Official Transcript of Proceedings ACRS T-3404

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control
Systems Subcommittee

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, September 13, 2007

Work Order No.: NRC-1770 Pages 1-251

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

TRO

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

September 13, 2007

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on September 13, 2007, as reported herein, is a record of the discussions recorded at the meeting held on the above date.

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)

+ + + + +

SUBCOMMITTEE ON DIGITAL INSTRUMENTATION

AND CONTROL SYSTEMS

+ + + + +

THURSDAY,

SEPTEMBER 13, 2007

+ + + + +

The meeting was held in Room T-2B3, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, at 8:30 a.m., Dr. George Apostolakis, Chairman, presiding.

MEMBERS PRESENT:

GEORGE E. APOSTOLAKIS, Chairman

OTTO L. MAYNARD, ACRS Member (ex officio)

SAID ABDEL-KHALIK, ACRS Member

MARIO V. BONACA, ACRS Member

NRC STAFF PRESENT:

GIRIJA SHUKLA

GARY HAMMER

BELKYS SOSA

NRC STAFF PRESENT (Continued):

IAN JUNG

MICHAEL WATERMAN

PAUL REBSTOCK

PAUL LOESER

JACK GROBE

WILLIAM KEMPER

MARIO GARERI

NORBERT CARTE

RUSS SYDNOR

STEVE ARNDT

SCOTT MORRIS

MIKE MARSHALL

MICHAEL BOGGI

STEVE PERSENSKY

ALSO PRESENT:

KIMBERLY KEITHLINE

GORDON CLEFTON

RICH MILLER

WES BOWERS

TOM HAYES

JIM RILEY

TABLE OF CONTENTS

P R O C E E D I N G S

(8:15 a.m.)

CHAIRMAN APOSTOLAKIS: The meeting will now come to order. This is a meeting of the Digital Instrumentation and Control Systems Subcommittee of the Advisory Committee on Reactor Safeguards.

I am George Apostolakis, Chairman of the Subcommittee. ACRS members in attendance are Mario Bonaca, Otto Maynard, and Said Abdel-Khalik.

Sergio Guarro is also attending as a consultant to the Subcommittee.

Girija Shukla of the ACRS staff is the designated federal official for this meeting.

The purpose of this meeting is to discuss the digital INC entering staff guidance, as well as the digital INC project plan. We will also hear presentations from the Nuclear Energy Institute and the NRC staff.

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

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

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

A transcript of the meeting is being kept and will be made available as stated in the Federal Register notice. Therefore, we request that participants in this meeting use the microphones located throughout the meeting room when addressing the subcommittee.

The participants should first identify themselves and speak with sufficient clarity and volume so that they may be readily heard.

We will now proceed with the meeting. I call upon Ms. Belkys Sosa of the NRC staff to begin.

MS. SOSA: Thank you.

Good morning. My name is Belkys Sosa, and I'm the Director of the Digital I&C Task Working Group. In this capacity I report directly to Mr. Jack Grobe. He's the Chair of the Digital I&C Steering Committee.

As Dr. Apostolakis mentioned, the purpose of today's meeting is to provide the ACRS with a status update of the staff efforts in the activities of digital I&C and the development of the internal staff guidance.

Today's agenda, first of all, I'd like to say that this is an information briefing. The staff is not at this time requesting a letter. A formal ACRS review and approval process is built into the project plan as part of the long-term activities, and this is associated with the standard processes for updating reg. guides and the standard review plan. So that's built into the long-term activities.

Of course, we appreciate any feedback that you have to give us during the meeting. That would be welcome.

Today I will provide a very high level view on the digital I&C Steering Committee activities and as well as the project plan. Following my presentation industry will discuss their perspective on the issue being addressed by the interim staff guidance.

The meeting will continue later today with the staff's presentations on the details of the interim staff guidance. What has been developed today is considered a draft and is currently going formal concurrence by the Steering Committee as well as OGC, and we plan to issue the four interim staff guidances we're discussing today at the end of this month, with possibly one exception, and we will get to that later

today, which will be cyber security.

All things from staff guidance that we prepared today are on the website, on the digital I&C webpage. They're available to you, and industry has provided comments that have been discussed at public task working group meetings.

Here with me today I have the managers of the task working groups for the four areas that we'll be discussing. In the area of integrated highly control room communications we have Mr. Bill Kemper, who is going to be assisted by his technical lead, Mr. Paul Rebstock.

In diversity and defense-in-depth we have Ian Jung, Mike Waterman and Paul Loeser.

And the staff has also prepared an update regarding the ACRS recommendations from our last meeting in May and to assist Ian Jung with that, we will have Russ Sydnor as well as Steve Arndt from the Office of Research.

Later this afternoon to address the cyber security interim staff guidance we will hear from Mr. Mario Gareri of NSER.

And in the area of human factors we will have Mr. Mike Marshall, Mike Wolfe and Jake Berzinski from the Office of Research.

A little bit of background here. Following the Commission briefing on November 2006, the EDO established a Steering Committee, and this was in response to a staff requirements memorandum from the Commission.

The primary responsibilities of the Steering Committee are to interface with industry on key digital I&C issues, to facilitate consistent resolution of digital I&C issues, both technical and regulatory issues, and to provide oversight and guidance to the NRC line organizations on those issues; also, to assure timely resolution of any strategic or policy issues associated with deployment of digital technical at near reactor, operating reactors, as well as fuel cycle facilities.

Staff briefed the ACRS in May of 2007 on digital I&C issues. On June 22nd, the staff requirements memorandum directed the staff to incorporate the ACRS recommendations into the digital I&C project plan, and the staff has done that.

In addition, the Commission directed the staff to provide interim staff guidance by the end of this month, September 2007, and the staff will provide an update on the record that are on the way in response to the ACRS recommendations as part of

today's update.

CHAIRMAN APOSTOLAKIS: So the interim guidance then, there will be no ACRS letter on that because we don't --

MS. SOSA: We're not requesting a letter. This is an information briefing.

CHAIRMAN APOSTOLAKIS: We could have volunteered one, but there is no time for that, right? Because you are starting a team by the end of the month, and the next full Committee meeting is in October.

MS. SOSA: That's correct.

CHAIRMAN APOSTOLAKIS: And I understand there will be a presentation on this stuff in October?

MR. SHUKLA: Yes, yes.

CHAIRMAN APOSTOLAKIS: Why, if there is no chance for a letter? Why do we have this briefing in October?

(No response.)

CHAIRMAN APOSTOLAKIS: Okay.

MS. SOSA: The staff --

CHAIRMAN APOSTOLAKIS: What is your deadline, September 30th?

MS. SOSA: That's correct. Now this is --

CHAIRMAN APOSTOLAKIS: We could comment

anyway, right?

MR. HAMMER: Right. George, this provides an opportunity for the Committee to weigh in on any issues they'd like to.

CHAIRMAN APOSTOLAKIS: Well, but it's a bit unfair to the staff who do not have a chance to respond.

MR. HAMMER: Right.

CHAIRMAN APOSTOLAKIS: Jack, do you want to say something?

MR. GROBE: George, I always want to say something. The interim staff guidance that we're issuing, we will issue many of them by the end of September. Some will come out in October and November. They're interim. They're going to continue to be refined before we get to the point of incorporating them into reg. guides and standard review plan updates.

So if the Subcommittee wants to send us a letter, we're certainly going to take any verbal feedback.

CHAIRMAN APOSTOLAKIS: Yeah, we can send a letter.

MR. GROBE: I think your point is well taken, and we look for your guidance. I'm not sure

it's necessary at this point to have a full Committee meeting on these issues because this is an evolving process. There's regular procedures for interaction with the ACRS on updates of reg. guides and standard review plan activities. So we would be looking for formal feedback from the ACRS as part of that process, and that's built into our project plan.

CHAIRMAN APOSTOLAKIS: I guess at some point maybe I should know this, but can you explain to me what "interim" means? At some point it will become final.

MR. GROBE: That's correct.

CHAIRMAN APOSTOLAKIS: So "interim" means what? Well, I know what it means in English, but in the NRC world, what does it mean?

MS. SOSA: Let me say what the purpose of us pushing this forward quickly is. We have two licensees, operating reactor licensees, that either have an application in or it will be coming in shortly for significant digital upgrades. That's Wolf Creek, using field programmable Gator As (phonetic) in their main steam and feed isolation system, and Okonee is contemplating a significant retrofit for digital.

So the purpose of getting this guidance out is for those licensees to have the benefit of the

latest thinking in the work that's been going on between the staff and the industry.

In addition, there's a number of COL applications that are anticipated to come in in the fall, as well as design certification activities for new reactors.

So the purpose of the interim guidance is to get as much information out to our stakeholders as possible to streamline the process of reviewing the applications and make it as predictable as possible.

The official process for doing this, of course, is updating reg. guides and updating the standard review plan, and we'll get to that as soon as we can. It will probably be during 2008, but so "interim" just means that it's something that is provided for the industry's use, for public stakeholders to be aware of what we're doing in this area, to insure that the communication with the industry is as effective as it can be.

CHAIRMAN APOSTOLAKIS: Doesn't this create a precedent though.

MR. GROBE: No, we use interim staff guidance in a number of areas. We've used it in the fuel cycle area. We've used it in license renewal. So this is a standard, and if you go to the NRC

webpage, there's an interim staff guidance link where you can find all of these interim staff guidance, and there's a separate link on that page to the digital interim staff guidance.

CHAIRMAN APOSTOLAKIS: But, I mean, the final document that will go to the SRP may be different from the interim guidance.

MR. GROBE: I expect it will be, and the industry has indicated an interest in continuing to engage with us after we issue the first revision of the interim staff guidance to further refine it before we get to the regulatory guides.

CHAIRMAN APOSTOLAKIS: And the two licensees who will be reviewed under the interim guidance are aware of the fact that maybe the final will be different and they have to go back?

MR. GROBE: They've been participating in many public meetings we've had.

CHAIRMAN APOSTOLAKIS: Okay. Good. Thank you.

MS. SOSA: The most recent Commission meeting on the status of digital I&C project took place on July 18th. The Commission supported the staff's approach as described in the digital I&C project plan, which was approved July 12th of this

year.

Key challenges. Again, assure predictability as Jack was describing. We have successfully used prime (phonetic) guidance to review and approve digital I&C applications. The objective of the interim staff guidance, again, is to provide clarity. There was a lot of questions about the upcoming upgrades for digital I&C systems and how that relates to the COL applications or the signed certification applications that we're expecting.

And, again, what we wanted to do was communicate clearly what the criteria is going to be that we're going to use to review these applications and what we're putting forward is essentially one acceptable method in a lot of these cases. It's not the only answer. It not -- certainly means that applicants are not going to be able to come in with a different approach and eventually we would review that, and after a few rounds of REIs probably find it acceptable or make a determination. That's still open.

But what we wanted to do is clearly communicate an acceptable method, and that's the purpose of the interim staff guidance.

As digital technology continues to evolve

and is applied more comprehensive to safety systems, we expect the regulatory guidance on positions will need clarification. So the Digital I&C Steering Committee and the task working groups is the process for us to be able to enhance and continue to clarify the guidance as they are formalized in the reg. guides.

As Jack mentioned, the process that we've established for developing and issuing interim staff guidance is described in a document which is on the website and has been successfully used in the past for site permits as well as license renewals.

Again, I'm repeating a lot of what's already been said. So I'm just going to quickly go through this.

CHAIRMAN APOSTOLAKIS: What international interactions do you have?

MS. SOSA: International interactions? For instance, during this year the staff was involved in the digital instrumentation control; the international symposium on digital common cause failures, which was sponsored by IAEA.

We were also engaged in a full day meeting with regulators from seven different regulatory agencies to discuss diversity and defense-in-depth

technology and other regulatory issues, and this has been ongoing. These are two recent examples that I can cite.

CHAIRMAN APOSTOLAKIS: Your impression that we are behind?

MS. SOSA: I think the staff has been plugged into the efforts that are going on internationally. So from a staff perspective I think we are on top of the issues.

When it comes to developing guidance and regulations, I think we're lagging in some areas and in other areas we're just right there. Everybody is trying to figure out what the right answer is to these questions.

MR. GROBE: I believe several months ago we provided the committee with a listing of international interactions in the digital arena over the past several years. Yeah, everybody is nodding. So you have a listing that showed an extensive amount of interaction internationally.

We've been supporting a lot of the international application, from a regulatory perspective, application of digital. A number of the reactors and a number of the regulatory bodies that have been challenged to deal with this new technology.

CHAIRMAN APOSTOLAKIS: Now, the workshop on common cause failures, was it the place that everybody recognized that this is an important problem or did anyone offer a solution?

MS. SOSA: I'd like to get some assistance from Mr. Bill Kemper who was there perhaps.

MR. KEMPER: Yes, Bill Kemper here.

I chaired that session, and, yes, it was recognized by all of the participants that this is a key issue worldwide that has to be addressed. Many different options for coping with common cause failure was discussed by several of our international guests as well as vendors in the U.S. as well. So for sure this is a significant issue that everyone is grappling to cope with.

MEMBER BONACA: But as I understand it common cause failure is part of the design basis in Germany, for example, the Siemens design, where one is not part of the design basis in the U.S. So to what extent has that requirement, you know, provided some kind of leave work on the part of some international participants like the Germans?

I mean, are they to assume common cause failure in their accident analysis? And so they must have had some lead or some experience that we have not

because, I mean, we seem to have made common cause failure not part of the design basis.

MR. KEMPER: Well, we found out that during that conference as well as the one-day meeting that Belkys mentioned just prior to that there's many international regulators already have requirements for diverse back-up systems to cope with that. So in other words, they acknowledge the fact that it's real, and as you say, some of them consider that a design basis event. Of course, we don't here in the NRC in the U.S. It's beyond a design basis event, which we'll talk about at length here shortly.

MEMBER BONACA: So there is some experience we can draw upon in other countries.

MR. KEMPER: Yes, absolutely. Yes, that was the purpose of that conference, quite frankly, and we did gain a lot of insights from that conference.

MEMBER BONACA: Okay. Thank you.

MS. SOSA: This is the structure of the Steering Committee. Again, we're structured to interact with industry to identify issues and priorities.

CHAIRMAN APOSTOLAKIS: We have seen this.

MS. SOSA: Yes, we've seen this before.

CHAIRMAN APOSTOLAKIS: Can we move on?

MS. SOSA: The only thing that I'd like to point out is that in August the Steering Committee established a new task working group, one that is specifically going to deal with fuel cycle facilities, and it's not on this graph yet. We haven't had a change to update.

They are planning their first task working group meeting with industry, a public meeting for the beginning of October, and it's specifically to deal with regulatory issues for fuel cycle facilities.

CHAIRMAN APOSTOLAKIS: Good.

MS. SOSA: And they plan to engage with the Advisory Committee on Nuclear Waste and Materials. So that's in the works as well.

The structure of the project plan based on the December 6th memorandum, as well as the charter for the Steering Committee. The project plan was approved July 12th and a copy of it is available on the website, as I mentioned earlier.

The near term objectives of the project plan is to issue interim staff guidance to clarify the staff's positions and expectations on a time frame that supports industry needs and provides a regulatory framework to assure high level of confidence in NRC staff acceptance of an application.

This approach has been successfully used in other areas of licensing reviews. We mentioned earlier license renewal as well as early site permits. The longer term objectives of the plan are to complete additional development work, which is being conducted in the Office of Research to further refine the interim staff guidance as appropriate and incorporate that guidance into the NRC's existing regulatory framework, like the standard review plan as well as the reg. guides and new regs.

We expect to complete most of the interim guidance in 2007, as well as continue to work with industry to revise our regulatory tools as necessary.

In summary, I'd like to state that the Steering Committee is functioning effectively. The project plan is in place. We plan to continue stakeholder interactions through the public task working group meetings with industry, and the staff is currently on schedule to complete the interim staff guidance by the end of September in accordance with the near term objectives of the project plan.

We will continue to coordinate efforts with industry to resolve digital I&C issues in the long term in order to refine and enhance staff guidance, and we believe the staff has done an

outstanding job in preparing this interim staff guidance, and we appreciate the committee's interest in this area.

That concludes my presentation.

MEMBER MAYNARD: I'd like to go back to Mario's question for just a minute because I was at that international meeting along with a couple of the other ACRS members, and I agree that everybody recognized it as a problem. One of the main differences though is that each country has got a little bit different regulatory philosophy, and there are some advantages and disadvantages to each.

We tend to want to be a little more prescriptive. Some of the others tend to have the requirement, but leave it up to the vendor to come in with a proposal and they discuss it and come to an agreement.

So I'd say the biggest differences that I saw was kind of how some of the regulatory bodies would handle a requirement, and like I said, there's pros and cons to tall kinds of ways there, but everybody did recognize it as an issue.

MEMBER BONACA: Well, at least in Germany I'm familiar with they have, you know, implemented back-up systems. They have a systematic approach to

the inclusion of common cause failure in accident analysis, and that cascades into, you know, all kinds of requirements. Their break (phonetic) system is supposed to provide success not only for the first scram, but also for the back-up scram, and in the U.S. we allow for the first scram to be successful, the second one is too damaging and there's something happening. So there are really different requirements there.

I'm telling you that they spend a lot of time on those issues. We may learn something from it. I mean, we don't have to endorse what they do, but they may have gone, you know --

MEMBER MAYNARD: Right, but there were other regulatory approaches to some of those same issues that were different.

MEMBER BONACA: Well, I agree. I'm not saying that we should endorse whatever, but there is the thing there is significant experience out there that can be leveraged.

MEMBER MAYNARD: But I saw a wide spectrum on how they dealt with some of the requirements. Most of them had requirements, but there was a spectrum in how they dealt with it.

MEMBER BONACA: Sure.

CHAIRMAN APOSTOLAKIS: Okay. Thank you.

MS. SOSA: I believe next is industry.

CHAIRMAN APOSTOLAKIS: NEI. Who is making the presentation?

MS. KEITHLINE: I am.

Good morning. Please let me know if you can't hear. I'm used to yelling without microphones. So I don't want to yell, and I do want to be heard. I'll try to do my best.

We do appreciate -- oh, I brought along with me Jim Riley, my boss at NEI, and Gordon Clefton is here also. He's been following one of the specific groups and will be able to answer questions about the communications group.

We appreciate the opportunity to meet with you today, and we appreciate the ability to share our perspective on what has been really quite an effort over the last few months. We'd like to spend just a little bit of time this morning providing our thoughts on four of the task working groups, the ones that are finalizing interim staff guidance in the next few weeks or so. One may be lagging a little bit behind, but that's okay.

We are very encouraged by the interactions that we've had with the staff in several areas related

to digital I&C and human factors over the last few months. There's been very good open discussion and sharing of ideas. They've been listening to our concerns. We appreciate that.

The creation of the I&C Steering Committee and the task working groups has been very helpful in focusing the efforts and driving toward resolution of the issues. That's been a very positive thing.

Having said that, I would like to note that we'll need to be a little bit careful and not to let the cart get before the horse as we move forward. Things are moving very quickly, and that's good. There may be a couple of areas where more work is needed to really produce real good, usable guidance for the longer term, and as Jack mentioned, we are planning to continue working together to further refine that guidance.

We'll start with the task working group that really had a head start on this whole effort. The Task Working Group No. 4 that you'll hear more about later from Bill Kemper and company had a very clearly defined problem when they started. The IEEE Standard 7-4.3.2 has an annex, annex Echo that provides guidance for communications independence.

However, when Revision 2 of Reg. Guide

1.152 was issued, it specifically did not endorse that annex, and it said that there was insufficient guidance in the annex for it to be endorsed. So this Task Working Group No. 4 has been working on developing additional guidance to help close that gap and provide guidance to both industry and the regulators on ways to do communications and maintain appropriate levels of independence.

Industry kind of kicked off this effort by submitting a white paper on the subject to start the discussion, and I've lost track of how many meetings there have been, but there have been a lot of meetings, public meetings, to discuss this subject. About every three weeks since the beginning of the year. So there has been a lot of interaction.

And based on all of that the staff appears to be well on track to issue interim guidance this month, I believe, on this subject. We're up to at least Rev. H. So it has gone through quite a process of review and revision, and then the IEEE group working on in parallel a revision to 7-4.3.2 has been following what this task working group has been doing and hopes to be able to incorporate much of the new guidance into the standard.

It will have to be, you know, an industry

consensus standard, but the ideal goal is to then have the standard revised, and the next time that Reg. Guide 1152 is revisited, it could hopefully endorse the standard, and the guidance would be out there in multiple forms able to be used.

I just looked to Gordon for a second to see if there are any points on this one. this is his task working group, and if there's anything else that he'd like to add.

MR. CLEFTON: I'd just like to say that we certainly appreciate the effort that Bill and Paul have done in listening to us and comments. We've had some aggressive discussions and meetings. We haven't always agreed. We've agreed to disagree on a few items, but it's not a closed issue even though we're issuing this Rev. H or I at the end of the month. We'd like to say that the ISG is still an ongoing issue, that we hope to continue communication details as progress goes with the IEEE standard and our development with the industry.

My name is Gordon Clefton. I'm with NEI.

Thank you.

MS. KEITHLINE: Thanks, Gordon.

With this one and the other ISGs that come out, this one we feel is in very good shape. The real

test, of course, will be when it's actually used by both industry and the reviewers to work through a submittal, and then we may find some things that need further refinement, but we'll deal with that.

The next group, Task Working Group No. 2, has the area of diversity and defense-in-depth, and this group really took on quite a challenge initially identifying eight problem statements to go tackle and resolve, and these problem statements were intended to answer the following questions.

What constitutes adequate diversity?

How can operator action be used as a defensive measure?

And what are acceptable assumptions for operator response time?

When are independent displays and controls needed?

And can you have component level actuation?

What effects need to be considered for common cause failures? And that means if it just fails to actuate or do we need to look at spurious actuations, things like that?

Are there design attributes that are sufficient to eliminate consideration of common cause

failures? Are there some systems or components that can be simple enough or something else enough so that you don't need to consider a common cause failure?

Another question is do the four echelons of defense always need to be diverse from each other. Does your reactor trip system always need to be diverse from your SFAS, or if they're not truly backing each other up, is it okay to have a common platform?

Additional clarification was also requested regarding the acceptance criteria for addressing common cause failures compared to the acceptance criteria for addressing the design basis single failure? And we've been working on that.

You'll note that one of these eight items listed has been crossed out.

The third problem statement that was initially developed was eventually deleted from the list, and where this came from , in the previous version of the branch technical position 719, there was toward the end some discussion on what to do if identified vulnerabilities are not addressed, and there was an example given, and it said that, for example, INC system vulnerability to common mode failure affecting the response to large break loss of

coolant accidents and main streamline breaks has been accepted in the past.

This acceptance was based upon the provision of primary and secondary coolant system leak detection and predefined operating procedures that together enable operators to detect small leaks and take actions before large breaks occur.

A few months ago industry desired additional guidance on how that type of an example could be used as we go forward. The standard review plan was being revised in parallel with the efforts of these task working groups, and in the current revision of Branch Technical Position 7.19 that came out in March, that example was deleted from the branch technical position.

That problem has been deleted from the list of problems to be addressed. I shouldn't speak for NRC. I think it was judged to be a very difficult one to take on, and that there was not a high expectation of success in terms of further refining how this could be used.

A real sensitivity that I understand to not wanting to have it look like or even have it may be that we were applying a leak before break mentality in an application it wasn't intended for. But this is

an area that I'll explain why maybe some reasons that this was important. Industry thought this may be worth considering.

Okay. We have two most significant challenges related to diversity and defense-in-depth, are related to how to take credit for manual operator actions and whether and how to incorporate the idea of using risk insights in the diversity and defense-in-depth evaluation process.

One of the draft interim staff guidance documents -- what I'm seeing down here is going in and out. So I'm sorry about that -- one of the interim staff guidance documents, the first one that came out in draft form in June included a 30 minute criteria for determining whether an automatic diverse actuation function is necessary. That initial draft ISG said in those instances where protective action is required in less than 30 minutes, an independent and diverse automated back-up achieving the same or equivalent function should be required.

Industry was concerned that such guidance could result in the need for additional automation and complexity that would not really enhance safety. The industry's fundamental belief is that credited manual actions taken to initiate protective functions must be

demonstrated, and that specific time frames for execution of manual actions should be evaluated by NRC during the review of D3 evaluations.

We don't agree that a specific time limit can be applied across the board for all scenarios. We just don't think that's appropriate.

Industry has recommended a process for determining appropriate operator response time assumptions for diversity and defense-in-depth evaluations. Because of time constraints and resource limitations that we understand we haven't been able to incorporate that approach into this first round of interim staff guidance.

We would like to continue to work with the diversity and defense-in-depth task working group and the human factors task working group to further refine that guidance and incorporate it eventually so that we have a process for deciding what assumptions make sense about operator actions rather than using just one fixed time limit.

CHAIRMAN APOSTOLAKIS: In the case of fires there is a regulatory guide that deals with manual operator actions, manual actions where they do this. They --

MS. KEITHLINE: Have a process?

CHAIRMAN APOSTOLAKIS: They look at the -- there is an estimate of how long it will take for the fire to grow and do damage, and then the response time of the operators, and then they put the margin because it's supposed to be a deterministic evaluation. So if, for example, the fire will take 20 minutes to damage something, then there is a safety factor or a safety margin. So the operators should demonstrate that they can take actions, say, in 12 minutes. I'm pulling numbers out of the air now, but is that something you have in mind rather than a fixed time?

MS. KEITHLINE: Right. The basic way you've described that is very similar to what we're thinking. Look at the indications, the emergency operating procedures, the training, and use some way of validating the assumptions.

CHAIRMAN APOSTOLAKIS: So you may look at that regulatory guide. I think it's 1852.

MR. RILEY: It is, yes, NUREG-1852.

MEMBER BONACA: Also ATWS provides you some examples, right.

CHAIRMAN APOSTOLAKIS: The ATWS rule?

MEMBER BONACA: The ATWS rule.

CHAIRMAN APOSTOLAKIS: I think it's more about the equipment.

MS. KEITHLINE: Right. I was thinking of ATWS more in terms of which types of functions need to be backed up automatically, which does lead kind of into the next point here, I think.

MR. GROBE: Kimberly, if I could just make one comment --

MS. KEITHLINE: Yes.

MR. GROBE: -- before you go on. It's important to understand that the interim staff guidance does not establish new requirements. What the interim staff guidance does is establish the parameters for the HOV lane on the highway. This is the fast lane.

If licensees meet all of the expectations of the interim staff guidance, then the NRC review would be significantly reduced. If they are going to try to do something different than the interim staff guidance, then the level of review would be greater. So the 30 minutes is not a requirement. It's a guideline that establishes the level of effort that we're going to end up putting into the review.

CHAIRMAN APOSTOLAKIS: But the guidance at this time does not say that there may be other approaches that will require review.

MR. GROBE: Right. That's just a

fundamental definition of what the interim staff guidance is. We're always available to review other approaches.

MS. SOSA: I believe the words are in there that allow some flexibility.

CHAIRMAN APOSTOLAKIS: I don't remember them, Belkys.

MS. SOSA: Maybe it's in the latest revision that's going around.

CHAIRMAN APOSTOLAKIS: I looked at the one that was on the website yesterday.

MR. GROBE: That's a good point.

MS. SOSA: Which is already --

CHAIRMAN APOSTOLAKIS: Maybe a few words to the effect that, you know, other approaches would be entertained.

MR. GROBE: That's a good point.

MS. SOSA: Let me get the latest.

MR. JUNG: Yes, this is Ian Jung. I am the D3 working group lead.

There is a couple of sentences related to this specific that allows other method to be used by the applicants, and the staff will review that.

CHAIRMAN APOSTOLAKIS: Has the sentence been added or will be added? I don't think it's there

now, is it?

MR. KEMPER: The latest one. Bill Kemper.

PARTICIPANT: Let me deal with that.

CHAIRMAN APOSTOLAKIS: That's okay. It's not big deal, as long as you say you're going to do it.

MR. KEMPER: I think there should be a preamble at the beginning of each ISG that explains what the purpose of the ISG is.

CHAIRMAN APOSTOLAKIS: Exactly, exactly. I think that would be great.

MR. KEMPER: Let's do that. Let's add a preamble section, introductory section to every ISG that clarifies that.

CHAIRMAN APOSTOLAKIS: But since in this particular case we have a regulatory guide in the different context that begins with a similar situation it wouldn't be a bad idea maybe even to mention it because, you know, it has been reviewed. We went through it with the staff, and they had to make a few changes. So it's just a thought.

