Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
APR1400 Subcommittee: Open Session

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Monday, June 20, 2017

Work Order No.: NRC-3135 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

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

APR1400 SUBCOMMITTEE

+ + + + +

MONDAY

JUNE 20, 2017

+ + + + +

OPEN SESSION

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., Ronald G. Ballinger, Co-Chair, presiding.

COMMITTEE MEMBERS:

RONALD G. BALLINGER, Co-Chair

MATTHEW W. SUNSERI, Co-Chair

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR., Member

WALTER L. KIRCHNER, Member

JOSE MARCH-LEUBA, Member

DANA A. POWERS, Member

GORDON R. SKILLMAN, Member

JOHN W. STETKAR, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTOPHER BROWN

CHRISTINA ANTONESCU

ALSO PRESENT:

TONY AHN, KHNP

JOSEPH ASHCRAFT, NRO

DAVID CURTIS, NRO

ISMAEL GARCIA, NRO

JAMES GILMER, NRO

DAWNMATTHEWS KALATHIVEETTIL, NRO

ALSO PRESENT (CONTINUED):

CHANGHO KIM, KHNP

HANG BAE KIM, KEPCO E&C

JINKU KIM, KHNP

JUNGHO KIM, KHNP

SEJUN KIM, KEPCO E&C

YOUNGGEUL KIM, KHNP

YEONGSU KIM, KHNP

YONGHUN KIM, KHNP

YOUNGLEI KIM, KEPCO E&C

YUN GOO KIM, KHNP

CAROLYN LAURON, NRO

JEONGHYEONG LEE, KEPCO E&C

DAEHEON LIM, KEPCO E&C

MIKE MCCOPPIN, NRO

KENNETH MOTT, NRO

WARREN ODESS-GILLETT, Westinghouse

EUNG SE OH, KHNP

JIYONG OH, KHNP

JAE HYUK PARK, KEPCO E&C

YOU SUNG RO, KEPCO E&C

CAYETANO SANTOS, NRO

ROB SISK, Westinghouse

DAVE WAGNER, KHNP

WILLIAM WARD, NRO

ALSO PRESENT (CONTINUED):

DEANNA ZHANG, NRO

JACK ZHAO, NRO

CONTENTS

P R O C E E D I N G S

8:30 a.m.

CO-CHAIR BALLINGER: Good morning. The meeting will now come to order.

This is a meeting of the APR1400 Subcommittee of the Advisory Committee on Reactor Safeguards. I'm Ron Ballinger, Chairman of the APR1400 Subcommittee.

ACRS members in attendance are Dick Skillman, Dana Powers. Matt Sunseri is here. Dennis Bley will be here shortly. John Stetkar, Jose March-Leuba, and Charlie Brown.

I might add that Jose is conflicted in two areas here, one related to setpoint methodology and another related to the core protection calculator. So, we have to be aware of that.

We also have our consultant Myron Hecht here with us, and Walt Kirchner just arrived.

The purpose of today's meeting is for the Subcommittee to receive briefings from Korea Electric Power Corporation and Korea Hydro & Nuclear Power Company regarding their design certification application and the NRC staff regarding their Safety Evaluation Report with open items specific to Chapter 7, Instrumentation and Control, and tomorrow we will review Chapter 18, Human Factors Engineering. And I understand that, if we finish today, we will try to make arrangements, if we can, to pick up, start on Chapter 18. Okay.

The ACRS was established by statute and is governed by the Federal Advisory Committee Act, FACA. That means that the Committee can only speak through its published letter reports. We hold meetings to gather information to support our deliberations.

Interested parties who wish to provide comments can contact our offices requesting time after the meeting announcement is published in The Federal Register. It already has.

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

I might add that, also, this will be open and closed sessions. And the handouts that are here for the members contain both proprietary and non-proprietary information, and we need to be sure that we collect the appropriate stuff at the end.

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

The rules for participation in today's meeting were announced in The Federal Register on Tuesday, June 14, 2017. Again, the meeting was announced open/closed public meeting, closed-to-the-public meeting. As noted in the agenda, certain parts of the meeting will be closed to the public to protect information proprietary to KHNP or its vendors.

No requests for making a statement to the Subcommittee have been received from the public.

A transcript of the meeting is being kept and will be made available, as stated in The Federal Register notice. Therefore, I request that participants in this meeting use the microphones located throughout the room when addressing the Subcommittee. Participants should first identify themselves, press the little button to make the green light come on, and speak with sufficient clarity and volume so that they can be readily heard.

We have a bridge line established for interested members of the public to listen-in. The bridge number and password were published in the agenda posted on the NRC website.

To minimize disturbance, this public line will be kept in the listen-only mode. The public will have an opportunity to make a statement or provide comments at a designated time toward the end of the meeting.

And now, I will turn it over to Bill Ward for some opening comments.

MR. WARD: Thank you, Dr. Ballinger.

KHNP and the Office of New Reactors are very pleased to present Chapters 7 and 18 today and tomorrow, as they represent something of a milestone for us. With the presentation of Chapter 18 tomorrow, this will be the completion of phase 3 Subcommittee presentations for all chapters. There's a couple of chapters to be presented to the full Committee still, but we are glad to get through all the Subcommittee meetings and be moving on in phase 4.

These two chapters also have a personal connection with me because I was the Chapter PM for both of them until I took on the role of Lead PM. So, I am fairly familiar with them.

But I won't delay any more and turn it back over.

CO-CHAIR BALLINGER: Okay. I guess we are ready, Rob.

MR. SISK: Again, thank you, Dr. Ballinger.

Yes, I do want to comment. We are looking into seeing what we can do on Chapter 18. We can't confirm anything yet, but we are looking to see what we can do.

With that, we are looking forward to a good discussion today on Chapter 7. And without further delay, I would like to introduce Jinku Kim, which will get us started on Chapter 7.

MR. J. KIM: Okay. Good morning, ladies and gentlemen. My name is Jinku Kim, working for KEPCO E&C.

We are very pleasured to have the introduction of our APR1400 I&C system to ACRS members. So, from this time, the Korean team will present the design description and the features of the I&C system for the APR1400.

In this open session, we will present the Sections 7.1, 7.4, 7.6, and 7.7 in sequence. As the first presentations, I would like to present Section 7.1 that addresses the overall design information of our APR1400 I&C systems.

This slide shows the sequence of the order of the sections in this open session. So, we will present 7.1, 7.4, 7.6, and 7.7.

APR1400 already submitted the document as shown on this slide.

So, the APR1400 I&C system used advanced design features. The I&C system fully complies with the proven technology in Korea and other countries. These I&C systems are implemented by three diverse platforms: the PSA platform used for the safety system, the non-safety, non-qualified distributed control system. These are used for the non-safety system and FPGA. The logic controller is applied into the diverse activation system. The other communication system maintains independence between each of the divisions, between the safety system and the non-safety systems.

The coping analysis of the common cause failure is performed for the safety system as well as the non-safety system. The design of the I&C system is to comply with the related 10 CFR 50, Reg. Guide, IEEE standard, and the interim safety guidance.

This picture shows an overall architecture diagram for I&C systems. The blue color boundary is here and here. The blue color boundary illustrates the non-safety systems, and the pink color boundaries illustrate the safety system. And the brown color boundary indicates the diverse activation system here.

As explained on the previous slide, APR1400 I&C systems are implemented by PLC, DCS, APP-based logic controller platform, and the independently-dedicated systems.

Non-safety control systems, with the blue-color boxes, are used with the DCS platform.

Safety and the protection system, with the pink-color boxes of the system, devices are implemented by the PLC, qualify the PLC platform.

The diverse supportive system, with the brown-color boxes of the system, is implemented by the FOPJ-based platforms.

And the green-color device, the green-color boxes indicate independently-dedicated systems, including the external here, external communication system for the emergency response facility.

The yellow-color device, the yellow-color boxes indicate the safety and non-safety human system interface devices.

The APR1400 I&C system also has a data communication system, the interconnecting various systems, and the components, such as the lighter dotted line, this line, the lighter dotted line is for the serial data link. The lighter solid line, this line, is the Safety System Data Network. Or we call it the SDM.

And the blue solid line, this line, the blue solid line indicates the non-safety Data Communication Network Information. We call it DCN-I.

And the blue dotted line, this line, the blue dotted line indicates the ethernet network.

MEMBER BROWN: May I ask you a question before you switch slides? Are you switching slides or not? Are you staying on this slide for a minute?

MR. J. KIM: Yes.

MEMBER BROWN: Yes, I had a question. When you talked about the green color being dedicated equipment for the system, I'm trying to remember back when I was reading. Does that fundamentally mean they are not software-based systems? Aren't those largely analog or relays, contact switches, and stuff like that?

MR. J. KIM: For example --

MEMBER BROWN: When you talk about the dedicated equipment for the CIM, the APCS --

MR. J. KIM: Yes. In case of the APCS and the CIM, this model is implemented by the analog devices.

MEMBER BROWN: Analog? Okay, thank you.

You answered my question. Thank you.

MR. J. KIM: Okay, okay.

MEMBER BROWN: I just wanted to confirm that. That's what my understanding was.

MR. J. KIM: Yes. And in case of the CIM devices, I will explain at Chapter 7.3 --

MEMBER BROWN: Thank you.

MR. J. KIM: -- in detail.

This table shows some of the hierarchical I&C system. At the human system interface level, this level, the main control room of the APR1400 provides a conventional hard-wired minimum switches and the segregator software control -- we call it the ESCM -- as a safety human system interface device system.

The Information Flat Panel Display, IFPD -- we call it IFPD -- that are non-safety devices are provided on the operator console.

The MCR also provides a diverse indication system and diverse manual ESCM activation switches as a diverse indication and the manual control devices.

At the processing system, the safety class QIAS-P, Qualified Indication and Alarm System, dash "P", QIAS-P, and the Non-Safety Information Processing System, and the QIAS, Qualified Indication Alarm System Non-Safety, QIAS-N, are provided.

At the control system level, the safety control and the protection system consist of a plant protection system, core protection calculator system, engineering adaptive features, the component control systems, and the processor component control system and the power control system are provided as a major system of the non-safety control system.

The Safety System Data Network, we call it the SDM, and the Serial Data Link, or SDL, and the DCN-I are applied for safety and the non-safety data communication systems.

That is my presentation on Section 7.1, yes.

MR. HECHT: Good morning, Mr. Kim. My name is Myron Hecht, and I am not a member of the Committee. I'm a consultant.

MR. J. KIM: Okay, thank you.

MR. HECHT: My question is -- and it may not be the right time to ask this question and, if so, please let me know -- but the DCN-I network is a ethernet-type network, and it involves non-safety as well as diverse systems. Have you considered the cybersecurity defenses that might be necessary for such a system?

MR. J. KIM: Okay. We were concerned

about cybersecurity as well as the SSDOE plan during the design development. And also, we finished the evaluation for the vulnerability of the SSDOE, about the whole I&C system.

