some other aspects of the actual sighting.

So I will let it go at that.

MS. KENT: So with respect to operating experience, the operating experience implementation plan talks about collecting recent operating experience that has -- could be gained from operators at Shin Kori 3 and 4. And using that as an input to the ---

(Simultaneous speaking)

MEMBER KIRCHNER: Yes, but it's just not the control room and the control panel ---

MS. KENT: Right.

MEMBER KIRCHNER: Layout that I am talking about. I am talking about the actual plant as an integrated --

MS. KENT: So it sounds like your concern is ---

MEMBER KIRCHNER: Integrated system.

MS. KENT: Changes to the design that are coming later in the design process? Is that your concern? I just want to understand the concern.

MEMBER KIRCHNER: That they may not make any significant changes based on what they learn. I should let it go at that. I just feel that this exercise in human factors engineering at this point is too retrospective and not forward looking.

MR. SANTOS: Okay. We will continue on to the conclusions slide. So for the Phase 2 SER staff concluded that there is reasonable assurance that the design process described in the application conformed to HFE guidance and will result in a design that supports that safe plant operation. But however the staff is waiting for KHNP to respond the six RAIs that was described earlier and that these responses will be incorporated into the SER and will have to be resolved before the Phase 4 SER is issued. So we hope to able to discuss the resolutions of these issues with you in the Phase 5 meeting early next year. And that concludes the staff's presentation unless anyone has any other questions.

MEMBER BALLINGER: Any questions? Now is it appropriate to go to the room? And then outside?

CHAIRMAN BLEY: Exactly appropriate.

MEMBER BALLINGER: Exactly appropriate. So are there any comments from the room? And I think we are getting the phone line, if it isn't already open, open. Hard to tell.

I didn't hear the crackling. Are there anybody on the phone line that would wish to make a comment?

(No response.)

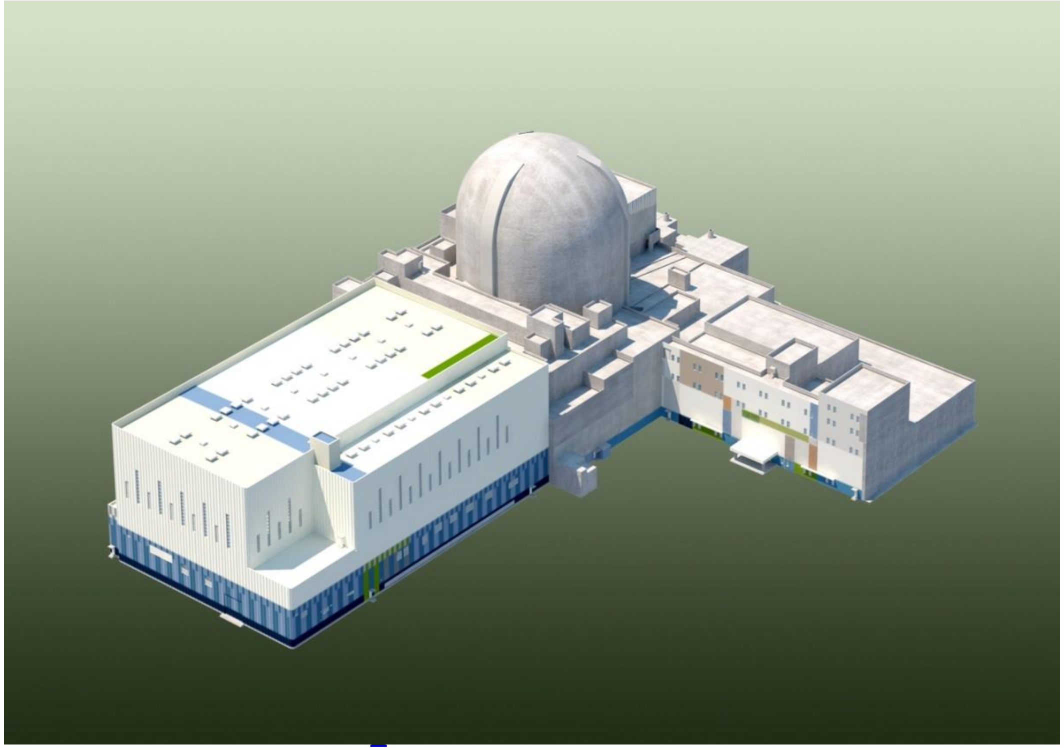
MEMBER BALLINGER: Hearing none, and assuming that the phone line is open --- it is? Then I think we are okay. And I will turn it back to you, Mr. Chairman.

CHAIRMAN BLEY: Thank you. At this time we are going to go off the record and then we will reconvene for the committee to discuss its upcoming meeting with the commission next month. We are off the record.

(Whereupon, the above-entitled matter went off the record at 11:12 a.m.)