I mean something that's so similar and it's acceptable in another context.

MR. GROBE: The risk is that there's many other complex issues associated with operator

reactions within the control room in response to digital. For example, their ability to identify that they have a problem is different, whereas, you know, fire is pretty easy to identify that you've got a problem.

So there's many of the human reliability attributes that are going to be the same.

CHAIRMAN APOSTOLAKIS: And these can be recognized.

MR. GROBE: Right.

CHAIRMAN APOSTOLAKIS: I'm not saying just copy the guy.

MR. GROBE: Right.

CHAIRMAN APOSTOLAKIS: Okay, Kimberly.

MS. KEITHLINE: Okay. The second major bullet on this slide says use of risk insights, and that's where industry believes that there really is a need to consider risk when making diversity and defense-in-depth decisions.

CHAIRMAN APOSTOLAKIS: Yeah.

MS. KEITHLINE: We are concerned that the deterministic approach to D3 might result in the use of automatic diverse actuation systems that do not improve plant safety, and in some cases might actually degrade safety because of the increased complexity and

the potential for spurious actuations.

We've been discussing this or we've started to discuss this with the PRA task working group, and we need to coordinate those discussions with the diversity and defense-in-depth task working group. We believe that the use of risk insights for current plants' license amendments involving digital technology would be beneficial in focusing on those aspects that are important from a plant safety perspective.

And this is where we view it as being similar to the way risk insights influence the development of the ATWS rule. It didn't apply -- it didn't have to back up every function in the reactor protection and safety systems, but rather those that were determined to be most beneficial from a risk or safety standpoint.

The challenge is to determine how best to apply such insights, recognizing that probabilistic modeling techniques for digital I&C are still evolving, and we believe that D3 evaluations can benefit from use of risk insights, and so we hope to continue to pursue this one with the task working groups.

CHAIRMAN APOSTOLAKIS: The document issued

by EPRI two or three years ago or the deals with this staff, is that what you're referring to, this approach using risk insights in D3? I don't need --

MS. KEITHLINE: I think it goes beyond the -- I think I know which document you're referring to, one on diversity and defense-in-depth --

CHAIRMAN APOSTOLAKIS: Yeah.

MS. KEITHLINE: -- that EPRI submitted. This concept may go beyond that, what was just in there, and look at going through a thought process of if we looked at what we've learned and are learning from PRAs by adding new systems, are we actually improving the core damage frequency or could we risk making it worse? And we factor that into the decision making process.

CHAIRMAN APOSTOLAKIS: Well, my problem with that document was that it kept talking about risk insights, but I didn't know what insights those were.

MS. KEITHLINE: I think we have more homework to do here. We've started to do some work. EPRI has through their contractor Dave Blanchard to look at an example PRA for I believe it's a Westinghouse plant.

CHAIRMAN APOSTOLAKIS: That would be very useful. Is that something that's near completion

or --

MS. KEITHLINE: I don't think it's near completion. It's in the early stages where we've started to have some discussions, but we have more homework to do to be able to stand up here and give a presentation that proves why adding certain systems may really be detrimental.

CHAIRMAN APOSTOLAKIS: All right. That would be interesting.

MS. KEITHLINE: That was just begun.

CHAIRMAN APOSTOLAKIS: That would be interesting.

MEMBER ABDEL-KHALIK: Do we understand the failure modes in sufficient detail to be able to make that assessment?

MS. KEITHLINE: We're also looking at operating experience data to try to better understand how these systems and components have failed in the past, and we're starting with our own nuclear power plants, recognizing that there is a larger group of industries out there that we could learn from.

We're starting to get some insights from that that we would factoring back into this effort, and my last slide has a few bullets on that. And I think the staff is also planning to talk about that

later today.

The third task working group is really Task Working Group No. 5, has four problem statements related to human factors. The first two on this list were determined to be the most urgent and have been what's being worked on for the near term interim staff guidance.

The third and fourth ones on the list will also be worked on, but they just have a longer term schedule here.

The original plan for this group was for industry to provide reports on minimum inventory and computer based procedures before the new regulatory guidance was developed, and the idea was that there would be industry reports that hopefully the NRC could endorse, EPRI reports that could be endorsed, and industry did submit a report on minimum inventory. I believe it was in late May, and then the schedule accelerated a little bit for issuing interim staff guidance, and we shifted our effort away from the second report and into a mode of frequent conversation with the staff to provide input to those two interim staff guidance documents that were being developed and tried to share ideas and comments and answer questions.

So we're still working on the second report, the computer based procedure report, and we intend to submit that to NRC, and we'd like to eventually get endorsement of those two reports. Those two reports are longer and more detailed than the first round of interim staff guidance. So they would provide additional guidance to industry.

And then our other longer term efforts include developing guidance for those other two problem statements, a grade approach, and the safety parameter display system, and I think the staff, Mike Marshall, is probably planning to talk in more detail about those later today.

The challenges really over the summer were directly related, I think, to supporting the accelerated schedule for the interim staff guidance. That group had to do a lot of work during July and August to develop guidance kind of ahead of completing the reports, and there were very good interactions, lots of ideas shared.

One challenge was making sure that we could get interim staff guidance out quickly enough to support the stakeholder's needs and still have enough information in that guidance to make it really helpful, and so longer term there are probably going

to be opportunities to provide some additional guidance to help both the industry know what to expect and the reviewers know what to look for, and here I've already mentioned that we hope to have endorsement of EPRI reports. We're dealing with resource constraints certainly at NRC and also in the industry to really have time to work on these issues, but so far the people have been putting in the long hours and really working hard, and we've got to finish developing the plans and schedule for completing this work in the longer term.

CHAIRMAN APOSTOLAKIS: Well, one thing that would really help me understand how these things work is to go back and take a look at one past incident. I have a representation from Brookhaven that was on a project that was sponsored by the NRC where there was an attempt to look at the past experience, and there were, for example -- they identified an incident that happened at Turkey Point in 1994, one at Pilgrim in 1997, Palo Verde 2 in 2005.

Take a few of those and say: look now. If we had implemented what we're proposing, this is what would have happened and would have saved the day. Because that's really using operating experience, and I would find that very, very useful rather than

talking at the level at which we usually talk, where it's really an argument from either side.

If you are willing to do it, and not only you but the staff as well, and that was really one of the motivations for us to request from the staff to go back and look at experience, as you probably know, because that will make it real.

You know, look. They had the problem with the diesel sequencers at Okonee, and this is where it would have been caught if we had implemented this idea. I think that would be very useful at least to me to understand the effectiveness and the usefulness of what is being proposed rather than making arguments and so on.

At some point it would be useful to see something like that. Take a few examples, you know, from past experience and try to see how this guidance would have helped. Okay.

MS. KEITHLINE: And we certainly agree with that. Jumping ahead, and I will come back to cyber security briefly, but on the last slide, I have a few bullets on a review that we started in May, just a few months ago, and it was maybe triggered by or Mike Waterman helped us because he had been doing some of this on his own. He likes to work late at night

and on the weekends.

So we started with --

CHAIRMAN APOSTOLAKIS: As he should.

MS. KEITHLINE: Mike had quite a list of failures in digital systems.

CHAIRMAN APOSTOLAKIS: Do you want a tear from us?

(Laughter.)

MS. KEITHLINE: Just a pat on the back for Mike.

CHAIRMAN APOSTOLAKIS: I'm going to get it. Somebody work on the weekend? Heavens.

MS. KEITHLINE: But so Mike had a head start on the list of failures, and it was more than a couple hundred, I believe, and we decided we'd try to find documentation on those failures and see what we could learn from them.

Some of them were hard for us to find the documentation, but we did find documentation on over 300 nuclear power plant digital failures or failures that occurred in digital systems or components, and when you dig deep into them some of them tend not to may be digital in nature.

We got this information from the NRC and INPO databases, and we're currently trying to review

this to pull, okay, what are the lessons learned, what was the nature of the failure, what defensive measures could have prevented this, how many of these are really common cause.

And also we're identifying, you know, a handful that are really interesting ones that would be good to pursue further like you said, as specific examples to use as lessons learned. We've had a few discussions with the staff about what we're doing. We want to keep them informed so that we can make sure that what we do complements what they're doing.

Because some of our information is from the INPO database, we're working with INPO to find out what we can share with others. It will have to be sanitized to some extent, but we are trying to issue a white paper this month on the high level findings, the key things that we take away from this separate and how we might apply that to all of this other work, especially in the area of D3 NPRA.

CHAIRMAN APOSTOLAKIS: That would be very useful.

MS. KEITHLINE: And then if I could quickly go back to cyber security. This is the last task working group I'm going to talk about this morning because this is the fourth one that's working

on near term interim staff guidance.

Now, this is Task Working Group No. 1, but I put it last. Last October the industry met with the NRC and discussed methods to resolve differences between the cyber security guidance in Reg. Guide 1.152 and NEI 04-04, and the Task Working Group No. 1 was established to address these issues and insure that the cyber security guidance that's provided is coherent and consistent.

Industry was concerned that they'd be off. Utilities would have to go. They already have to implement programs to show that they meet NEI 04-04, and they're looking at Reg. Guide 1.152 saying do we need two separate programs. You know, it's a little cumbersome. It would be nice if we could have one program, one document.

So that's really the desired outcome, to get to a point where NEI 04-04 is sufficient, and we will say you can use that and you'll satisfy the needs.

Now, to resolve this and the differences between those two documents, the task working group conducted a gap analysis to identify where the two documents overlapped or were inconsistent, and based on that gap analysis, industry has made some changes

to NEI 04-04. A few more changes may be necessary.

In August, the staff expressed concern regarding the ability to directly correlate the topical elements that are embodied within Reg. Guide 1.152 to the programmatic guidance that's in NEI 04-04, and to try to address that concern industry has created what they call a draft cross-correlation table to show where in NEI 04-04 the guidance from 1.152 is being addressed.

And there was a public meeting earlier this week, just Monday afternoon, to discuss that draft cross-correlation table, and the staff is still reviewing it because they only had a few days to look at it for the meeting. They're going to give us additional comments that we will incorporate, we'll address, we'll try to put what's really needed into NEI 04-04, and then hopefully we'll get to the point where we'll have an interim staff guidance document that says that NEI 04-04 is sufficient, contains the guidance that's needed.

MEMBER MAYNARD: Does NEI 04-04 go into more detail? I'm trying to figure out if once we get these documents consistent, is there a need for two documents?

MS. KEITHLINE: We hope that there won't

be a need for two in the longer term. We're not to that point yet, and Bill Kemper may want to add something, but my understanding is that it's adding some more design criteria to NEI 04-04 which in general is a much broader programmatic document for how a plant should -- a program that they should have to address cyber security.

Bill.

MR. KEMPER: Yes, this is Bill Kemper.

I guess the difference is NEI 04-04 is a programmatic document, as Kimberly says, for evaluating in situ digital systems, digital equipment on a site, and also it has programmatic requirement for how you maintain that in the future, you know, how you modify it and so forth.

Reg. Guide 1.152 has licensing criteria. Okay? So when NEI 04-04 was written, if I can speak for the industry, and approved by the staff anyway, it was not approved from the perspective of a licensing document, if you will, for new safety related digital assets.

So that's what the task here is, is to try to revise the language or certain sections of NEI 04-04 so that it can serve as a licensing document, as well as a programmatic document for each site.

And you know, if there is any deltas, slight differences in that, then that will be contained in the ISG, which Mario's going to explain that. I don't mean to steal your thunder here, Mario.

MEMBER BONACA: No, that's fine.

MR. KEMPER: And ultimately though, hopefully, you're right. One document, NEI 04-04, can serve both of those functions.

MR. GROBE: But it's very typical that when the industry develops a tool to provide more detail on how to implement a regulatory requirement or some regulatory guide, that we endorse that through an official agency document, either in a regulatory guide, sometimes in a regulatory information summary.

So we review and endorse industry standards for implementing various attributes of our regulatory responsibilities. So there's always going to be two documents. The best situation would be to have one where the NRC regulatory document would endorse an industry implementation standard.

MR. GARERI: I just want to add also to the mix there's going to be a reg. guide -- sorry.

CHAIRMAN APOSTOLAKIS: Tell us who you are, please.

MR. GARERI: Mario Gareri from NSER.

I just want to add to the mix by saying that there is going to be a reg. guide developed to support the proposal that's coming out on cyber security. So once that reg. guide comes out, then that will determine on what happens to this additional guidance that's being proposed right now.

I just wanted to make sure everybody was aware that there is a reg. guide being developed.

Thank you.

CHAIRMAN APOSTOLAKIS: Good.

MS. KEITHLINE: Okay. My final slide we've already covered most of it. I think I mentioned at the beginning that the real test for these interim staff guidance documents will be using them. I think we'll find some things that could be applied as we try to use them both on the industry and on the NRC side.

We're currently talking to a couple of licensees about whether they'd be willing to participate as sort of pilots. That's probably not the right word, but the concept would be that as they go through a review process, have your Steering Committee, the industry counterparts to the Steering Committee kind of watching more closely to see how well this is working and where we may need to make some changes as we go forward.

And then we talked about reviewing the operating experience data.

There are three other task working groups that are doing very important things. I did not include them in my presentation because I recognized that your day is very full and it looked like the subject of the meeting was the efforts related to near term interim staff guidance. So we'll look forward to discussing those other groups at some point in the future.

CHAIRMAN APOSTOLAKIS: Sure.

MS. KEITHLINE: We think we're pretty well coordinated, NRC and industry. I would like to ask though that if there are any significant surprises that come up during the rest of the day, that maybe we could have a chance to make a couple of additional comments at the end if that occurs.

CHAIRMAN APOSTOLAKIS: Absolutely.

MS. KEITHLINE: Okay.

MEMBER BONACA: Let me just say one thing here. Before you were expressing a concern regarding implementation of the CAP (phonetic) systems and the possible spurious actuation again. My suggestion is that you also don't limit yourself to just the domestic database or operating experience.

Again, I mean, there have been, you know, regulatory environments, and I quote Jim as an example, where they have, in fact, implemented back-up systems, et cetera. It would be interesting to know if they've had spurious actuations and the effects of those.

And I'm sure that there is literature about that information because that was an area of great focus in the '80s and '90s by the regulators in Germany. So there should be papers. There should be information. So my suggestion is that you don't limit yourself to domestic database. Just look at the effects of spurious actuations if there are any and what the experience has been.

MS. KEITHLINE: Okay. We'll do that, and I believe NRC staff is doing that through COMSYS if that's another means. So thank you.

Any other questions? Are we ready to turn it over?

CHAIRMAN APOSTOLAKIS: What kind of digital systems are we talkinga bout for reactors? Is it just actuation systems or are they going to control also the performance of the cooling system, for example, feedback and control?

MS. KEITHLINE: Feed pump --

CHAIRMAN APOSTOLAKIS: Feedback and control.

MS. KEITHLINE: Yes. I mean, they are control systems.

CHAIRMAN APOSTOLAKIS: Both?

MS. KEITHLINE: Reactor protection systems.

MEMBER BONACA: The feedback system.

CHAIRMAN APOSTOLAKIS: There are feedback.

MS. KEITHLINE: -- Systems have already done some digital upgrades, and we have Wes Bowers from Exelon is here.

CHAIRMAN APOSTOLAKIS: Safety systems? Safety systems?

MS. KEITHLINE: Let's see. I've got Rich Miller from GE is jumping up to help answer this question.

MR. MILLER: Rich Miller from General Electric.

All systems are digital basically on the General Electric's new designs. So trip systems, actuation systems, all your non-safety systems. Very few is analog.

CHAIRMAN APOSTOLAKIS: So once the safety system is actuated, then it's controlled by the

digital system again, halting the flows and everything?

MR. MILLER: The function logic is in a digital platform, right.

MEMBER BONACA: This guidance is going to be applicable to new designs.

MS. KEITHLINE: Yes.

MEMBER BONACA: And you know, one thing we discussed in the research reported to you was somewhat a concern I had with the whole philosophy of new design seems to be, you know, dimension and says if something happens just back off and don't intervene.

Now, for many compensatory actions to date we have taken credit for further action, in fact, to correct some problems caused by possibly digital I&C data. How do we reconcile this requirements?

I mean from one end, you know, you stay away from the controls. Just back off and do it the way that, again, the Germans have done for a long time, and from the other end compensating for possible malfunctions.

MS. KEITHLINE: That will be one of the challenges. The airline industry has taken different approaches to dealing with failures of digital systems or the operator's ability to intervene and interact.

From what we've read Boeing and Airbus take different approaches on how much to operate the pilot in their case is allowed to take over and override the system.

There are going to be issues, probably human factors type issues that need to be addressed. The more you automate things normally, that's going to affect how you do your training, how you write your procedures, how you keep the operator sufficiently informed of plant status and what's happening so that he or she can jump in if that's your approach and take over if necessary. There's probably a bit of work to be done in that area still.

MEMBER MAYNARD: The real key will be in the back-up systems as to how automated the back-up is and how hands off you want that to be. I personally have concerns if we try to make the system so complex that you step back, and even if the primary system is malfunctioning everything else takes care of it.

I do think it's reasonable that -- and, again, identification is the real key. If you can identify what it is, you know, the procedure stuff out there are very good at stepping through, and if you identify that the system didn't work, then you can initiate another action or something like that.

I think it's more in the back-up system

probably than the primary systems. How long do you require a hands off approach?

MEMBER BONACA: On the other hand, I mean, many of the positive experience in events or accidents, whatever, comes from, in fact, operator understanding the situation, and in part, oftentimes because he wasn't trained properly. I mean TMI is a classic example, but there have been many others.

So it's a complex issue, and I agree that designers should focus on that, but here we're talking about regulatory requirements, and when are we going to accept manual actions as a compensatory action in this kind of new environment?

Anyway, it's just another (pause).

MS. KEITHLINE: Oh, Wes Bowers from Exelon jumped up a minute ago, and it may have been related to the question about digital systems in power plants, and he would represent an existing plant perspective.

MR. BOWERS: Just following on, Wes Bowers from Exelon.

Following on with the comment that Rich made from GE for new plants, I'm with Exelon, and we have a bunch of digital applications in the current plants. In safety related systems currently it's mostly I'll call it discrete devices, like reactor

water lever, pressure compensation determination, suppression pool, bulk average temperatures and recorders, individual controllers that are digital.

For the most part at least in Exelon plants we don't have an integrated control system that's digital for safety related. We do have them for balance of plant. Turbine EHC control, recirc, feedwater. We have feedwater in just about all of our plants that's digital. So those are more of the type of control systems, the big control systems, that are currently in the plants, and then you heard earlier about Wolf Creek and Okonee proposing a more integrated control system for part of the safety systems that's digital.

MEMBER MAYNARD: Thank you.

MR. RILEY: This is Jim Riley at NEI.

Just a quick statement to reiterate or emphasize and agree with what Jack had said earlier, that it's very important to us that this effort continue after September 30th. There's a lot of work still to be done. You probably picked it up from Kimberly's comments and some of the issues we're continuing to work on.

So we recognize the priority, and we will be supporting this to the best of our ability, but it

may be a good idea to brief you guys down the road here a little bit and let you know how things are coming six months from now so that you can see that we've continued to make progress here.

CHAIRMAN APOSTOLAKIS: Well, we would always welcome presentations from the industry. When we meet with the staff, just ask and you will get some time.

And I was very pleased to see you using slides.

MS. KEITHLINE: I thought you would be.

CHAIRMAN APOSTOLAKIS: I've been on this committee for 12 years. It's the first time NEI is using slides.

(Laughter.)

CHAIRMAN APOSTOLAKIS: The very first time.

PARTICIPANT: Kimberly, how could you?

MS. KEITHLINE: Okay. If there aren't any other questions, you can turn it back over to the staff then.

CHAIRMAN APOSTOLAKIS: Okay. Thank you very much.

Now I have a problem with the schedule. We cannot stop the next presentation, can we?

MR. SHUKLA: We have ten minutes earlier for the break.

CHAIRMAN APOSTOLAKIS: yeah.

MR. SHUKLA: Do you want to have a break now?

CHAIRMAN APOSTOLAKIS: Okay. We'll be back at ten o'clock.

(Whereupon, the foregoing matter went off the record at 9:35 a.m. and went back on the record at 10:01 a.m.)

CHAIRMAN APOSTOLAKIS: Okay. We are back in session.

The next presentation is by Mr. Kemper of NRR on highly integrated control rooms, right?

MR. KEMPER: Yes, correct. Thank you.

Are we ready to go? Okay. Well, good morning, and it's good to be here.

As Belkys gave you the background, obviously this is one of the TWGs that the industry wanted us to focus on.

Oh, let me start with I'm Bill Kemper. I'm the Chief of the Instrumentation and Control Branch in NRR. I've also served as a management lead for this TWG sine it began.

I also have Paul Rebstock sitting next to

me. He's a senior I&C engineer who has served as the technical lead for the TWG, and basically the ISG we're going to be discussing today he's been the principal author for.

So I will cover in my presentation some of the TWG action, activities, problems, statements, logistics that ultimately led up to the development of the ISG, and Kimberly covered some of that. So I'll embellish a little bit more. And Paul will actually provide a detailed presentation of the ISG itself.

So next slide.

The TWG was initially formed about the beginning of this year. Our initial meeting was in February. The TWG is comprised of NRC members from the Officer of Research, from NRR, NRO, and NMSS. There are also members of the industry and NEI who are participating in the TWG meetings who have provided significant input on behalf of the industry and provided comments on the various products that we produce, such as the problem statement itself, the action plan, and of course, the ISG which were going to cover with you today.

We have conducted ten public meetings sine the inception of the TWG, and really our objective while working together is to understand industry needs

in terms of clarification of licensing criteria and applicable communications independence in both new and operating plants to gain technical insights into the designs and communications, independence strategies for highly integrated control rooms, and also to insure that the interim staff guidance addresses the appropriate design issues.

As I said, we've had ten meetings over a period of about 24 weeks. So that equates to about every three weeks we would have a meeting.

CHAIRMAN APOSTOLAKIS: What's the definition of "highly integrated"?

MR. KEMPER: Highly integrated control room is one kind of that's really flat panel displays. Okay? Think of a room such as this with a bunch of flat panel displays, you know, computer monitors, if you will, sitting around, and it doesn't have a traditional bench board design that we have now in current operating plants.

A highly integrated control room would have, you know, a big screen for plant status monitoring, if you will, and then a number of --

MR. GROBE: I don't think you're answering George's question. Do we have a definition for a highly integrated control? You're describing what one

looks like. I don't think we have a definition. Do we?

MR. KEMPER: I don't think so, no.

CHAIRMAN APOSTOLAKIS: I don't know.

MR. KEMPER: I don't think so. We talk about it in many aspects in the ISG itself.

MEMBER BONACA: I'd appreciate a description, too.

CHAIRMAN APOSTOLAKIS: The description is useful though. It really is useful.

MR. KEMPER: Okay. I thought that was what you were asking for. Sorry.

And these were just to follow on, and of course, these flat panel displays can be used either for just monitoring or for control and monitoring through either the touch screen technology or through keyboards. So it's quite a divergence from the traditional analog plants that we have in operation now, a whole new design concept, and we're going to talk about many of the technical nuances associated with that.

MR. GROBE: We conducted one of our Steering Committee meetings up outside Pittsburgh at the Westinghouse facility, and they have a mock-up of the AP 1,000 highly integrated control room. It's

going to be the simulator eventually or the design for the simulator. They have some provisions already existing where they demonstrated a steam generator tube rupture, for example.

I know that the ESBWR has one down I think it's in North Carolina or South Carolina that they're working on, and one of our Commissioners is going to go visit that facility in the next month or two.

It might not be a bad idea for the Subcommittee to think about whether or not, you know, a field trip would be a useful thing to actually see how these things work. It's quite impressive.

MEMBER BONACA: Do you have controls of the board, I mean, that you operate there or do you operate from a screen, from the computer?

MR. KEMPER: It varies. It depends on the designs. They have got both different concepts. Some of them are using touch screen technology. Some of them are using keyboard as screen access.

MR. GUARRO: Are the displays dedicated to a singular function or they can be used as bi-capsule displaced? In other words, different information can be presented on one display or they're dedicated to have one of the control.

MR. MILLER: This is Rich Miller from GE.

Do you want me to give an idea?

MR. KEMPER: Yeah, why don't you explain the GE concept?

CHAIRMAN APOSTOLAKIS: Your name again.

MR. MILLER: Rich Miller from General Electric.

The ESPBR is designed to have touch screen control. There's alternate methods that we're also looking at, but basically we have four divisions of safety visual display units that are used for control and monitoring for each division.

We also have nonsafety visual display units where any of the visual display units can bring up any of the non-safety systems. So you can bring up any system on a VDU, and you can drive down to the lowest level. On the non-safety side you have monitoring and control. On the safety side for the trip system we do not have control. That's all automatic. For the actuation system it's control and monitoring on that display.

On the wide display panel, okay, we're still in, I guess, our third phase of new technology evaluation, but we're looking at the wide display panel as being maybe several different types of new technologies. It could be a wide, okay, flat panel.

It could be ceramic, okay, tiles.

Also, on the side we have a wide variable display where you can bring up on a large screen any of the systems in the non-safety area so you can see that.

We pass through isolation devices information from the safety side to our non-safety side so that we can combine all four divisions in a trend. So on the non-safety side an operator can see the trend on level pressure, et cetera.

So that gives you an idea, but there is some manual switches. Okay? We have a few. An example would be for scram, for MSIB isolation, a couple, but most of the stuff now is not hard wired. It's all touch screen, okay, or some type of digital type of control.

MEMBER BONACA: The safety system, do you have a dedicated display?

MR. MILLER: You have dedicated displays for DIB 1, 2, 3 and 4, four displays for your diverge protection system. You have displays on your safety side for that because that's in our non-safety side, and depending on how many non-safety screens you would want used for manual operation also, we have our HFE group evaluate how many of the non-safety VDUs we

have. Say we have seven or five so that you can bring up enough screens so that the operator feels comfortable with operating them through VDU and not shifting back and forth.

MEMBER BONACA: Yeah, one thing that is typical of the current designs is that there is some similarity between different designers. I mean, the control rooms are pretty much similar.

MR. MILLER: I think everybody is going with the flat panel displays of VDUs on the operator consoles.

MEMBER BONACA: In an effort on the part of the industry to also achieve some consistency of design?

MR. MILLER: I think there's consistency maybe 60 percent, but not 100 percent across the board, and then some vendors will have not only maybe their digital VDUs. They might have hardware back-up also. So like in Europe they have that type of control system.

MR. KEMPER: And from what we've seen from interacting with the vendors, there is some consistency. I agree with Rich, but there's also a fair amount of differences and diversity in their design approach.

And you know, for these TWG meetings, typically we've had about 20 attendees to each meeting with many members of the industry and participation, as well as the vendors as well, and the vendors are pretty much the major vendors: Westinghouse, Areva, Invensys, Mitsubishi, and GE, which has really been great because this is really the task at hand is to understand the details of their design and come up with guidance by which they can implement their designs and still meet their regulatory requirements.

So next slide, please.

During the first couple of public meetings with the industry they identified several sources of licensing or guidance independence that needed further clarification. This slide is a little busy, but I just wanted to show you basically the four bulleted items here are the principal areas of existing guidance that ultimately produced the problem statement, and the problem statement, as it says, is industry and NRC guidance documents now defined at a sufficient level of detail, the requirements for interdivisional communications independence.

So the staff agreed that although existing guidance is adequate and has been used to license new reactor designs, there is considerable room for

interpretation.

So we embarked on this project to produce the interim staff guidance that clarifies the licensing guidance and review criteria related to communications independence for highly integrated control rooms, and again, as I say, this guidance applies not only to new reactors but also to current operating reactors because what we're seeing is some of the same hardware and design strategies are being deployed in existing plants for upgrades as we see for new plants.

MR. GUARRO: Excuse me again, Bill. On the fourth bullet, what was the nature of the conflict? I didn't quite get.

MR. KEMPER: Yeah, Kimberly alluded to it. Basically as she said, in Reg. Guide 1.152 we did not endorse Annex E of IEEE 7432, and we referred to the SRP for guidance. Unfortunately it was an administrative blitz. The SRP then referred back to the IEEE standard. So it was a loop that you couldn't get out of.

So that's been corrected, and the SRP is very clear now that it works out.

MR. GUARRO: Thanks.

MR. KEMPER: So let's see. So the focus

of the ISG on specific technologies being proposed at new and operating plants. Has industry identified many technical areas concerning communications independent for which they requested further clarification.