MR. HECHT: Well, SSDOE is one aspect which relates to the development environment. I'm thinking more of the Reg Guide 5.71 type of requirements which refer to the need to define containment boundaries.

MR. J. KIM: Yes.

MR. HECHT: And I would imagine that part of those containment boundaries might be encryption and authentication on the DCN-I network.

MR. J. KIM: Yes.

MR. HECHT: I didn't see anything about that in the Chapter 7 description or in any of the supporting technical reports. Was that considered?

MR. J. KIM: During the licensing process, we considered for the security environment for the development pace. But we think for Reg Guide 5.71, we considered that guidance, a commitment for that guidance in the COL.

MR. HECHT: In the?

MR. J. KIM: COL.

MR. HECHT: COL?

MR. J. KIM: Yes.

MR. HECHT: All right. Perhaps we will learn more later in the briefing.

MEMBER BROWN: Okay. Let me amplify for a few minutes. It is relative to your figure here. And I had kind of the same question when I was going through this. It is one of the few areas where I had additional through processes or questions relative to my overall review.

He is talking about the authentication cycle. Cybersecurity 5.71, really I'm focused on you have got a number of networks, and it is really a 603.1991 function of control of access to those networks.

And what you do in your DCD and what you have described in the safety system I&C technical report, it largely discusses internal controls, supervisory controls, locks, keys to get into cabinets, and stuff like that, in terms of getting into the equipment, you know, the various systems. But there was no discussion in the DCD at all or in the other reports relative to external access or gateways into either the DCN, the QAIS, QIS network, or the SDN network in terms of how it communicates outside the plant boundaries, like to the internet.

So, we don't have to talk about that now.

The communications or network discussions, really I think it's Chapter or Section 7.9, or something like that. And I presume we will get to that at some point in the overall discussions.

But that is the thought process. It is really a control of access and how you do it. What is done off in the software development area when you are at the vendor's developing it, that is a whole other circumstances in terms of how you maintain the security of the systems and the software as it is being developed. So, I am trying to separate those two to keep them separate from each other, if I am being clear.

So, if we can talk about the control of access during the latter part of the meeting, that would be useful. I will also talk about it with the staff. They will be very happy to do that.

(Laughter.)

It's not like they haven't heard this before, and they will hear it again.

So, thank you very much. You can go ahead.

MR. J. KIM: Okay.

MR. RO: I am You Sung Ro of KEPCO E&C.

Let me explain about system required for safe shutdown. This is a picture of the APR1400 main control room. The instrumentation information displays and controls for safe shutdown are provided in the main control room.

The APR1400 main control room consists of control-based I&C system such as operator console, safety console, and RAS display panel.

The main control provides all human system interface devices to operate the plant safely under all conditions and maintain it in a safe condition under DBA conditions. The main control room provides control means of safety and non-safety equipment for our almost all operations, including accident situations. The main control room provides display devices that require continuous monitoring and control over the plant during normal and emergency operation.

The I&C system in the main control room is composed of operator consoles, RAS display panel, and safety console. There are five identical compact operator consoles for a reactor operator, turbine operator, reactor core operator, shift supervisor, and shift technical advisor.

Each operator console consists of four non-safety information plant panel displays, and these are analyzed for ESF-CCS of the control module. The information flat displays support process monitoring of all information for plant operation and control of non-safety equipment. And the ESF-CCS of the control module supports control core safety equipment.

CO-CHAIR BALLINGER: I would like to make a comment. This chapter has the world's record for acronyms -- (laughter) -- so many that we have actually printed five or six pages' worth of acronyms, so we could keep track of them. So, you know them back and forward, but we may not know them. So, when you see ESCM, can you say what it is as opposed to just using ESCM going forward, so that we understand? Because there are just so many acronyms that we can't --

MR. RO: I'm sorry.

CO-CHAIR BALLINGER: You know them; we don't so much.

MEMBER BROWN: How much additional time do you think we are going to need to do that, Ron?

CO-CHAIR BALLINGER: An hour or two.

(Laughter.)

MEMBER SKILLMAN: Sir, you mentioned there are five identical consults.

MR. RO: Yes.

MEMBER SKILLMAN: Among the responsibilities of the individuals who occupy those consoles, is there a hierarchy of who may enter a command to the plant and who may not? In other words, is there a voting logic where the reactor operator takes precedence over the steam plant operator or over the electrical operator? If all of the consoles are identical, then that would suggest that any of the operators can take control of any variable at any time that individual wishes; whereas, if there is a hierarchy, then the reactor operator might have the privileged action. So, my question is, is there a hierarchy among the consoles?

MEMBER BROWN: Can I phrase that slightly -- make sure I understand your question? There are five identical consoles. Is one dedicated to reactor functions and the other ones dedicated to turbine functions? So the one that is dedicated to reactor functions cannot do turbine functions and it cannot do electric plant functions and it can't do shift supervisor functions? Is that what you are trying to get at, as opposed to what operator can take control and do things? I am trying to make sure -- I don't want to get this --

MEMBER SKILLMAN: The question that you have posed is a clarification of where I was going. I hadn't been smart enough to go to the level that you had gone.

The gentleman said there are five identical consoles.

MEMBER BROWN: Exactly.

MEMBER SKILLMAN: I know what it is like to operator a console. If someone said, "I've got a console and he's got a console, and they're identical," then I would presume that either one of us could take command of anything we wanted on that console anytime we wished.

MEMBER BROWN: And that's why I asked to make sure. I am trying to clarify. That is why I was trying to get him to tell us that explicit.

MEMBER SKILLMAN: But that clarification would certainly head towards the root of what I am asking about.

MEMBER BROWN: For example, if you look at your figure, there is a reactor operator console, you know, the second one off from the left in your figure. That console will not take control of the electric plant? It cannot fulfill the functions of the electric operator? Is that true or not? I was hoping for a yes-or-no answer.

(Laughter.)

MR. J. KIM: Okay. This is Jinku speaking from KEPCO E&C.

Everyone knows that we already -- there

is five identical consoles in the main control room, and each operator console are assigned into each operator; for example, the reactor operator and the turbine operator and the electric operator. But the electrical operator -- this console, for example, the electrical operator console can control the whole plant. However, that operator only have a control for the bare -- he's a processor.

MEMBER BROWN: So, you're going to trust him not to try to operate the electric plant? Okay, let me step back.

MR. J. KIM: Okay.

MEMBER BROWN: Can a reactor operator console --

MR. J. KIM: Yes.

MEMBER BROWN: -- if somebody else comes over and sits -- say the electrical operator came over to that console.

MR. J. KIM: Yes.

MEMBER BROWN: Can he run the electric plant from the reactor operator console? That's not a yes or no?

MR. J. KIM: Yes. Yes, but all operators are controlled by the shift supervisor.

MEMBER BROWN: I understand that.

MR. J. KIM: Yes.

MEMBER BROWN: What we are trying to figure out, does every console have the same functionality --

MR. J. KIM: The same functionality --

MEMBER BROWN: -- and is able to control every one of the functions --

MR. J. KIM: Yes, every one.

MEMBER BROWN: -- even though it may be controlled by the shift supervisor in terms of giving direction?

MR. J. KIM: Yes, yes, he can, but, however, in normal operations the shift -- this console don't have the control capability. The shift operator and the shift technical advisor -- however, the electric console and the turbine operator console, for example, the shift supervisor can go to the other operator to control the whole plant. That is our design concept.

MEMBER BROWN: Okay, let me -- I'm not sure.

CO-CHAIR SUNSERI: I think what he said is, if I understood it right, the three operator consoles are totally functional, but the shift supervisor and the technical advisor monitor only, is what I thought I hear him say.

MEMBER BROWN: Yes, which means that a shift supervisor and the technical advisor aren't necessarily identical, I guess. I mean, I got the words that he, the shift supervisor, could not take control of the reactor from his console; whereas, the electric operator could walk over to the reactor operator's console and use that to control the electric plant.

We will have to work on that. We ought to be go on. I don't want to -- unless you've got a little bit more you wanted to suck out of this one.

CO-CHAIR SUNSERI: No, I don't have --

MEMBER BROWN: Rob, do you understand the question we are trying to drag ourselves through here also?

MEMBER SKILLMAN: Let's do this. I get the gist. To me, I've got a couple of other issues --

MEMBER BROWN: Well, go ahead.

MEMBER SKILLMAN: -- that are less hardware and operator machine interface that get to who's licensed to do what. Who can take precedence and take action? Where is my SRO? Who's in charge? Can the RO take charge of the output breakers? Can the turbine operator add reactivity?

There are some fundamental questions that have to do with five identical control consoles. And

I am not trying to make more complex than it needs to be. But my real question is, if there are five, who is in charge? Does the reactor operator really stay focused on control rods and reactivity? Does the turbine operator really stay focused on LP1 pressure condenser and inlet pressure and the crossovers? And is the electrical operator focused on volts and cycles?

It is just that simple. But it seems, if there are five consoles, then at least it raise in my mind -- excuse me -- five identical consoles, it raises in my mind who is able to do what and how is that controlled. That is the --

MEMBER BROWN: I understand that one. The advantage of having three or four, whatever it is, operator modules that are functionally identical, that if you have a failure of one, you have someplace to go.

MEMBER SKILLMAN: That's a good --

MEMBER BROWN: You could still maintain --

MEMBER SKILLMAN: Yes.

MEMBER BROWN: You've still got the chain of command from an operator standpoint as to who can do what that you have to deal with.

MR. SISK: This is Rob Sisk, Westinghouse.

And just clarifying what I'm

hearing/understanding, there are two issues here. One is the availability of consoles to interact. If one fails, you have backups, and what have you, as Charlie indicated.

But, Dick, I think you are leading to procedures, training, qualifications, which is another part of the discussion. You know, how does the licensee train, qualify, and what procedures do they use in the control room, which leads, then, of course, to the hierarchies of, is an EO able to go to an RO or is there a qualification program from EO, TO, to RO, or this kind of question. So, that is a different question than just the I&C functionality.

MEMBER SKILLMAN: Well, in part, Rob, that is accurate, but it begins with the notion of five identical consoles.

MR. SISK: Right.

MEMBER SKILLMAN: And if the consoles -- and I am looking at the slide, which is why I raised the question -- five identical operator console for -- and it gives the five stations -- if those truly are identical, then at the very outset of the design, there is at the STA panel or the shift supervisor, the STA console or the shift supervisor console the capability to override the reactor operator.

So, there is a design issue here that seems to me to be important to the philosophy of the design of the station. And that is a design issue. If there are five identical consoles, then, in theory, any one of the five could take any action related to any of the five stations.

MR. SISK: Rob Sisk, Westinghouse.

But that is assuming that that console at that time is aligned to perform that function or can perform any function at the same time. And the EO panel is set up with the electrical system and the EO operator can operate the EO panel.

Now the ability of that panel to be --

MEMBER SKILLMAN: Shifted.