NON-PROPRIETARY

APR1400 DCA
Chapter 7: Instrumentation and Controls



ACRS Full Committee Presentation
KEPCO/KHNP
September 7, 2017

ACRS Meeting (September 7. 2017)

Contents

- Overview of Chapter 7 (Section Overview)
- Related Document Submitted
- Section Summary
- Acronyms

Overview of Chapter 7 (Section Overview)

Section	Major Contents
7.1 Introduction	Introduction (Identification, Criteria)
7.2 Reactor Trip System	System Description, Design Basis, Analysis
7.3 Engineered Safety Features Systems	System Description, Design Basis, Analysis
7.4 Systems Required for Safe Shutdown	System Description, Design Basis, Analysis
7.5 Information Systems Important to Safety	System Description, Design Basis, Analysis
7.6 Interlock Systems Important to Safety	System Description, Design Basis, Analysis
7.7 Control Systems Not Required for Safety	System Description, Design Basis, Analysis
7.8 Diverse Instrumentation and Control Systems	System Description, Design Basis, Analysis
7.9 Data Communication Systems	System Description, Design Basis, Analysis

Related Documents Submitted

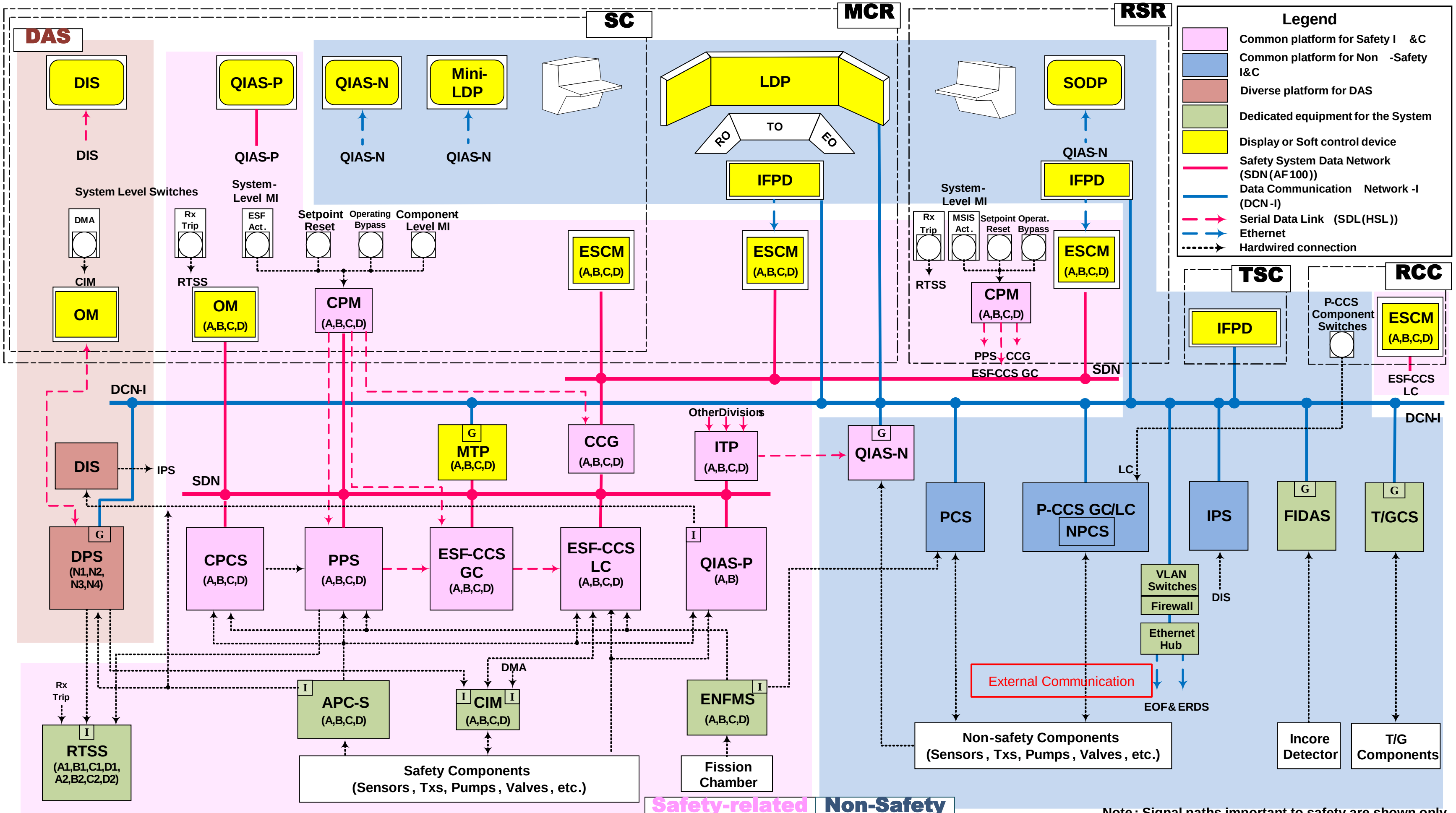
Document No.	Title	Rev.	Type
APR1400-Z-J-NR-14001-P & NP	Safety I&C System	1	IBR
APR1400-Z-J-NR-14002-P & NP	Diversity and Defense-in-Depth	1	IBR
APR1400-Z-J-NR-14003-P & NP	Software Program Manual	1	IBR
APR1400-Z-J-NR-14004-P & NP	Uncertainty Methodology and Application for Instrumentation	1	IBR
APR1400-Z-J-NR-14005-P & NP	Setpoint Methodology for Plant Protection System	1	IBR
APR1400-Z-J-NR-14012-P & NP	Control System CCF Analysis	1	IBR
APR1400-Z-J-NR-14013-P & NP	Response Time Analysis of Safety I&C System	1	IBR
APR1400-Z-A-NR-14019-P & NP	CCF Coping Analysis	1	IBR
APR1400-E-J-NR-14001-P & NP	Component Interface Module	1	IBR
APR1400-E-J-NR-16001-P & NP	Selection of Accident Monitoring Variables	0	TER
APR1400-F-C-NR-14001-P & NP	CPC Setpoint Analysis Methodology for APR1400	0	IBR
APR1400-F-C-NR-14002-P & NP	Functional Design Requirements for a Core Operating Limit Supervisory System for APR1400	0	IBR
APR1400-F-C-NR-14003-P & NP	Functional Design Requirements for a Core Protection Calculator System for APR1400	1	IBR
APR1400-A-J-NR-14003-P	APR1400 Disposition of Common Q Topical Report NRC Generic Open Items and Plant Specific Action Items	0	IBR
APR1400-A-J-NR-14004-P	Common Q Platform Supplemental Information in Support of the APR1400 Design Certification	0	IBR