We consolidated the technical areas, and there were many of them, into nine high priority issues, if you will, through kind of a binning process, and then attempted to prioritize them, and it turns out that they were all high priorities as far as the industry was concerned.

So in order to manage this and develop guidance, we further distilled those down into four areas of interest based on common attributes really for the technical issues identified, and they are as stated on the slide here interdivisional communications, command prioritization, multi-divisional control and display stations, and we'll talk a lot about that in a minute, and digital system network configurations.

The ISG includes separate sections for each of the areas one through three. However, for area four as we got into discussing this, we found that really the implications of networking applies to the first three areas in a large extent. So the ISG

just decided it would be better to incorporate any guidance applicable to networking into those three areas. So there is no specific area for item number four.

Next slide, please.

So, again, the staff has developed ISG that clarifies licensing acceptance criteria related to the four major areas of interest. Public comments have been received and addressed via the TWT process. The final ISG will be issued for use by September 28th.

The ISG is consistent with existing regulations, and there are no new policy issues pertaining to this guidance.

We believe that there is good alignment with industry on the technical aspects of the ISG. We've had very, very good interactive and consistent participation by the industry and the vendors on this TWG and it's much appreciated.

However, there is one technical issue that remains unresolved and that is the need for safety grade controls and indications for safety related components. Albeit that's a little outside the scope of this ISG, but it has a significant impact on the design of the control room, a highly integrated

control room, and Paul Rebstock will cover that a little bit more in detail during his presentation.

So if there's no questions at this time, I think I'll hand it over to Paul so that he can start going through the ISG.

MEMBER BONACA: I have a question that is outside your presentation. However, maybe you can answer it. Why was the statement made on page 3 to Problem 4. "Software CCF was declared to be beyond a design basis event by the Commission."

What's the basis for that? What was the basis at that time?

MR. KEMPER: Software common cause --

MEMBER BONACA: Yeah.

MR. KEMPER: -- being declared beyond design basis --

MEMBER BONACA: Yes.

MR. KEMPER: -- design basis event? As has been explained to me -- this is quite some time ago -- the rationale for that was this is a low probability event that affects multiple channels simultaneously, albeit the consequences are high, but it's very low probability. So that typically is put into beyond design basis arena, if you will, rather than within a design basis.

MEMBER BONACA: Well, was an assessment of low probability that led to that?

MR. KEMPER: That's my understanding, right.

MEMBER BONACA: Okay.

MR. KEMPER: Typically, you know, if this were a single failure, if you will, we would mitigate that with redundancy, you know, and obviously redundancy won't do anything for a common cause failure.

CHAIRMAN APOSTOLAKIS: Even for hardware, common cause failures are not considered part of the single failure.

MR. KEMPER: That's right.

MR. REBSTOCK: But there's a provision in the IEEE standard that addresses this, that makes a distinction between failures and design errors, and I think that may be where the Commission was coming from, although the documentation from the Commission doesn't say what the basis is, I guess.

MEMBER BONACA: Okay.

MR. KEMPER: And in fairness, the next presentation is going to talk about that in a fair amount of detail.

MEMBER BONACA: I appreciate it. I

just --

CHAIRMAN APOSTOLAKIS: So it's more of a policy issue.

MEMBER BONACA: A policy issue. It's not a technical thing.

MEMBER MAYNARD: George is right. It's really the same whether you talk a digital I&C or the hardware in the plant, wherever. Common cause is not a design basis act.

CHAIRMAN APOSTOLAKIS: It's not a design basis, and even in a single human error, it was not part of the single failure. Strictly hardware.

MEMBER BONACA: Okay. Thank you.

CHAIRMAN APOSTOLAKIS: That's why PRAs are useful.

MEMBER MAYNARD: Now, the fact that it's not a design basis accident doesn't mean that you don't necessarily have to have compensatory measures or other things you do. It's just not a design basis accident.

MR. REBSTOCK: So I'll go through the interim staff guidance and talk about sort of the highlights of each of the sections, and I'll start off with the way it's organized.

The top level organization, the very

highest level organization was established by the Steering Committee and should be common to the guidance produced by various groups. Then in the more detail is going to change from group to group.

So we've had a scope discussion, a rationale of why this guidance exists and what this guidance is trying to do, a set of references, and then the technical discussion. And as was said, with guide technical section for three of the areas of interest that Bill mentioned, and the network considerations is distributed through these.

Overall scope of the communications ISG is that an appeals with communications between safety divisions and between safety entities and things that aren't safety related. The three sections within the guidance addressed different aspects and different implications of those concepts.

And we've also got provisions written into the first section of the ISG that says that nonconformance to the ISG doesn't constitute grounds for rejection of the design. We will consider alternative designs, and as Jack pointed out, the ISG is the entrance to the fast lane, but it's not the only way to do it.

I would also point out that past

acceptance of alternative designs was based on specific considerations based on those designs and doesn't necessarily constitute a precedent for future variance from ISG. Everything has to be taken in context and in total.

And those last things, those apply to all of the ISGs, but they asked us to mention it here as the first technical discussion.

The rationale is that safety systems have to be independent and reliable. That's for all of the provisions within this ISG. That's not only a matter of common sense. It's also required by IEEE 603, which is cited in 10 CFR 50.55(a)(h).

The rule cites the 1991 edition of the IEEE standard. It has been revised, I believe, twice sine then. We're not going to go into or we haven't taken into consideration the later revisions because the policy is that we're using the old revision.

And 7-4.3.2, Annex E, has also been mentioned. It addresses interdivisional communications, but the one thing that staff doesn't feel that it is adequately specific, and for another thing, that is an informative annex of an IEEE, and the way the IEEE works is that informative annexes don't get the same kind of voting that the main body

does. So even if it did indicate things that the staff thought was sufficient, it doesn't have the same cache as the base of the standard. So we don't feel that informative annexes are appropriate for citation and reg. guides.

Seven, four, three, two is also currently undergoing revision, and we're expecting that it will address what's in the communications ISG. Both the NRC staff and the -- one member of the NRC staff is on that committee, and one of the members of the industry consultants for the task working group is also on that committee. So we've got pretty good connections with them.

The first section within the ISG is on interdivisional communications, and this is the definition. We've given the definition of what we mean by that in this particular context, in this particular document. You may find other people mean other things. This is what we're working on.

The existing standard review plan accepts unidirectional communications outbound from the safety system with no reply or interaction with the non-safety destination. I would characterize this ISG as saying that there is zero directional communications as far as the safety function processor is concerned.

The ISG stipulates that there be a communications processor separate from the function processor that handles communication process, and the function processor is dedicated exclusively to performing whatever the safety function is.

The safety function and the communications processor exchange information through shared memory. Both of those processors and the shared memory are all safety related.

This diagram tries to illustrate the independence of the two processors, and the safety function processor has a sequence of operations that it follows regularly without interruption. It gets data from its own division. IT gets outside data. It does a safety thing. It sends out outputs and so on and never deviates. It gets information that it needs from the shared memory, and it deposits information that it wants to transmit in the shared memory and then goes on about its business.

If the shared memory somehow has a failure, the processor can't get what it wants, can't access the shared memory, it just moves on.

Now, given an analogy of how this would work, imagine that you're working on something and you need data from outside. I know what you need, and I

can go get it.

So I get the information. I write it on the blackboard. I can't call your attention. I can't give you any instructions, and I have to write specific data in specific locations on the blackboard.

You look up and read the data when you feel like it. You look in a specific location on the blackboard to get the specific datum that you're interested in at that particular time, and you act on those data in accordance with whatever is your pre-established plan.

You write on the blackboard whenever you feel like it. I get that information and go deliver it someplace, and it's my responsibility to take care of that process before you've overwritten it. So your job is never interrupted. That's the way the safety function processor works.

We don't want the safety function processor to be burdened with extraneous tasks. So we've stipulated in the interim staff guidance that the interdivisional communication must support safety. As an example, online monitoring is often cited as a reason for going digital. You can compare outputs from various sensors and get information regarding censor calibration.

That is a very good process and a very good thing to do, but it's not really directly related to the safety. It may give the operator advice that Transmitter B over there is getting a little flaky and you go fix it, but it doesn't affect the safety process directly. We feel that that should be carried on in a non-safety related processor that's separate from the safety function and not complicate the safety function.

The other provisions are that, as I described in the blackboard, the information transferred between this communications and the function processors, is transferred through the shared memory with the shared memory allocation preestablished. The trip status of Division B always shows up in exactly the same location on the shared memory. So there's no need for the function processor to interpret where it's coming from. The idea is to keep it simple.

The guidance includes a sample list of examples communication faults, and it addresses bandwidth problems, and there has been recent experience with data stored in a nuclear power plant that put the plant down. Those are included among the examples.

But it's indicated in the ISG that that is not a comprehensive set. Those are things to look for.

And vital communications, and in this context when we say "vital communications," we mean communications that are vital to this function processor for achieving its safety function. Those communications need to include error checking, and they need to be direct point to point between the source and the destination rather than network.

An example of vital communications would be the transfer of trip status from other divisions into the voting logic (phonetic). Some manufacturers do that in the function processor. Some manufacturers, I believe, do it in a separate processor, but in any case that's what we mean by vital.

There are provisions for certain parameters to be adjusted by way of the shared memory. Sometimes it's necessary to make adjustments to set points or to other parameters in the system, and so the ISG recognizes that there is a way to do that.

But access to the function processor for normal parameters is transferred through the shared memory, but the maintenance panel which has access to

the basic program of the function processor and can do anything it wants to the function processor, that access has to be highly restricted so that there's no possibility of interfering with the function during normal operation.

So we've included a provision in the ISG that says that there has to be a key-lock switch or physically unplug the cable, and there has been some discussion and confusion as to exactly what mean by a key-lock switch. So I made these diagrams. It means a switch. The electron can't get from here to there. It opens the circuit.

We will go so far as to say that a hard wired AND gate would count. It will interrupt the flow of the information with sufficient reliability, but we won't go further than that.

There have been indications that some software should be used, that when you throw the switch, it should set a big and then the software reads that bit and says, "Oh, I can't talk now." We don't consider that to be acceptable. We don't want it to rely on software at all.

There will obviously be software interfaces because when you throw that switch there's no communication. Therefore, the processors need to

know they can't talk to each other and, therefore, they might want to do something about it. So there's software involved, but the software can't be what inhibits the communication.

MEMBER MAYNARD: Does a key-lock switch mean you actually have to have a key to --

MR. REBSTOCK: Yes, physical key, and those keys are controlled and there's only so many of them, and they're in a locked cabinet and checked out and all of that.

MEMBER MAYNARD: If you allow a cable to be unplugged, does that cable require a special cable that has to be locked up or is that --

MR. KEMPER: It should be. That's right, to follow that same administrative controls strategy.

MR. REBSTOCK: Actually we've not had anybody propose that. I threw that in as a possibility, but that hasn't been proposed. Key-locks is the only that we have heard.

MR. GUARRO: Is there going to be any build specification of what type of communication from non-safety to safety provisions are possible? Because your check number ten, it says that ISG endorses bi-directional communication.

MR. REBSTOCK: Bi-directional in the sense

of what's shown on Slide 11

MR. GUARRO: By way of the shared memory.

MR. REBSTOCK: but no communication at all with the function processor.

MR. GUARRO: Okay. So that you're saying that the writing to shared memory by non-safety functions would be allowed?

MR. REBSTOCK: No.

MR. GUARRO: Well, that's important.

MR. REBSTOCK: The communications processor is what takes care of all of the interface with outside, with other safety channels and with non-safety related stuff. Stuff within the same division is able to come from within the division is able to come from within the division and doesn't need to --

MR. GUARRO: Okay. I'm trying to understand. If there is information, whatever information you allow from the non-safety side, where does it go?

MR. REBSTOCK: It has to come -- the non-safety system tells the communications processor it has a message. The communications processor receives that message, validates it, sees what the data is that is trying to be communicated to the safety function processor and writes those data in the appropriate

places in the shared memory.

MR. GUARRO: Okay. So through the validation of the communication processor, you and that accessing the shared memory.

MR. KEMPER: Well, no, there's one other point here, too. See, from non-safety to safety there has to be there's an interface first. Okay? What we've seen so far there's either an isolation device or there's an interface panel like in the Siemens or the Invensys design or -- excuse me -- Areva. I'll get it right. The Areva design.

Okay. So the non-safety information comes in through an interface panel, in which case it's converted to safety related components, and then that is translated just like Paul has it shown here into the shared memory.

MR. GUARRO: Okay. So there is some process of validation by which that non-safety information becomes safety information; is that right?

MR. REBSTOCK: No, no.

MR. GUARRO: No?

MR. REBSTOCK: Well, there's information. There is information isolation and there is physical isolation. I'm not even talkinga bout the physical isolation. That's no different digital systems than

it is from anything else, and most of this is by optical cables anyway so you don't propagate faults through optical cables unless there's a guide wire, which you're not supposed to have.

So the information that comes in only gets written into the shared memory if it's accepted by the communication processor, and then what gets written is a number. It's not a command. So the outside can't tell the function processor to do something different.

MR. GUARRO: Yes, I know. I had assumed that. There was some number, you know, that relates to some plant status, you know, parameter, whatever, and I just wanted to understand what is the process by which that number is validated and becomes usable by the safety part of the process.

MR. REBSTOCK: The safety processor would know that it got that information from the interface memory, the shared memory that's associated with non-safety related stuff. Therefore, the function processor would know that that's a piece of non-safety related data.

And the function processor's program would tell it what to do with that particular non-safety related information.

MR. GUARRO: My ultimate concern is

whether there is a mechanism by which, you know, there have been historical occasions of memory corruption, et cetera.

MR. REBSTOCK: I understand.

MR. GUARRO: And something that was supposed to go here ends up there, and is used for some other purpose.

MR. MILLER: Rich Miller here.

I think what might clear it up is when that data comes over, that data has a boundary of acceptance. Okay? So you would say it has to be within this range. Otherwise it's not good data. So there is a validation process there at least on some of the different vendors.

MR. KEMPER: The message itself has a unique identifier in the message. In other words, if it's a 32-bit message, then, you know, the first 24 bits all are involved with identifying that particular message.

Now, the processor, looking at receiving that in shared memory, will only accept information with that particular construct. So there's very sophisticated means that the vendors are using now to be able to insure that only the right data makes it through the safety related barrier, which is this

dashed line on the right-hand side, if you will. We didn't provide much illustration there, and then the function processor itself will only react to information that is in the right configuration, has the right construct.

So those are the methods that the vendors that we've seen so far are using to provide protection against corruption of the safety system by non-safety input.

MR. REBSTOCK: One of the things that you mentioned that I want to make sure that we address is one thing that goes wrong in networks sometimes, in communication strategies, is a buffer overflow condition where an incoming message is bigger than it was supposed to be, and it overwrites its buffer, and the extra information goes someplace else in memory and corrupts the behavior of the processor. That's one way that things get into your home PC, and it has caused other problems.

That's absolutely impossible with this structure because the information coming in from outside gets written to a specific spot there in the shared memory. It has nothing to do with the register or the program that the safety function processor is executing. It's some number, a certain number of

bits, and that's it.

When the safety function processor reads the shared memory, it reads those bits. Even if somehow it got corrupted and turned out bigger than it was supposed to be and overflowed, it wouldn't make any difference. What it would mean is the safety function processor is reading garbage. So it wouldn't be able to use it, but it's not vital to the safety function anyway. So that doesn't matter.

So there's no way for something to get in and corrupt this guy. That's what the shared memory is for.

MR. GUARRO: Okay. Thank you.

MR. REBSTOCK: Okay. The next issue that we address in the guidance is command prioritization, and the definition is given on the screen there, the process of selecting which command the piece of safety related equipment should obey when different systems want it to do different things. That's basically what command prioritization is.

MR. KEMPER: And do you need any additional explanation on these priority modules? Is everybody familiar with that?

In other words, these new systems are proposing to use devices, if you will, to execute this

function here, and they vary in their composition. Some of them are software based. Some of them are discrete electronics based. Some of them take place in the electronics microprocessor themselves at the platform level.

So that's why it's kind of broad or apart. So Paul is going to go into that a little bit as he goes through.

MR. REBSTOCK: We'll detail that a little bit, yeah.

The fundamental ground rules that the safety command from the safety system has to have priority, has to have top priority. Non-safety commands it has been pointed out that the diverse actuation systems are typically non-safety related, but sometimes the non-safety related system has to tell the pump to run when the safety related controls are telling it not to run, but the safety related control that tells it not to run isn't the safety function. The safety function is running. So the priority module understands all of this stuff and works it out and makes the pump run when it needs to.

The details of what has priority like the example I just gave which gets to be a bit complicated can be very complicated, application specific. So the

details of what the prioritization logic means and which signal wins under what circumstances has to be worked out individually case by case for each actuated device.

I'm not going to go into that in the discussion of priority modules. The discussion of priority modules presumes that you figured that out, and now we'll talk about how you make that happen.

MEMBER BONACA: You went through bullet number two, but I didn't understand it. So if you could go over it again.

MR. REBSTOCK: Yes. The initial thinking would be that the safety system always wins. So let's talk about a containment isolation valve, and the safety condition or the safe condition is for the valve to be closed, and let's not talk about the one in auxiliary feedwater, which gets really messy, but some other line, where the safe condition is for the valve to be closed and the normal condition is for the valve to be open.

If the safety system says close the valve, we want the valve to close. If the safety system says open the valve because there's an error in the safety system and the valve really should be closed and the diverse actuation system says close the valve, under

that circumstance, you want the diverse actuation system to override the safety system.

But the point is that the safety system command that says open the valve isn't the safety function. It's from the safety system, but it's not a safety function. So to have the DAS override that makes sense.

But if the safety system is saying close the valve and the DAS says open it, then you have a safety system providing a safety function that says close, and the DAS shouldn't be able to cancel that.

The implementation of that hardware, of that logic is the responsibility of the priority module. The derivation of that logic is a case-by-case analysis for every component that might get into this situation, and we don't address how you come up with that logic in the ISG We say once you've determined the logic this is how you would make it happen.

MEMBER ABDEL-KHALIK: Now, why would a safety system issue a command that is inconsistent with the DAS?

MR. REBSTOCK: There could be an error in the safety system, which is the reason you have the DAS, is to accommodate errors in the safety system.

MR. KEMPER: Common cause failure.

MR. REBSTOCK: Yeah, or you may be doing some testing and the safety system said close the valve in order to test it, and then the test is over, and so you say now open the valve, and then the open command gets stuck and never goes away. So it's still present and you don't know it. So you have an unidentified failure.

Now, later on something nasty happens inside the containment and you really do need to close the valve. If the safety system isn't working, the DAS has to be able to close it even though the safety system is saying stay open.

Like I say, that logic gets kind of complicated, and any example I give you you can find a counter example of why that doesn't work. So it has to be done every component one by one, which is really what you do right now anyway.

The diverse actuation systems are one of the implications of D3 considerations. D3 considerations though, diversity and defense-in-depth considerations indicate that you can't use the system that you're trying to replace in order to execute the DAS function. So you have to bypass the safety system, and the implications of that will become clear

in a minute.

As Bill mentioned, there are two ways to do prioritization, and the most common approach that we've seen is with the physical priority module, which is a physical device that's interposed between the safety system and the actuated device, and it receives the safety commands and receives everything else that might influence that device, figures out the priority, and tells the device what to do.

The ISG requires that that device be fully tested, all combinations of inputs and whatnot be adjusted or be verified in proof testing to show that the design is sound.

The ISG requires that that device be fully tested, all combinations of inputs and whatnot be adjusted or be verified in proof testing to show that the design is sound. It may contain software to do its job for processing of the non-safety related commands, but if that software affects the output, if it affects the prioritization, then that's safety grade software.

Obviously the module is going to include both safety related and non-safety related stuff because it receives commands from safety systems and from non-safety systems, and the logic should be non-

volatile logic, Eve-prong (phonetic) of field programmable gate array. So whatever, it doesn't require power to be maintained. It can be rewritable, but it should not be reprogrammable in place. So when the device is installed, the logic is fixed and can't be changed.

Software based priority modules would refer to a module of computer code rather than a physical module, and these are things that might be executed in the function processor, and there may be some reason to do it in the function processor, but if you do, then it can't be used for diversity and defense-in-depth because if the processor failed, the signal doesn't get through.

The software has to be safety related software because it's running on a safety grade, safety related processor, and if a plant has both kinds of modules, then there has got to be some kind of design control to make sure that future modifications apply the right kind. If software based modules are available, we need to make sure that ten years from now somebody doesn't install a diverse actuation system and use the software based module with it because it would defeat the purpose of the system.

MEMBER BONACA: When you say the code must be safety grade, could you expand on the second bullet? What does it mean exactly?

MR. REBSTOCK: the code must be safety grade? The program fragment that is contained within the priority module is executed on the function processor, safety function processor. Everything that can affect the operation of the safety function processor has to be safety grade. So this software would have to be safety grade.

Even if you made a case that it was a non-safety function, which I don't know how you could make that case, but even if you did, it's being executed on the safety processor and, therefore, has the possibility of diverting that processor and causing some kind of an error along --

MEMBER BONACA: I understand the need for it. I was asking what do you have to do to make it safety grade.

MR. REBSTOCK: Oh, the same as any other safety grade software. There's V&V requirements --

MEMBER BONACA: All right.

MR. REBSTOCK: -- extensive testing requirements, configuration control requirements that are more detailed than you have in ordinary --

MEMBER BONACA: I guess I was till thinking back about a slide you described before where you had no safety grade system of providing the known safety grade function of a safety grade system, and I was trying to understand the significance of not being safety grade.

I mean, you know, you have the bullet that you went back to on page 14, and when you say non-safety commands for safety system can be overridden by non-safety diverse actuation system.

MR. REBSTOCK: These are really two different things. This second bullet on this slide is talking about the prioritization of logic --

MEMBER BONACA: Yes.

MR. REBSTOCK: -- and how you decide what to do.

MEMBER BONACA: Okay.

MR. REBSTOCK: Okay?

MEMBER BONACA: I agree with that.

MR. REBSTOCK: The second one, this is talking about the qualification of the code that's needed to make that happen.

MEMBER BONACA: Okay.

MR. REBSTOCK: Okay?

MEMBER BONACA: Yes.

MR. REBSTOCK: In some ways this multi-divisional control and display stations is perhaps kind of a big deal. It's one of the more significant items in the ISG, and what we mean, the definition I've provided there, is that it's a non-safety related or a control station that has access to multiple safety divisions and also non-safety devices. Well, it says non-safety related control station.

We have also within the guidance allowed for the possibility of a safety related station that can control things in other divisions. I've never seen that proposed. I'm not really sure why you would want to do it, but at the stage that we're writing the guidance right now, I felt that it made sense to accommodate all possibilities. So there's words about it in the guidance.

But basically what we're talking about is non-safety related control stations that have influence or that can control safety related stuff or display information from safety related stuff.

MR. KEMPER: Now, this is a major paradigm shift, is what I was speaking to earlier in our discussion. Obviously in today's world safety related systems are typically controlled by safety related controls and indications. This is a major paradigm

shift to allow those same safety related systems to be controlled by non-safety related equipment.

All of the new reactors -- I shouldn't say "all" -- most of the new reactors that I'm familiar with use this concept to a very large extent.

CHAIRMAN APOSTOLAKIS: I mean, why is this allowed?

MR. REBSTOCK: Well, maybe we need to restrict this a little bit further. This is talking about control and display station. It's not talking about the control processor. So if you've got a safety related control valve that needs a PID control function, that PID control function. That PID control function for that safety related valve is controlled by a safety related processor that is in that channel.

What the control station does is say open it a little more, close it a little more or do something with it, and it's able to give commands to that valve to tell it what to do. Under circumstances where there's no safety condition that needs it to be in a certain way.

Under normal operation the safety system isn't interfering. Under normal operation, the safety system just sits there. It doesn't do anything. Then you need to be able to control the plan. When

something goes wrong and the safety system has to take over, then it needs to be able to get hold.

What we're talking about here isn't the control. When we say "control," we mean control in the sense of the operator. I push this button and that valve opens. I'm not talking about the thing that makes the valve open. That has to be in the same division that the valve is in. This is control from the point of view of the operator, not from the point of view of the generation of the commands that actually go out there.

Okay. So we're not talking about having non-safety related control processors having direct control over safety related stuff. This is the operator station, which talks to whatever control processor is necessary to control the stuff.

MR. GROBE: Paul, I think George's question was why do we permit this, and I think the answer to that lies in the fact when you have analog controls, the controls were very clear and they were connected with a component, and if for a non-safety reason a flow control valve was going to go open or closed, it would go through that safety grade control system.

Here you have this integration of safety

control function and non-safety control functions that are all within a digital system or digital framework, and the reason this is permissible is because of that blackboard. I like his examples because I can deal with that, that there's a clear separation and a prioritization of the safety function over the non-safety function, but it's all within an integrated control system.

And this really gets to your earlier question: what is a highly integrated control room? This is really getting into some of those complexities.

Did that help? Did I say that right, Paul?

MR. REBSTOCK: Close.

(Laughter.)

MR. REBSTOCK: The key is that we're talking about control from the point of view of the operator, not control from the point of view of the control device.

Do you want to chime in, Wes?

MR. BOWERS: Wes Bowers from Exelon.

I'm part of the communications task working group. I think I'll use slightly different language to describe it. When you're looking at the

safety function, you have to make sure that you can do the safety function with safety related controls, but if the component like a valve has a non-safety related function also, that's what Paul is talking about, that you can use a non-safety related control to do the n on-safety related function of the valve, the pump, the whatever, and that's where the highly integrated control system comes from.

So you can use a non-safety related display to do the non-safety related function, to control the non-safety related functions, and you may be controlling a device that has a safety related function.

So the control of a safety related device to do the safety related function obviously comes from the safety related operator display station, but if you're doing a non-safety related function, then it could be from the non-safety related control device.

So in IEEE 603 it talks about the design basis for your system. So one of the things you start out with is defining your design basis for the system, what manual controls there are, what automatic controls, what function, manual functions, automatic functions you have to do, and then you figure out where your controls are.

In the old analog situation, it was just easier from a separation viewpoint to say, oh, yeah, everything about this system is going to be controlled by safety related controls. Now that we've gotten into the highly integrated control systems, it's much better from a design viewpoint to really look at the function to figure out where that function is going to be on the operator display station.

MR. GUARRO: Would an example of the use of the non-safety control be to test the valve and, you know, when the safety system is not working you'd go to that panel and you'd operate from there for testing purposes?

MR. MILLER: Rich Miller.

MR. GUARRO: I'm trying to understand what circumstances.

MR. MILLER: Rich Miller here from GE.

I guess even though you're performing this non-safety function, if there is a need for the safety function to be performed, that would override that. Is that right, Wes?

MR. REBSTOCK: Yeah, we'll stipulate that that interface be through the priority module. I'm not sure if we've gotten to the slide that discusses that. Some of this is getting a little bit ahead in

the presentation.

MR. HAYES: This is Tom Hayes from Westinghouse.

I'm going to agree with these, but as an example of the why, and I'll use Paul's simple containment isolation valve example, the safety system closes the containment isolation valve because we need a containment isolation. For our design, now once the need for the containment isolation has gone, whatever condition it was in the plant is gone away. The operator ultimately needs to reset the safety signal, but we still don't want that valve to open because the operator resets the containment isolation valve. We don't want a dozen valves suddenly opening.

So now the safety system is happy. There's no need for a containment isolation. Those valves happen to still be closed. We as the non-safety system for the operator to go say, "Okay. I want to open my compressed air valve. I want to open my hydrogen valve," or nitrogen valve, these various valves are opened individually by the non-safety system to keep that level of complexity out of the safety system.

One of the design goals of a safety system is keep it as simple as you can. So we're trying to

take those functions that don't need to be safety out of the safety system.

MR. REBSTOCK: What we've tried to do in --

CHAIRMAN APOSTOLAKIS: I think we -- we don't need that.

MR. KEMPER: We're touching on the one issue that I mentioned up front that we're going to talk about at the end of this as well, which there is still a bit of a disagreement.

I respect what Tom and Wes just said, but we're not completely in harmony on that.

MEMBER BONACA: How different is it from what they're doing right now? Could you tell me just how different that is? I mean, the explanation was very clear, but it seems to me that right now for current reactors, I mean, it was an effort to separate safety functions from non-safety functions totally. So if you had a command to isolate containment, which is a safety command, and then the need for it was gone and now you needed to open compressed air, for example, you had a separate control for that.

MR. REBSTOCK: There would be a separate switch on the control panel to do that.