MR. SISK: -- shifted is one question, but it is not that the EO panel, the RO panel, and the TO panel are all open at the same time on the console at the same time, such that an operator, whether he's the EO, TO, or RO, could be, "I'm the electrical operator, but, oh, look, there's the reactor operation. I can inadvertently," which gets into the human factors and performance aspects of the design, "inadvertently go over and trip a pump from the electrical panel." When the electrical panel is up, I'm not controlling -- I don't have access to that panel at that time, the functionality of the reactor operator panel.

MEMBER SKILLMAN: If it's designed that way, I would concur with you.

MR. SISK: Okay. I just wanted to put that out as clarification to understanding.

MR. HECHT: Well, I'm sorry, this is Myron Hecht again.

Is it designed that way or is it not designed that way? In other words, does the reactor operator log in and have a role saying, "I'm reactor operator," and at that point the distributed control system systems say, all right, I'm going to put up displays for the reactor operator? And somebody else logs in as the turbine operator. And then, the DCS says, I'm going to put up controls for the turbine. Is that how it works? Or does any person sitting at a console have the ability or does every person have all the displays?

MR. SISK: Rob Sisk, Westinghouse.

J.H. Park, could you maybe provide --

MR. PARK: Yes. This is J.H. Park.

As I understand, operator RO can log on. If he gets accepted, he can control, have the system, and the same case is applied to the TO. So, only one-time access is controlled by the SRO or something like that.

MR. SISK: Okay. Thank you, Mr. Park.

I would like to recommend we maybe re-explore this question a little bit more with Chapter 18.

MEMBER SKILLMAN: Yes, I agree with that.

MR. HECHT: I was just going to make the same suggestion, that there are some things to be discussed in Chapter 18 which would also touch on this issue.

MEMBER KIRCHNER: Just a question of clarification: your labels obscure what display is available to each of the operators. Do they each have three panels showing the entire plant function?

MR. RO: The entire plant function.

MEMBER KIRCHNER: They can see, they can access the entire --

MR. RO: Yes, yes. Yes, yes, they can access the entire plant function, yes.

MEMBER KIRCHNER: Thank you.

MEMBER MARCH-LEUBA: I'm not conflicted on this. So, I can talk.

Typically, what you have is a screen-oriented display. So, you have a screen for this all, and then, you push F8 and you get the screen for the turbine.

MEMBER BROWN: I understand all that.

MEMBER MARCH-LEUBA: You don't have three different panels; you have only one and you flip through the screens. That's correct?

MEMBER SKILLMAN: He said three panels.

MEMBER BROWN: I think it is three. Does each station have three monitors?

MR. J. KIM: No, four.

MEMBER BROWN: Each station, like the reactor operator has four monitors and --

MR. J. KIM: Yes, four monitors.

MEMBER BROWN: And turbine has four monitors? Electrical has four monitors?

MR. J. KIM: Yes, yes, the same thing.

MEMBER MARCH-LEUBA: No, no.

MEMBER BROWN: Well, that's what they said they are doing. Okay?

MEMBER MARCH-LEUBA: There are 25 screens.

MEMBER BROWN: Oh, I understand that, and they do exactly what you say on each of the four monitors. Okay, you can switch; I understand your point.

I just lost my other question. Can you

please re-engage my brain, find the locator bit for me?

(Laughter.)

CO-CHAIR BALLINGER: It's a one-way diode.

(Laughter.)

MEMBER BROWN: Oh, I know what it was. On your diagram here you show blue lines, red lines, and some other kinds of network lines. And you show blue lines going up to the large display panel. You show blue lines going up to the -- I have to look it up -- the IFPD.

MEMBER SKILLMAN: Information Flat Panel Display.

MR. J. KIM: Information Flat Panel Display.

MEMBER BROWN: All right. Okay, Information Flat Panel Display.

And you've got a red line going up to the ESCM, which is the Soft Control Module doohickus.

MR. J. KIM: Yes.

MEMBER BROWN: But there's no lines going to the RO, TO, and EO panels. What feeds those panels? Is it the DCN? Is it the SDN?

MR. J. KIM: Each operator console consists of the four Information Flat Panel Display.

MEMBER BROWN: Is that part of the -- oh, speaker? I'm sorry. I'm sorry.

So, excuse me. The IFPD controls those three consoles? Is that what you are telling me? Okay. The IFPD?

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

And each operator console consists of the four Information Flat Panel Displays and the four ESFCM.

MEMBER BROWN: Okay. So, an IFPD is sitting at each of those locations?

MR. J. KIM: Yes, right.

MEMBER BROWN: Got it. Thank you.

MR. J. KIM: Yes.

MEMBER BROWN: Yes, finally got it. I think I'm there.

CO-CHAIR SUNSERI: So, one last clarification. As you contemplate what we are going to discuss in Chapter 18, I guess what I am hearing from this whole discussion -- I am less concerned about three panels being identical and operating the whole plant. Because, in my mind, that is like having one switch that anybody can operate.

But the interesting thing, in my mind, is the command-and-control authority. How are those consoles going to be operated from a command-and-control authority, not a training-and qualification, but command-and-control?

MEMBER SKILLMAN: That is Chapter 18, right?

CO-CHAIR SUNSERI: Well, I mean, that is what we are going to talk about. We are going to talk about this in Chapter 18. So, that would be my input to the conversation we are going to have.

Thank you.

MEMBER KIRCHNER: Wait a minute. It is not Chapter 18 necessarily. If it is a hierarchy and it is hard-wired, it is this chapter.

MR. RO: I am You Sung Ro of KEPCO E&C.

The safety concern is provided to mitigate the accident and maintain the plant in safety condition. When our proprietary consoles are unavailable, the safety concern is configured as a hybrid-type console which contains hard-wired minimal inventory switches and FPD-based instruments such as the ESCM, many RAS display panels, and our own system displays.

The Diverse Indication System and Diverse Manual ESF activation switches are also provided on the safety console. The safety console is physically and electrically separated from the operator consoles.

The proposal, the RAS display panel is to provide plant-level overview information and safety information to the operators via special rededicate and continuous display.

The RAS display panel is configured to fix the sections.

The remote shutdown room provides control and monitoring means against the fire or unlikely event that MCR becomes unhabitable. To achieve the plant hot standby, hot shutdown, and cold shutdown, the remote shutdown room provides the remote shutdown console, which are identical design with operator console or with the main control room.

The Shutdown Overview Display Panel provides the similar information to system mini-displays or larger display panel.

The main control room, the remote shutdown room, the master transfer switches, transfer controls between the main control room and the remote shutdown room. The master plant's power switches are located in I&C rooms and remote shutdown rooms which are electrically and physically separated from the main control room.

Excess control provision is provided for in the remote shutdown room, and the mater transfer switches provides for each safety and non-safety division. During remote shutdown room mode, all main control room signals are disabled and remote shutdown room signals are enabled.

Younghun Kim will present the next section.

MR. YONGHUN KIM: Good morning, ladies and gentlemen. I am Yonghun Kim from KEPCO E&C.

I will present Section 7.6, Internal Functions Important to Safety, and Section 7.7, Control Systems Not Required for Safety.

Functions important to safety have the following internal functions: interrupt to prevent overpressurization of low pressure systems, interrupt to prevent overpressurization of the reactor coolant system during low-temperature operations of the reactor vessel, interrupt to ensure the availability of safety injection tanks, interrupt to ensure the availability of competent cooling water supply and the return head tie-line isolation, interrupt to preclude inadvertent inter-ties between redundant or diverse safety systems.

This page is about the joint features of the shutdown cooling system and the safety injection tank. The shutdown cooling system is a low-temperature and low-pressure system. This system has a suction line isolation barrier and a suction line relief barrier. The suction line isolation barrier has internal function to prevent overpressurization of low-pressure systems when they are connected to high-pressure systems.

And to satisfy this internal function, the shutdown cooling system prevents suction line isolation valves from being opened if RCS pressure does not decrease below a setpoint.

The shutdown cooling system suction line relief valves, self-actuating, spring-loaded relief valves with no control circuitry. These valves prevent overpressurization of the reactor coolant system during low-temperature operations of the reactor vessel. And these valves open when RCS pressure exceeds a setpoint.

The safety injection tank is a high-pressure system and has isolation valves. These isolation valves can be manually closed when RCS pressure drops below a setpoint, so that self-injection tanks cannot close overpressurization of the shutdown cooling system.

Self-injection tank isolation valves automatically open when RCS pressure exceeds a setpoint, so that SITs are available for injection during plant startup.

Component cooling water supply and return header tie-line isolation valve have varying interrupts. Component cooling water is supplied to non-safety components, SERS safety components during normal operation.

Isolation valves automatically close on safety injection actuation signal or component cooling water surge-tank-level signal in an accident or a transient.

Component cooling water closed connection line isolation valves as the following interrupts: isolation valves can be manually opened to supply component cooling water flow if one division fails. Isolation valves are normally locked close and automatically closed on self-injection actuation signal or component cooling water surge-tank-level signal in an accident or transient.

Do you have any questions?

MEMBER SKILLMAN: Yes, please.

On the prior slide, the last bullet, you indicate, "Isolation valves manually close -- these are the safety injection tank close -- manually close when the RCS pressure drops below a setpoint." I understand that. That prevents from overpressuring your safety injection system.

MR. YONGHUN KIM: Right.

MEMBER SKILLMAN: At the top of the next page, slide 16, you indicate that those valves automatically open. Are those the same valves? In other words, manual close, but an overriding open signal on open, on pressure?

MR. YONGHUN KIM: Right. It's the same valves and have a different setpoint.

MEMBER SKILLMAN: Yes, for increasing pressure.

MR. YONGHUN KIM: Yes, for increasing pressure.

MEMBER SKILLMAN: What I am really asking is, when they are manually closed, is the signal to the automatic open defeated?

MR. YONGHUN KIM: The safety injection tank isolation valves has two setpoints. The first setpoint is about 600 -- I'm not sure -- but 600 psia.

MEMBER SKILLMAN: Okay, approximately. Okay.

MR. YONGHUN KIM: And it can be open automatically at the startup, during the startup. And it has another setpoint for manual, for admitting manual close. It's about 400 psia, and it can be closed only manual for the safety function.

MEMBER SKILLMAN: Okay. So, if you have

a permit to close manually, but you have an additional automatic to open at a certain raising pressure, then a spurious command to open can overpressurize your low-pressure system. So, my question is, how do you preclude inadvertent opening on a spurious command to open?

MR. YONGHUN KIM: Manual close is possible when the RCS pressure is below 400 psia.

MEMBER SKILLMAN: Uh-hum. That's a permit. It's a permit to close.

MR. YONGHUN KIM: Yes.

MEMBER SKILLMAN: So, you close the valve.

MR. YONGHUN KIM: When, during a shutdown the operator can check the RCS pressure and he can manually close the --

MEMBER SKILLMAN: The valve?

MR. YONGHUN KIM: -- self-actuation isolation valve.