*TER: Technical Report, **IBR: Incorporated by Reference

7.1 Introduction (Design Features)

- I&C systems are fully digitalized with proven technology.
- I&C systems use three major diverse platforms;
  - Safety system : programmable logic controller
  - Non-safety system : distributed control system
  - Diverse actuation system : FPGA-based logic controller
- Data communication systems maintain independence between each divisions, between safety system and non-safety systems.
- Software common cause failures are analyzed.
  - Safety system
  - Non-safety control system
- The design of I&C systems complies with related 10 CFR 50, RGs, IEEE standards, and ISGs.

7.1 Introduction (Overview Architecture)



Note: Signal paths important to safety are shown only

APC-S: Auxiliary Process Cabinet - Safety
CCG: Control Channel Gateway
CIM: Component Interface Module
CPCS: Core Protection Calculator System
CPM: Control Panel Multiplexer
DAS: Diverse Actuation System
DIS: Diverse Indication System
DCN-I: Data Communication Network -Information
DMA: Diverse Manual ESF
DPS: Diverse Protection System
ENFMS: Ex-core Neutron Flux Monitoring System
EOF: Emergency Operation Facility
ERDS: Emergency Response Data System
ESCM: ESF-CCS Soft Control Module
ESF-CCS: Engineered Safety Features - Component Control System
FIDAS: Fixed In-core Detector Amplifier System
G: Gateway
GC: Group Controller
I : Isolator
IFPD: Information Flat Panel Display
IPS: Information Processing System
ITP: Interface and Test Processor
LC: Loop Controller
LDP: Large Display Panel
MCR: Main Control Room
MI: Minimum Inventory
MTP: Maintenance and Test Panel
NPCS: NSSS Process Control System
MSIS: Main Steam Isolation System
OM: Operator Module
P-CCS: Process-Component Control System
PCS: Power Control System
PPS: Plant Protection System
QIAS-P/N: Qualified Indication & Alarm System – P / Non-safety
RCC: Remote Control Center
RSR: Remote Shutdown Room
RTSS: Reactor Trip Switchgear System
Rx: Reactor
SC: Safety Console
SODP: Shutdown Overview Display Panel
T/GCS: Turbine/Generator Control System
TSC: Technical Support Center , Txs: Transmitter

Rev.1

ACRS Meeting (September 7. 2017)

7.1 Introduction (Design Features)

- I&C systems configuration

Systems	Safety	Non-Safety	Diverse
Human System Interface	• Minimum Inventory Switches • ESCM	• IFPD	• DIS • DMA Switches
Processing Systems	• QIAS-P	• IPS • QIAS-N	
Control System	• PPS • CPCS • ESF-CCS	• P-CCS • PCS	• DPS
Data Communication System	• SDN • SDL	• DCN-I Network	

7.2 Reactor Trip System : PPS

- **Functions (Plant Protection System)**
  - **Protects core fuel design limits and reactor coolant system pressure boundary following anticipated operational occurrences.**
  - **Provides assistance in mitigating the consequences of PAs.**
- **Design features**
  - **Provides auxiliary support features such as operating bypass, setpoint reset, trip channel bypass, and surveillance testing.**
- **Westinghouse NSAL-17-2 (July 5, 2017)**
  - **The letter states *"AC160 Processor Module Stall Timers is not activated as described in licensing basis."***
    - **The stall timer provides diagnostic functions following a severe software fault and is not required for the system to perform its safety-related functions. Despite that this feature had not been activated as intended, Westinghouse concluded that there is no impact to the safety-related function or operability of the affected safety systems.**
  - **The APR1400 design is based on the currently licensed Common Q design.**
    - **Should the licensing basis be changed, the COL applicant will address the change.**

7.2 Reactor Trip Systems : CPCS

- **Functions (Core Protection Calculator System)**
  - Protects reactor core integrity from exceeding safety limit during plant operation.
  - Calculates departure from nucleate boiling ratio (DNBR) and local power density (LPD) values and generates trip signals to PPS whenever DNBR and LPD exceed the trip setpoint.