MEMBER BONACA: That's right.

MR. REBSTOCK: Right. The only difference --

MEMBER BONACA: But even in that case then the no safety related switch would override the safety related control because you don't need that translated anymore.

MR. REBSTOCK: Well, the complication comes here. In a conventional plant there's one control panel, but that control panel if you look behind it is a maze of separations. It has got all four safety trains and non-safety related all mixed in together.

MEMBER BONACA: That's right.

MR. REBSTOCK: There's no way to do that on one of these, and even if I make that safety related, it's only in one separation group. So it doesn't have the other separations or the other divisions, and so that's where the issue comes in.

That's conceptually fundamentally different from what exists now. What we've tried to do in the guidance is to say let's not talk about why you to do this, but if you did want to do this, here's what you need to do in order to make it acceptable. That's the focus that we're taking here.

MEMBER BONACA: Thank you.

MR. REBSTOCK: Let's get back on track.

Okay. We've mentioned in the ISG a condition that came up when we were thinking about controlling display stations and might actually go beyond that, and I captured it in the ISG to make sure that it gets captured. Ultimately whether it belongs there or someplace else I'm not really sure, but that's where we have it for now, and that is the issue that says that when you're using a digital system, the system has failure modes that are different from hard-wired systems, and the possibility of common failures that are different from hard-wired systems.

Your safety analyses look at what can happen in the plant and say why it's okay and demonstrate that the plant will remain safe, and we have a concern that those safety analyses are based on conditions that might exist under the current designs. When you introduce digital systems, you have the possibility for simultaneous failures or multiple actuations. That could alter the initial conditions for an accident or it can alter an accident progress.

So somehow the safety analysis has to take account of the behavior of the digital system. So we've included a provision in the ISG that says watch out for that. It's an area that will probably require

somewhat more investigation and deeper guidance, but at least it's highlighted.

One of the examples is there was an incident on June 18th at the Honeywell International Fuel Facility in Region 2. The control system that operates that facility suffered a loss of power and the UPS that it was connected to didn't help. I don't know exactly what caused it, but somehow the control system lost power and then regained power.

When it lost power, the system went into the safe state, but when it regained power, some of the valves transitioned, and as a result of that, some different areas of the piping system became pressurized, and the end result was a uranium hexachloride release and exposure of some workers.

That's not control logic, but it's the kind of a thing that wouldn't necessarily happen in an analog system, but it was something about the way the system was configured that permitted that to happen. That's an example of things that I think need to be addressed in safety analysis.

MR. GROBE: The safe state in that case was a cold plant condition line-up, and they call them reactors, but these are chemical reaction tanks. There were a number of tanks that were hot and

pressurized. So the safe state resulted in over pressurization of the tanks and lifting of relief valves.

MR. REBSTOCK: It's not really a digital event, but it's --

MR. GROBE: It's an example of --

MR. REBSTOCK: -- a partial consequence of the nature of the control system.

MR. GROBE: -- of how you cannot have sufficient foresight in programming to anticipate all potential eventualities of what will happen during operation of this system over a period of an extensive number of years.

MEMBER MAYNARD: I don't disagree with the need. I'm not sure I understand why that's not also applicable to analog system, and yet take the same considerations. You lose power and you restore power. What has happened?

I'm not disagreeing that there's a need to address this and do it, but I'm not sure it's all that unique to digital in some of these.

MR. REBSTOCK: No, I don't think it is, but what I'm thinking of in here isn't that digital is unique. It's that it's different. When you create the safety analyses on the basis of what an analog

system can do, that might not be the right mindset for digital systems.

MEMBER MAYNARD: I understand that.

MR. GROBE: Yeah, I was going to say that in an analog system many of these issues are much more transparent. They're much easier to observe on the part of the designer.

In the complexities of the digital system, some of these issues aren't as transparent, and consequently, they can be overlooked, and that's why we have the concern with common cause failure.

MEMBER ABDEL-KHALIK: But if a possible cause for this is design error, how can you anticipate this and include it in the safety analyses?

MEMBER BONACA: That's right. That's it exactly.

MR. REBSTOCK: But that's why I say this is an area that requires further investigation.

MEMBER BONACA: If you don't know it and are going to model it, you have to get the --

MR. KEMPER: Well, the guidance right now requires that the vendors or designers of the system identify the critical failures within their system and then provide a means within a design of the system to cope with that. And if they can't cope with it, then

the safety analysis has to envelope that effect. That's what we're trying to say.

MEMBER BONACA: Well, typically for the systems, I mean, it used to be that they used to do this casualty analysis. You know, they were really default trees. I mean the early time before there was PRA.

And I would expect that if you do that thoroughly, you should identify some of this failure force.

MR. REBSTOCK: That's exactly right. Hazards analysis is the tool that would typically be used to identify those types of digital or failures unique to the digital system, right.

Because the multi-divisional control and display station is able to influence everything in the plant, safety and non-safety alike, we feel that it needs to be qualified physically to the same level that safety related controls need to be.

So the hardware would be seismically qualified and environmentally qualified and so on, qualified to be able to withstand whatever environments are applicable at that location, and the reason is that you don't want an earthquake to set off a bunch of actions.

The equipment doesn't have to function during or after the earthquake. The point is that it has to demonstrate that there's no spurious actuations as a result. And the software that's running on it doesn't need to be safety grade software because it's obviously not affected by environment.

Also we've got a provision that says there should be at least two positive operator actions in order to do anything. For example, you select a pump and then you turn it on. You don't push a button and the pump just changes state, and the reason for that is somebody bumps the control panel; you don't want anything to happen.

There are human factors implication that also talk about the need for positive actions and dual actions, and we don't go into that, and in the guidance we point out that such things exist and refer over to the human factors guidance to get those details.

But as a minimum as far as the communications TWG is concerned, in order to make sure that the equipment functions properly, there needs to be two steps from the operator.

The HF, the human factors guidance would probably go beyond saying are you sure, yes, like your

Windows PC does and people just hit it. That's not what we're getting. What we're getting at is that the equipment shouldn't make an accidental actuation.

We've got provisions in the ISG for explicit consideration of power surges, power loss, and so on, and also provisions for disabling the control stations in the event that the control room has to be evacuated. If there's a fire or flood, some reason to evacuate the control room, there should be some means of disabling the control station so that that very flood can't cause short circuits that cause things to start actuating, and the whole point is minimizing spurious actuations.

And some of the discussion a couple of minutes ago jumped ahead to the next two bullets on here. Staff believes that there should be safety grade controls for each safety related device. That is what's present in current plans right now.

The ISG represents that. The ISG says that there should be safety related controls for each safety related device. We feel that if you omit that in new designs you're somehow making the new design less robust. We don't see a significant penalty in providing it since there have to be safety related control stations anyway. So we've written the

guidance that way.

Industry has indicated that they feel that it's not necessary to have component level control if you've got system level control, and I don't know what their plans are. I'm not right up to date, but at one point they were talking about the possibility of a topical report to address this.

So, you know, there's further discussion. It also has implications from human factors and minimum inventory and so on. So right now the guidance just says do it and explain why not if you don't.

MR. KEMPER: And the staff is also doing research ourselves trying to see if we can get more information on, you know, some of the assertions that are being made like it was just easier to use safety related control and indications for safety related components rather than put an isolation device in there and use non-safety related controls.

Now, we've talked with some of our more senior designers that are out there, and we haven't found anybody to confirm that. There's a couple of different thoughts here. One paradigm is what you just heard. The other one is, well, it was a given. That was a standard design expectation. So whether it

was written in an IEEE standard or not, that was the basis for providing safety related controls and indications or -- excuse me -- safety grade controls and indications to safety related components.

So we're still trying to sort through that, and eventually we'll come up with a position that gives us a little bit more granularity, if you will, to this requirement here or maybe eliminated it altogether, depending on what we come up with.

But this, as Paul says, is the expedited, streamlined way of complying with this guidance.

MR. REBSTOCK: There are some other human factors interfaces I'll call them between the communications working group and the human factors group itself. There are a lot of human factors related concerns that have to do with the design and the application of digital control panels, and we're not going to go into all of that stuff.

But there's one thing that gives us a little bit of pause. If all of the controls are on a single panel, including all of the controls for all of the safety related devices and you can make that work, that's fine. But if that panel becomes unavailable, it is non-safety related. So it might become unavailable. The operators are going to have to go to

the safety related control and display stations in order to maintain the plant.

That's a substantially different process of operating than operators normally use through the main control stations, and we've got a concern that that change in focus, that need to change in focus and the different operation into the different behavior of those stations could lead to operator errors.

MEMBER BONACA: I mean, this is a true new challenge from a human factors standpoint. I mean, this is a big change from what we've seen before, and so it's a big challenge. You have the test group that looks at it, right?

MR. KEMPER: Right, yeah. It's really a human factors issue, but it manifests itself because of the designs that we're trying to provide guidance for, if you will.

MR. REBSTOCK: Yes. The ultimate resolution of that will be through the human factors group, and in ISG, we raise that as an issue to be aware of and then cross-reference the human factors design.

MEMBER ABDEL-KHALIK: Wouldn't that be taken care of as a part of operator training?

MR. REBSTOCK: That's what many people

say, and that is --

MR. KEMPER: Should be.

MR. REBSTOCK: -- quite possibly a way to do it, but it depends on how you have the systems design, how much practice the operator gets, how you do the training.

MEMBER BONACA: And those are the kinds of information and the amount of information that you provide. I mean, experience has shown that too much information -- that's right -- the organization of the information is fundamental. For example, if you got to recirculation through the PWR, you have the sequence of switches that you want to have simple location and the logical way.

You know, it's all of those things that we have learned through the years that don't apply here.

MR. REBSTOCK: Yes, but in a conventional control room, present day control room, all of that stuff is on the control panel, and it stays put. When the operator is in an emergency mode or a normal operation, it doesn't make any difference. The same place and the same switch in the same place, you know, nothing changes.

MEMBER BONACA: Nothing changes.

MR. REBSTOCK: Now we're talkinga bout

that panel evaporates, and now he has to go over here. That seems to raise the possibility of problems.

As far as D-cubed is concerned or diversity and defense-in-depth is concerned, we don't feel that there are direct implications for the communications, as far as communications are concerned. So the ISG recognizes that D-cubed considerations may influence the way you design your control stations. D-cubed might say you need safety related; you don't need safety related; you need to do this; you need to do that, but this guidance talks about how the control stations are designed and configured. The D-cubed considerations would say how you use them and what you put on them.

So I don't see a whole lot of overlap between the two of them. So we've got a cross-reference that says look to the D-cubed side to make sure you understand what's needed in the control room, but I don't expect it to directly influence the things that the ISG already says.

MR. KEMPER: Okay. Yes, Id' like to wrap it up, if I may. We're getting pretty close to the end of our time here.

Next slide, please.

So our path forward. the staff will work

with the industry to have the ISG incorporated into industry standards, and as we said earlier, most likely that will be embodied largely in IEEE 7-4.3.2. And then the staff will endorse that standard, and others, if appropriate, with Reg. Guide 1.152 in all likelihood and, of course, include whatever interim staff guidance that was not incorporated into the IEEE standard.

And then we will revise the standard review plan to reference the reg. guides and incorporate the ISG as appropriate, and that should bring this to a conclusion.

So that really concludes our presentation, and if you have anymore questions, we'd be glad to answer those.

CHAIRMAN APOSTOLAKIS: Okay. Thank you.

The next presentation is on --

MR. BOWERS: Can I make one comment?

CHAIRMAN APOSTOLAKIS: Yes, sir.

MR. BOWERS: Wes Bowers from Exelon.

We've had a really good working relationship between staff and the industry representatives on the task working group, but I just wanted to make a comment about this one issue, the one Paul was talking about there about the safety grade

controls.

It's a discussion item because there's many people in the industry that feel that -- and if you go back to Slide 20 just to refresh your memory about what it as -- it was where the staff generally believes that all safety related plant devices need to have safety grade controls. We believe in the industry that that's an extension or actually a new requirement. It's not in IEEE 603. So it's not in the regulations, that it's not in the plant designs today.

An example would be the reactor protection system. The design basis that you come up with coming out of IEEE 603 would say you have to have the ability to manually scram your rods and you have to have the ability to do that on a system level.

There's nothing in IEEE 603 that would say you have to be able to do that on an individual rod basis. So in the plant designs, the way it's actually implemented saying a BWR today is we have the ability to automatically scram, to manually scram on a system basis, but the ability to individually control a control rod is on a non-safety related basis. The reactor manual control system, non-safety related gives you the ability to drive rods in.

So the individual control of a rod is non-safety related, but the ability to manually initiate the scram on a system basis is safety related, and the ability to automatically initiate the scram on a system basis, whereas we believe this requirement the way it's worded now would in this example force you to have safety related ability to scram each rod or control each rod from the operator display station.

So that's kind of the heart of the issue when we look at what's in IEEE 603 and, therefore, in the regulations, and the way it has been implemented in existing plants or new plants.

For existing Westinghouse EP 1000 has a certification where they have the safety related functions are on a system level or controlled by safety related devices, but the individual controls very often are non-safety related. It depends on the design basis of the system.

So there's both precedence set in the existing designs and in the new design certifications that would support the industry position that this is essentially a new regulation.

MR. REBSTOCK: Yes, I would like to comment on that. There's two things.

For one, talking about control rods, I'm

not sure that that's an appropriate example. You tend to not use control rods individually. There are issues about keeping control rods working together, but let's say other kinds of plant equipment.

The staff recognizes that there is no explicit guidance that says that you have to have an individual safety control for each individual component. There's an implication in GDC-13 it can be read as requiring that or it could be read as not requiring that. It's unclear.

Our feeling though is that, for one thing, existing designs have it. For another thing, at the time these rules were written, it wasn't possible or it wasn't feasible to make non-safety related controls for the safety related equipment. There was no reason to do it. If you had a safety related gizmo, it just made more sense to control it from a safety related device so that you didn't have to mess around with associated circuits and isolation and so on.

So we feel that it's not addressed in the existing rules because it wasn't on the radar screen at the time, not because it wasn't necessary.

CHAIRMAN APOSTOLAKIS: Okay.

MR. KEMPER: We probably will come back to you all once we get all of our thoughts together and

so forth and share this with you maybe at a later presentation somewhere down the road. So there's lots of, I'm sure, good discussion and debate we'll have on this.

CHAIRMAN APOSTOLAKIS: Thank you very much. Thank you.

MR. KEMPER: Thank you.

CHAIRMAN APOSTOLAKIS: So diversity and defense-in-depth.

(Pause in proceedings.)

MR. JUNG: Good morning. My name is Ian Jung. I'm the Branch Chief for the Instrumentation and Controls Branch in NRO, and I'm also the D3 working group lead, and here today with me is Mike Waterman on the left. You know him pretty much, I think. He's a senior I&C engineer for many years, and Paul Loeser also from NRR has been on this table, you know, several times, multiple times, and you've seen him before.

So both of these gentlemen and some other members from also NRO and the NMSS comprises this technical working group. And I thank this subcommittee for giving us the opportunity to brief on this particular topic. I'm sure you have been aware of this topic for a while. We are back here with the

latest and the status of the ISG.

We have had significant interactions with industry. We had a total of six public meetings since February time frame. Many of these meetings were full-day meetings. We had a lot of participation from individual vendors and utilities participated. Being one of the key subject issues involving digital I&C systems, I think it really gained a lot of visibility, and we appreciate industry participating and providing a lot of inputs. In many areas I think we came to a reasonable compromise, and in some areas we have a little bit of delta, but as we emphasized earlier, the purpose of the ISG was to provide one method that is sort of an HOV lane for staff review and approval of the potential future applications coming in.

But if there are other methods that can provide an either clear or with a sufficient basis, then we will have to probably look at it on a case-by-case basis, and again, it may not be a HOV lane, given, for example, D3. If somebody proposed more of a process driven methodology instead of putting in the design space, obviously process involves literally a more in depth review and interaction.

So that's what we are trying to provide in this D3 guidance document.

Currently the D3 ISG for all seven problem statements that we have is under OGC and the Steering Committee review. We had planned to issue this ISG by September 28th of this month, and we are on schedule right now. Again, the purpose was -- I mentioned this as sort of a clarification -- the only guidance that we're going to accept is clear.

Next slide.

Yes, we have seven problem statements, and Kimberly Keithline from NEI mentioned about originally having leak detection. We took that particular problem statement out of it, and we have seven problem statements. Number seven, single failure, was the one that the Chairman and also other members discussed earlier about beyond design basis and single failure. We wanted to make sure we got an OGC opinion about that. So we recently got their opinions confirming our understanding of single failure, common cause failure being not within the scope of the GDC single failure criteria. So which we are providing the industry with a clear guidance, and the feedback we just got is industry is very happy with that.

Given that, I'll turn it over to Paul Loeser. Paul developed most of the initial staff guidance on all of these subjects, and Mike Waterman

and other members providing a lot of input. So I'll turn it over to Paul Loeser.

MR. LOESER: Okay. The first of the initial draft staff guidance concerns problem statements one and two, that is, what is adequate diversity and defense-in-depth, and the second one is when is manual action sufficient diversity and defense-in-depth and no diverse automated system is required?

We have come up with a number of points here. The first is that the methods within this are not the only methods, but these are the ways where if they are used, very little additional staff review will be required. If other methods are used, we're going to have to look at them into significantly more depth.

One of the questions that was asked of the overall NRC is what do we have to do to get a nice, simple review as opposed to these long, involved ones and many years. So that's what we were trying to answer here.

As was said before, there are also alternate methods.

We have also said that there should be no difference in the D3 guidance for the reactor

protection systems for new plants or for existing plants. The requirements are basically the same.

CHAIRMAN APOSTOLAKIS: Reactor protection system means what?

MR. LOESER: This is the trip system and the emergency core cooling systems.

CHAIRMAN APOSTOLAKIS: RPS is just the trip system, right?

MR. LOESER: We tried to distinguish between the RPT and the RPS.

CHAIRMAN APOSTOLAKIS: I noticed that.

MR. LOESER: We are saying that while common cause failures in the software and digital systems is beyond design basis, the RPS system is important enough that it still needs to be protected to some degree from this type of common cause failure, not in the same manner that we would if this was considered a within design basis accident, but it still requires some protection.

CHAIRMAN APOSTOLAKIS: Well, let me come back to your first bullet.

MR. LOESER: Yes.

CHAIRMAN APOSTOLAKIS: The interim guidance says that if you have at least 30 minutes, the protective action may be performed by manual

operator actions. The licensee will be required to demonstrate that sufficient information and controls, safety or non-safety, independent and diverse from the RPS discussed above are provided in the main control room and that the information displaced, and so on.

So the licensee will come to you and say, "Okay. We have 40 minutes."

MR. LOESER: Yes.

CHAIRMAN APOSTOLAKIS: Now they have to convince you that the manual actions will be good enough.

MR. LOESER: Will be accomplishable.

CHAIRMAN APOSTOLAKIS: Right.

MR. LOESER: That they will accomplish the same --

CHAIRMAN APOSTOLAKIS: So they will start arguing in terms of time. If they're aware of this 1852 document, they will say, "Okay. For this action so much time is required to do it and our operators will do this A, B, C, and there is sufficient margin." And you will review that.

MR. LOESER: Yes.

CHAIRMAN APOSTOLAKIS: And you pass judgment whether you like it or not.

MR. LOESER: Yes.

CHAIRMAN APOSTOLAKIS: So what if they use that also for times that are less than 30 minutes? You will have to review it anyway.

MR. LOESER: Yes.

CHAIRMAN APOSTOLAKIS: I mean the way the first bullet is stated is that, you know, the 30 minute is fine. If they want to use something else, we'll have to review it and police it, the consequence, I guess, or threat that that will take time, but you will have to do the review anyway for the actions beyond 30 minutes.

So what's wrong with reviewing the method and allowing them to use it for any time?

MR. LOESER: Well, it's --

CHAIRMAN APOSTOLAKIS: See, that takes away, it seems to me, some of the argument for imposing the 30 minute rule, not rule; I mean requirement.

MR. LOESER: It's a matter of degree of review. If they postulate or show us that 30 minutes is achievable, that is, the operators can sit on their hands for 30 minutes or that whatever the protective action is not needed for at least 30 minutes, then they don't have to go through nearly as much detail in how quickly will the operator recognize the problem;

how fast can he isolate it down to a component; what if the operator is wrong. It's a significantly simpler review, which is what we were asked to do: come up with a reason why we have a high probability of success in this review, I believe was the terms used, as opposed to if they are doing the same thing saying that in the case of a licensee recently who made a submittal, who said, "We think the operators can take action within two minutes," and this would be much more difficult.

Then we would have to say what is the postulated failure; how will the operator recognize it. In the event of digital systems, the failure is not necessarily obvious. You can have, for example, a partial activation or an indication that the actuation has taken place, but it hasn't or vice versa.

When you start talking about this, there is a lot more things that have to be considered. If they follow the 30 minute criteria, the review becomes much simpler.

I will grant you there is still a review, but it's not nearly as much. We're trying to provide a fast lane for approval, as opposed to the long, complex side road. That's the difference between the

30 minutes.

MR. GROBE: The review that would be done, if I understand correctly, would be limited to does he or she have the controls and the indication necessary to do the action. If it's greater than 30 minutes, the deal is done essentially. If it's less than 30 minutes, then you get all kinds of issues regarding human reliability, information availability, ability to discern the problem, and identify what action correctly needs to be taken. It's a much more complicated question, and the question gets more and more complicated as the amount of time goes down.

MR. WATERMAN: I think this issue applies to the heart of what we've been saying, Dr. Apostolakis. Right now we don't know what the failure modes are.

I'll give you a case of where we may not be anticipating the worst case failure, which is really what we're talking about here, is how long does it take to figure out what to do if a worst case failure occurs.

Let's go back to an analog system where in analog systems we assume the failure is what? A fail high, fail low, fail as is, right? That seems to cover the whole gamut, and that did cover the whole

gamut until we had an event at Rancho Seco and an event at Crystal River in a non-safety system where the integrated control system, which is plus or minus ten volts DC at that time, had a loss of voltage, failed to zero volts.

Some of the indications were above zero volts. Some of the indications may have been below zero volts, but everything went to zero volts, mid-scale. Operators were totally confused about that. Where is my plant? What is it doing? How do I recover from this?

That's just analog systems. Now we're into digital systems where they are much more complex. Now we get a failure we may not be anticipating as a worst case failure. The reason we chose 30 minutes in addition to what other countries have done was what if the operators get faced with an event where they don't know what's going on and they have to figure out what to do. What's their plant status? Should we say an operator has got two minutes to do that or should we be on the conservative side and say let's assume that it takes the operator 30 minutes to figure out what in the heck is going on with my plant?

So the 30 minutes seemed like a very reasonable period of time for us to give the operator

to understand what's going on. We're not saying the operator cannot take actions before 30 minutes. We're simply saying we need to put in enough time there so that an operator in a worst case failure, which we don't even know yet -- we might figure that out -- in a worst case failure can do the correct action, and that's all of the basis for the 30 minutes, I think.

CHAIRMAN APOSTOLAKIS: Jack mentioned earlier this morning that you may want to put a sentence or two up front that, you know, this is one way of doing it. There may be others. And judging from your answers, which make sense, it's a matter more of a presentation rather than substance.

If you said up front, which you say later, by the way, in other instances, for example, you talk about the available time and -- where was that? Yeah, for example under Problem 3, you talk about a time that the actuation would be required with sufficient time available for the operators to determine the need for protective action.

If you set it up in a way that says you're allowed to take credit for manual actions, you have to demonstrate that there is enough time to recognize what is going in, blah, blah, blah, blah, blah, blah, blah, and because the issues will become more complex

the shorter the time becomes and because we don't know the failure margin and so on, here is another way around it. If it's 30 minutes, just do it. Beyond 30 minutes, argue.

I think that that is much closer to what you are saying you have in mind rather than what's on the paper. The paper says, here, 30 minutes, do it this way. Beyond 30 minutes, worry about the operator.

And I think that will be also closer to what the industry wants. If they can really come up with arguments that can convince you that even when the issue is a 15 minute issue it makes perfect sense to rely on operators, if they can convince you, then give them the option. So I would say --

MEMBER BONACA: But I heard something else from Mr. Waterman.

CHAIRMAN APOSTOLAKIS: Yeah?

MEMBER BONACA: He said, you know, not clear what the failure mode may be and the 30 minutes give us some comfort at least that it's time for doing some troubleshooting or whatever in thinking about it.

CHAIRMAN APOSTOLAKIS: Yeah, that's part of the answer, and that can be accommodated, I think, in this.

MEMBER BONACA: Yeah.

MEMBER MAYNARD: Well, I agree with George. The one thing I'd add is I think ultimately when it comes down to it the amount of time for the review should depend on the situation probably more so than a 30 minutes arbitrary limit. I would think there would be some things under 30 minutes that are going to be clear and easy to deal with and lots of margin and shouldn't take as long a review as something that may be even closer to 30 minutes that may be more complicated.

So I think it really needs to boil down to the situation more so than an arbitrary 30 minutes.

MR. LOESER: I think you're correct that some things will take more time than others. The problem we have is we don't know which of those is going to occur. Looking at it right now, we don't know what the next digital failure will be, and we don't know if it's going to be something obvious or if it's going to be something very subtle. So we are trying to put a conservative value in here to take care of the subtle issues.

CHAIRMAN APOSTOLAKIS: But, Mr. Loeser, I don't disagree with you. You can put all of these statements in the document to warn people that when it

comes to shorter times, all of these concerns become real.

But there is no reason to say, you know, 30 minutes this and that. You can say if you guys can convince us, fine, but here are the issues that we are worried about.

Now, a way out of it is, you know, if the time is up to 30 minutes and you do this, that's fine. I mean, then in other words, it's presented in a different way that's closer to a process rather than an apparently arbitrary -- because, after all, when you talk about failure modes, will we have any guarantees that 40 minutes later we will know what the failure mode is?

And the other side is it's conceivable that they will know what failure has occurred in 20 minutes. It's not clear that, you know, we will not know or we will know.

MR. GROBE: Just a couple of observations. This was really intended to provide an opportunity for applicants to do cost-benefit analyses. The dialogues in my office and Kemper's office and Ian's office on whether 30 or 20 or 25 or 35, what's the right number, were frequent and the decibel level occasionally was quite high.

We settled on 30 as a threshold that we would be comfortable at a reasonable assurance level that we have sufficient confidence that that's a good threshold and we're not going to do a lot of review. To get additional insight, we had this international conference on diversity and defense-in-depth common cause failure, and I think there were -- somebody could correct me if I get these numbers wrong -- but there were like seven countries involved. Four of the seven had established 30 minutes as their criteria for the exact same reason. I think one had 15 minutes, and the others had no currently established criteria.

What we're trying to do is establish a very predictable environment where the utilities will understand that if it's greater than 30 minutes, it's going to be like a hot knife through butter. If it's less than 30 minutes, there's going to be additional analysis.

Those additional analyses and dialogues with the staff cost money. So they have the opportunity to make a cost judgment of do I just change this design a little bit and put in my independent shut-down -- what is it?

MR. WATERMAN: Diverse actuation.

MR. GROBE: That's the thing, or do I

simply get into the analysis? What's the costs of these two different approaches?

We wanted to give the industry an opportunity to understand this is good enough. We know this is good enough. Something else might be good enough, too, but it's going to take more work on our part and more work on your part.

CHAIRMAN APOSTOLAKIS: I think we're talking about two issues here. One is is it 30 minutes or 25, and I agree with you. You have to pick a number. You try to see what other people are doing. You have discussions among your staff, and you say 30. Okay? Great.

But the other issue is how to present this 30 minute thing, and I think that's where we are not doing a very good job right now. Because all of these arguments that you, Jack, and Michael and Paul and Bill earlier gave us, if I read the document and I don't talk to you, I don't know that stuff.

MR. GROBE: We're going to fix that.

CHAIRMAN APOSTOLAKIS: Now, I don't know if you have enough time to do this.

MR. GUARRO: It sounds like from what I was listening to, it sounded like one key issue is, you know, the form in which this unspecified failure

modes manifest themselves because I think for operator action, you know, he has to know what's going on.

CHAIRMAN APOSTOLAKIS: Yes.

MR. GUARRO: So I think probably one could complement the 30 minute thing with some statement that says, "Or in cases in which there is clear indication of the nature of the failure mode," for example, as opposed to some, you know, confusing, conflicting type of display that the operator needs to really analyze in depth before he can figure out what was really the action that he has to take is supposed to be.