MEMBER SKILLMAN: Uh-hum. So, when the pressure comes back up, you're starting up, you get a command to open?

MR. YONGHUN KIM: Right, automatically.

MEMBER SKILLMAN: Automatically?

MR. YONGHUN KIM: Yes.

MEMBER SKILLMAN: What prevents a spurious command to open from occurring at low pressure?

MR. YONGHUN KIM: Spurious -- actually, this manual close, this prevents overpressurization of the shutdown cooling system, which is a low-pressure system. The shutdown cooling system has another relief valve in each suction line. And if the case happened, the relief valve opens when RCS pressure exceeds the setpoint.

CO-CHAIR BALLINGER: So, what you are saying is that, when you are cooling down and you are shutting down, you get a permit to close. And so, you close it. But, when you are starting up, the reverse is automatic.

But what Dick was saying is that, during shutdown, is it possible for a random or some error signal or some action that somebody takes place, that opens the valve, and you are saying that that actually could happen, but that relief valve now operates and protects the system? Is that what you are trying to say?

MEMBER SKILLMAN: Well, I think that is what the gentleman said. I can tell you from firsthand experience what you normally do is you depower the valve --

CO-CHAIR BALLINGER: Yes.

MEMBER SKILLMAN: -- to ensure that you cannot have a spurious command to open that valve and destroy your low-pressure systems. But what I heard the gentleman say is, on increasing pressure on startup, there will be an auto command to open those valves. I understand that. A real question is, how do you prevent a spurious signal when you are shut down from dumping the SIT through your low-pressure system that could be opened in other places? So, it seems to me that that might be something you need to look at.

MEMBER KIRCHNER: Dick, unless the relief valve capacity is --

MEMBER SKILLMAN: You don't want that to happen.

MEMBER KIRCHNER: Yes.

MEMBER SKILLMAN: You don't want that happening. Then, you've got water, you've got primary coolant everywhere you don't want it.

MEMBER KIRCHNER: It is not going to relieve the SIT injection, yes.

MEMBER SKILLMAN: I mean you don't want that to happen.

CO-CHAIR SUNSERI: But if you're going to de-energize the valve, then you might as well take away this interlock then --

MEMBER SKILLMAN: Bingo.

CO-CHAIR SUNSERI: -- because it will be overridden over time.

MEMBER SKILLMAN: Bingo.

CO-CHAIR SUNSERI: But I think that is an important airlock, though, right.

MR. SISK: This is Rob Sisk.

We've captured the note. We understand. It is an interesting discussion. We have captured it. I think the design has been explained, and we will have to explore that further.

MEMBER SKILLMAN: Okay. Thank you. All right.

CO-CHAIR BALLINGER: One last thing. What you are actually saying, if all this is taken literally, is that that relief valve capacity had better have the capacity of the safety injection system.

MEMBER SKILLMAN: That's exactly accurate, which is huge.

CO-CHAIR BALLINGER: Which is one heck of a relief valve. That's a big relief valve.

MEMBER SKILLMAN: It is going to have a relief valve as big as the discharge and stuff, yes --

CO-CHAIR BALLINGER: Yes.

MEMBER SKILLMAN: -- of the SIT. Okay.

Thank you, Mr. Kim. Thank you.

CO-CHAIR SUNSERI: But just remember the SIT has that flow-limiter device which controls the discharge flow rate based on the differential pressure, too.

MR. YONGHUN KIM: Section 7.7 is control systems not required for safety. Control systems not required for safety have the following functions and design features: the primary function of the non-safety control system is to maintain process barriers and systems within normal operation limits. Non-safety systems that interface with safety systems are designed so that credible failures in the systems do not impact operation of safety systems.

Non-safety systems have physical separation and reactor core isolation and maintain communication independence from safety systems. Safety analysis of Chapter 15 does not rely on operability of any non-safety system control functions to provide reasonable assurance of safety.

In safety analysis, the effects of both control system action and connection are considered in assessing transient response for accidents and AOOs.

The non-safety control system consists of the power control system and the process component control system. The power control system includes the reactor regulating system, the reactor power contact system for controlled rod control and this digital rod control system for control rod drive.

The process component control system includes the enterprise process control system and BOP control systems. The enterprise process control system includes the feedwater control system, the steam bypass control system for turbine bypass control, and the pressurizer pressure control system, the pressurizer level control system.

This page shows the effects of control system failures. The control system failures caused by a single failure as an initiating event do not cause plant conditions more serious than those described in the safety analysis of AOO in DCD Chapter 15.

The following postulated failures caused by a shared unit failure and control system CCFs are evaluated, come from the event consequences of Chapter 15 as detected and analysis accident criteria are met.

The effects of multiple function failures due to a single failure of a shared unit, the effect of multiple failures of a signal control group due to a CCF, the effect of multiple failures of more than one control group due to a CCF, the effects of multiple failures of Information Flat Panel Display control commands due to a CCF.

A shared signal is a signal whose failure causes multiple function failures in two or more control groups. The postulated failure boundary of a control system CCF is as follows: the CCF within a single controller or a single control group is considered, and the CCF within all the non-safety control system is considered.

As the Information Flat Panel Displays provides control commands through the controller, the CCF within the Information Flat Panel Display is considered.

This page shows control group assignment for the control system CCF evaluation. Control functions are assigned to a separate control group that consists of at least one separate controller. Each control function is assigned to a separate control group using independent controllers, so that the result of multiple failures due to the CCF of a single control group can be limited and meet the AOO acceptance criteria of Chapter 15.

The control function that can cause excessive transients in the process due to the CCF can be assigned to more than one control group to limit the failure effects. On the contrary, more than one control function can be assigned to a single control group if the result of the multiple function failures the AOO acceptance criteria.

Control functions and control groups are as follows; evaluation result of control system CCF are as follows: the evaluation concludes that all multiple failures caused by a shared signal or a control system CCF do not cause plant conditions more serious than the acceptance criteria of the DCD Chapter 15 AOOs and postulated accidents.

The result of multiple failures due to a single failure of a shared signal meet the AOO acceptance criteria of Chapter 15. The result of multiple failures of a single control group due to a control system CCF meet the AOO acceptance criteria of Chapter 15. The result of multiple failures of more than one control group due to a control system CCF meet the postulated accident acceptance criteria of Chapter 15. The result of multiple failures of Information Flat Panel Display control commands due to a control system CCF meet the postulated accident acceptance criteria of Chapter 15.

The detailed assumptions and evaluation results for the above postulated control system CCFs are provided in the control system CCF analysis technical report.

MR. HECHT: Mr. Kim?

MR. YONGHUN KIM: Yes?

MR. HECHT: On chart 21, which was the previous chart, you indicated the fact that there can be multiple control groups assigned to control functions and multiple control functions assigned to a single controller or control group. In the Chapter 7 documentation, there was very little about the DCS itself, the Distributed Control System, and it wasn't clear how that architecture works.

The controllers are actually software processes, is that correct, running on the DCS?

MR. YONGHUN KIM: Right.

MR. HECHT: Okay. So, when you have multiple control functions assigned to a controller, does that mean that the controller is running continuously monitoring these multiple control functions? In other words, if I assign a controller to do pressurizer level control and a CVCS control, is it doing both simultaneously?

MR. YONGHUN KIM: Okay. There are four failure types we evaluated, and the failure type 2 is the effects of multiple failures of a single control group like pressurizer level control system or CVCS. So, we evaluated multiple failures of a single control group.

So, at first, the pressurizer level control system multiple failures are evaluated, and the evaluation measure, we check the evaluation measure with the AOO acceptance criteria.

MR. HECHT: But it seems to me that there are a lot of different combinations of control function and control group assignments that would have to be evaluated if you can assign any control function to any control group.

MR. YONGHUN KIM: So, the failure type 3 is to control multiple failures of more than one control group. It shows all control groups. So, we considered the effects of multiple failures of all control groups due to a CCF in a failure type 3 evaluation.

MR. HECHT: I'm not sure I understood the answer to that question. I've asked a simple question about assignment of control groups to control functions, and it seems as if your answer is that any control function can be assigned to any control group and that multiple control functions can be assigned to a single control group. Is that correct?

MR. YONGHUN KIM: Maybe clarify your

question again. So, control function assignment is for the control CCF evaluation, and we assign the control group to find out that the multiple failure of the control group is limited, the evaluation result is limited and meets the AOO acceptance criteria. To do that, each control function is assigned to a separate control group, and if the multiple failure of that control group can cause excessive transient in the process, at that time the control function, it cannot meet the AOO acceptance criteria at that time. We separate the control groups in the same function.

So, one SVCS has the function to control the turbine bypass barrier, but the multiple failure of SVCS control function cannot meet the AOO acceptance criteria. So, we separate the control -- we separate the SVCS function to two separate control groups, SVCS main and SVCS permissive. By doing that, the multiple failure of a single control group can meet the AOO acceptance criteria.

MR. HECHT: Okay. Well, this means that you have some rules -- I would call them allocation rules -- for how you assign control functions to control groups. And you are saying that you would have had to have considered a lot of combinations in order to make those allocations because it seems that you have at least it looks like about 10 control groups listed in that last chart, and I don't know how many controllers you have. But if you have four controllers or four control groups, that means that you could have -- four times, three times -- 240 combinations I think.

MEMBER BROWN: I don't want to get -- we're getting way down into detail. But I guess my point, from listening, I got the same -- this was a very general discussion in the DCD. It was not -- and my memory is telling me this. An example would have been useful in terms of how this whole combination of control groups or spreading of control groups or splitting them out, an example would have been useful to try to make heads or tails or understanding, create an understanding of what this means.

I think we're getting a little bit confused. I don't want to take up the whole morning on this, but I think we ought to raise the point as to how can we get a better grasp of how this works. Is that --

MR. HECHT: Well, yes. I guess, in general, a more detailed discussion of the DC --

MEMBER BROWN: In the DCD, because it's not --

MR. HECHT: Well, there's lots of "DCs".

I'm talking about the Distributed Control System.

MEMBER BROWN: No, I understand that, but, I mean, in the DCD --

MR. HECHT: Yes.

MEMBER BROWN: -- in the design, in Chapter 7, there should be some -- an example would have been useful to try to understand how that -- we've got all these control groups. How do you make these selections because there's a lot of combinations?

MR. HECHT: That kind of -- it is related to, but not completely the point that I was trying to make. That is that the DCS I think has to be described, and it is not.

MR. SISK: This is Rob Sisk, Westinghouse.

I am going to ask Mr. Warren Odess-Gillett to comment, if I may.

MEMBER BROWN: As long as Ron doesn't object.

(Laughter.)

MR. ODESS-GILLETT: Good morning. I'm Warren Odess-Gillett from Westinghouse.

If you go to the CCF report, it clearly outlines the allocation of functions to control groups, and that is where you can find that information.

MEMBER BROWN: Okay. But now, what about

a description of the DCS?