- **CPU load test**
  - An ITAAC (Table 2.5.1-5 item 27) will be included to provide the commitment to satisfy CPU load restrictions.
  - The CPCS is designed to meet the 75% CPU load restrictions by the vendor.
  - APR1400 CPCS is identical to the Barakah NPP (BNPP) CPCS. The BNPP tests demonstrated that the CPCS CPU shows deterministic behavior when CPU load is increased to 75%.
  - The RAI 7887-7.1-25 response was revised to include the results of BNPP CPU load test.

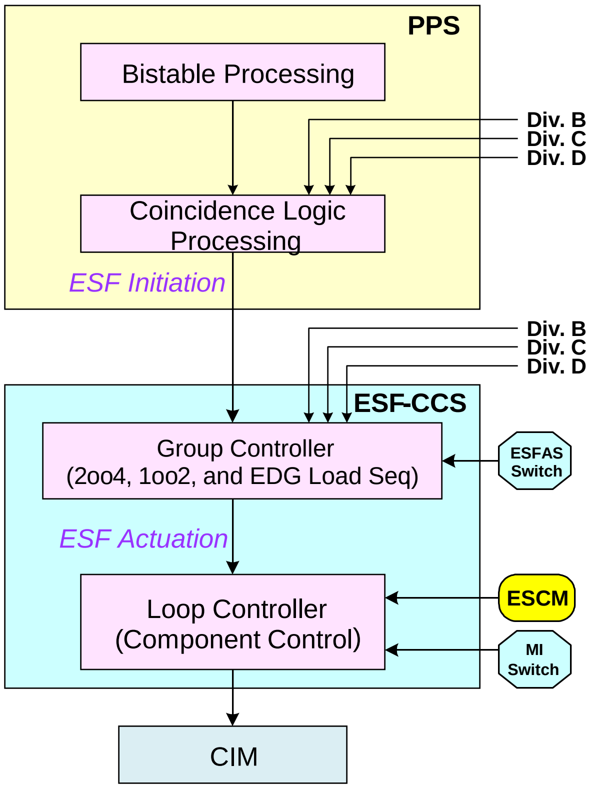
7.3 Engineered Safety Features System

• Functions

- Serves as interface between ESFAS portion of PPS and field actuated devices.
- Provides; discrete and modulation control of safety systems, and automatic and manual control of ESF systems.