MEMBER ABDEL-KHALIK: Help me if you will. Somebody comes to you and says, "This thing happens, and based on our analyses, if the operator responds within 40 minutes we'll be okay." Now, who determines whether or not that statement is correct and what the error bar in that 40 minute number is?

MR. WATERMAN: Well, we're going to have to do an independent evaluation obviously to confirm that, yes, they're okay for 40 minutes. The reason for the 30 minute limit incidentally was to identify whether or not a diverse actuation system needs to be installed in the plant or not.

A licensee says that they've done their

analysis. They show they can go 40 minutes. We have our Reactor Systems Branch in NRO, and it's something like the NRR, something like NRO. They're going to have to review those analyses obviously to confirm, yes, the analysis is correct and it's conservative and, indeed, if the operator doesn't take any action, it looks like they will still be within their design basis after 40 minutes.

We do need to check their --

CHAIRMAN APOSTOLAKIS: A significant amount of review will have to be done.

MR. LOESER: Done before that.

CHAIRMAN APOSTOLAKIS: There's no question.

MR. LOESER: Well, but remember though that the analysis that will be required is not a worst case analysis. It's a best estimate analysis. they do not have to use worst case numbers. They don't have to use the longest response time or any of this stuff. They can use what is considered realistic numbers.

Second of all, the requirement is not really to stay within the design basis, but to meet the requirements of BTP-19, and that is no more than a ten percent release of the Part 100 limits.

MR. WATERMAN: No containment failure and no reactor coolant system failure.

MR. LOESER: So it is a much simpler analysis than the type that is typically required for design basis accidents.

CHAIRMAN APOSTOLAKIS: I don't think we disagree actually. There is no disagreement here, I mean, judging from your answers. It's just that, as I said, if I read the document without talking to you, I get a very different request.

You are offering a way out of having interminable discussions whether six minutes or ten minutes or nine minutes and this and that. Present it as such. That's all I'm saying.

MR. GROBE: We describe them as wonderful, interesting discussions. The utilities describe them as interminable discussions.

(Laughter.)

MR. JUNG: Mr. Chairman, we'll take your suggestion to heart and I will try to fix that.

MEMBER BONACA: No, I mean, I thought I understood from the text what the 30 minutes really -- it's really something they set for themselves as a decision point for the level of review they do, and you can still defend the lesser time.

CHAIRMAN APOSTOLAKIS: I didn't see that, Mario. That's where I got the -- I didn't see that. It starts out by saying in those instances where the protective action is required in less than 30 minutes, an independent and diverse automated back-up achieving the same or equivalent action should be required.

MEMBER BONACA: Well, that's true. You're right.

CHAIRMAN APOSTOLAKIS: That's what it says. Now, if you change the presentation that "should" goes away and you present it in a different way. The end result might be the same. Okay? But it's a different way of doing it.

This failure mode business bothers me though because I'm not sure. I know you have to pick a number, and I don't have a better number, but --

MS. SOSA: Just to add a point to kill the horse at this point, I think what the staff is trying to do is communicate their expectations clearly. So, you know, there was a lot of discussions, anywhere from two minutes to ten minutes to 15. Thirty is the number that we picked. We have some basis to defend that number. It just clearly communicates the staff's expectations.

It's not a requirement, and I agree that

that sentence needs to be clarified, but at the same time we want to maintain what we consider to be regulatory certainty by offering a number.

CHAIRMAN APOSTOLAKIS: And I repeat. I don't disagree with your number.

MS. SOSA: Okay.

CHAIRMAN APOSTOLAKIS: "Should be required" is really --

MEMBER BONACA: Yeah, it's a demand there.

CHAIRMAN APOSTOLAKIS: Did you want to say something, Kimberly?

MS. KEITHLINE: Can I make a comment? This is Kimberly Keithline.

I'm not sure if this is on or not.

The problem we have is that we read it the way you did, Dr. Apostolakis, and that although this offers the fast lane the HOV approach, industry is concerned that if they choose to try to justify something other than the 30 minutes, that without clear criteria for how to do that, how to justify, how to show that the operators can be relied upon, that we really probably have no chance of success there, which is why we want to pursue the process, the methodology.

CHAIRMAN APOSTOLAKIS: Right, yeah, and as I said, in other parts of the document there are hints

that one has to worry about the timing, the actions, the available time, and as we said this morning, I mean, we already have a document that has been reviewed in the context of fires.

Now, there are several pages there discussing the special circumstances for fires, the environments you have and the actions of people. In your case in a future document you may have several pages where you discuss the special circumstances of digital I&C so that the applicant will know what kinds of issues they will have to address, and in fact, Paul here keeps raising a few that certainly have to be there.

But at least we have a precedent. Okay? Now, I'm not saying take the document and go to Word and everywhere it says "fire" replace it by "digital I&C." No.

(Laughter.)

CHAIRMAN APOSTOLAKIS: That would be different, I think, but the conceptual approach is the same, and the concerns that have been raised, you know, you have similar concerns. So we can build on that. That's all.

MR. GUARRO: Again, I think the key seems to be to have some criteria to add the 30 minutes.

CHAIRMAN APOSTOLAKIS: But that has to be a separate document because it can't be part of the interim guidance, it seems to me. The interim guidance has to be published as soon as possible.

MR. JUNG: Yes, we recognize that. We heard the concerns. I think given the need to issue this ISG in a timely manner, if you look at our project plan, we have longer term activities, and we'll continue to work with the industry on other activities that's going to come in the next two or three months that's actually related to adequate diversity attributes coming along. That will also provide another opportunity for us to take a look at what additional guidance is needed.

CHAIRMAN APOSTOLAKIS: Kimberly, are you saying that you want to see those criteria in the interim guidance? That's going to take a while.

MS. KEITHLINE: I don't think we -- we can't come through it by the end of September. I would like to make sure that we all recognize that that is something that still needs to be done.

CHAIRMAN APOSTOLAKIS: Absolutely. I don't think anybody disagrees.

MS. KEITHLINE: Right. In the interim, I don't think anyone will be able to justify actions

less than 30 minutes, and that's a concern for the industry.

MR. GROBE: That clearly is not correct. I mean, that clearly is not correct. For example, the Okonee application that is coming in October, November, December or whenever it's coming in is going to include justifications for less than 30 minutes. I mean, that would infer that we're not capable of considering something or not interested in considering something less than 30 minutes, and that's clearly not true. That's just not the case.

The purpose of the Steering Committee is to make sure that the guidance that is on the street is as clear as possible and provides as predictable as possible a licensing process for digital, and the interim staff guidance is not the end of the road, and I believe the specific you already mentioned has been mentioned many times and it's part of our longer term plans that we'll provide guidance on what kinds of things go into -- it's already been discussed extensively.

So I talked with Alex -- I think I saw him walk in a minute ago -- on Tuesday that we need the industry to more clearly define exactly what areas it has identified that it wants to continue to develop

and evolve this guidance as we go forward because we're putting together right now the project plan for the longer term activities.

We believe we understand what those areas are, and the one you mentioned is one of them, and we're working that into the long-term plan. But there's no question that something less than 30 minutes can meet the reasonable assurance criteria, and the staff is ready and able to consider the question.

MS. KEITHLINE: Okay. My understanding is that Okonee needed to add diverse actuation system functions because they couldn't justify less than 30 minutes, and if that has changed, that may be a good thing.

MR. GROBE: No, the 30 minute criteria didn't exist when Okonee came in with their application, and they were talking about things that were in the two minutes and six minutes and eight minute range, and there was a lot of discussion, and our intention is to provide more clarity to how those discussions should proceed if the licensee chooses to come in with an operator action that has to be accomplished in three minutes or something of that nature.

We're also intending to provide applicants the opportunity to understand that if they come in with something at this level that they're not going to be a lot of discussion.

MR. KEMPER: This is Bill Kemper.

If I could just add one comment, too, I have to state the obvious here. All of this can be avoided, of course, if a designer builds in the appropriate diversity and defense-in-depth into the primary reactor protective system. So the only way we get into this situation is if a designer chooses not to build in sufficient diversity and defense-in-depth.

So it's kind of like we're floating all around the primary issue here. It's very possible to build a system with sufficient diversity and defense in depth, I believe, such that you won't need a back-up system.

MR. GROBE: Or if you do as other countries have, you have a complete diversity actuation system for all safety functions.

So those are the ends, the bookends, and we want to make everybody clear that we're willing to consider something in the middle, and we're trying to provide some criteria for how that consideration will go forward, and we're going to continue working with

the industry on refining those.

CHAIRMAN APOSTOLAKIS: Okay.

MR. LOESER: Well, I think we've covered Statements 1 and 2 sufficiently. So we'll go on to Problem 3, and I will try to cover them fairly simply.

CHAIRMAN APOSTOLAKIS: Good, good.

MR. LOESER: This was a question on BTP-19, the position four challenge, and the specific requirement was that in BTP-19 is that the system has to be a system level actuation, and industry wanted to know could component level actuation be considered sufficient.

And the simple answer is yes. We had said that the thing of it that's really required is that the operator action be possible from the control room, that there be sufficient time for it, that it be simple, that it be achievable, and considering all of those, component level activation would be considered acceptable, and we're planning to change the words within BTP-19 to address this.

Problem Statement 4 was concerning whether --

CHAIRMAN APOSTOLAKIS: Mike, would you please remind me. What does "problem statement" mean?

MR. LOESER: We had came up with the

seven problem statements for this particular task working group.

CHAIRMAN APOSTOLAKIS: And these came as a result of the industry --

MR. LOESER: The industry and us talking together, we asking them what are the things that are really bothering you about in this case diversity and defense in depth. What are the hard points? What do you need clarification on?

And we came up with -- I don't know -- 20 or 30 different things. We talked it over among ourselves, and narrowed it down to eight and now seven.

CHAIRMAN APOSTOLAKIS: Okay. Thank you.

MR. LOESER: Okay. The Problem Statement 4 was on spurious actuation. Does this need to be considered as well as failure to actuate? And our statement on that basically was for a design basis accident, yes, you need to consider challenges to the safety system, but this is a beyond design basis event.

The primary thing we are worried about is if a common cause failure is such that when you need a protective action, it doesn't occur. This is when you have a real problem. A spurious actuation while

a challenge to the safety system is inherently self-announcing. If something spurious actuates, you know about it. So this is of lesser concern than an unknown failure, one that will prevent an actuation, and as such we said when doing the common cause failure analysis, you need to emphasize the failure to actuation and not the spurious actuation.

Problem Statement No. 5, industry asked us are there combinations of design attributes, such as simplicity, testability, other things, such that if these are all done we don't even have to consider the fact that this system may have a common cause failure, and we said it's possible, but it's going to be difficult. We said that if the system already has sufficient diversity built into it. An example we gave is a system that has two channels of one type and two channels of the other type.

Yeah, you can pretty well say no single failure because there isn't common software so you don't have a common software failure.

The other possibility we allowed for, and once again, we're not saying that there aren't others; these are just the ones we could think of right off the top of our head, and once we get the research report or if industry proposes other things, we

certainly will evaluate them, but the other one we had is if a system is sufficiently simple that it is fully testable, then you can test every combination of input, every combination of circumstance, every combination of plant condition and show that you only produce correct results.

Now, with a microprocessor based system this is probably going to be somewhat difficult, but with a simpler system, with a component logic design or maybe with an FPGA or some types of application specific integrated circuit, this may be possible. It all depends on the simplicity of the system. If you have a comparatively simple system, it's going to be more reasonable to assume 100 percent testability than for a very complex system.

For Problem Statement 6, the question was on echelons of defense. Can you combine particularly the trip systems and the emergency core cooling systems into one overall system? This was proposed, for example, at Okonee.

CHAIRMAN APOSTOLAKIS: Are there any other regulatory documents that use the word "echelon"?

MR. LOESER: Yes.

CHAIRMAN APOSTOLAKIS: Well, okay.

(Laughter.)

MR. LOESER: Well, among other things --

MR. GROBE: Was yes or no sufficient?

CHAIRMAN APOSTOLAKIS: Have you seen it in another context?

MEMBER BONACA: No. He said yes, and that's the first.

CHAIRMAN APOSTOLAKIS: Go ahead.

MR. LOESER: BTP-19 specifically addresses that.

CHAIRMAN APOSTOLAKIS: No, no, no, no, no. I mean other than I&C.

MR. LOESER: I don't know of any.

MR. CARTE: Excuse me. Norbert Carte from I&C.

Yeah, there is a current rulemaking in the process which talks about diversity and defense-in-depth for non-LWR reactors.

CHAIRMAN APOSTOLAKIS: Where? Diversity where? I&C?

MR. CARTE: Plant level diversity and defense-in-depth.

CHAIRMAN APOSTOLAKIS: But in the I&C context.

MR. CARTE: No.

CHAIRMAN APOSTOLAKIS: General common

cause failure? Really?

MR. CARTE: Well, it talks about diversity and defense-in-depth at the plant level, not just --

CHAIRMAN APOSTOLAKIS: And it uses the word "echelon"?

MR. CARTE: I believe so.

CHAIRMAN APOSTOLAKIS: Gee, it spreading.

MR. CARTE: It at least references the IAEA's inside reports that use "echelon."

CHAIRMAN APOSTOLAKIS: I think it's Greek, but I'm not sure.

MEMBER BONACA: Sounds Greek to me.

CHAIRMAN APOSTOLAKIS: Even to me. Do you believe that?

MR. LOESER: I'm sure the root of the word is Greek. That's the case in most of our words.

CHAIRMAN APOSTOLAKIS: Thank you very much.

(Laughter.)

MR. LOESER: However, what our statement was is that if you follow the criteria for Problem Statements 1 and 2, you can -- that is, the 30 minute rule and the manual actuation and the sufficient indications and controls and all of that -- then you can combine the echelons and there will be no further

discussion.

However, if you don't need these, then there will be further discussions on how you will approach a common cause failure, how the single failure criteria continues to be met for other than common cause software failure, how the common cause failure analysis requirements will continue to be met.

So once again, we're saying if you do follow the original interim staff guidance, it's pretty much a done deal. We don't have to discuss it more. Otherwise we will have to have further discussions.

And the final one on Problem Statement 7, industry asked us to clarify just what the requirements were regarding single failure as opposed to a common cause software failure, and this really went back to the original discussion of is a common cause software failure really a single failure. Is it really multiple failures? Should it have been within design basis or shouldn't it?

And I think industry wanted some reassurance that we weren't going to change our mind later on. And the conclusion we had drawn, we spent a fair amount of time arguing about this particular item just within house, and what we came up with is,

number one, policy says it's not a single failure, but we were trying to come up with why did policy say this. What is the real technical justification for this?

There's also various legal justifications. Being an engineer not a lawyer, I was looking for a technical reason.

First of all, the applicable design or applicable IEEE regulation, IEEE 379, talks about specifically exempting design deficiencies, manufacturing errors, maintenance error, and operator error, and these are where mistakes in software actually come from, and the reasons these were exempted was because they said that the requirements for design qualification, quality assurance, high quality design, without specifically mentioning the NRC requirements, but the general requirements, provide protection against this type of design error and make it highly improbable, and we agree with that.

In addition, if you look at the definition within Appendix A of a single failure, it talks about the result of failure of a component, and you could consider software a type of component, but a single occurrence.

A software common cause failure is not

really a single occurrence. It's four occurrences. It has a common cause, which is the name behind it, but it's four things failing, not really one thing failing. So we looked at that and said it really doesn't fall into the spirit or the language or the intent of the definition of a single failure.

Now, you could argue about this and it may be at some time in the future the definition of single failure will be changed, but right now we feel that's the best concept, and that was the reason behind this.

And since we continued with our existing definition and concepts, we have not had any disagreement from industry.

CHAIRMAN APOSTOLAKIS: They didn't argue to bring into the design basis?

MR. LOESER: No, they did not.

MEMBER BONACA: I have a couple of points I'd like to make. One, clearly 1993 there was a decision that software common cause failure is beyond design basis because of low probability.

MR. LOESER: Well, actually it went beyond that. It also went into the definition within 379 of what needs to be considered during in a single failure analysis and with the specific exemptions from design error and specification error we said --

MEMBER BONACA: I'm not proposing here that we introduce it now as a single failure. No, what I'm trying to raise is that this was 1993. Now, since '93 there have been a significant number of applications, and operating experience should tell us something regarding this probability of common cause failure.

I mean, the reason why I raise this issue is that some time ago in some presentation we were given some information regarding some events which are pretty surprising, I mean, and I'm not proposing that one does an automatic change here, but again, since you're collecting operating experience and events that occurred, I think that these assumptions should be verified.

MR. LOESER: Well, we have looked at a number of events. I believe Mike collected over 300.

CHAIRMAN APOSTOLAKIS: Yeah, we have a presentation.

MR. JUNG: Yeah, the next presentation will cover some details.

MR. LOESER: But from our point of view we looked at it and said yes. A common cause failure does occur. It is possible, but it doesn't happen very often, and most of the time when it happens, it

doesn't have the safety significance. It doesn't occur just at the moment where you need that particular safety system. It's still possible, but we haven't had any plants melt because of this. We haven't even had anything come close.

The failures we have had tend to reinforce our belief that while a common cause failure is possible and needs to be protected against to some degree, it does not rise to the level that would be required to make it within design basis.

MEMBER BONACA: Good. I guess my comment was prompted by when I look at the bottom bullet that you have. Again, you're making a statement there without a justification. It says even when caused by error, it is considered a failure that's beyond design basis. You provided me already with some good reasons why.

MR. LOESER: I believe that if we ever decide to change our mind or have evidence that we should change our mind, you will hear about it very rapidly.

MEMBER BONACA: Good.

CHAIRMAN APOSTOLAKIS: Even better.

MR. GUARRO: Is there any plan to look at, you know, the comparison of common cause failure

versus software in terms of frequency? Because you're talking about local ability. What does that mean?

MR. LOESER: We are. We do have a research plan that is looking at all of the various failures within digital systems and trying to classify them into hardware failures, system failures or software failures.

MR. GUARRO: What I meant was a different thing. Because the criterion for school in common cause failure of a hardware nature was, you know, the design error, et cetera, et cetera, which for sure in hardware systems are low probability, is that an intention of looking at whether that type of problem in software is as low probability as it is in hardware.

MR. WATERMAN: Actually we've already seen some common cause software failures of safety systems. They just didn't get manifested at the time of an event. I think there's a natural tendency to think that everything works fine. You don't have any errors or failures until, boom, all at once something happens and then it fails.

But I think Turkey Point demonstrated that the low sequencer event in 1994 demonstrated the failures could have actually occurred significantly

sooner and over a longer period of time, and they were waiting to manifest themselves as a risk to public health and safety if an event occurred that ran smack up against that player.

In the case of the Turkey Point load sequencer failure there was a self-testing routine that would lock out the HPI pumps and keep them from starting. Well, there was something like four tests out of 11 that would do that, and the unlock came with the next test that was to be executed would unlock it, and when that system was originally designed, both tests were continuous. They just ran continuously, and they were initiated by a little relay that would close and tests would initiate and the relay close. The relay burned out. So they decided they didn't need to do that, but that failure sat there waiting to happen locking out the HPI pumps on the system, and it was just waiting for a LOCA to come along and it needed HPI, and it occurred at just the right time. It had to be during one of those four events, and the only way they discovered it was one unit was up. Another unit was down, and they wanted to do a start of the HPI pump switched over to another unit because they can share that capability, Turkey Point 3.

And then they discovered the HPIs were

locked out, and they couldn't get them unlocked. But those failures had already occurred, right? I mean it was there.

CHAIRMAN APOSTOLAKIS: I think we are discussing now a different issue, whether the staff should go to the Commission and say reconsider the decision of '93. That's a different issue.

MR. LOESER: We are not considering that. We are not considering that at this time.

CHAIRMAN APOSTOLAKIS: You guys have to develop your guidance and everything respecting the Commission's decisions. So they said, the Commission said the CCF is not within the design basis. then it is not, period. This guidance will be developed under that thing.

Now, if you want to go beyond that and go back to the Commission and ask them to reconsider, that's a different issue which I'm not sure you're willing to --

MR. LOESER: We are not planning to do that at this time. I don't know of any --

CHAIRMAN APOSTOLAKIS: So if we move to Slide 16, would you object to that?

MR. LOESER: No. We're back to you.

MR. JUNG: Okay. Thanks.

As I said earlier, staff plans to continue to work with industry to refine the ISGs as necessary and as appropriate, and eventually produce regulatory guidance document in the form of most like an SRP in this case and other insights, as we learned, specially operating experience and other information. There are multiple projects domestically, internationally that are ongoing and related to operating experience which will be presented in the next session. You'll see the scope of what we are doing.

So I think if --

CHAIRMAN APOSTOLAKIS: Why are you assessing the recommendations? It seems to me you have accepted them and you're doing it.

MR. JUNG: Probably that's not, yeah, the right expression, but that second bullet is something that we're going to present that after lunch.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. LOESER: We took the ACRS recommendations on assessing operating experience.

CHAIRMAN APOSTOLAKIS: No, it says stop assessment for --

MR. LOESER: Yeah, wording change.

CHAIRMAN APOSTOLAKIS: Oh, okay.

MR. JUNG: So are there any other

questions?

MEMBER ABDEL-KHALIK: I'd like to go back to the question I raised earlier about somebody coming to you and saying, "I need 40 minutes to do this," and, therefore, you're going to go through the fast lane in your review, and you said that the independent analysis is done by somebody else within the process to determine that that 40 minutes is true.

Now, given the nature of NRC review, these analyses are not done sequentially, are they? These reviews are not done sequentially.

MR. WATERMAN: Sequentially?

MEMBER ABDEL-KHALIK: Yes. I mean, you don't wait for somebody else --

MR. WATERMAN: Oh, no, no.

MEMBER ABDEL-KHALIK: -- to tell you that, okay, I have checked the veracity of this analysis and determined that the 40 minutes that the applicant estimates is, indeed, correct.

MR. WATERMAN: If I were doing it the way the standard review plan is laid out is when an application comes in, it's assigned a primary organization to review, such as instrumentation and control. The secondary organization is providing support. In a case like this, the secondary

organization would be like the Reactor Assistance Branch in NRR. It has the secondary responsibility of performing independent thermal hydraulic analysis of the licensee's claims.

Eventually when the SER is written, they would put draft input to our safety evaluation report that would approve the application, but we need all of that input from the different organizations into that SER to wrap it up.

You're expecting that to be somewhat concurrent.

MR. LOESER: I think to answer your question if I was doing the review, this would be assigned to another group. I would start doing my SER and all of my investigation and my writing with the assumption that what the licensee said was correct.

Then at the time that I received this analysis it will be easy to put in. There would be a simultaneous review by them and by me on other aspects of the instrumentation, for example, the software, and we would just come together at the end of the review.

I wouldn't be sitting around waiting for someone from Reactor System to say, "Yeah, they were correct. Go ahead and finish the rest of review."

MEMBER MAYNARD: But it would all have to

come together before the SER.

MR. LOESER: Oh, absolutely.

MEMBER MAYNARD: And this is fairly common in a number of things. It would be parallel efforts going on, and at the end if something wasn't able to be confirmed, if that becomes a big issue to deal with.

MEMBER ABDEL-KHALIK: I was just wondering if there was a built in efficiency inasmuch as that would require you to do the analysis twice.

MR. LOESER: We don't really have time for built in efficiencies.

MEMBER ABDEL-KHALIK: Well, I mean, that's what I'm trying to find out.

MR. LOESER: We do our best to avoid that kind of thing. I can't say that it's 100 percent, but whenever possible, this is taken into consideration and the conduct of the review to try to use as much parallel effort as possible to make it as short. As possible, as it is the reviews are complex enough and take a long enough time.

So, yeah, we consider this kind of thing, and we tried to get rid of any possible built in inefficiencies like this.

MR. WATERMAN: And incidentally, it isn't

totally a waste because the review that we're doing in instrumentation and control is not going to change if the thermal hydraulic analysis isn't correct. We're still looking at things like, well, the quality was good. They followed all of the process. We followed the requirements down through. We have reasonable assurance that the application is sound.

Now, Reactor Systems may come back and say there's no way that 40 minutes is sound. They can't last ten minutes. We then go back to the applicant and we'd say, "Look. You know, 40 minutes didn't make it on our analysis. You need to resolve that."

That may require them to make another submittal for a diverse actuation system, but it didn't change our original I&C stuff. That's not a waste. That was still productive work. It's just a matter of wrapping up the open items, such as, you know, 40 minutes wasn't valid.

MEMBER ABDEL-KHALIK: Thank you.

CHAIRMAN APOSTOLAKIS: Any other comments or questions from the members?

Okay. Thank you very much gentlemen.

We will recess until 1:15.

(Whereupon, at 12:16 p.m., the meeting was recessed for lunch, to reconvene at 1:15 p.m., the same day.)

AFTERNOON SESSION

(1:18 p.m.)

CHAIRMAN APOSTOLAKIS: Back in session.

And the next presentation is under operating experience.

MR. JUNG: Okay, gentlemen. This is, again, Ian Jung, and I'm the D3 technical task working group lead, and with me today is Steve Arndt from Research and Russ Sydnor from Research. He's the Branch Chief for the I&C area in research as well.

A little introduction. Next slide.

Again, I thank ACRS for this opportunity to greet you on the status of the staff's assessment of, you know, operating expense and inventory and classification that those recommendations were made by ACRS.

Going back, a little bit of background where we are, how we ended up here. The Commission directed -- there was a Commission interaction with ACRS on digital I&C. In May 18 this year ACRS generated a letter to the Commission recommending the two items that are listed: develop an inventory and classification of existing and potential nuclear power plant digital and software systems and evaluate digital system operating experience in the nuclear and

other industries to obtain insights regarding potential failure modes, and this information is supposed to be used as an input toward the staff guidance for the D3 and beyond.

In response, the Commission directed NSRM to add these recommendations into D3, digital I&C project plan which we did. On July 2nd, the staff provided a memo to the EDO and EDO concurred on responding to their recommendations. Specifically in that memo, the staff fully agreed with the ACRS recommendations and the staff appreciates the committee for providing valuable inputs and recommendations which will be conducive to a person developing future guidance document.

On July 10th and as a follow-up, July 10th, some of the staff members got together with the Chairman in an informal manner to make sure what we are planning to do is consistent with the ACRS expectations. The next slide has a table that we shared with the Chairman at the time, and it's been a little bit tweaked to add your comments on adding a box related to other industry operating experience element.

And let's see. I want to go to the next slide.

The key purpose of this short-term activity was to perform a quick assessment of existing information related to digital system operating experience and inventory and classification to identify insights and findings which may impact the ISGs under development, and we have a short term and longer term activities.

The short term activities are related to that. So I just want to go over the table to have it provided in the same place. The action one is inventory and classification. The box itself is an activity that we propose, and Steve Arndt and some of the research staff worked on it, which we will give you some insights to the findings out of the activities in the later slides.

In action two, delayed operating experience, we wanted to specifically identify the type of activities and sources to look at operating experience, and some of the previous research activities that's been done and some of the other activities that we know of because operating experience could be interpreted as very broad. It could go, you know, way far. So we wanted to sort of narrow it down, what we have and what's valuable for us.

So these are the items: talking to EPRI and also other industry data that we've gathered so far and LER data and also capture insights from the COMPSIS, computer based systems important to safety project, the international project as well.

Those two boxes, action one and action two will be fed into staff assessment for any major issues or common themes that could influence the current development of ISGs specifically for D3 and beyond it as necessary. And that is due by the end of this month.

So we are not quite there yet, but the reason we are here is to give ACRS and other participants the status of our assessment, and eventually the preliminary assessment will be completed by the end of this month, and eventually the final outcome of the short-term assessment will be an assessment result with certain recommendations and final conclusions.

And longer term activities are sort of the same. I think these two topics, the operating experience and the classification inventory are very important topics even in the longer term. So we envision having some activities in the longer term that will feed into a longer term update or refinement

of the regulatory guidance documents related to these that you see.

CHAIRMAN APOSTOLAKIS: Why is Action 2 feeding into Action 1?

MR. JUNG: Actually it's not feeding into one. Both of the Action 1 and Action 2 are being fed into a staff assessment results. The second box from the --

CHAIRMAN APOSTOLAKIS: The staff assessment to look for major issues, what does that mean?

MR. ARNDT: That means we're going to take what we learned from Action 1 and 2 in the short term and see whether or not we need to make an assessment to see whether or not we need to update or change or do something different in our other short-term activities like the ISG work.