MR. ODESS-GILLETT: Okay. I was only trying to answer your question --

MEMBER BROWN: Right.

MR. ODESS-GILLETT: -- about I can't find where the allocation of functions are to the control groups. It is defined.

MEMBER BROWN: Okay.

MR. ODESS-GILLETT: And that is what I was trying to answer your question as to where is it defined.

MEMBER BROWN: Okay. All right. Thank you.

MR. ODESS-GILLETT: I can't answer the question about where the DCN is or the DCS is described.

MEMBER KIRCHNER: Ron?

CO-CHAIR BALLINGER: Walt, did you have something? I'm sorry.

MEMBER KIRCHNER: I was just going to say, Rob, I think perhaps here the viewgraph leads one to believe that there are more permutations than combinations. I think there's -- I shouldn't use the word "hierarchy" -- but there is already an allocation. Allocations have been made to look at, to address each of these bullets. In other words, there are different transients possible, right? And there are different control functions that can help deal with the transients. So, depending on going through all of these, then an allocation has been made as to assignment of control functions to groups of some kind, so that you can withstand all these common-cause failure initiators. Do you know what I'm saying?

MR. SISK: Yes.

MEMBER KIRCHNER: But that is not apparent from this. It looks like you could just randomly assign all these functions. That is not the case.

MR. SISK: This is a higher overview. If you go to the CCF report and others, you will have much more detail.

MR. YONGHUN KIM: Younghun Kim, KEPCO E&C.

All control groups are listed in Tier 1, Table 2.5.5-1.

MEMBER BROWN: Tier 1?

MR. YONGHUN KIM: 2.5.5-1.

MEMBER BROWN: 2.5, 2.5.5 or -5?

MR. YONGHUN KIM: 2.5.5-1.

MEMBER BROWN: -1. Okay. Thank you.

MR. HECHT: I'm sorry, in which document?

MEMBER BROWN: Tier 1, DCD. Is that a table?

MR. YONGHUN KIM: Yes.

MEMBER BROWN: Okay. That's a table. It is a table. Okay. Thank you. And that is the control group assignments?

MR. YONGHUN KIM: Right.

MEMBER BROWN: Okay. That's a useful response.

(Laughter.)

Thank you.

MR. YONGHUN KIM: That's it. So, do you have any additional questions?

MEMBER BROWN: It's the acronym page next time. We don't need to go over that. Is that okay?

(Laughter.)

MR. SISK: This completes the open portion of our presentation today for Chapter 7.

CO-CHAIR BALLINGER: Thank you.

And then, we now switch out --

MEMBER BROWN: I do have one additional question. It is just a followup on something that I had asked earlier.

Back to your big picture again, slide whatever it is, it is a really simple question. And I just probably got it wrong. Right there.

The IFPD, you made it clear that's functionality that covers the RO, TO, and electrical operator stations or monitors. The IFPD implies that it is just an Information Flat Panel Display, but there is a blue line that comes out of it that goes down to the DCN. And those stations all control plant function. So, I presume that overall IFPD configuration also allows control functions to be transmitted from each of those stations down to whatever needs to be controlled in the plant. Is that correct? And they go via the DCN.

MR. J. KIM: Okay. Jinku Kim speaking, KEPCO E&C.

In the case of the Information Flat Panel Display, this panel display provides two kind of a major function. One is the control function for the non-safety component.

MEMBER BROWN: Okay.

MR. J. KIM: Thinking about this command --

MEMBER BROWN: I think you just answered my question.

MR. J. KIM: Okay, yes.

MEMBER BROWN: Did I get that right?

CO-CHAIR BALLINGER: What was the answer?

MEMBER BROWN: You said that provides the control functions to the PCS --

MR. J. KIM: Right, right.

MEMBER BROWN: -- all that stuff down there in blue?

MR. J. KIM: That's correct.

MEMBER BROWN: As well as the displays for the operator?

MR. J. KIM: It is for the safety and the non-safety information.

MEMBER BROWN: That's right. Okay. You answered my question. Thank you.

Okay, we can roll.

CO-CHAIR BALLINGER: Let's roll.

Changeout for the staff.

MEMBER BROWN: Are you read, Deanna?

MS. ZHANG: I hope so.

Before we begin, I would like to pass another acronym packet. This is for our presentation, and it is only one page and about a quarter of the --

CO-CHAIR BALLINGER: Oh, we can memorize that in five minutes.

MS. ZHANG: Good morning.

MEMBER BROWN: Now, if I look at your presentation, this is a non-proprietary part and this looks like it is about three-and-a-half minutes long. So, you will be back on schedule at 10 o'clock, correct?

MS. ZHANG: Depending on the questions.

MEMBER BROWN: Well, there's no technical information at all in this. I'm just pulling your chain, Deanna. You are very nice. That is why I can do that.

(Laughter.)

MS. ZHANG: So, once again, good morning. Good morning, everyone. My name is Deanna Zhang, and I am the lead reviewer for the APR1400 Chapter 7, which is on Instrumentation and Controls.

I, along with my colleagues Jack Zhao, Kenneth Mott, and Dawnmatthews Kalathiveettil, as well as our PM Bill Ward, are here to present to you the results of our phase 2 review, which is on the Safety Evaluation Report with open items for Chapter 7.

Next slide.

So, the staffing tends to present the results of the staff's review on the APR1400 I&C systems and their conformance to NRC regulations and guidance. The staff aims to establish a common understanding of the APR1400 design, the staff's evaluation efforts, and the current status of the review.

The staff hopes by the end of this meeting that the staff would have answered all of the members' questions and that we get a clean letter from the members with no additional recommendations.

MEMBER BROWN: Not a chance.

CO-CHAIR BALLINGER: I think it will be physically clean, but I'm not sure --

(Laughter.)

MEMBER BROWN: You know you're going to get at least one.

(Laughter.)

MS. ZHANG: So, I would like to introduce everyone involved in this review effort from the I&C Branch, including myself, which I supported the overall review as well as the data communications review. Dinesh Taneja, who performed the software program manual review; Ken Mott, who performed the reactor trip system as well as Core Protection Calculator System alternative request review; Jack Zhao, who performed the ESFAS review; Joe Ashcraft, who performed the systems and quarantine staged shutdown, the post-accident monitoring system, and the interlocked systems and quarantine safety review; Wendell Morton, who performed the control systems review; Dawnmatthews Kalathiveettil, who performed the Diversity in Defense-in-Depth review.

Although the aforementioned staff are all from the Instrumentation and Controls Branch, I want to mention that we did coordinate heavily with other branches and staff from Reactor Systems, Balance of Plant, as well as Human Factors, Tech Specs, et cetera.

Next slide.

KHNP submitted their APR1400 design certification application in December of 2014. It was subsequently accepted for review.

The staff's review is based on the information in FSAR Tier 1 and Tier 2, Chapter 7, as well as a number of technical and topical reports which I will identify in the next slide.

The staff reviewed the following technical reports identified in this table. The Applicant has committed to incorporate by reference the technical reports so that it becomes a part of the licensing basis for this design certification application.

In addition, since most of the safety-related systems in this design use the Common Q platform, the staff's review also incorporated the information presented in the Common Q Topical Report, Revision 3, which has been previously reviewed and approved by the staff. The Applicant has also agreed to incorporate by reference this topical report into the FSAR.

Next slide.

The staff reviewed the design in accordance with the requirements of 10 CFR 50.55(a) --

MEMBER BROWN: Deanna?

MS. ZHANG: Yes?

MEMBER BROWN: Rev. 3, is that a proprietary topical report?

MS. ZHANG: Yes. So, it has a non-proprietary version, but --

MEMBER BROWN: Rev. 3 has a non-proprietary --

MS. ZHANG: It does have a non-proprietary version.

MEMBER BROWN: I think Christina sent me one, but it wouldn't open.

MS. ZHANG: Oh.

MEMBER BROWN: So, I have not been able to look at that. I did read the one back in Rev. 0 or Rev. 1, or whatever it was six years ago.

So, I would like to make another attempt. I think we are supposed to have another meeting, aren't we, Ron, later after this one? Is there going to be a meeting that's all open items closed?

CO-CHAIR BALLINGER: Yes. In November.

MEMBER BROWN: In November? Okay. If we can try to get that somehow to me via some system --

MS. ZHANG: Okay.

MEMBER BROWN: -- where I can actually open it, that would be useful.

MS. ZHANG: We will take note of that.

MEMBER BROWN: And let me make, while you are on this page, I took a quick look through your slides, and the other part I was interested in was the supplemental information on the Common Q. There's 28, or something like that, changes since Rev. 0 or 1, or whichever one it was. And there was a discussion of that but, without Rev. 3, I was unable to integrate that information.

So, hopefully -- I don't think you are going to talk about that in this presentation -- but at some point, even in the next meeting, we need to go through the general generic open items and the plant-specific ones on some level.

MS. ZHANG: Okay.

MEMBER BROWN: I don't mean digging down to the absolute bare bones and the bone marrow of the things, but to explain why you all come up with acceptance of that.

MS. ZHANG: Okay. We'll do.

MEMBER BROWN: Okay? And let me, was there -- I am just trying to give you a calibration for later. I think you covered the CPCS stuff and the shared routine of the control element sensors. And I hope it is better than the writeup in the SER, which was -- at 11 o'clock at night it was kind of hard to understand that.

MS. ZHANG: It is difficult to understand.

MEMBER BROWN: Yes, very, very, and I had still walked away -- I know you've got an open item on it, but that is not related. The way I read it, you accepted the shared part. So, I hope you are going to do a little bit more on why you accepted it. You had something else that maintained it has an open item, some other information. But I'm not sure I've got that right. So, you can just explain that to me later.

MS. ZHANG: So, we will be going in detail about the --

MEMBER BROWN: Okay. All right.

MS. ZHANG: -- CPCS system and what we have.

MEMBER BROWN: Okay. And the loading issue you covered. So, all right. Excellent. Thank you.

MR. HECHT: So long as we are on the subject of the Common Q platform, I was able to read both the proprietary -- or the proprietary version of the report, which I believe is Version 3. And while it did go down to a certain level, it really didn't describe the processor or the operating systems or the more detailed software architecture. Did you have that information and did you review it?

MS. ZHANG: So, are you talking about the detailed like architecture of the operating system? I do not believe we --

MR. HECHT: No, but the fact that -- what was the operating system first?

MS. ZHANG: So, for the AC160, it is the VRX operating system. For the Flat Panel Displays, it is the QNX operating system. Those are proprietary operating systems.

MR. HECHT: VRX did you say?

MS. ZHANG: Oh, VRTX.

MR. HECHT: VRTX. Those are available.

Was that information actually in the Common Q report, because I couldn't find it?

MS. ZHANG: Yes, it was.

MR. HECHT: It was?

MS. ZHANG: Yes.

MR. HECHT: Okay.

MEMBER BROWN: Let me make one other clarification.

MS. ZHANG: Okay.