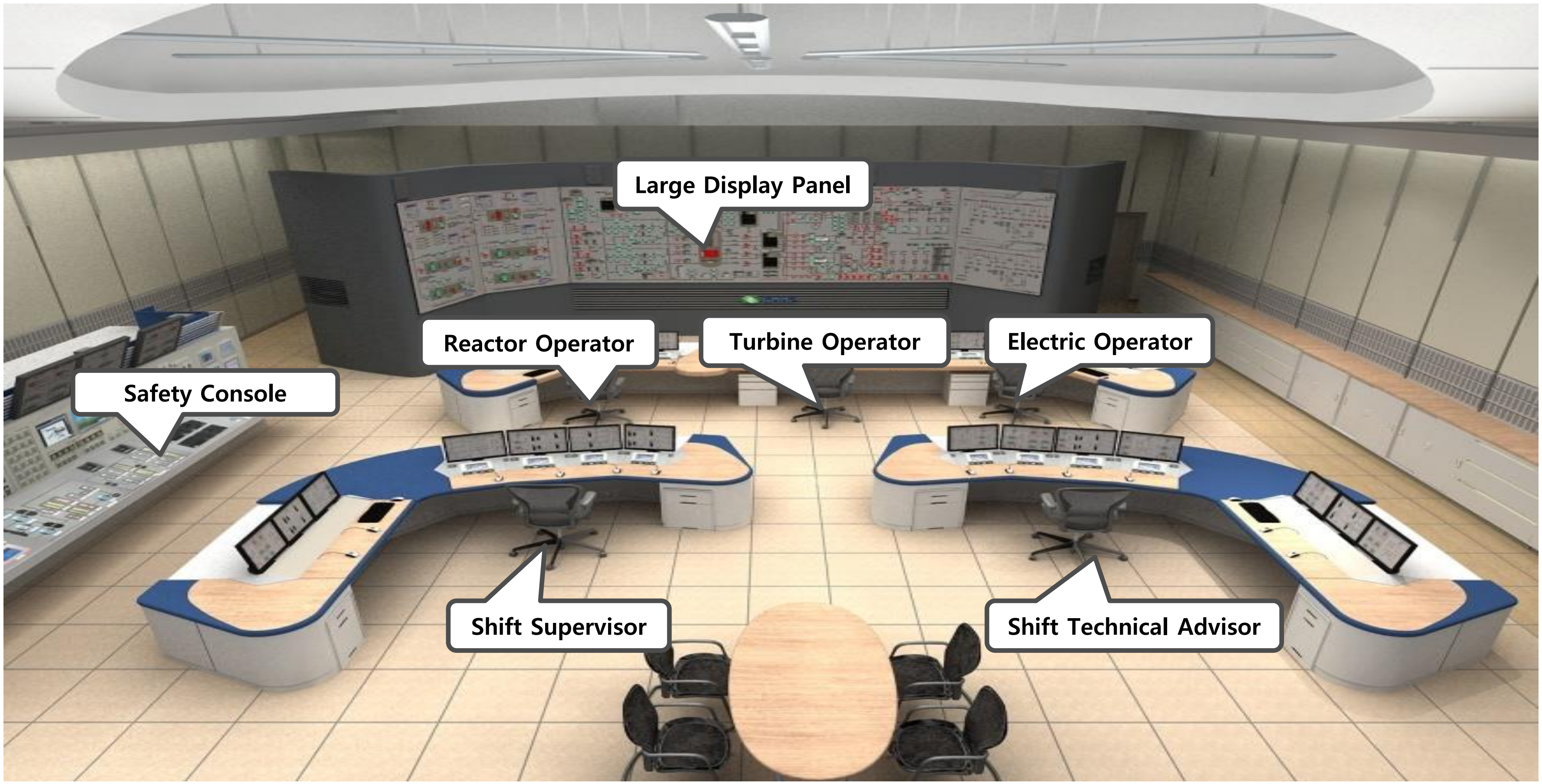
• Design features

- Consists of group controllers, loop controllers, safety data communication systems, safety-grade soft control (ESCM), and gateways.
- Has four independent divisions which are physically separated and electrically isolated.



7.4 Systems Required for Safe Shutdown

- Main control room (MCR)



7.4 Systems Required for Safe Shutdown

- **Functions (MCR)**
  - **Provides all human system interface devices to operate the plant safely under all conditions and maintains plant in a safe condition under design basis accident.**
- **Design features (MCR)**
  - **MCR is composed of operator consoles, large display panel (LDP), and safety console.**
- **Functions (Remote Shutdown Room: RSR)**
  - **Provides control and monitoring means against fire unlikely event that MCR becomes uninhabitable to achieve hot standby, hot shutdown, and cold shutdown.**
- **Design features (RSR)**
  - **Remote shutdown console has identical design with operator console of MCR**
  - **Shutdown overview display panel is similar to system mimic displays of LDP.**

7.5 Information Systems Important to Safety : QIAS-P

- **Functions (Qualified Indication and Alarm System-P)**
  - Displays accident monitoring instrumentation (AMI) Types A, B, and C variables (RG 1.97).
  - Indicates the approach to and the recovery from inadequate core cooling (ICC) (NUREG-0737).
  - Displays AMI variables (channel A, B) at safety console (except 4 channel containment isolation valve status).

- **Design features**
  - The QIAS-P provides the continuous real-time display for AMI Type A and B variables.
  - The IPS displays ICC variables as a primary on the LDP and the QIAS-P displays the variables as a backup.

7.6 Interlock Systems Important to Safety

- Functions (interlocks required to:)
  - Prevent over-pressurization of low-pressure systems.
  - Prevent over-pressurization of the reactor coolant system during low-temperature operations of the reactor vessel.
  - Assure the availability of safety injection tanks.
  - Assure the availability of component cooling water supply and return header tie line isolation.
- Design features
  - Shutdown cooling system suction line isolation valve interlocks
  - Shutdown cooling system suction line relief valve interlocks
  - Safety injection tank isolation valve interlocks
  - Component cooling water supply and return header tie line isolation valve interlocks
  - Component cooling water cross connection line isolation valve interlocks

7.7 Control Systems Not Required for Safety

- **Functions**
  - **Maintain process variables and systems within normal operational limits.**
- **Design features**
  - **Physical separation and electrical isolation from safety systems.**
  - **Control system CCF analysis to confirm that the event consequences of Chapter 15 are still effective and the acceptance criteria are met.**
- **Major control systems**
  - **Power control system**
  - **Process – component control system**

7.8 Diverse Instrumentation and Control Systems

- **Functions**
  - ➢ **Diverse I&C systems (DPS, DIS, DMA Switches) have sufficient diversity and defense-in-depth to tolerate;**
    - **ATWS (10 CFR 50.62)**
    - **Safety systems software common cause failure**
- **Design features**
  - ➢ **DPS provides diverse reactor trip, turbine trip, auxiliary feedwater actuation, and safety injection actuation functions.**
    - **Consists of four channels.**
    - **Diverse (compared with the PPS) from sensor output to shunt trip coils of RTSS trip circuit breaker,**
    - **Diverse from sensor output to the CIM for the ESF actuation of auxiliary feedwater and safety injection.**

7.9 Data Communication Systems

- **Functions**
  - Provide data transfer between digital I&C systems.
- **Design features**
  - Three major data communications (SDL, SDN, DCN-I) with different protocols
  - Deterministic behavior for safety system
  - Communication independence is analyzed in the Safety I&C System TeR as per ISG-04.
- **External data communication**
  - Plant data from the IPS are externally sent to the EOF, the NERC, and to the NRC operations center via a unidirectional hardware based firewall implemented by a fiber optic link (NUREG-0696).
  - A VLAN switch provides a link interface to each external location.

Summary

- In Chapter 7, the design features of the instrumentation and control system of the APR1400 are described.
- The functions and design features are presented.
- Key features (e.g., WDT, CPU load test, continuous display, external communication) are explained.
- The design complies with related 10 CFR 50, RGs, IEEE standards, and ISGs.