CHAIRMAN APOSTOLAKIS: So, for example, they find in evaluating the operating experience that certain failure modes are relevant only to one particular group of I&C systems --

MR. ARNDT: Correct.

CHAIRMAN APOSTOLAKIS: -- whereas the interim guidance applies to everybody.

MR. ARNDT: Correct, or we may find that

we are making a certain assumption about the way systems fail, and many of them fail in this way and not so many fail in the other way, and the trend may not be --

CHAIRMAN APOSTOLAKIS: So the center box then is the second one. That's the one that should have been in bold faced letters because that's really where you're doing something useful.

MR. ARNDT: Yes, sir.

MR. SYDNOR: The assessments will provide useful insights.

CHAIRMAN APOSTOLAKIS: Yeah.

MR. SYDNOR: That's what we're hoping.

CHAIRMAN APOSTOLAKIS: I mean, it's the assessment that feeds into the regulatory system.

MR. SYDNOR: And Action 1 and Action 2 are more the detail of what we're doing --

CHAIRMAN APOSTOLAKIS: Right.

MR. SYDNOR: -- to provide the assessment.

CHAIRMAN APOSTOLAKIS: Exactly. So I would make that bigger than --

MR. ARNDT: Put a double line around it.

CHAIRMAN APOSTOLAKIS: Yeah, or something, and the others feed into it. Because looking at the bold faced letters Action 1 and 2 I thought, you know,

the whole action feeds into the other action, but you said, no, it wasn't.

MR. ARNDT: There is some synergism between the two activities, and we'll talk about that.

CHAIRMAN APOSTOLAKIS: So the deliverable is December, right, for the input to NRR and NRO?

MR. JUNG: That's the final outcome. Actually we will have a draft report for D3 group to take a look at it.

CHAIRMAN APOSTOLAKIS: Oh, well, this is very nice that things are happening with such speed. When will you have the interim report?

MR. JUNG: By the end of this month.

CHAIRMAN APOSTOLAKIS: And that's a report we can review?

MR. JUNG: I think we promise that we'll share that with you by the end of this month.

CHAIRMAN APOSTOLAKIS: Okay. Everything is happening by the end of this month.

(Laughter.)

MR. JUNG: I just want to give you a perspective on it because during the last month and a half, close to two months, the staff really worked hard, several staff members from Research and from NRR, to really look at this closely.

CHAIRMAN APOSTOLAKIS: As I said this morning, you're not going to get much sympathy from the committee for working hard.

MR. JUNG: I understand. We'll still try to get some.

CHAIRMAN APOSTOLAKIS: Are you working hard, Steve?

MR. ARNDT: The last time I checked.

CHAIRMAN APOSTOLAKIS: Okay.

MR. SYDNOR: One other comment on the short-term activities. It was narrowly focused on D3 because it was a short term, and we didn't have a lot of time. So we really focused on what we could learn that may influence the D3 interim staff.

CHAIRMAN APOSTOLAKIS: Yeah, yeah.

MR. ARNDT: There are broader implications. We'll talk about those.

CHAIRMAN APOSTOLAKIS: Of course there are, yeah, yeah.

Where is Guarro?

Well, your guys are looking only at nuclear experience, right?

MR. ARNDT: No.

MR. SYDNOR: No, no, it's broader.

MR. ARNDT: It's broader.

CHAIRMAN APOSTOLAKIS: Where?

MR. JUNG: Bottom box of the first column on the --

CHAIRMAN APOSTOLAKIS: Oh, from other industry.

MR. JUNG: That's specifically to your comments that you have given.

CHAIRMAN APOSTOLAKIS: Oh, yeah.

MR. JUNG: So we added that.

CHAIRMAN APOSTOLAKIS: So you think there is enough time and you will have a draft report by the end of this month. That's interesting. So you must have already --

MR. ARNDT: Pieces of it.

MR. JUNG: We have pieces of it.

CHAIRMAN APOSTOLAKIS: -- approached all of these people. I mean these organizations, right? You have already gotten some information.

MR. ARNDT: Some information, yes. It's a short-term activity. It's not going to be completely comprehensive.

CHAIRMAN APOSTOLAKIS: But will it be at some point in the future?

MR. ARNDT: That's the longer term activities.

CHAIRMAN APOSTOLAKIS: Where does it say that? Oh, evaluation? Is that what --

MR. ARNDT: Yeah, evaluation of operational experience.

MEMBER BONACA: Will you have only domestic experience?

MR. ARNDT: Say again.

MEMBER BONACA: Will you have only domestic experience?

MR. ARNDT: I hate words like "all." We are planning on trying to gather all of the relevant domestic experience.

MEMBER BONACA: Okay, but not foreign experience.

MR. ARNDT: We're going to try to get as much of that as possible.

MEMBER BONACA: Oh, okay.

CHAIRMAN APOSTOLAKIS: But I thought there was an international --

MR. ARNDT: Yeah, we're going to go in that, but the middle box there is the COPSIS. That's the international nuclear database.

MR. SYDNOR: We'll talk through each of these data sources and try to characterize them for you in a later slide so that you have a better feeling

for it.

CHAIRMAN APOSTOLAKIS: I mean, there is a mechanism already for getting --

MR. SYDNOR: All of these are ongoing activities. These were not new activities generated because of the SRM.

CHAIRMAN APOSTOLAKIS: Okay. Because I do know that there was one on the common cause failures for hardware.

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: Is it the same group that's expanding into digital I&C?

MR. ARNDT: It's a separate group, although it is out of the same organization, and we're working with them actually. Our project manager is behind it that does the common mode failure database, is doing this database. So there's discussion between them.

MR. JUNG: Yeah, at this point it's really for your long-term activities we didn't want to really, you know, specify what specific actions we're going to take or recommendations we want to make. That should sort of -- we believe that should come out of this short-term assessment because there are a lot of activities that are ongoing now. We don't want to

create something that is part of what was happening right now.

So I think it's an objective view of all the tools and make sort of formal recommendations through line organizations of NRO, NRR who needs this information to review. So that's going to be the next step.

CHAIRMAN APOSTOLAKIS: Now, about a year or so ago we had a representation from Brookhaven. Is that effort dead?

MR. ARNDT: No, that is an ongoing effort associated with our long-term digital system risk analysis effort.

CHAIRMAN APOSTOLAKIS: No, but they were collecting data.

MR. ARNDT: They were collecting data to support that particular part of it. That piece is one of the many data sources. We don't have every single data source here.

CHAIRMAN APOSTOLAKIS: Okay. So you are taking advantage of that.

MR. ARNDT: We're taking advantage of that.

CHAIRMAN APOSTOLAKIS: They are continuing that effort, right?

MR. ARNDT: They are continuing that effort. There's a whole set of very specific information we're trying to gather as part of the digital system risk work. Including that, we're talking with EPRI and with INPO and with NEI about getting some vendor data, very specific vendor data in that. So all of that is part of it.

We're not focusing on that today, but that's all part of it.

CHAIRMAN APOSTOLAKIS: Okay, all right.

MR. JUNG: Okay. The next slide, I'll turn it over to Steve Arndt, who is much more familiar with this topic.

MR. ARNDT: Okay. I'm not going to go into gory details because the effort is not complete, but I do want to tell you what we've done, why we did it the way we did it, and the general focus of the inventory and classification scheme.

The idea here is to provide a mechanism by which we can have a framework for collecting and analyzing the operational data and also have a framework for translating that information into regulatory guidance. What is the information telling us in terms of complexity and other things like that?

You heard earlier today in the D3

discussion that one of the characteristics of deciding whether or not you're going to have a certain level of guidance is how complex the system is. That's a characteristic of the system in terms of things like communications. There are certain characteristics that we can use to form a classification scheme so that we can understand what the data is telling us and also classify the systems so that we can better put them together.

Now, there's a number of different ways you can do this, and if you go to the literature, which we've done, lots of different people have done it in lots of different ways.

One way is based on a regulatory structure, and I'll use a couple of nuclear examples which are going to the FAA or the DOD or others. You can classify systems by safety versus non-safety. The Europeans use safety systems, systems important to safety and industrial systems. As you know, we've done a classification scheme for risk informed classification of SSCs based on both their safety class and their risk importance.

So you can go about a classification scheme along those lines. From a more theoretical standpoint there's been a number of people who have

looked at classification based on design attributes.

CHAIRMAN APOSTOLAKIS: Let's go back a minute.

MR. ARNDT: Okay.

CHAIRMAN APOSTOLAKIS: Risk informed grading systems. Now, it will be very hard, it seems to me, to try to apply the ideas we used in 5069 to digital I&C, but you can apply to the systems or the components of the control --

MR. ARNDT: You can, and this is not a "this is what we want to do." This is an example of how you go about going from what is it you want to what is it you want to get.

We did the safety classification scheme for SSCs. We wanted a better way of breaking up the system functions so that we could determine what level of qualification we wanted, and this is the mechanism we cam up with.

For digital systems, we're trying to understand communications. We're trying to understand diversity and defense-in-depth. We're trying to understand cyber. Those are the driving factors which will drive us to a slightly different kind of classification scheme.

The idea here is just to motivate what it

is we're trying to do and how it is you could go about doing it.

MR. GUARRO: Steve, well, what about -- well, I don't see there -- what about just functionality of the system?

MR. ARNDT: We'll get to that.

MR. GUARRO: Okay.

CHAIRMAN APOSTOLAKIS: Yeah, I was about to ask that, if you can.

MR. ARNDT: Functionality is in part based -- is basically imbedded in the design basis. What is it you're trying to accomplish and what decisions are you making about how you are accomplishing it?

Basically that's what Rashly did in his classification. He looked at safety critical systems, and he looked at how you're accomplishing their mission and what the timing requirements are, what the safety requirements are and what the fault tolerant requirements are.

CHAIRMAN APOSTOLAKIS: So if I'm going to look at systems that actuate something versus controlling its function that would be here?

MR. ARNDT: It would be here, but actually this is in how you implement that function.

CHAIRMAN APOSTOLAKIS: So it's simply the

function, as Sergio says, you know, that this thing is supposed to trigger a reactor trip, period. That's all it does.

MR. ARNDT: That's all it does, but what's important is how it does it. If it does it in a very simple way, then the requirements can be very simple.

CHAIRMAN APOSTOLAKIS: Exactly. That's why we want the classification.

MR. ARNDT: Right, and this is -- the design basis type classifications tell you how it's choosing to implement the function.

CHAIRMAN APOSTOLAKIS: So you will tell us this is the function and this is how it's going to do it.

MR. ARNDT: Right, and if it does it in a simple way, then it falls in one category. If it does it in a complicated way for whatever design reasons, it falls in a different classification.

CHAIRMAN APOSTOLAKIS: Okay.

MR. ARNDT: In a similar way, Perrow did this, and he looked at systems based on their interactions and how tightly coupled they are with the process. So, for example, a system that just has a simple trip function is not very tightly coupled with the process, but if it has a control function, it is

much more tightly coupled with the process, and it also has to do in his analysis of how much interplay and what the timing is and things like that.

When Aldemir did his analysis, he looked at the kinds of interactions, whether they were interactions within the system, like interchannel communication, or within systems and the communications systems.

Go to the next one.

CHAIRMAN APOSTOLAKIS: On the European A, B, C, did you tell us what these are?

MR. ARNDT: Yeah, I did, if you go back one. That's basically they use -- as opposed to a non-safety and a safety, they use a safety, an important to safety and a traditional.

CHAIRMAN APOSTOLAKIS: Oh, okay.

MR. ARNDT: Another way of doing this is looking at operational characteristics, operational data, the way they fail. One analysis that was recently done, and I chose this one -- I could have chosen lots of others -- was the one that the NASA representative presented at the Commission meeting.

CHAIRMAN APOSTOLAKIS: Right.

MR. ARNDT: They broke down their classification based on the way systems tend to fail.

this is basically what we looked at, and they had three categories basically: systems failing due to translation type errors, basically not translating the requirements into the design properly; V&V type errors basically associated with poor coating or not catching coating or simply typos and things like that, and specification based errors.

CHAIRMAN APOSTOLAKIS: So this is a classification of failure.

MR. ARNDT: Of how the systems failed as opposed to how they operate and how they failed to operate. So there's several different ways you can classify this.

So what we learn by going out and looking at the way other people classify? What we learned is, one, if we look at the operational data they'll talk about a little bit more in a few slides, the kinds and classes of failures for nuclear data are very similar to the ones that we see in other safety critical applications and the kinds of functional differences you see, actuation versus control, coupling and various other things are similar to what other people have seen, which is something we've discussed in this committee a number of times.

So basically that gives us an indication

that if we use what other people have done with modifications for what we care about, it should make sense.

So basically what we did is we developed a classification scheme based on three attributes, and the first attribute is basically what we talked about in D3, the complexity of the system, how it's doing its function, and this is not just how many lines of code it is and things like that, but whether it is testable or not and things like that.

The interactions is the second axis of the classification, if you will, and that's based on issues that we care about in terms of communications.

Finally, how much interaction is there? How important is that interaction? Is there feedback simply within the system itself or is there feedback with the actual process that's controlling?

And then the last classification is basically similar to the Rashly safety classification or, in our case, the importance to safety from a risk informed type perspective, and we're using attributes not just associated with risk importance or things like that, but also how important from a system maintenance of defense-in-depth and the consequence of safety failure it is.

CHAIRMAN APOSTOLAKIS: What can be perhaps of help to you there is to consult with what happened in 5069. There's an expert panel that ultimately decides on the importance of the various inputs. One of them is risk --

MR. ARNDT: Right.

CHAIRMAN APOSTOLAKIS: -- input, but many others are does it support safety functions, is it released with defense-in-depth. So you don't have to reinvent. You may want to modify.

MR. ARNDT: Yeah, and currently the attribute you see here is what we're planning on using as the modification of that, some kind of risk importance factor, a qualitative, how important is the system to maintaining defense-in-depth, and a qualitative what's the consequence of safety failure if it does fail.

That's our going in position as we further develop and actually run the classifications. We've only done this for a few systems just to see if it works. At this point we may have to modify it.

So it's similar to what was done in 5069.

So where are we? We've got a system that we propose. We've bounced it against what we've learned in our operational data, and we've looked at

it against what other people have done successfully in other industries that have similar kinds of failures. So what we're going to do is use it to help us understand failure history and failure modes and the potential consequences of how you put together a classification scheme.

Once we're done we're going to do an inventory of all the systems based on that, and populate a set of data, that that's at least at a preliminary point what we're going to do between now and December.

So that's where we are based on what we've done so far, and Ian will do this in a wrap-up. The kinds of things we're learned validate what we've said in terms of, for example, ISG No. 5 from diversity and defense-in-depth. If it's really simple, we may not need to do as much from a diversity standpoint. It's also validated at least as far as we can go, some of the communications actions.

MEMBER ABDEL-KHALIK: Can you give us an idea about the size of that database?

MR. ARNDT: I don't know yet because it depends on how great a level of detail we go. We've got three or four major vendors and tons and tons of minor vendors, and depending upon how you count, maybe

50 different systems that would be nominally classified as digital I&C systems. And you have components and subcomponents and various other things. So it could turn out to be quite large. We have to do it and then decide how useful it is to go further and further and further down.

I wouldn't anticipate it going any further down than what the operational data is pegged to. So if you look at the LER database, for example, it will say this system failed and will usually say a feedwater control system or the RHR control system or the turbine control system or the load generator, turbine diesel generator load sequencer, and then maybe have a manufacturer.

So it will probably be no greater detail than a component and a manufacturer, a major manufacturer. But if it turns out we cannot get the information we need at that level and we have to go to subcomponent, it just makes it a much more tedious process.

And at this point we're simply trying to inform our regulatory guidance. If this turns out to be effective, then we can revisit whether or not we're going to use it specifically for regulatory guidance as opposed to inform regulatory guidance. At this

point we're simply trying to inform the regulatory guidance.

MEMBER ABDEL-KHALIK: If you don't have an idea about the size of the database, what do you think that the report that you will prepare by the end of the month will have?

MR. ARNDT: The report that we have at the end of the month will be what is the classification, how does it work, and how do you go about classifying systems, and a couple of examples just to show how you would do it. By the end of the year if you go back to that first chart, there's a December box that basically says -- I forget what the verbiage is -- provide an assessment paper and recommendations, and the recommendations paper will have more of the actual system level list of classifications and what it tells us, what the recommendations are for long-term action.

MR. SYDNOR: The short-term assessment was really narrowly focused on are we heading in the right direction with the D3 interim staff guidance. Was there anything we can learn in a month, a month, two months, where we would recommend to change direction. That was really the focus of that first initial --

MR. ARNDT: First three months.

MR. SYDNOR: -- validation assessment.

MEMBER ABDEL-KHALIK: Well, without looking at the data, I mean, how can you provide guidance?

MR. SYDNOR: We haven't talked about that part yet.

MR. ARNDT: We are going to talk about what the operational experience is telling us about it.

MR. SYDNOR: I'm going to review briefly what we were able to look at in this time frame and sort of give you some characterization of the nature of the data in these various sources.

The first bullet talks about an internal assessment. By "internal" this was some couple of pieces of work done internal to research. We have compiled over 300 digital system failures, and we're using those. We have used those to influence our research plans and support of, you know, research plan, support future regulatory actions and guidance.

And we're also using that because it's all LER based as a screening tool for what we are going to input into the COMPSIS database that we're currently inputting and are going to input in the future.

You see the time frame there, and again, based on our internal criteria at the time we came up

with about 300 hits of digital system failures that we think are important enough to look at.

The second item we looked at was a previous piece of work, and you can see the dates there. This was really completed a number of years ago, but was really -- had its own categorization scheme, and I'll talk about that in a minute, but it looked at over 5,000 LERs and came up with, again, about 446 digital related failures, and they were classified by whether hardware related software related, whether human factors interface to digital system related. They were broken down by vendor type, systems, subsystem type, and plant impact. So it was an interesting piece of work, but with that short time period, we could combine these first two bullets and, again, these are all internal work done in the Office of Research over a period of time.

It has been ongoing work. We're using it to build input, screen out which failures we think are important to get into the COMPSIS database, and also it has been used to influence direction on and thinking on D3. Mike Waterman I know has used the data extensively to calibrate his assessment of digital systems, and so that's the type of work that is.

Now, COMPSIS, Computer Systems Important to Safety, is an international effort. We're participating with nine other countries. So Germany is in there, Japan, Korea. There's a number of other countries that are going to be contributing to this database.

Now, where that's at, it's still in development. We are currently inputting LER failure data into that database. It's an ongoing effort and the other countries are in the same place we are. So that database has a detailed classification and inventory structure that was designed for data input, which is a little bit different than what Steve's talking about.

You can have one structure for data input because you need to have structure in order to get everything consistently binned in order to get any meaningful information out, but you may need additional tools, some of the things Steve was talking about in order to do a better analysis if what it's telling you.

The analysis piece of the COMPSIS database is not developed yet. It's still being developed, and so we have a chance to influence that through our work here.

The next bullet.

Kimberly talked about this earlier. EPRI has an ongoing effort which they're going to try to complete by the end of the month, and we're collaborating with them on that. We're sharing thinking. We shared data. We shared our data I was referring to previously. We shared that with them so that they could take that data and go an extra step and find perhaps more failure detail than we had on some of those events, and so that's an ongoing effort.

Additionally, the next item refers to we already had some research on emerging technologies, and as part of that we tasked Oak Ridge to help us go out and find sources of digital I&C fire information in the non-nuclear industry, and they recently gave us a report of that. You know, that report has a lot of information about failures, data sources, quite a bit, more than we could possibly look at in a month and maybe more than we could look at in a year.

But they did look at some. They looked at the aviation industry, telecommunications. They looked at one other one, aviation, telecommunications. What was the other one?

PARTICIPANT: Railroad.

MR. SYDNOR: Railroad, railroad industry.

PARTICIPANT: Department of Defense.

MR. SYDNOR: Petrochemical was another one they looked at.

And so they gave us some input there, but it was really more of an assessment of the quality of the data and we'll speak to that in a minute.

And the last thing we've looked at, we have looked at some NASA data. Steve was referring to that earlier. I don't know if there's anything you wanted to add on that bullet.

Additionally, the work we were doing with Oak Ridge also we had some input from things that NASA had done.

So that's the nature. There's literally hundreds if not thousands of pieces of failure data out there. One thing I've learned in the last month is that everybody who does it bins it differently and has their own classification and inventory system. And so one thing I think COMPSIS is going to do for us is drive standardization of how you classify things on a system basis, how software is classified, and standardize how the failure data is entered, and then that will give us the opportunity to have better analysis of it when we use that data.

So that's the listing of things that we

were looking at on the short term.

Preliminary findings, the one thing that's troublesome is the availability of quality data is limited. By that I mean it's easy to find events, very hard to find additional detail, especially really true root cause analysis. That's the second bullet there.

Even in the LER databases because of the summary nature of some of that reporting you don't get all of the causal data that would help you bin the failure down to, you know, what type of software failure was it. What type of subsystem was involved? Sometimes that is not readily available. So it makes it very hard to analyze.

The one thing that we did conclude in looking at all of this, and this was independently. I had three to four people working and looking at different pieces of this, is that the one thing that's common, and it's not in the nuclear industry, is that common mode failures, common cause failures are credible.

And the other thing we learned is that it's not just the nuclear industry that's using diverse systems to mitigate that. You know, we had certainly the example that NASA shared with us, and we

also have some other examples from other industries like the railroad industry where they don't rely on digital systems for critical safety protection features.

The other thing we wanted to say to the ACRS is that the ongoing NRC programs, they have a very extensive operating experience which you're well aware of, and it's very valuable to collect and analyze and distribute information. We get very on time reporting of digital failure events in the industry. We're on top of them as soon as they happen, as soon as they're reported within a day or days of the event. So it's an excellent system, and it's very helpful to us.

So our preliminary conclusion is that on the basis of the assessment we've done over the last month looking at all of these various sources of failure information, digital systems, is that we didn't find anything that really advised us or advised us of a course correction that the D3 PWG would need to make. The interim staff guidances there are on track, and that was really the key purpose of the short-term assessment. Do we need to change direction? Is there one of those guidances that needs some adjustment?

An answer to that at this point is no, and we'll be formalizing what we did and going through some review on that. This is a status report at this point in time, but that's a preliminary conclusion.

MR. JUNG: Okay. Thank you.

Any questions before I go to future plans?

Okay. Wes.

MR. BOWERS: Wes Bowers from Exelon.

The one thing I didn't see in your list here is the EPICS data from INPO. Are you using that?

MR. SYDNOR: Yes. The EPRI effort is using that.

MR. BOWERS: Because there's a tremendous amount of failure data out there that's not in LERs. LERs are just a really, really small subset of everything.

MR. SYDNOR: We have used that database when we can't find enough information in LERs. We have interrogated that database. Our operating experience, folks here at the NRC also use that.

MR. BOWERS: Okay. Are you using any of the CAP data, corrective action program data, from the individual utilities? Because that would also be a very valuable source for you.

MR. SYDNOR: It could be. I don't have

access to that right now. I know EPRI is looking, at under the NEI effort, is looking at tapping into some of that type of information to get further causal information because as you know, some of the causal details in LERs and even in the INPO database is not always that --

MEMBER MAYNARD: I would think that would have to be something that the industry would have to do and provide because basically the corrective action data is available to the NRC to look at, but that's not something that's submitted. I think if that's to be used, I would think the industry would need to put that together.

MR. JUNG: That's correct. I attest that that data right now is limited. So, I mean, we have to work with the industry counterpart to get the data if we want to.

MEMBER MAYNARD: The CAP data, corrective action programs, at the various utilities evolve.

CHAIRMAN APOSTOLAKIS: The EPRI effort is ongoing and will finish when?

MS. KEITHLINE: This is Kimberly Keithline.

They've got a near-term effort to finish and issue a white paper hopefully this month

summarizing their key findings. They do have plans for additional more detailed work, and I don't think they developed a time frame for that yet.

CHAIRMAN APOSTOLAKIS: And this report this month would be shared with us?

MS. KEITHLINE: Yes. EPRI is though discussing with INPO how much has to be sanitized out, you know, what level of detail can stay in because most of the information has come from INPO databases. So all of the detail can't be shared. So we have to find the right balance of providing sufficient information without -- bare details we just can't share.

CHAIRMAN APOSTOLAKIS: If you take the names of the facilities out.

MS. KEITHLINE: Yeah, yeah.

MEMBER MAYNARD: But that can't be tied to a specific plant or --

MS. KEITHLINE: Right, right. So we've got to clean it up that way and get permission, but the intent is to share it with you.

MR. ARNDT: We're slowly getting better at that. We're going through that with the international database as well. I want to point out that as you mentioned earlier, there's a number of other input

sources that we're using, including the reliability database that was developed last year. We're working with some of the vendors to get access to their proprietary development databases. So the issue associated with how good the data is and how do you integrate it and how hard it is to get at the details is something that's a real challenge, but we'll try to pull all of the strings that we can.

CHAIRMAN APOSTOLAKIS: Okay.

MR. ARNDT: Thank you.

MR. WATERMAN: If I may, this is Mike Waterman, Research.

With regard to using the data to develop diversity strategies, it's not so important -- I don't believe it's so important to actually have quantified numbers of how many failures were due to bad V&V, how many were due to specification. Rather, from a qualitative perspective if we see, for example, that there haven't been a lot of common cause failures due to signal, that tells us that any diversity strategies out there that are hinged on signal probably aren't very good. So we can sort of screen out those aspects of the diversity strategy that just haven't exhibited a lot of failures in industry.

And by "a lot" I mean, well, you know, not

a specific number, but relative to everything else, we find that, for example, a large number of failures that have occurred have been because of translating specifications into requirements. Perhaps that suggests that a good diversity strategy would have something in there with diverse requirements off of the same specification.

So an important aspect of that failure data is to identify not only what is important, but what we can screen out as not important.

MR. ARNDT: And that kind of thing is what we were talking about earlier about providing insights into the requirements and the ISGs.

CHAIRMAN APOSTOLAKIS: Okay, Ian.

MR. JUNG: Thank you.

So I think the two large bullets there, the ACRS Committee , we will see the outputs coming out by the end of this month. We'll have preliminary results of the assessment to influence ISGs. So with some of the insights and some of the conclusions you'll see the report.

In the next three months or so what we'll do is it will come to the D3 working group, and we'll have a dialogue with industry and also NRO/NRR line organizations to see where we are and develop, plan as

we read the recommendations and conclusions that what we need to do and feed recommendations to the research or industry or working group and what's the best way to capture these elements.

The eventual goal is to come up with the guidance document that will help the industry and the NRC staff in evaluating our future applications, and more importantly, the big picture and prevent the future significant events down the road.

And you know, beyond that, once the recommendations are made, obviously individual organizations will put that into their plan, research plan, for example, and the NRR/NRO. They'll have to look at, you know, how they're going to capture those things as we go.

So development of these activities is a probably good future topic for ACRS interaction in the future.

CHAIRMAN APOSTOLAKIS: Good. Thanks.

Other questions or comments around the table? No?

Thank you, gentlemen.

We continue with the cyber security presentation. It doesn't say who is going to make it.

MR. GARERI: Mario Gareri from NSER. I'm

the TWG for cyber security lead.

This morning Kimberly gave a presentation on this, and she covered most, if not all that I'm going to be covering in the slides. So if at any point you feel I need to move on a little faster, feel free to tell me

CHAIRMAN APOSTOLAKIS: Move fast.

MR. GARERI: Okay. What I plan on doing is just covering most of the background, which is why we're at the point where we are as far as industry needing clarification on cyber security guidance. Then I'll go through the ISG itself and the status of where we are and the path forward.

Before I touch on the first bullet, I guess it's important for everyone to know that cyber security is fairly new to the industry here, and pretty much post 9/11 is when the requirements came out as far as the NRC issuing orders. And then industry guidance was developed and in parallel the NRC updated the Reg. Guide 1152 to Rev. 2 so that it would incorporate and actually include cyber security.

So since it is fairly new, the industry has come to the NRC right now and actually asked us to provide some additional clarification of this guidance, and as you can see on the second bullet, the

specific clarification they're looking for is as it relates to Reg. Guide 1152, which was revised to have cyber security to address safety systems.

And the current cyber security guidance that's being used by industry is NEI 04-04, Rev. 1, which was accepted by the NRC.

So the TWG -- we'll go to the next slide -- the specific problem statement you can see there. It's one problem statement. We don't have multiple problem statements as the other groups, and it's pretty straightforward. Basically the industry is looking to use 04-04 in replacement of the reg. guide because they feel that having both -- I'm sorry --

MR. MORRIS: I didn't know if you need my moral support.