MEMBER BROWN: Other than the supplemental information, you all have, you all did approve the original or you approved it for use --

MS. ZHANG: Yes, yes.

MEMBER BROWN: -- six years ago or seven years, whatever it was, because we used it in another project. Is the platform, other than these supplemental information changes, it should be the same, is that --

MS. ZHANG: No.

MEMBER BROWN: It's not?

MS. ZHANG: Yes. So, the staff does have a slide that talks about some of the differences between what was used for the AP1000 --

MEMBER BROWN: Yes.

MS. ZHANG: -- versus what is used for the AP1400.

MEMBER BROWN: Yes. Go ahead.

MS. ZHANG: So, we will be presenting that. There are a couple of modules that were not approved for use.

MEMBER BROWN: At the time?

MS. ZHANG: It wasn't discussed at that time for the Common Q Topical Report, Rev. 3. The staff did ask some supplemental RAIs on those particular modules and why it was acceptable for use.

MEMBER BROWN: Okay. Well, I don't want to go back and try to redo whatever we agreed with before. I am only interested in ensuring we understand what was now new approved that went with it. I remember the AC160 stuff.

MS. ZHANG: Yes.

MEMBER BROWN: We went through all that before on the earlier project.

MS. ZHANG: Yes. There are just a couple of modules that were not described in the Common Q Topical Report that are being used for the APR1400 systems.

MEMBER BROWN: Okay. All right. And you will have a short discussion on it?

MS. ZHANG: Yes, we have a --

MEMBER BROWN: Well, you will have a discussion?

MS. ZHANG: We will have a discussion.

MEMBER BROWN: Okay. All right. Thank you.

MR. HECHT: I'm sorry, but I wanted to go back to the QNX operating system --

MS. ZHANG: Uh-hum.

MR. HECHT: -- on the Flat Panel Displays. I mean, that is not a -- VRTX I think did go through some kind of acceptance by the FAA, for example, for DO-178. How did you verify or accept the QNX operating system?

MS. ZHANG: So, this was approved as part of the original Common Q Topical Report, Rev. 0. And I'm not so sure what about what was done back then, but, as I understand it, the whole Common Q platform was a commercial grade dedication.

MEMBER BROWN: That's correct. That's what you told us before.

MS. ZHANG: Yes, yes.

MR. HECHT: Okay. And is there information on the amount of operating time and the amount of failures that you had in that when you did that commercial dedication?

MS. ZHANG: So, as I said, that was part of the Revision 0 approval. Currently, I do not have with me the --

MR. HECHT: Okay.

MEMBER BROWN: We're not going to work on that right now. Okay?

MR. HECHT: All right.

MEMBER BROWN: I want to go on and hit the other stuff. I don't want to revisit what we have already agreed with in the past. We have already approved it, and I don't think we can go retrace that and try to mouse milk it anymore. Okay? So, all right. So, let's go on.

MS. ZHANG: Okay. So, just to continue on, the staff also reviewed the design against the requirements of the applicable General Design Criterias such as GDC 13, 19, 21, and 24.

The staff also reviewed the design to the TMI requirements in 10 CFR 50.34(f)(2) as well as the ATWS requirements in 10 CFR 50.62.

For this review, the staff followed the Standard Review Plan, Chapter 7, and the Regulatory Guides and NUREGs applicable to I&C.

Next slide.

This table presents the number of RAI questions asked by the staff with respect to each of the sections identified in the Standard Review Plan and the corresponding open items identified in the SER.

As can be seen in this table, of the original 184 questions, the Applicant has resolved a majority of the issues. I also want to note that, following the staff's completion of the SER with open items, the Applicant provided sufficient information to address an additional 12 open items. Thus, only 21 open items remain.

Next slide.

MEMBER BROWN: What were the general subjects that were closed?

MS. ZHANG: For example --

MEMBER BROWN: Are there any big ones or just they really all are little trinkets?

MS. ZHANG: They are little trinkets. In particular, 7.8 was explanation of 100-percent testing.

MEMBER BROWN: Okay.

MS. ZHANG: Some with 7.3 was providing additional information for the control of certain functions.

MEMBER BROWN: Okay. All right.

MS. ZHANG: Okay. The staff identified key issues related to data communications independence between redundant portions of safety systems and between safety and non-safety systems, as well as issues with setpoint methodology, secure development and operational environment as it relates to the vulnerability analysis; control system failure analysis, and the basis for selection of post-accident monitoring system variables.

So, this concludes the staff's, the open portion of the staff's presentation. Are there any additional questions?

(No response.)

CO-CHAIR BALLINGER: If there aren't any additional questions, I think we need to ask if there is anybody in the room that would like to make a comment from the public.

(No response.)

Hearing none, I am assuming the bridge line is open.

MR. T. BROWN: Bridge open.

CO-CHAIR BALLINGER: Is there anybody out in the public that would like to make a comment?

(No response.)

I don't hear -- oh, I hear the crackling. Okay.

(No response.)

Hearing none, then, I think we are good there.

Before we go into the closed session, I need to correct an error which I made, actually, an error of omission. Christina Antonescu and Chris Brown are the Designated Federal Officials for this meeting. That is a serious error on my part.

So now, we need to be able to go to the

closed session. So, we need to switch out presenters, I'm sure.

MEMBER BROWN: Are we going to have a break or not, according to your agenda? We're on schedule.

CO-CHAIR BALLINGER: Yes, we have a break.

MEMBER BROWN: Okay.

(Laughter.)

CO-CHAIR BALLINGER: We have a 15-minute -- we are recessed for 15 minutes.

MEMBER BROWN: This is a lesson. You have to keep track for him.

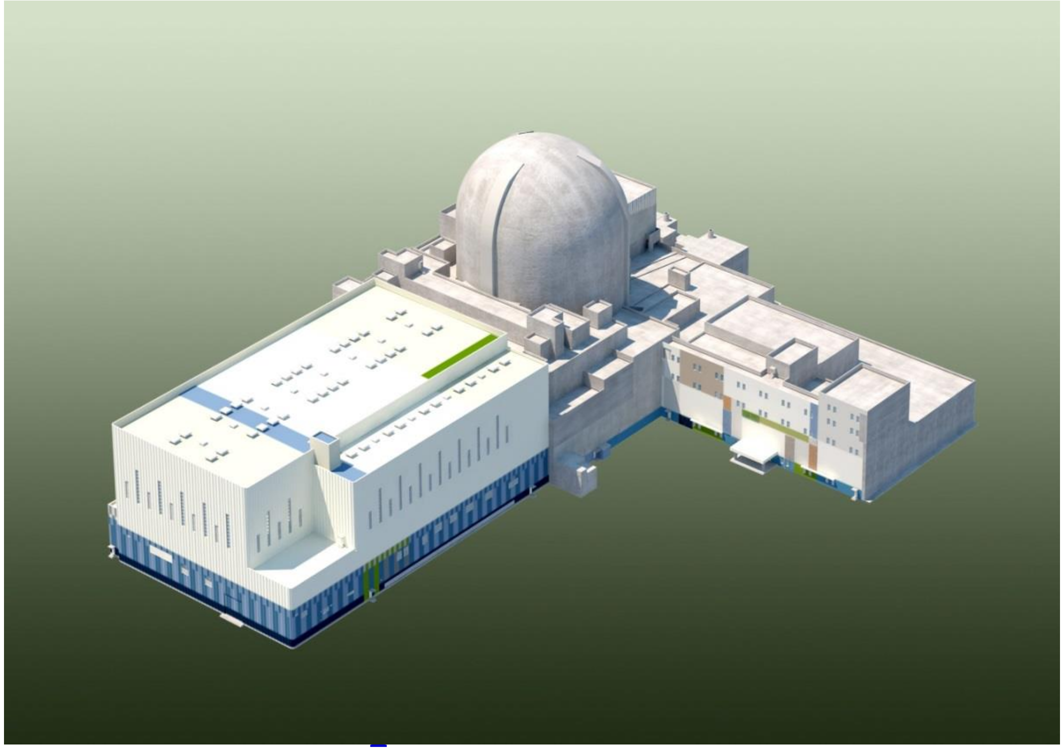
(Laughter.)

CO-CHAIR BALLINGER: So, 10:16 or thereabouts.

(Whereupon, at 10:02 a.m., the meeting recessed to reconvene in closed session at 10:18 a.m.)

NON-PROPRIETARY

APR1400 DCA
Chapter 7: Instrumentation and Controls



KEPCO/KHNP

June 20, 2017

Contents

- Overview of Chapter 7
  - Section Overview
  - Related Documents Submitted
- Section Summary (7.1, 7.4, 7.6, 7.7)
- Attachment
  - Acronyms

Overview of Chapter 7 (Section Overview)

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

Related Documents Submitted

	Title	Rev.	Type
APR1400-Z-J-NR-14001-P & NP	Safety I&C System	0	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