Attachment : Acronyms

AMI	accident monitoring instrumentation
CCF	common cause failure
CPU	central processing unit
DCN-I	data communication network - information
DNBR	departure from nucleate boiling ratio
EOF	emergency operation facility
ESCM	ESF-CCS soft control module
IFPD	information flat panel display
FPGA	field programmable gate array
ICC	inadequate core cooling
LPD	local power density
NERC	nuclear emergency response center
NSAL	nuclear safety advisory letter
PLC	programmable logic controller
SDL	serial data link
SDN	safety system data network
VLAN	virtual LAN
WDT	watch dog timer

* Other acronyms are shown in page 5.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Presentation to the ACRS Full Committee

Korea Hydro Nuclear Power Co., Ltd (KHNP)
APR1400 Design Certification Application Review

Phase 2 Safety Evaluations for Chapters 7 and 18

September 7, 2017

Chap 7 – Instrumentation & Controls

- **The staff focused on the following items:**
  - Independence
  - Deterministic Performance
  - Diversity & Defense in Depth
  - Redundancy
  - Setpoint and CPC Setpoint Methodology
  - Control System Failure Analysis
  - Post Accident Monitoring Variables

- **Phase 2 SER contained 33 Open Items and 109 Confirmatory Items**

Chap 7 – Instrumentation & Controls

- **At this time, there are five Open Items**
- **The key issues remaining concern the following topics:**
  - Setpoint Methodology
  - Restrictive Setpoints
  - SDOE Vulnerability Analysis
  - PAM Variables (selection justification)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

List of Acronyms

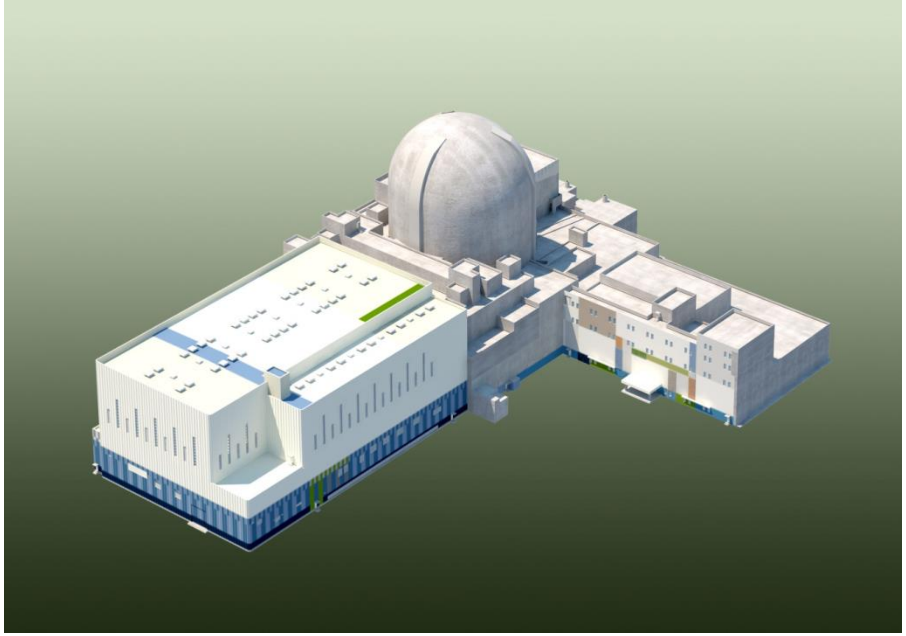
- CPC: Core Protection Calculator
- PAM: Post Accident Monitoring
- SDOE: Secure Development and Operational Environment

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Discussion / Committee Questions

NON-PROPRIETARY

APR1400 DCA
Chapter 18: Human Factors Engineering



KEPCO/KHNP
September 7, 2017

ACRS Meeting (September 7, 2017)

Contents

NON-PROPRIETARY

Overview of Chapter 18

❑ Section Overview

Section	Title
18.1	Human Factors Engineering Program Management
18.2	Operating Experience Review
18.3	Functional Requirements Analysis and Function Allocation
18.4	Task Analysis
18.5	Staffing and Qualifications
18.6	Treatment of Important Human Actions
18.7	Human-System Interface Design
18.8	Procedure Development
18.9	Training Program Development
18.10	Human Factors Verification and Validation
18.11	Design Implementation
18.12	Human Performance Monitoring

Overview of Chapter 18

❑ List of Submitted Documents

Document No.	Title	Revision	Type
APR1400-K-X-FS-14002-P and NP	Design Control Document TIER 2 Chapter 18, Human Factors Engineering	1	DCD
APR1400-E-I-NR-14001-P and NP	Human Factors Engineering Program Plan	1	IBR
APR1400-E-I-NR-14002-P and NP	Operating Experience Review Implementation Plan	1	IBR
APR1400-E-I-NR-14003-P and NP	Functional Requirements Analysis and Function Allocation Implementation Plan	1	IBR
APR1400-E-I-NR-14004-P and NP	Task Analysis Implementation Plan	1	IBR
APR1400-K-I-NR-14005-P and NP	Staffing and Qualifications Implementation Plan	1	IBR
APR1400-E-I-NR-14006-P and NP	Treatment of Important Human Actions Implementation Plan	1	IBR
APR1400-E-I-NR-14007-P and NP	Human-System Interface Design Implementation Plan	1	IBR
APR1400-E-I-NR-14008-P and NP	Human Factors Verification and Validation Implementation Plan	1	IBR
APR1400-K-I-NR-14009-P and NP	Design Implementation Plan	1	IBR
APR1400-E-I-NR-14010-P and NP	Human Factors Verification and Validation Scenarios	1	TER
APR1400-E-I-NR-14011-P and NP	Basic Human-System Interface	1	IBR
APR1400-E-I-NR-14012-P and NP	Style Guide	1	IBR