MR. GARERI: If you want to stay here in case I say the wrong thing, that's fine.

You have two targets now. So it's much better.

So what I was saying -- did you want to? Scott Morris.

MR. MORRIS: Yeah, I'm Scott Morris, Deputy Director of Security Policy in NSER. Mario works for me, and I'm also on the Digital I&C Steering Committee.

MR. GARERI: Okay. So as I was saying, the problem statement is pretty straightforward. Industry is looking to use 04-04 in lieu of the reg. guide, and what the goal of the TWG is to provide the additional clarification on the cyber security guidance as a whole, but we're looking at the reg. guide and 04-04 and seeing whether there are gaps or inconsistencies.

So what the TWG did is we developed a gap analysis, which is that other bullet there, and I'll go into more details there, to see what the inconsistencies were or the overlaps that the industry was talking about or that they had concern about.

From the first bullet, you can see after we did the gap analysis after many interactions with industry, we basically found some overlap in the guidance, but we did not find any inconsistencies or conflicts between the two documents, and actually they were complementary to each other, and the reason for that is because they serve different purposes.

You know, Reg. Guide 1152 was intended for safety systems and as far as licensing is concerned, and NEI 04-04, Rev. 1 was really an entire cyber security program that was going to be put in place for industry current operating plants.

So although there was some overlap, there was really no inconsistency because, again, the two documents serve different purposes. So what we did at that point is we went through the gap analysis with industry, and there was a consensus there on what the gaps were and the overlaps.

At that point industry committed. Again, we had met actually our TWG goal at this point to demonstrate that there's no inconsistency. We could have ended at that point, but industry had an interest in updating NEI 04-04, Rev. 1 so that they could actually capture or incorporate what's in the reg. guide so that the industry could use one guidance document rather than using both when they have submittals or are dealing with safety systems.

So the TWG staff agreed to just go along with that and actually see because it would help out industry to use one document rather than using the two.

So next slide.

One of the things that will happen is that we told industry that basically they would have to update the NEI 04-04 based on our comments, and there were some comments that the industry went back and forth with the staff, and at this point the reg. guide

has been updated to the point where we feel it captures most, if not all, of what's inside the reg. guide as far as safety systems.

MR. MORRIS: You mean the NEI document.

MR. GARERI: The NEI document, Rev. 2, which, you know, has not been submitted yet for approval to the NRC.

And, again, the NRC has to receive the NEI 04-04, Rev. 2 document still to get a formal acceptance, but at this point it's a working document and we thought we were actually pretty much completed and we were going to get ready to issue the ISG because we had addressed, again, the problem statement and even some more.

But then NRR and NRO had some concerns as far as industry or actually the reviewers using this document, using NEI 04-04, Rev. 2 for license and submittals.

So what the industry agreed on is to provide a correlation table, to actually show where the elements of the reg. guide are, 2.1 through 2.9, requirements from the reg. guide or regulatory positions, I should say, are actually captured and found inside NEI 04-04, Rev. 2, because it would be very difficult for reviewers and industry as well to

dig through that new document being that it wasn't really intended for that purpose.

So we go to the next slide, which brings us to the ISG itself. The ISG will basically clarify, in general, cyber security as it applies to, you know, safety systems. But the main point is how will NEI 04-04, Rev. 2 be used in lieu of, which is what the industry is interested in, of Reg. Guide 1152, Rev. 2.

And what we're going to do is the ISG will actually include the correlation table once we come to a consensus so that that table can be used by reviewers and industry to have a better idea when doing licensing or, you know, just to facilitate the licensing process.

Again, the correlation table was not an absolutely necessary thing to be done, but it will just help out in the licensing process, and we felt that it was important for additional clarification to be provided to industry and the reviewers.

So what we're working with right now is getting that correlation table to the point where there's consensus between the staff and the industry so that we can revise the ISG that's on the Website, which is already being revised as we speak here, to incorporate that table, which I might add also the

table itself will be 2.390 information. So it will be withheld from the public even though the ISG itself, the body will be publicly available because NEI 04-04 is sensitive security information.

And at the point that we're at right now is we're just trying to come to a consensus with the industry, and you know, we're going back and forth. We're about to provide comments back to industry, and I'll cover that on my next slide, but the next thing that would have to happen is once there is consensus, the last bullet there says that the ISG will indicate clearly that Reg. Guide 1152, Rev. 2 needs to be used until 04-04, Rev. 2 is officially accepted by the NRC because it will have to be submitted separately. It's not a question of the TWG accepting the document. That has to go through a different process.

Where we are right now is we had a meeting this past Monday, and again, we went back and forth. It was a good exchange, but there's some work to still be done on getting that correlation table where the staff agrees with industry.

So we're in the process of revising the ISG, incorporating the correlation table and then what we're going to do is we're basically going to send that correlation table and the ISG to industry, wait

for their comments, and the idea is that by the end of October we'll hopefully have, you know, an ISG that's acceptable to both the NRC staff and the industry.

Path forward. If you have any questions, just interrupt. The path forward is basically to complete the review of the most recent cross-correlation table, as I said earlier on the other slide, and incorporate into the ISG, send that off to industry.

Then we wait for their comments after they review it, finalize the ISG with the industry comments being considered obviously, and then we just have to wait for NEI to submit Rev. 2 of NEI 04-04 for them to actually be able to use that document in lieu of the reg. guide.

And that's pretty much where we are with that. If you have any questions.

MEMBER ABDEL-KHALIK: Are there any incidents that could be viewed as violations of cyber security?

MR. GARERI: I'm not sure I understand.

MEMBER ABDEL-KHALIK: Prior incidents.

MR. GARERI: I don't -- well --

MR. MORRIS: By prior incident, you mean? I'm struggling with the question, too.

MEMBER ABDEL-KHALIK: I'm trying to see how you come up with guidance. How would you verify that guidance?

MR. GARERI: Okay. Let me add maybe one more thing and maybe it will help you with the question. Again, and, Scott, jump in at any time.

I think I mentioned that earlier when I commented at the microphone there is additional guidance being developed by the agency to support the proposed rule on cyber security, and those are the things that we're actually looking at. The scope of this task working group was not to address cyber security. It was just to address this specific problem statement.

So to answer your question, we are looking into that, and it will be addressed by the guidance that will be available to support the rule. Until -- go ahead, Scott, if you want to add anything to that.

MR. MORRIS: I mean, I'm not exactly sure of your question. I will say that the scope of NRC requirements that are in play right now are very limited. They are in and reside in post 9/11 orders that we issue, not in regulations, other than to say the design basis threat rule, which just was updated and finalized in April of this year, which adds an

external cyber attack as an element of that, is one of the adversary characteristics that licensees have to be able to defend against with high assurance.

The scope of inspection work that we've done to validate what the licensee community has done in this area has been very limited for a variety of reasons, not the least of which is the skill sets that we have in this agency are limited to just a few folks, and that's another issue we're trying to resolve.

So we're building an inspection program. At the same time we're codifying the orders that we issued into regulations, which is part of a very large Part 73.55 rulemaking that we're in the midst of and for which regulatory guidance that Mario just referred to is being developed.

And, again, this as far as operating experience or events that occurred out there, I am not aware of anything at this point, including, you know, you've heard references to the Davis Besse event a few years ago and perhaps this information notice that was issued on Browns Ferry about a year ago. There is no compliance issue associated with any regulatory requirement, either an order or regs. associated with either of those, and they didn't resolve that any

safety related equipment being compromised.

So I don't know if that scratches your itch or not, but --

MEMBER ABDEL-KHALIK: The bottom line, you know, you'll come up with some guidance, and I'm just trying to figure out where that guidance -- how one would go about verifying that that guidance is adequate.

MR. MORRIS: If you're talking about safety related systems, and again, the scope of the working group that Mario is talking to is a safety related digital I&C systems only. That's all we're talking about in the context of the TWG.

The rulemaking that we're doing is much broader than that. It's not only safety related equipment, but it's also systems that affect site security and emergency response.

With respect to the safety related piece, we built in conjunction with NRR at the time, Reg. Guide 1.152 and added a separate section to that, it's Positions 2.1 through 2.9, which gives a life cycle approach guidance to designers and to our review staff on what the things that we expect be in place for anybody who proposes to use a digital I&C system in a safety related application.

That is the metric. Those are the metrics that we'll use to decide whether or not or what a licensee or applicant proposes is acceptable or not in licensing space.

In inspection space after the licensing work has been done, again, I think we're still working on our oversight program.

MR. GARERI: We're putting together an inspection number site program, including the training program for the inspectors. There's a lot of work being done in that area. We're just not there yet.

MR. MORRIS: When it comes to the licensing, once the new rule gets published, it encompasses a broader spectrum of systems, again, safety systems, security systems and emergency response systems. The licensing work will be a little bit different because it will be more of a programmatic -- the new requirements in the proposed rule are performance based, risk informed, more programmatic in nature.

In other words, something more analogous to what NEI 04-04 provides. So the scope of our review in the context of that rule will be sort of broad. We'll be looking for different programmatic elements as opposed to down in the weeds. What is

this new digital system? Where do the wires go and how do they connect?

I doubt we'll ever get to that level at least under the 73.55 rule. Now, with respect to the safety related systems that are being put in place that our NRR and NRO folks are going to look at, that's precisely what Reg. Guide 1.152 was supposed to do. The industry doesn't want to have to deal with two different documents. So they said, "Well, we'll just use NEI 04-04."

And we said, "Well, show us where in there we can find all of that technical minutiae that we need so that we can write a safety evaluation that you can stand on."

And that's the whole point of the technical working group, is to be able to carve out of NEI 04-04 the things that the technical reviewers in NRR and NRO need to have to pass judgment on.

MEMBER ABDEL-KHALIK: That's fine. Thank you.

CHAIRMAN APOSTOLAKIS: Okay. We can take a break until 2:35 and start a little earlier with the next presentation. Is that okay?

(Whereupon, the foregoing matter went off the record at 2:22 p.m. and went back on

the record at 2:36 p.m.)

CHAIRMAN APOSTOLAKIS: Okay. We are back in session.

The next presentation is on human factors, the next group of presentations actually.

MR. MARSHALL: Good afternoon. My name is Michael Marshall. I'm the manager for the Task Working Group on Human Factors.

We have two interim staff guidances we'd like to present today. The first one will be on computer based procedures. The second one is on minimum inventory, and we'd like to thank you for the opportunity to present our ISGs, and I'll go straight into the speakers.

Mike Boggi is our first speaker on computer-based procedures.

MR. BOGGI: Again, my name is Mike Boggi, and I'll be discussing the interim staff guidance regarding human factors and aspects of computer-based procedures.

I'll quickly tell you where we are or where we were, where we started from, and where we want to go.

The basis for the ISG. On March 1st, 2007, the NRC had a Category 2 public meeting with

members of the industry to discuss the human factors issues with highly integrated control rooms. Problem statements were presented and reviewed, and later it was agreed to go forward with an ISG regarding computer-based procedures.

The problem statement on the screen that you're seeing right now is the most recent version. The gist of the problem statement says that to address human factors aspects of computer based procedures and the soft controls used within the computer based procedures.

It goes on saying that multiple stakeholder meetings were held to discuss the interim staff guidance.

So the resolutions to the problem. In the short term obviously to prepare the interim staff guidance, the ISG is additional review guidance. We already have some guidance on computer-based procedures in NUREG 0700. The ISG goes one step farther and fills in some of the gaps that were not included in NUREG 0700.

A long-term deeper dive -- and I mean deeper dive as it relates. To date staff and industry agree that there are several issues that need to be addressed, and also deep dive meaning that we need to

do -- how shall I put it? -- more rigorous, proper research to develop this review guidance, meaning that the follow our research methodology and before we go and try to update NUREG 0700.

Again, this guidance is at the review guidance level, probably a level of detail or two more granular than you've heard most of the day, which is more of a higher level guidance. These are actually review criteria that the reviewer will take with them in reviewing computer-based procedures.

The purpose of a computer-based procedure, and I'm going to read this right out of 0700, is to guide the operators' actions in performing their tasks in order to increase the likelihood that the goals of the tasks are safety achieved.

One of the ways to do that is with automation. We think this is a really good definition, and automation in a computer-based procedure can perform several actions or procedure steps at the same time, reducing the likelihood or potential that the operator would make an error, the basis for that definition.

Anther of the principles that we used was to maintain the operator in control of the procedure system, and that will be a theme that you will hear

from me in my short period of time, that the operator is maintained in control of the procedure system.

CHAIRMAN APOSTOLAKIS: You could say this for anything though, right? the operator's actions, I mean.

MR. BOGGI: The reason I say that --

CHAIRMAN APOSTOLAKIS: Written procedures try to do the same thing, the written procedures from hard copy. They try to do the same thing, to guide the operators. So what is the extra advantage or purpose, I guess, of computer based? Was it just because we can do it we computerize them or there is a benefit?

MR. BOGGI: There are potential benefits, yes.

CHAIRMAN APOSTOLAKIS: So this statement from a year ago, 700, it's too general I think, and I hope in the NUREG itself "in order to" is not hyphenated.

(Laughter.)

MR. BOGGI: It may or may not be. I hyphenate.

CHAIRMAN APOSTOLAKIS: You cut and paste it, you know.

MR. BOGGI: I didn't cut and paste it.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BOGGI: That's my writing.

CHAIRMAN APOSTOLAKIS: But do you agree with me that this is really a general statement that would apply to any kind of procedure?

MR. BOGGI: Yes. Out of context, read just as it is, I agree it is possibly certainly too generic.

CHAIRMAN APOSTOLAKIS: Why are we computerizing it? Easy access?

MR. BOGGI: There are potential benefits to putting a procedure into a computer-based system. For instance, using technologies such as Web technology, a hyperlink, to click on hyperlink and call up charts or graphs --

CHAIRMAN APOSTOLAKIS: I see.

MR. BOGGI: -- or additional information that the operator would need while performing the procedure itself. It could be all right there, and then the next step might be the technology such as automation, where once the operator tells the system to go, it could perform two or three or four procedure steps, like starting a pump I use as an example. The control system can open the suction valve, insure that there's minimum flow, that there is one resultant, and

then start the pump, and at the same time present information to the operator that the pump amps, starting amps, have gone up, the flow, or whatever the parameters are being or can be displayed to the operator at the same time.

So that is simplifying the operator's tasks, at the same time doing a job and presenting all of the information that the operator needs to do his job.

CHAIRMAN APOSTOLAKIS: The choice of the procedure is still up to the humans, right?

MR. BOGGI: The choice is. We've said that specifically in the guidance.

CHAIRMAN APOSTOLAKIS: So do you propose to computerize that, too? Why did you feel that it was necessary to actually say that?

MR. BOGGI: We felt it was necessary to say that the operator should select the procedure because we're not certain that the diagnostic or that the computer can diagnose the event.

CHAIRMAN APOSTOLAKIS: I understand that, but did anybody propose to actually computerize that?

MR. BOGGI: Not that I've heard.

MEMBER ABDEL-KHALIK: How about checking the setpoints for switching between procedures?

MR. BOGGI: The computer-based system we're saying can prompt for the operator to enter a procedure or to go to a different procedure or that the entry conditions for the procedure are now satisfied and the operator can exit the procedure.

MEMBER ABDEL-KHALIK: But it would still be the operator's decision to override that, to go to another procedure --

MR. BOGGI: Definitely.

MEMBER ABDEL-KHALIK: -- if the setpoints for switching procedures have actually been satisfied?

MR. BOGGI: It would be the operator's prerogative to continue in the procedure or close the procedure as his indications are presented to him, as today, as it is today.

MEMBER MAYNARD: If I understand what you're saying, you may get to a step in the procedure where it would be time to go to another procedure.

MR. BOGGI: Right.

MEMBER MAYNARD: You don't want it to where the computer is going to automatically do that. It's probably going to bring up a prompt and the operator will select yes to go to the procedure or whatever.

MR. BOGGI: That is one acceptable way,

yes.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BOGGI: I want to fill in a point regarding automation. A computer-based procedure system could literally have zero automation where it's just something like a PDX displayed on the screen, or it could have intermediate levels of automation that we talked about, hyperlinks and low level automation, or more full levels of automation, such as I just mentioned regarding providing different control functions.

The interim staff guidance is, again, review guidance and it is review guidance for procedure systems, as well as the procedures themselves.

The staff rationale for the interim staff guidance is the content and development of a paper-based and computer-based procedure can essentially be the same. Both can and should be easy to use. The difference is, as one example, automation possible with computer-based procedures should not limit the control -- again, the word "control" -- operator control, nor the operator situation awareness, what's going on with the procedure.

Examples of how to keep the operator in

control is found in the review guidance for automation. This is found in the ISG numbers eight through 12. Automation should not select nor initiate the procedure to be used. We just talked about that, operators in control.

Computer-based procedures should not initiate control actions without first receiving a command from the operator to do so. The operator is in control. The computer-based procedures systems did not change the procedure. Like, for instance, a dynamic procedure, plant conditions change. Oh, I've got to do something different. It can prompt you to go to another procedure, but it can't dynamically change an approved procedure, and no one is recommending we do that either.

A hold point should be established to effectively monitor automation progress. Hold points are one of the things we need to talk about in the longer term guidance. Hold points are different than an interrupt. In an interrupt, the operator can interrupt a procedure at any time. We're writing that in, but a hold point is something that happens, is programmed into the computer. For instance, if there's a caution or a warning in the procedure, the automation should stop, cautions or warnings meaning

that there's some potential danger to plant equipment or harm, potential harm, to plant personnel, certainly a case where you would want to have a human decide whether to take that action or not.

Another example, procedure steps that require the operator to make a decision when a peer check is used or when actions taken at the next step could impact compliance with plant tech specs, technical specifications.

Review criteria examples regarding soft controls, soft controls being any control that is on the computer screen as opposed to a hand switch or push button that's on a typical control panel.

CHAIRMAN APOSTOLAKIS: If you touch it.

MR. BOGGI: Touch it, use a mouse.

The computer-based procedure system should contain a concise set of soft controls whose meaning is obvious to the users. Soft control display properties should not violate stereotypes of hard nor soft controls already in place in the main control room, and that was written mainly for a modernization project where they're going to back the computer-based procedure system into an existing control room.

And the control of plant equipment should take at least two discrete control actions, and you've

heard that already today from Paul Rebstock in his presentation.

So in conclusion, we feel that the MCF guidance is a good interim measure. There was a lot of good, cooperative work with industry. Industry stakeholders were actively involved in the process, but long term what it's going to take is an update to NUREG 0700.

MEMBER ABDEL-KHALIK: The third criterion on your list which says the control of plant equipment should take at least two discrete actions, what if that falls into the procedure? The procedure doesn't do that. The procedure, just -- you know, this is no different than paper procedures.

MR. BOGGI: I won't argue that point, that they're very, very similar. What we're saying regarding a computer-based procedure, we can postulate that there might be a hyperlink or let's call it a hot spot in the procedure where you click to start a pump, and you click on that. It opens up a control window that has the pump control and whatever functions opens two valves to start the pump would be contained in that dialogue box, that window, and so you would then be able to start that control action.

So it wouldn't just be that one action of

clicking that hyperlink or that hot spot to start that piece of equipment.

MR. MARSHALL: This goes back to an earlier question. What's the difference between paper and computers? Well, with the computer-based procedures, there's two areas that might be different because one is automation, which we've talked about, and two is imbedding soft controls directly into the procedure.

MEMBER ABDEL-KHALIK: Thank you. I understand.

CHAIRMAN APOSTOLAKIS: Any other comments, questions?

All right. Let's move on.

MR. MARSHALL: The next presenter will be Jay Persensky, and he'll be making a presentation on an interim staff guidance on minimum inventory.

MR. PERSENSKY: And the Chairman has asked that I try to speed this up. So I think we're only going to use Slides 3, 4 and 6. How's that?

CHAIRMAN APOSTOLAKIS: Oh, boy.

(Laughter.)

MR. PERSENSKY: And I'm probably going to even ignore them, but in any event.

(Laughter.)

MR. PERSENSKY: I'll just ask are there any questions.

No, the one thing I want to point out to start off with is that minimum inventory at this point, we're only looking at applications for new reactors. This is not something at this point that we'd be looking at for upgrades to current reactor control rooms, even though something like computerized procedures we could see. It's all the basis really of minimum inventory in this context, is we're talking about the controls, displays, and alarms that are necessary to implement your EOPs, to bring the plant to a safe condition, and to exercise those operator actions that the PRA has shown to be important to safety. So these are the controls, displays and alarms you need to do those things.

The reason this came about, and this was done at the first new reactor design certification, which was the ABWR back in '92, was, gee, we don't have a fully control room design. So the staff had no basis to go in and do an entire review of the control room design. So we felt that there had to be something that the vendor would commit to that would be in that control room, and we've also expanded this a little bit to include the remote shutdown panel,

which may be two different kinds of things that would be available.

So the real basis for this is the fact that at the design cert. stage we do not have a full control room design.

Also we've talked about D3. We've talked about communications. There are some elements in there that we're not sure. Okay. What things need to be there all the time? What things need to be spatially dedicated? What things need to be accessible through one step versus or are only there at all times?

So there are a lot of questions that are still facing the staff as well as the vendor at the design certification. So the staff came up with this concept, which was approved by the Commission, for actually the four currently certified designs, ABWR, CE System 80+, AP 600 and AP 1000, where the vendor actually came in: this is the particular list of displays, controls and alarms that we're going to have in our plant as a minimum. We may have a lot more once we get a design, but this is what we're going to have so that you can do these things.

One of the things that the industry came into and when we were looking at this problem was

that, in fact, even having that list may be a problem. The preferred method would be to have some sort of process not unlike what you were talking about earlier with 1852, that there would be a process to make some of these decisions.

So they proposed a process in their white paper. We've reviewed that. We've also looked at where we have been in the past. In the past, the list was in Tier 1 information for the new reactor licensing. You can't change that without a rule change. Once it's in Tier 1, it's stuck.

We also talked about Tier 2 information. Tier 2 information is something the licensee can change following a 5059 process. So we would only look at it in a later stage.

There's another thing that came up called Tier 2-star, which would require a licensee if they wanted to make a change to this list, which we kind of expect they may, that they'd have to go through a process where we would have to approve that Tier 2-star information.

Basically what we've done, if you got to -- well, I said I'd do four. Four is our short term, which we would come up with the ISG, again, just for new reactors. The long term would be to get into

conventional reactors that are upgrading their control room, as well as get into some of these definitions that we still haven't locked in, like what things need to be continuously visible and what can be done or approached with a one-step process to get to it.

The purpose is what I've talked about, but the guidance that we put out, and here are a couple of examples of the guidance elements, is basically a two-step process.

One, you have to, in fact, define their process. How is it that they're going to select a minimum inventory? And they have to apply that process to at least a set of these alarms, controls and displays so that we would have that list in Tier 2, which means staff can have another review of it later on because we do expect that there's likely to be some changes, especially some additions to it.

MR. MARSHALL: Tier 2-star.

MR. PERSENSKY: Tier 2-star. I'm sorry.

And the second step is to have a verification program. How are they going to verify it using their verification process? And also they have to include information in their ITAAC so that whatever they use for verification in the ITAAC and the information would also be available to us and the

inspectors for going in and checking on whether or not the verification has been done to our satisfaction.

Again, there's a couple of examples, like it has to meet the Deep 3 evaluation. They have to consider credit of operator actions for the process, the minimum inventory. Some examples of minimum inventory, and I have the list from this happens to be AP 1000, are things like the containment pressure, alarm and display made of containment isolation as a control and with the verification process. We want to make sure it's compared to their risk significant actions, and that they've done a real test of this on full scope.

And we use the term ANS 3.2 because the ANS 3.2 is the standard that we use to evaluate simulators, but right now that standard is focused primarily on training and examinations. It is probably the closest thing the operator will ever get to the plant without actually trying some of these things out on the plant.

CHAIRMAN APOSTOLAKIS: With respect to the risk significance, you also say in Slide 5 that the purpose of the minimum inventory is to assure that the operators will carry out those actions shown to be important from the applicant's PRA.

MR. PERSENSKY: That they would have the information necessary to carry out those actions.

CHAIRMAN APOSTOLAKIS: It seems to me that they should be able to carry out all actions, not just the risk significant actions. I mean the risk significance may help you to focus on those during the simulation exercises and so on, but don't you think that all actions should be performed correctly?

MR. PERSENSKY: Again, yes, all actions should be carried out correctly, but the focus here was to make sure that they had the alarms, controls and displays that are necessary to at least meet these three.

CHAIRMAN APOSTOLAKIS: At least.

MR. PERSENSKY: At least.

CHAIRMAN APOSTOLAKIS: Yeah, so those words should be there somewhere because, you know, we are not going to start focusing only on what's risk significant. I mean, risk significance has a role to play in certain things, but it's not a universal principle.

MEMBER MAYNARD: Well, are these alarms, controls and displays a minimum list that must be in the control room or that must be available someplace?

MR. PERSENSKY: They have to be in the

control room. There are two sets of minimum inventory we talk about here in the ISG. One is for minimum inventory in the control room, and there's also minimum inventory which is probably a smaller set for the rim-out shutdown panel because the function of the rim-out shutdown panel is basically to shut the reactor down, and that's if they have to leave the control room.

They have to be in the control room. Many of them, the way they've been designing them that we've seen is they're actually on a separate control station with the safety related controls. All of those decisions with regard to what needs to be on a separate control panel, safety related and all of that, would be part of the D3 communications ISGs as well.

So we do have a linkage there with the other --

MEMBER MAYNARD: Because there are a number of actions that can be carried out by telling an operator in another building to start a POP or something. So there's a difference between controls that you have to have someplace and the controls you really have to have inside the control room.

MR. PERSENSKY: Well, the displays and

alarms are going to be in the control room. Most of these things that we talk about as far as minimum inventory are in the control room, but there's a possibility that there could be other controls outside of the control room.

MR. MARSHALL: As Jay mentioned earlier, the minimum inventory is what we're reviewing during the design certification in lieu of reviewing the entire complete control room design. So the focus for the minimum inventory is what's in the control room.

MEMBER ABDEL-KHALIK: So presumably this verification step includes sort of a cross-check against the EOPs and the normal operating procedures.

MR. PERSENSKY: Right. They would have to use the -- you know, when they get to the verification stage we're talking now about a completed design. They would be using their EOPs. They would be using the normal procedures, everything that they have in order to verify that everything is working properly. It's in there and working properly.

Now, there's a set. If you look at the ISG itself, there's like eight, five, you know, seven or eight criteria for each one of these different aspects of the review. I didn't include all of them here for the sake of time.

CHAIRMAN APOSTOLAKIS: Any other questions?

MR. MILLER: Rich Miller from GE.

You indicated you wanted a minimum inventory in the control room on the RO shutdown panel. What if you had these, I guess, controls, alarms and displays integrated in the control room and the remote shutdown panel versus just being in one concentrated area so that the operators dealing with the components of the system as they relate to system interaction, et cetera, versus, I guess, distinct on a display? Are you restricting it to one specific display area?

MR. PERSENSKY: No.

MR. MILLER: Or it can be integrated?

MR. PERSENSKY: It can be in the control room. It can be integrated. One of the things, one of the other drivers for the minimum inventory originally was talking about 1992 there was still a good deal of fear with regard to the reliability of digital systems, and there was talk, well, what do we need if we had a back-up system or what's that back-up system?

So the thought at that point was to have a separate handle that was safety related and all of

that.

We're now talking that a lot of this is still to be decided in the white papers that they're going to be presenting, but we do want certain information and controls in the control room, and they can be integrated, but probably not necessarily in the primary interface for the operator.

So if there is a catastrophic common cause or whatever you want to call it, crash of the primary control system, the primary display system, that there be enough controls, displays and alarms to bring the plant and keep the plant at a safe state until the primary system is brought back up.

MEMBER ABDEL-KHALIK: Is there any concern about the opposite problem where you have too many indications?

MR. PERSENSKY: That concern is generally handled during the reviews, the 0700 reviews when you're looking at the whole control room. Again, this is before you get to that final stage of review.

In a typical human factors review right now for the design certification, the vendor commits to NUREG 0711, which is a human factors engineering review process. So they are committing to a process that they will follow in developing their entire

control room.

Once that gets to the point where we can review the control room or they can review the control room, then they would use NUREG 0700, which is the primarily interface review guidelines, and the whole control room would then be looked at.

Again, this is the subset that they have to have somewhere, and the other is that if the primary system, which is where you might have too much information, bites down in some way, they would still have this minimum inventory to rely upon.