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

Related Documents Submitted

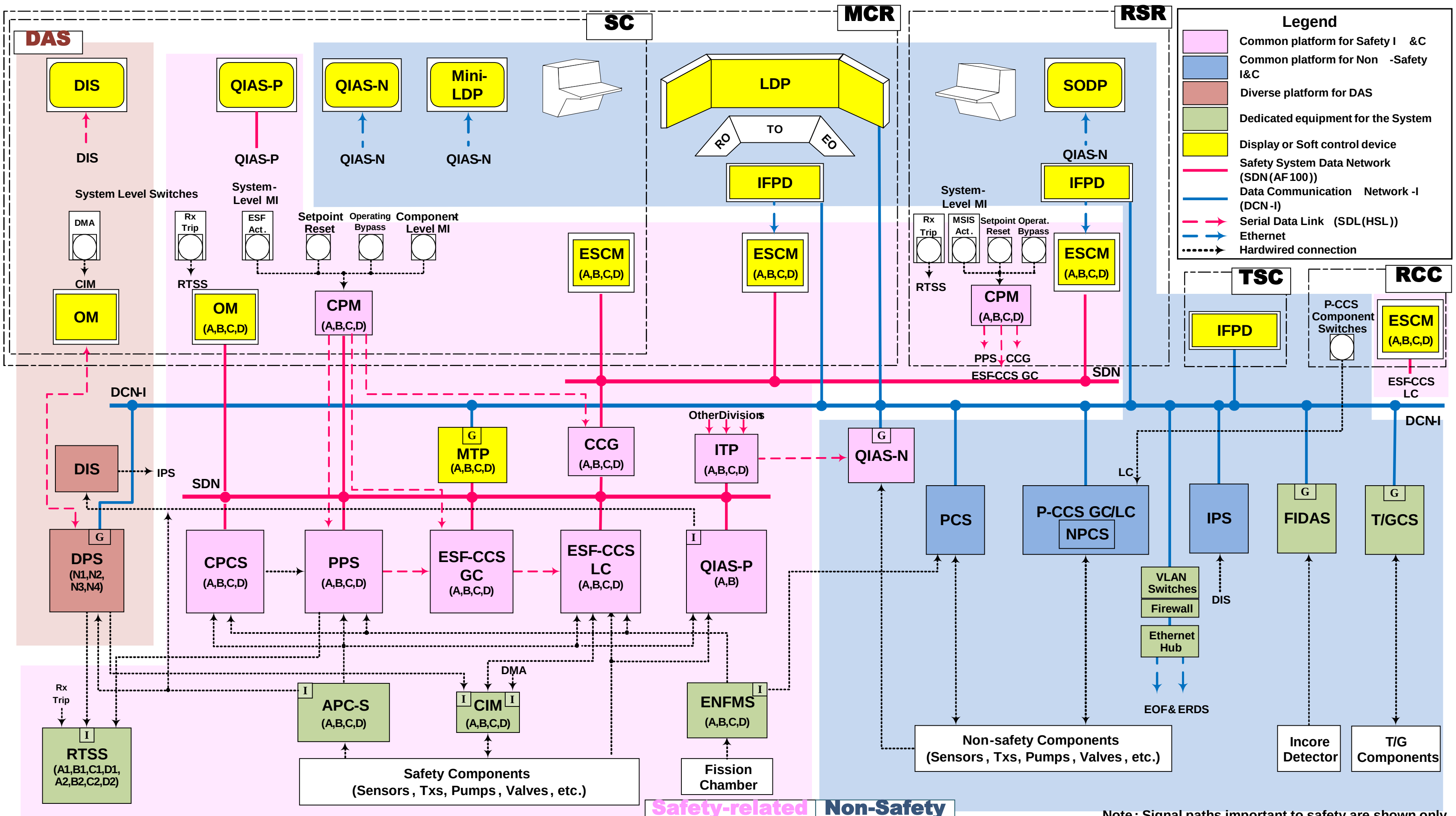
Document No.	Title	Rev.	Type
APR1400-A-J-NR-14003-P	APR1400 Disposition of Common Q Topical Report NRC Generic Open Items and Plant Specific Action Items	0	IBR
APR1400-A-J-NR-14004-P	Common Q Platform Supplemental Information in Support of the APR1400 Design Certification	0	IBR
WCAP-10697-P-A	Common Qualified Platform Topical Report	3	IBR
CEN-310-P-A	CPC and Methodology Changes for the CPC Improvement Program	0	-
CEN-312-P	Overview Description of the Core Operating Limit Supervisory System	1	-

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, RG, IEEE standards, and ISGs.

NON-PROPRIETARY

7.1 Introduction (Overview Architecture)



Note: Signal paths important to safety are shown only

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

Rev.1

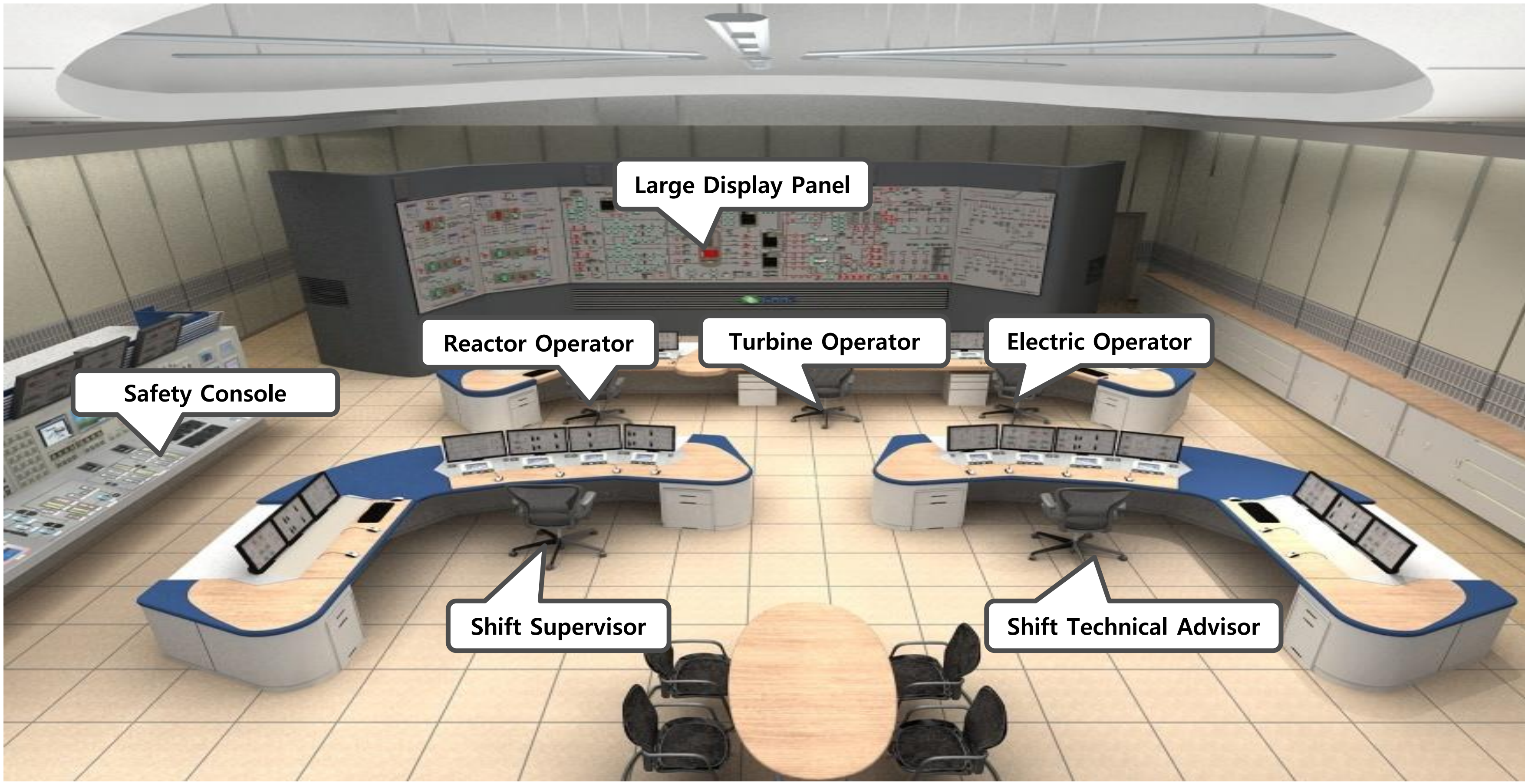
7.1 Introduction (Design Features)

● 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	

7.4 Systems Required for Safe Shutdown

- Functions (Main Control Room)



7.4 Systems Required for Safe Shutdown

- **Functions (Main Control Room)**
  - **Provides all human system interface devices to operate the plant safely under all conditions and maintain it in a safe condition under DBA conditions.**
    - **Provides control means of safety and non-safety equipment for all modes of operation including accident situations.**
    - **Provides display devices of variables that require continuous monitoring and/or control of the plant during normal and emergency operation.**

7.4 Systems Required for Safe Shutdown

- Design Features (Main Control Room)
  - Major equipment in MCR is composed of operator consoles, LDP, and safety console.
  - Operator Console
    - Five identical operator consoles for reactor operator, turbine operator, electric operator, shift supervisor, and shift technical advisor
    - Operator console consists of four IFPDs and divisionalized four ESCMs.
    - IFPD
      - Indication of all information for plant operation
      - Control for non-safety equipment
    - ESCM
      - Control for safety equipment

7.4 Systems Required for Safe Shutdown

● Design Features (Main Control Room)

➢ Safety Console

- To mitigate the accident and maintain the plant in safe condition, when all operator consoles are failed.
- Hybrid type of configuration
  - Hardwired MI switches
  - FPD-based ESCM, mini-LDP, QIAS-N, and QIAS-P
- Provision of diverse indication and controls (DIS and DMA switches)
- Physically and electrically separated from the operator consoles

➢ Large Display Panel

- Provision of plant level overview and safety information via spatially dedicated and continuously visible display
- Configured to fixed sections and variable sections

7.4 Systems Required for Safe Shutdown

- **Functions (Remote Shutdown Room)**
  - Provides control and monitoring means against fire unlikely event that MCR becomes uninhabitable.
  - Achieves the plant hot standby, hot shutdown, and cold shutdown.

- **Design Features**
  - Remote Shutdown Console
    - Identical design with operator console of MCR
  - Shutdown Overview Display Panel
    - Information is similar to system mimic displays of LDP.

7.4 Systems Required for Safe Shutdown

- **Main Control Room/Remote Shutdown Room Transfer**
  - **MCR/RSR master transfer switch (MTS)**
    - **Provision in RSR and I&C equipment rooms for transferring control capability from MCR to RSR**
    - **Location of MTS is electrically and physically separated from MCR.**
    - **Access control provision is provided.**
  - **Dedicated MTS for each safety and non-safety division**
  - **During RSR mode, all MCR signals are disabled and RSR signals are enabled.**

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.
  - Preclude inadvertent interties between redundant or diverse safety systems.

7.6 Interlock Systems Important to Safety

- **Design Features**
  - **Shutdown Cooling System Suction Line Isolation Valve Interlocks**
    - **Prevent over-pressurization of low-pressure systems when they are connected to high-pressure systems.**
    - **Prevent suction line isolation valves from being opened if RCS pressure does not decrease below a setpoint.**
  - **Shutdown Cooling System Suction Line Relief Valve Interlocks (self-actuating spring-loaded relief valves with no control circuitry)**
    - **Prevent over-pressurization of the reactor coolant system during low-temperature operations of the reactor vessel.**
    - **The valves open when RCS pressure exceeds a setpoint.**
  - **Safety Injection Tank (SIT) Isolation Valve Interlocks**
    - **Isolation valves can be manually closed when RCS pressure drops below a setpoint so that the SITs cannot cause over-pressurization of the Shutdown Cooling System.**

7.6 Interlock Systems Important to Safety

● Design Features (cont'd)

- **SIT Isolation Valve Interlocks (cont'd)**
  - Isolation valves automatically open when RCS pressure exceeds a setpoint so that SITs are available for injection during plant startup.
- **CCW Supply and Return Header Tie Line Isolation Valve Interlocks**
  - Component Cooling Water (CCW) is supplied to non-safety components as well as safety components during normal operation.
  - Isolation valves are automatically closed on an SIAS or low-low CCW Surge Tank level signal in an accident or transient.
- **CCW Cross Connection Line Isolation Valve Interlocks**
  - Isolation valves can be manually opened to supply CCW flow, if one division fails.
  - Isolation valves are normally locked closed and automatically close on a SIAS or low-low CCW surge tank level signal in an accident or transient.

7.7 Control Systems Not Required for Safety

● Functions and Design Features

- Primary function of non-safety control system is to maintain process variables and systems within normal operational limits.
- Non-safety systems that interface with safety systems are designed so that credible failures in the systems do not impact operation of safety systems.
- Non-safety systems have physical separation and electrical isolation, and maintain communication independence from safety systems.
- Safety Analysis of Chapter 15 does not rely on operability of any non-safety system control functions to provide reasonable assurance of safety.
- In Safety Analysis, the effects of both control system action and inaction are considered in assessing transient response for accidents and AOOs.