* TER: Technical Report, **IBR: Incorporated by Reference

Overview of Chapter 18

- **Goal of the HFE program is to ensure that the HSI design is properly developed and effectively implemented.**

  - **HFE Program Criteria**
    - The APR1400 HFE program complies with NUREG-0711 revision 3.
  - **HFE Program Duration**
    - The APR1400 HFE program has been in effect from the start of the APR1400 design.
    - It will continue through completion of initial plant start up.
    - The licensee will continue the HFE program in accordance with NUREG-0711 human performance monitoring program.

Overview of Chapter 18

ISV | CHT/ HFT | FL

No	HFE Program Element	DC Application	COL Application	Operation
1	HFEPP	HFEPP◆		
2	OER	IP◆	ReSR	
3	FRA/FA	IP◆	ReSR	
4	TA	IP◆	ReSR	
5	S&Q	IP◆	ReSR	
6	TIHA	IP◆	ReSR	
7	HD	IP◆	ReSR	
8	*Procedures*		*Procedure*	
9	*Training*		*Training Program*	
10	*Simulator*		*Simulator*	
11	HF V&V	IP◆	ReSR	
12	DI	IP◆	ReSR	
13	HPM		HPM IP	

◆ milestone HFE activity other activity

ITAAC CLOSE

ISV : Integrated System Validation
CHT : Cold Hydro Test
HFT : Hot Function Test
FL : Fuel Load

NON-PROPRIETARY

Treatment of Important Human Actions

Criteria

- NUREG-0711, Criterion 7.4(1), states: "The applicant should identify risk-important human actions (RIHAs) from the probabilistic risk assessment/human reliability analysis (PRA/HRA)."

Issues

- Some aspects of the site-specific PRA will likely not be determined until fuel load, which occurs after the control room has been constructed.
- The application does not address how the RIHAs identified from the site-specific PRA (e.g., seismic PRA) are implemented in the HFE program.

Treatment of Important Human Actions

❑ Preliminary Observation

- Design changes, including new RIHAs, identified after the HF V&V completion are implemented using HED resolution process of the HFEPP,
- The HED resolutions will be verified in the Design Implementation (DI) program element.
- Design changes after DI will be resolved using COLA's corrective action program.

❑ Resolution

- KHNP is working with the Staff to resolve this issue.

HFE ITAAC

❑ Criteria

- The design acceptance criteria (DAC) are to be objective (measurable, testable, or subject to analysis using pre-approved methods), and must be verified as a part of the inspections, tests, analyses, and acceptance criteria (ITAAC) performed to demonstrate that the as built facility conforms to the certified design.

❑ Issues

- HFE ITAAC is limited to only ISV and Design Implementation, and there are no other HFE ITAAC in the application to verify the completion of the other HFE activities.

HFE ITAAC

❑ Preliminary Observation

- In accordance with the HF V&V IP, completion of HFE analysis and designs are pre-requisites for the ISV start.
  - These are inherently encompassed by the ISV ITTAC.
- DI verifies any design changes that occur after the ISV and remaining as-built HSI design issues that can not be verified during the ISV.

  (e.g., MCR noise level, lighting level etc.)

❑ Responses

- KHNP is working with the Staff to resolve this issue.

NON-PROPRIETARY

HFE Program Milestones

ISV | CHT/ HFT | FL

No	HFE Program Element	DC Application	COL Application	Operation
1	HFEPP	HFEPP◆		
2	OER	IP◆	ReSR	
3	FRA/FA	IP◆	ReSR	
4	TA	IP◆	ReSR	
5	S&Q	IP◆	ReSR	
6	TIHA	IP◆	ReSR	
7	HD	IP◆	ReSR	
8	*Procedures*		*Procedure*	
9	*Training*		*Training Program*	
10	*Simulator*		*Simulator*	
11	HF V&V	IP◆	ReSR	
12	DI	IP◆	ReSR	
13	HPM		HPM IP◆	

ISV : Integrated System Validation
CHT : Cold Hydro Test
HFT : Hot Function Test
FL : Fuel Load

◆ milestone | HFE activity | other activity

ITAAC CLOSE

ACRS Meeting (September 7, 2017)

Procedures for ISV

❑ Criteria

- NUREG-0711, Criterion 11.4.3.3 (1) states, “The applicant’s testbed should represent completely the integrated system. It should include HSIs and procedures not specifically required in the test scenarios.”

❑ Issues

- The scope of the HSI Design (HD) for computer-based procedure (CBP) conversion is limited to the procedures used during the ISV.
- All other procedures should be converted to CBPs within the HD program element.

Procedures for ISV

❑ Preliminary Observation

- The operating procedures prepared and converted to CBPs for the ISV include procedures directly used in the ISV scenarios.
- Other procedures specifically included to ensure the CBP inventory does not influence operator decisions.
  - These procedures will be converted to CBP per the COLA's procedure development program.

❑ Responses

- KHNP is working with the Staff to resolve this issue.