7.7 Control Systems Not Required for Safety

- **Major Control Systems**
  - **Power Control System**
    - **RRS/RPCS: control rod control**
    - **DRCS: control rod drive**
  - **Process – Component Control System**
    - **NSSS Process Control System**
      - **Feedwater Control System**
      - **Steam Bypass Control System**
      - **Pressurizer Pressure Control System**
      - **Pressurizer Level Control System**
    - **BOP Control Systems**

7.7 Control Systems Not Required for Safety

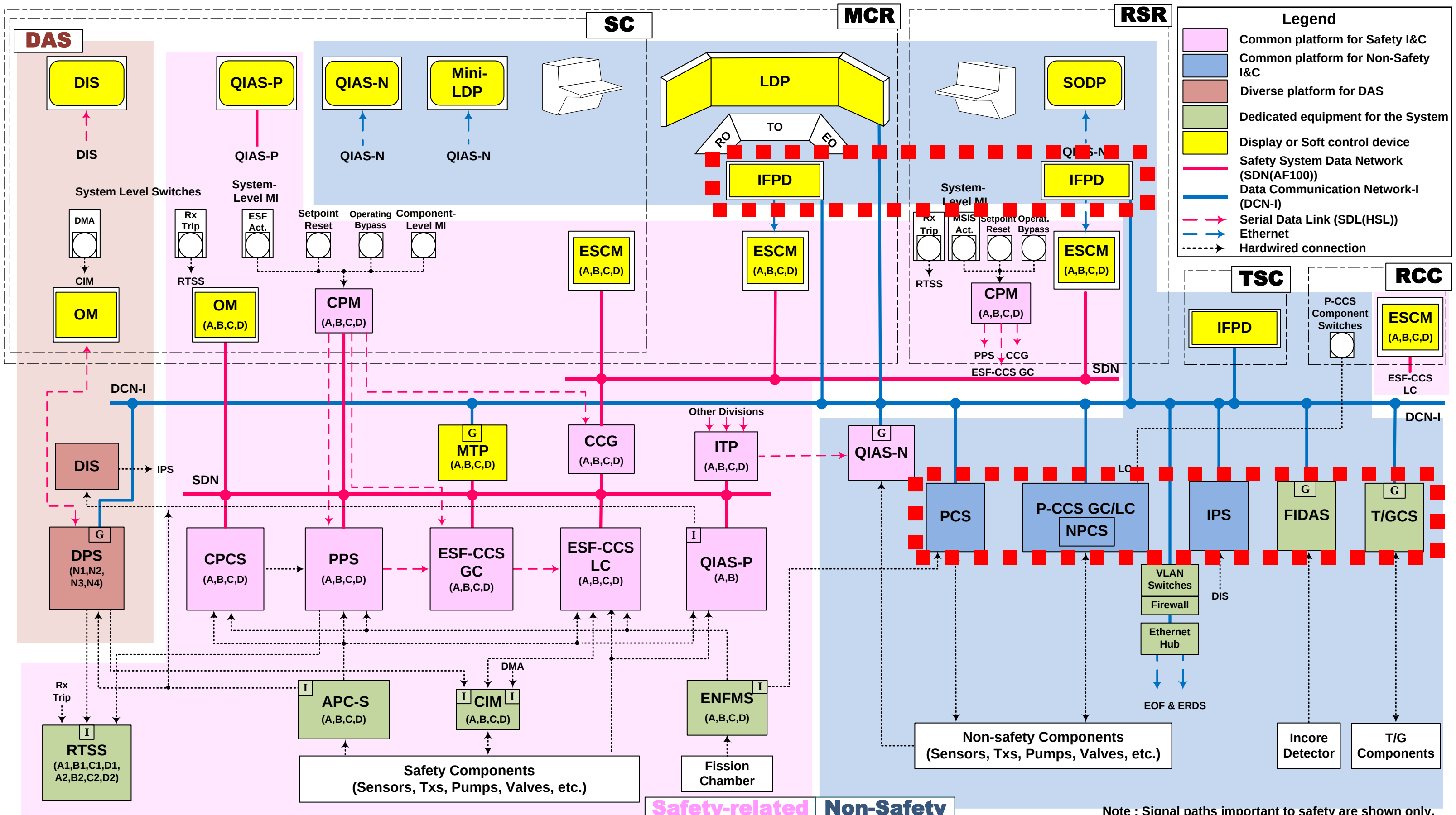
Effects of Control System Failures

- **Single Failure of Control Systems**
  - The control system failures caused by a single failure as an initiating event do not cause plant conditions more severe than those described in the safety analysis of AOO in DCD Chapter 15.
- **The following postulated failures caused by a shared signal failure and control system CCFs are evaluated to confirm that the event consequences of Chapter 15 are still effective and the analysis acceptance criteria are met.**
  - Effects of multiple function failures due to a single failure of a shared signal[1]
  - Effects of multiple failures of a single control group due to a CCF
  - Effects of multiple failures of more than one control group due to a CCF
  - Effects of multiple failures of IFPD control commands due to a CCF

[1] A shared signal is a signal whose failure causes multiple function failures in two or more control groups.

7.7 Control Systems Not Required for Safety

- Postulated Failure Boundary of Control System CCF



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 (June.20. 2017)

7.7 Control Systems Not Required for Safety

- **Control Group Assignment for the evaluation**
  - **Control functions are assigned to a separate control group that consists of at least one separate controller.**
    - **Each control function is assigned to a separate control group using independent controllers so that the result of multiple failures due to the CCF of a single control group can be limited and meet the AOO acceptance criteria of Chapter 15.**
    - **The control function that can cause excessive transients in the process due to the CCF can be assigned to more than one control group to limit the failure effects.**
    - **More than one control function can be assigned to a single control group if the result of the multiple function failures meet the AOO acceptance criteria.**
    - **Function [Control group(s)] : Control Rod Control [RRS/RPCS, DRCS], SG 1/2 FW Control [FWCS 1, FWCS 2], PZR Pressure Control [PPCS], PZR Level Control [PLCS], Turbine Bypass Control [SBCS Main, SBCS Permissive], Reactor Makeup Control [CVCS] and so on.**

7.7 Control Systems Not Required for Safety

- **Evaluation Results of Control System CCF**
  - **The evaluation concludes that all multiple failures caused by a shared signal or a control system CCF do not cause plant conditions more severe than the acceptance criteria of the DCD Chapter 15 AOOs and PAs.**
    - **The results of multiple failures due to a single failure of a shared signal meet the AOO acceptance criteria of Chapter 15.**
    - **The results of multiple failures of a single control group due to control system CCF meet the AOO acceptance criteria of Chapter 15.**
    - **The results of multiple failures of more than one control group due to control system CCF meet the PA acceptance criteria of Chapter 15.**
    - **The results of multiple failures of IFPD control commands due to control system CCF meet the PA acceptance criteria of Chapter 15.**
  - **The detailed assumptions and evaluation results for the above postulated control system CCFs are provided in the Control System CCF Analysis Technical Report.**

Attachment : Acronyms

- AOO: anticipated operational occurrence
- CCF: common cause failure
- CCW: component cooling water
- CVCS: chemical volume control system
- DRCS: digital rod control system
- FPGA: field programmable gate array
- FWCS: feedwater control system
- HSI: human system interface
- MTS: MCR/RSR master transfer switch
- PA: postulated accident
- PLCS: pressurizer level control system
- PPCS: pressurizer pressure control system
- RPCS: reactor power cutback system
- RRS: reactor regulating system
- SBCS: steam bypass control system
- SDL: serial data link
- SDN: safety system data network
- For others, see page 20.

Presentation to the ACRS Subcommittee

APR1400 Design Certification Application

Review Safety Evaluation Report with Open Items

Chapter 7: Instrumentation and Controls

June 20, 2017

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

Objective and Expected Outcome

Objective

Brief the Subcommittee on the staff's review of the APR1400 I&C system

Expected Outcome

Common understanding of the background, the staff's evaluation efforts, and the current status of the APR1400 I&C system review

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

Staff Review Team

Technical Staff from NRO/DEI/ICE

Deanna Zhang
Dinesh Taneja
Kenneth Mott
Jack Zhao
Joseph Ashcraft
Wendell Morton
Dawnmathews Kalathiveettil

Project Managers

William Ward
Michael Eudy

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

Introduction

- **KHNP submitted the APR1400 design certification application on December 23, 2014.**
- **This safety evaluation and related reports represent 2 years of effort for both staff and the applicant.**

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

Background

Major Documents Reviewed

Title	Revision
APR1400 FSAR, Tier 1 Section 2.5 and Tier 2 Chapter 7	0
Safety I&C System Technical Report, APR1400-Z-J-NR-14001-P	0
Diversity and Depth-in-Depth Technical Report, APR1400-Z-J-NR-14002-P	0
Software Program Manual, APR1400-Z-J-NR-14003-P	0
Control System CCF Technical Report, APR1400-Z-J-NR-14012-P	0
Setpoint Methodology, APR1400-Z-NR-J-14005-P	0
CPC Setpoint Analysis Methodology, APR1400-F-C-NR-14001-P	0
Component Interface Module Technical Report, APR1400-E-J-NR-14001-P	0
Functional Design Requirements for CPCS Technical Report, APR1400-F-C-NR-14003-P	0
Common Q GOI and PSAI Resolution for APR1400, APR1400-A-J-NR-14003-P	0
Common Q Platform Supplemental Information, APR1400-A-J-NR-14004-P	0

*Common Q Topical Report, WCAP-16097-A, Revision 3

Regulatory Basis

- **Regulations and Guidance**
  - 10 CFR 50.55a(h)
    - IEEE Std 603-1991
  - Applicable GDCs
  - 10 CFR 50.34(f)(2)
  - 10 CFR 50.62
  - SRP Chapter 7
  - Applicable Regulatory Guides and NUREGs

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

Status Overview

SRP Section/DCA Section		No. of Questions	No. of Open Items*
7.1	Introduction	73	17
7.2	Reactor Trip System	17	1
7.3	Engineered Safety Features Systems	22	3
7.4	Systems Required for Safe Shutdown	8	0
7.5	Information Systems Important to Safety	7	2
7.6	Interlock Systems Important to Safety	3	1
7.7	Control Systems Not Required for Safety	20	3
7.8	Diverse Instrumentation and Control Systems	15	1
7.9	Data Communication Systems	19	5
Totals		**184**	**33**

*Current status: 21 open items remain.

Significant Open Items

- Key issues remain regarding following topics:
  - Data communications independence (7.9)
  - Setpoint methodology (7.1)
  - SDOE vulnerability analysis (7.1)
  - Control system failure analysis (7.7)
  - PAMS variable basis (7.5)