Operating Experience Review

Criteria

- NUREG-0711, Criterion 3.4.1(2), states, “The applicant should address the HFE issues identified in NUREG/CR-6400 "HFE Insights For Advanced Reactors Based Upon Operating Experience".

Issues

- Operating experiences (OEs) with dates before the SKN 3&4 construction are assumed to be included in the APR1400 and are not screened again.
- How grouping OE into the categories used in NUREG/CR-6400 helps one to understand the similarities and differences between the OE lessons learned.

Operating Experience Review

❑ Preliminary Observation

- SKN 3&4 OE (up to 1996) was considered using the criteria of NUREG-0711.
  - Current OER IP (Rev. 1) includes INPO and WANO OE database.

- NUREG/CR-6400 provides expanded HFE design issue categories and proposed resolutions. OE grouping following this issue category helps designer to clarify his/her OE-related design issues and to decide the resolutions.

❑ Responses

- KHNP is working with the Staff to resolve this issue.

Site Specific Information

❑ Criteria

- NUREG-0711, Criterion 4.4(2), states, “The applicant’s FRA/ FA should be performed iteratively to keep it current during design development and operation up to decommissioning, so that it can be used as a design basis when modifications are considered.” Also, NUREG-0711, Criterion 5.4(8), states, “The applicant’s task analysis should be iterative, and updated as the design is better defined.”

❑ Issues

- Why it would be necessary to make generic assumptions during these activities when the COL applicant will be able to use site-specific information to develop the control room design at the site.

Site Specific Information

❑ Preliminary Observation

- The generic FRA/FA assumption provides the basis for the HSI design and supports an iterative process includes site-specific information as design develops.
- The Design Implementation program element requires confirming the application of the site specific assumptions or regression analysis to address any plant specific differences.

❑ Responses

- KHNP is working with the Staff to resolve this issue.

Summary

- In chapter 18, APR1400 HFE program has been established to satisfy the review criteria in NUREG-0711, Revision 3.
- KHNP has concluded that this will result in an acceptable HSI design.

Acronyms

CBP	computer-based procedure
COL	combined license
COLA	COL applicant
DAC	design acceptance criteria
DI	design implementation
FRA/FA	functional requirements analysis and function allocation
HF	human factors
HFE	human factors engineering
HFEPP	human factors engineering program plan
HRA	human reliability analysis
HSI	human system interface
ITAAC	inspections, tests, analyses, and acceptance criteria
ISV	integrated system validation
MCR	main control room
OER	operating experience review
PRA	probabilistic risk assessment
RIHA	risk-important human actions
TIHA	treatment of important human actions
V&V	verification and validation

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Presentation to the ACRS Full Committee

Korea Hydro Nuclear Power Co., Ltd (KHNP)
APR1400 Design Certification Application Review

Phase 2 Safety Evaluations for Chapters 7 and 18

SEPTEMBER 7, 2017

Chp 18 – Human Factors Engineering

- The staff reviewed the following items:
  - Conceptual design of the APR1400 HSI Design
  - Style Guide
  - HFE IPs
    - Describe the processes and methods to develop the APR1400 control room design (i.e., the DAC) using the conceptual design as the starting point
  - HFE-related ITAAC
- Phase 2 SER contains no open items and 55 confirmatory items

Chp 18 – Human Factors Engineering

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- 6 RAIs issued August 21, 2017, following consideration of issues raised during the APR1400 Subcommittee meeting on June 21, 2017
  - Use of PRA to identify important human actions
  - Identification of Tier 2*
    - SECY-17-0075 (Planned Improvements in Design Certification Tiered Information Designations)
  - Scope of procedures available during V&V activities
  - Operating experience
  - Use of generic vs site-specific assumptions
  - Intersystem leakage (Chapter 5 RAI)

Chp 18 – Human Factors Engineering

- Initial staffing assumption of 5 licensed operators is Tier 2 information in DCD
  - MCR crew includes an SS, STA, RO, TO, and EO
  - The EO position is unique compared to existing plants
- Change in Tier 2 identified as a departure in a COL application
- Final staffing level is the result of performing HFE implementation plans

Chp 18 – Human Factors Engineering

- Phase 2 SER Findings
  - The applicant's HFE design process conforms to NRC HFE-related guidance
  - The applicant's HFE design process provides reasonable assurance that HFE-related NRC requirements will be satisfied
- Staff waiting for KHNP responses to 6 RAIs issued in August 2017

Acronyms

COL: combined license
DAC: design acceptance criteria
DCD: design control document
EO: electrical operator
HFE: human factors engineering
HSI: human-system interface
IP: implementation plan
ITAAC: inspections, tests, analyses, and acceptance criteria
MCR: main control room

MCR: main control room
PRA: probabilistic risk assessment
RAI: request for additional information
RO: reactor operator
SER: safety evaluation report
SS: shift supervisor
STA: shift technical advisor
TO: turbine operator
V&V: verification and validation

Background Slides

NUREG-0711 HFE Program Elements

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Planning and Analysis	Design	Verification and Validation	Implementation and Operation
HFE Program Management	Human -System Interface Design	Human Factors Verification and Validation	Design Implementation
Operating Experience Review	Procedure Development		Human Performance Monitoring
Function Analysis & Allocation	Training Program Development		
Task Analysis			
Staffing & Qualification			
Treatment of Important Human Actions			