CHAIRMAN APOSTOLAKIS: Other comments or questions?

Well, thank you very much.

MR. PERSENSKY: Thank you all.

CHAIRMAN APOSTOLAKIS: Now, we will have some discussion among the members. The first open question is whether we should ask the staff to come to the full Committee in October to brief the members on these issues. Obviously it would have to be a much shorter presentation, and to write a letter, which by the way, you know, can be praise what the staff is doing, can say we agree, can offer some comments. So let's talk about that first, then move on to specific comments that the members might have.

So Otto, do you want to start?

MEMBER MAYNARD: Well, as far as whether we should have them come to the meeting, I guess I don't have a strong opinion. I'd say that it would need to be a very short meeting. It would not need to go into this level of detail at all.

CHAIRMAN APOSTOLAKIS: Absolutely.

MEMBER MAYNARD: I think that the one advantage of having them come and present a little bit would just be to show that progress is being made because one of my concerns was are we still just planning or is something actually being done.

You know, something is actually being done.

CHAIRMAN APOSTOLAKIS: Exactly.

MEMBER MAYNARD: So it might be good from our standpoint to show that things are being issued and by the end of the year there's going to be more. So, again, I think short on that would be --

CHAIRMAN APOSTOLAKIS: Short would mean and hour, an hour and a half?

MEMBER MAYNARD: Yeah, I don't think much more than an hour. An hour and a half maybe to have the discussion time and stuff, but I don't think it would need to be --

CHAIRMAN APOSTOLAKIS: And that would be followed by a letter?

MEMBER MAYNARD: As far as a letter, I don't think that there's a need. We don't need to be changing direction. I think for me the purpose of a letter would be, if we write one, would be to say, you know, that we reviewed it and we see progress being made and maybe, you know, provide a compliment. To me anyway, it would seem to be a compliment to the staff and to the industry working together and making things happen here.

But I don't think there's a need for a letter to change direction.

CHAIRMAN APOSTOLAKIS: Absolutely.

MEMBER ABDEL-KHALIK: I think it would be important to have a presentation to the full Committee. Like Otto said, it doesn't have to be a very long presentation. Maybe limit it to an hour and a half or so.

And as far as the decision whether or not to write a letter, that's really a committee decision. After listening to the presentation at the full Committee meeting, then the Committee as a whole has to decide whether or not it is appropriate to write a letter.

CHAIRMAN APOSTOLAKIS: Okay. Mario.

MEMBER BONACA: Yeah, I think that we should have presentation to the full Committee. I think there has been significant progress. I must say that the information that came was valuable. There is full blown organized program of the six working groups. So we have to have a meeting, and one and a half hour I agree should be the most that we dedicate to that.

As far as a letter, the Committee will have to decide, but I think we can provide significant recommendations. I'm not sure that a letter is needed at this time. I mean, this is more like getting the Committee informed about significant progress in this area.

I must say that I did not expect this letter.

CHAIRMAN APOSTOLAKIS: All right. So, Belkys, you're welcome to come back.

MS. SOSA: We certainly will.

CHAIRMAN APOSTOLAKIS: And we will arrange for at most an hour and a half, I think.

MR. SHUKLA: I have a question on that. Would you also like to have industry come back for presentation?

CHAIRMAN APOSTOLAKIS: Up to them. Kimberly, would you like to come? John? Sorry. Jim.

PARTICIPANTS: Yes.

CHAIRMAN APOSTOLAKIS: Okay. So an hour and a half then is fine because we can have a few minutes with the industry and then the staff or the other way. It depends on how it's appropriate to do it.

All right. Then the decision on the letter will be deferred until the full Committee hears the presentations.

Now I'd like to have some comments on what we've heard and so on. Sergio, do you want to start?

MR. GUARRO: Well, sure.

CHAIRMAN APOSTOLAKIS: Well, if you're --

MR. GUARRO: I don't have anything major. I think this was very informative, and it sounds like most of the issues are being addressed in the interim and there are plans for longer term activities.

I just took down some notes here and am looking at them.

CHAIRMAN APOSTOLAKIS: Well, you will send me also something in writing.

MR. GUARRO: Yeah.

CHAIRMAN APOSTOLAKIS: But just tell us.

MR. GUARRO: Yeah, I think, you know, obviously this issue of the 30-minute rule has come up, probably is worthwhile trying to see if there is anything that can be done to help out in that area.

Let's see. With respect to that, again, I think I've made the comment when I was asking the question that perhaps one way to address that would be, you know, since we don't have a full understanding of the types of failure modes, but at least to look at some classification of the way the failures manifest themselves. So are they very easily diagnosed versus are they -- you know, they have characteristics that make them difficult to pinpoint. I think that's really the distinguishing element at least from my point of view.

Let's see. Well, you know, I think I had mentioned to you before informally that when we were looking at the issue of if there is a distinction between software common cause failures versus, you know, traditional hardware common cause failure. I think it's worthwhile digging into that a little more.

CHAIRMAN APOSTOLAKIS: You mean to compare what?

MR. GUARRO: Well, to compare the experience that we have in both areas. I think, you

know, I have observed in other applications that these other common cause failures have the characteristic typically of being perhaps triggered by design errors, and in other industries they are not so rare. So I'm concerned about defining those as low probability, but that may not apply in the nuclear area, but until one looks at the data, I don't think it's going to be clear.

And that's about it.

CHAIRMAN APOSTOLAKIS: Thank you.

Do you have any comments on the inventory and classification or you're pleased with what you heard?

MR. GUARRO: Well, it sounds the approach is reasonable. I don't have any.

CHAIRMAN APOSTOLAKIS: Fine, fine.

Mario.

MEMBER BONACA: You know, I thought as was mentioned before that there was significant progress. I think that the whole organization, the Steering Committee and the six main review areas are well divided and organized, I think. It's a significant effort.

On the diversity and defense-in-depth, I mean, the 30 minutes, I don't feel as strongly as you

have felt, but I agree with you that we should not be prescriptive. I mean, clearly, it shouldn't be that if you do not meet the 30-minute rule you have to have a back-up system necessarily. I mean an automatic system should be written with the flexibility that was meant during the presentation, and I think the message already was delivered there.

I think insofar as the operating experience, that's a great initiative, and again, I will reiterate the fact that some foreign countries have considered common cause failure as sponsor a design basis, and they have treated them in accident analysis and the whole design of the plant. It would be interesting to know if there is a history of failures, if there is a history of peculiar saturations, for example, and I don't know to what extent they can be, you know, identified, but I would expect that the international database that was presented should contain that kind of information.

When I look at the highly integrated control room communications, I get kind of scared about all of the human factors concerns, I mean, that seem to derive from that. I'm talking about new designs. There is a high level of complexity. We're going from control rooms today where everything is

wired practically.

And you know, you have mostly actuation systems and you have feedback systems and controls. You don't have generally digital I&C now. There has been some progress there, but not as much, and looking at what was presented, a totally different story.

But I trust that I think we'll have to see as we progress on this effort what kind of issues come up that need to be dealt with. It seems to me for the presentation that the staff has a full understanding of this issue to the extent possible. So, therefore, they are able to deal with them, but that's an area where I certainly have interest to follow in the future.

That's pretty much that.

CHAIRMAN APOSTOLAKIS: Said.

MEMBER ABDEL-KHALIK: I guess by the time the full Committee meets, the staff would have issued an assessment of major issues and common themes as far as the inventory and classification and, therefore, it would be a good idea to present some detail and specificity as to how this is being done.

The other thing is I would like to see a better justification for that 30 minute criterion, and the difference between what the staff called sort of

the HOV lane process and the more in depth evaluation.

CHAIRMAN APOSTOLAKIS: Belkys, do you think we will have that draft report? The meeting is on October 4th.

MS. SOSA: The report is toward the end of this month. So I would expect that --

CHAIRMAN APOSTOLAKIS: Will you send us a copy?

MS. SOSA: -- at the minimum you'll have a pretty good draft.

CHAIRMAN APOSTOLAKIS: And maybe you can address it in the presentation.

Otto?

MEMBER MAYNARD: I've already given my bottom line here. I do want to compliment the staff and the industry. A lot of work has been done and progress has been made, and we're kind of moved out of the just planning stage and actually doing some things. So I think that's very good and good interaction between the staff and the industry, I think, in this area.

I'm not going to beat up anymore on the 30 minutes. I think we've talked about that. So I won't take another 30 minutes for that.

(Laughter.)

MEMBER MAYNARD: I do notice there's a number of long-term items here that we don't really have goals and milestones for and at some point are going to have to transition and start putting things down for that, too, so that we can start making progress on the long term there.

And also, I think that we talked a little bit in the meeting. At some point we've got to transition from interim staff guidance to regulatory framework, reg. guides or whatever the appropriate mechanism.

So I think we need to make sure we don't just stay in an interim type regulatory process here.

The last item that I would find interesting and I think we need to address some time probably in our Safeguard and Security Subcommittee is on the cyber security items because we are kind of entering into a new area there. I'd be interested in that, but I think that would be better handled in one of those subcommittee meetings.

That's all I have.

CHAIRMAN APOSTOLAKIS: Thank you.

Well, my comments have really been covered already. I think the 30 minutes should be 29.

(Laughter.)

CHAIRMAN APOSTOLAKIS: Anyhow, I'll compromise.

So unless somebody has a comment, I'd like to thank --

MEMBER BONACA: I would like to voice, to repeat what others said regarding the interaction between the industry and the NRC. I think it is extremely valuable. I think that those perspectives are important. They bring about insights that are important to develop regulations. So that's very good.

CHAIRMAN APOSTOLAKIS: All right. Any other comments? Yes, sir.

MR. SHUKLA: Staff is very interested to present the progress of research project that's being done. I have sent an E-mail on that. Would you like to hear about those from the research --

CHAIRMAN APOSTOLAKIS: Like what?

MR. SHUKLA: To get the progress report on may Steve then will tell us.

CHAIRMAN APOSTOLAKIS: With what?

MR. ARNDT: What he's talking about is that some time later in this calendar year we had asked if the Subcommittee would be interested in an update on some of the research programs, like in late

October or November, and that would be the OSU work, the Brookhaven work --

CHAIRMAN APOSTOLAKIS: Oh, yeah, yeah, yeah.

MR. ARNDT: -- and that would be a separate Subcommittee meeting.

CHAIRMAN APOSTOLAKIS: Yeah, that's different. Yeah, this Subcommittee is always willing to meet.

I guess there are no other comments on anything. So I'd like to thank NEI and the staff for coming here and making good presentations and speaking with sufficient clarity.

MEMBER ABDEL-KHALIK: And volume.

CHAIRMAN APOSTOLAKIS: And volume.

And we will see you in whatever, two weeks, two and a half weeks or so. Okay? An hour and a half, but the hour and a half is not all yours.

Okay, and with this we adjourn.

(Whereupon, at 3:21 p.m., the subcommittee meeting was concluded.)

CERTIFICATE

This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission in the matter of:

Name of Proceeding: Advisory Committee on Reactor Safeguards Digital Instrumentation

Docket Number: n/a

Location: Rockville, MD

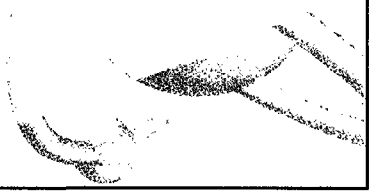
were held as herein appears, and that this is the original transcript thereof for the file of the United States Nuclear Regulatory Commission taken by me and, thereafter reduced to typewriting by me or under the direction of the court reporting company, and that the transcript is a true and accurate record of the foregoing proceedings.

Charles Morrison
Official Reporter
Neal R. Gross & Co., Inc.

Industry Perspective on Digital I&C Issues

September 13, 2007

NEI
NUCLEAR ENERGY INSTITUTE



Communications

- **Problem Statement:**
  - Need better guidance for inter-divisional communication
- **Milestones and Deliverables:**
  - Industry white paper
  - Interim Staff Guidance by 9/30/07
  - Revise IEEE 7-4.3.2, RG 1.152, and SRP

NEI

Diversity and Defense-in-Depth Problem Statements

- Adequate Diversity
- Manual Operator Actions
- ~~Credit for Leak Detection~~
- Clarifications to Point 4
- Effects of Common Cause Failures
- Common Cause Failure Applicability
- Echelons of Defense
- Common Cause Failure vs. Single Failure

NEI 3

Diversity and Defense-in-Depth Remaining Challenges

- Credit for manual operator actions
  - 30-minute criteria
  - Process vs. arbitrary time limit
- Use of risk insights
  - Consider risk vs. benefit
  - Potential to degrade safety

NEI 4

Human Factors
Problem Statements

- Minimum Inventory of Alarms, Controls, and Displays
- Computer-based Procedures
- Graded Approach to Human Factors
- Safety Parameter Display System

Human Factors
Milestones & Deliverables

- Industry Reports
- Interim Staff Guidance by 9/30/07
  - Minimum Inventory (MI)
  - Computer-based Procedures (CP)
- NRC Endorsement of MI and CP Reports
- Other Guidance, as appropriate

Human Factors Challenges

- Supporting accelerated schedule for ISGs
- Ensuring ISGs contain sufficient information
- Completing longer-term actions
  - Endorsement of EPRI reports
  - Resource constraints
  - Plans and schedule

Cyber Security

- Problem Statement:
  - RG 1.152 and NEI 04-04 have conflicting guidance
- Desired Outcome:
  - NRC will conclude that NEI 04-04, Rev 2 is an acceptable method for establishing and maintaining a cyber security program at nuclear power plants
  - NRC staff will accept the use of either RG 1.152 or NEI 04-04, Rev 2

Cyber Security

- Status
  - NEI submitted NEI 04-04, Rev. 2
  - NEI submitted draft cross-correlation table
  - Sept 10 meeting to discuss the draft table
- Path Forward
  - NRC staff provide comments on table
  - NEI modify table and NEI 04-04, if appropriate
  - NRC develop ISG

Other Activities

- Test ISGs on Licensee Submittals
  - Considering pilot(s)
  - Further refine ISGs, as appropriate
- Review Operating Experience Data
  - Obtain insights on failure modes
  - 300+ events (NRC and INPO databases)
  - Sharing information with NRC staff
  - Issue white paper this month

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

Presentation to the ACRS Subcommittee on Instrumentation and Controls (I&C)

September 13, 2007

Belkys Sosa
Director, Digital I&C Task Working Groups

Agenda

- **Digital I&C Steering Committee Activities**
- **Industry Perspective**
- **Interim Staff Guidance**
  - Highly-Integrated Control Rooms: Communications Issues
  - Diversity and Defense-in-Depth (D3)
    - Inventory and Classification System
    - Evaluation of Operating Experience
  - Cyber Security
  - Highly-Integrated Control Rooms - Human Factors:
    - Computer-Based Procedures
    - Minimum Inventory

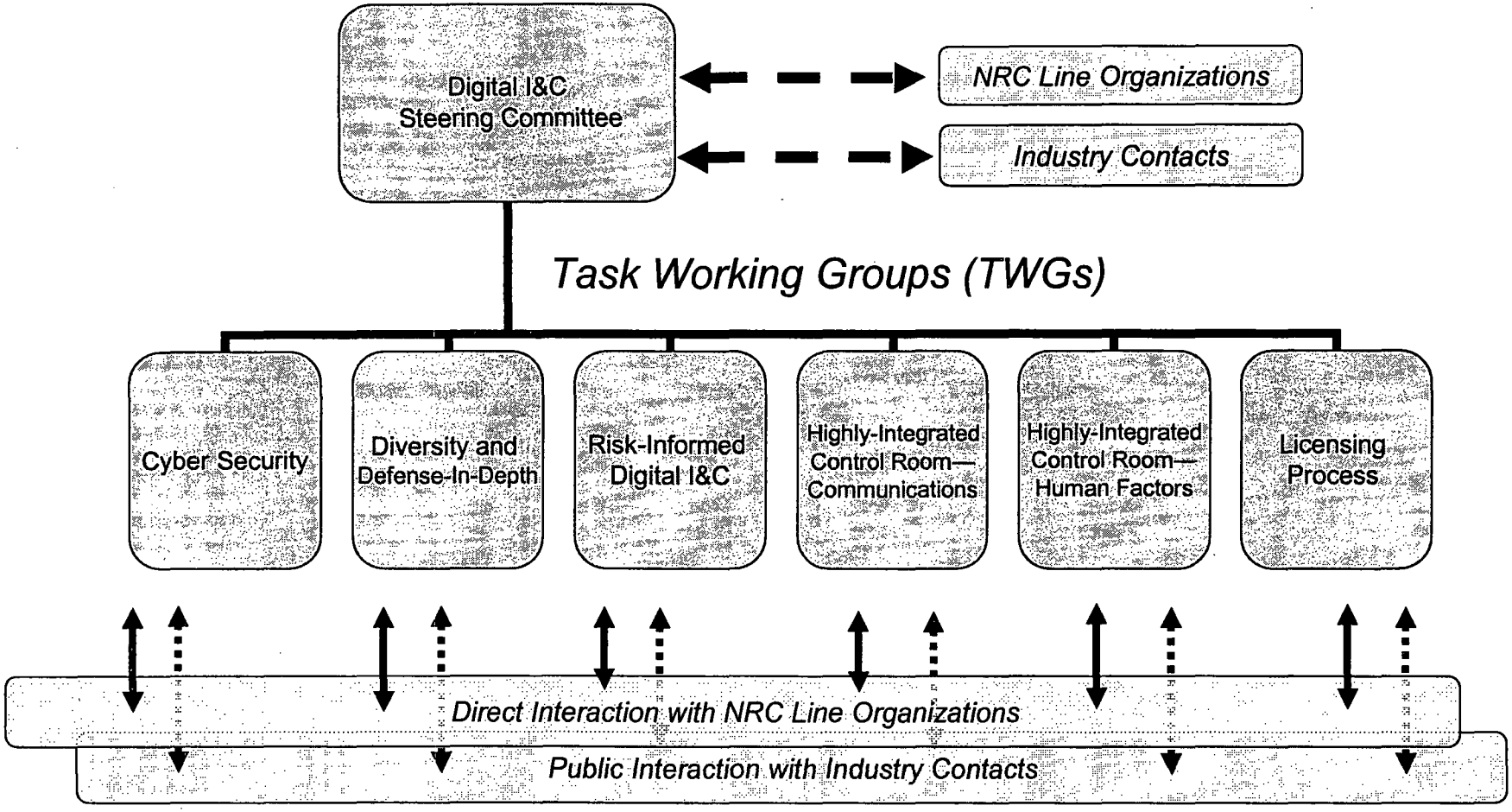
Background

- November 8, 2006, Commission briefing
- December 6, 2006, Staff Requirements Memorandum
- January 12, 2007, memorandum established the Digital I&C Steering Committee
- May 2007, Staff presentation to ACRS
- June 22 2007, Staff Requirements Memorandum following ACRS Commission briefing on June 7, 2007
- July 18, 2007, Commission briefing

Key Challenges

- Assuring predictability through refined Regulatory Guidance
- Anticipating future needs
  - Evolving technology
  - Industry priorities
- Improving stakeholder interactions
- Expanding national and international interactions

Steering Committee



Structure of Project Plan

- Defined problem statements under each Task Working Group
- Developing Interim Staff Guidance (near-term)
- Interactive effort with industry
- Revise Regulatory Guides and industry standards (long-term)

Summary

- Steering committee is functioning effectively
- Project plan is in place
- Interim Staff Guidance is being developed
- Stakeholder interactions
- Strong industry support
- Staff is on-schedule to complete near-term deliverables

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Interim Staff Guidance for Digital I&C

Highly-Integrated Control Rooms: Communications Issues (HICRc)

A Presentation to the ACRS Subcommittee on Instrumentation and Controls

Bill Kemper, HICRc management lead
Paul Rebstock, HICRc technical lead

September 13, 2007

HICRc Task Working Group

- Initial public meeting February 23, 2007
- NRC members from RES, NRR, NRO, NMSS
- Industry & NEI contacts
- 10 public meetings since inception

  Objectives:

  - Understand industry needs
  - Gain technical insight
  - Ensure guidance addresses appropriate design issues

HICRc Problem Statement

From the DI&C Project Plan for HICRc

"Industry and NRC guidance documents do not define at a sufficient level of detail the requirements for inter-divisional communications independence."

- IEEE 7-4.3.2-2003, concerning Digital Computers in nuclear safety systems, does not provide sufficient guidance for inter- divisional communications independence within digital systems.
- Regulatory Guide 1.152, concerning Digital Computers in nuclear safety systems, does not provide explicit guidance for inter-divisional communications independence within digital systems.
- 10CFR50.55a(h), which incorporates IEEE603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," does not define the degree of independence necessary to retain the capability to accomplish a safety function.
- Standard Review Plan (SRP) Chapter 7 includes conflicting guidance regarding communication independence.

Focus

- Industry identified many technical areas concerning communications independence for which they requested further clarification
- Consolidated to 9 high-priority issues in the Public Meeting of March 29
- TWG distilled these to 4 "Areas of Interest"
  1. Interdivisional Communications
  2. Command Prioritization
  3. Multidivisional Control and Display stations
  4. Digital System Network Configuration

Interim Staff Guidance

- Developed to clarify licensing criteria
- Public comments received and addressed
- Will be issued for use September 28, 2007
- Supports existing regulations
  - No new policy issues
- Good alignment with industry
- One technical issue remains unresolved:
  - Need for safety-grade controls & indications for safety-related components
    (will be addressed later in this presentation)

ISG Organization

- Scope
- General discussion of Rationale
- General references
- Technical sections
  1. Interdivisional Communications
  2. Command Prioritization
  3. Multidivisional Control and Display Stations

Scope

- Communications:
  - Between safety divisions
  - Between safety entities and nonsafety entities
- Briefly addresses nonsafety controls that could affect conformance to safety criteria (such as accident analysis assumptions)
- All existing guidance remains in-force and unaltered unless explicitly indicated otherwise

Rationale & References

Safety Systems must be independent and reliable

- 10CFR50.55a(h) invokes IEEE 603-1991
- Regulatory Guide 1.152 invokes IEEE 7-4.3.2-2003
  - Provisions for communications independence have not been endorsed (Annex E, an informative annex)
  - 7-4.3.2 currently undergoing revision

Interdivisional Communications

Communications among different safety divisions or between any safety division and any system or equipment that is not safety-related

Interdivisional Communications

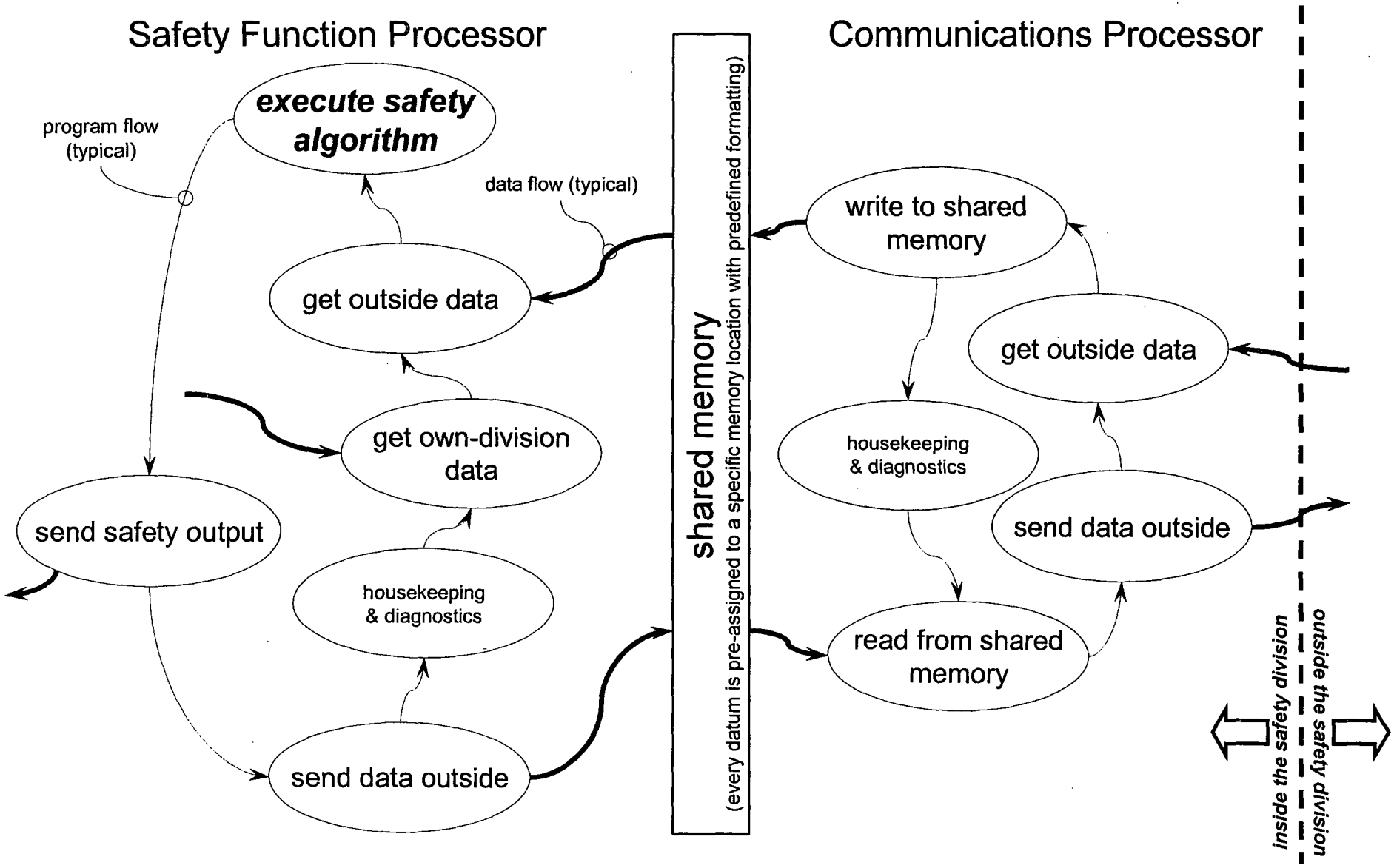
- Previously limited to one-way, outbound from safety system to nonsafety system
  - No communication from nonsafety to safety
  - No communication from other safety divisions
- ISG endorses bidirectional and interdivisional communications

...that do not involve the safety function processor

  - Communications processor handles all communications
    - Safety function processor may perform data validation for vital communications (voting logic)
  - No communications *at all* with safety function processor
  - Safety function processor cannot be diverted from predefined deterministic cyclical program

Interdivisional Communications

(normal operation – conceptual)



Interdivisional Communications

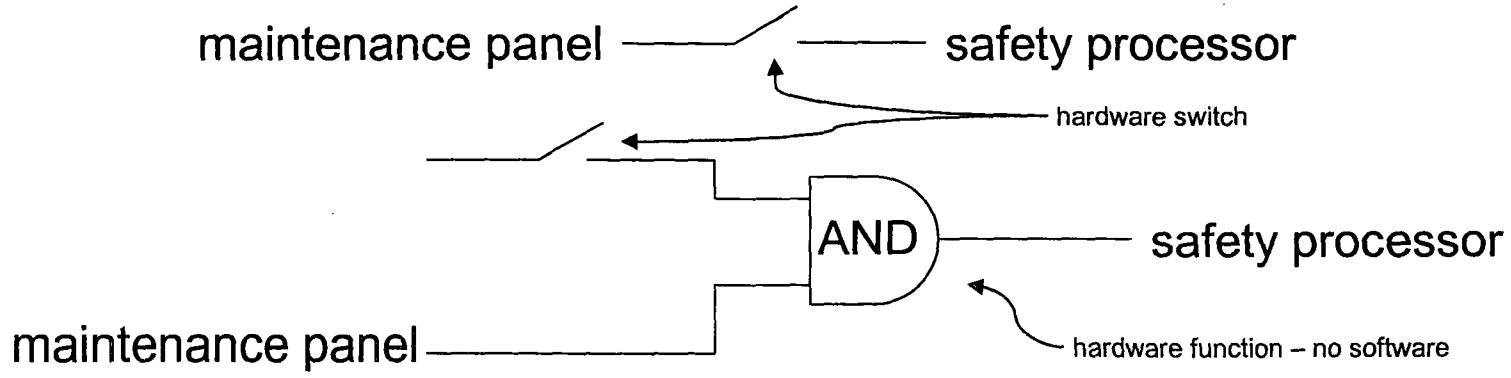
(general provisions)

- No interdivisional communications that do not support safety function
- No adverse effect upon any division
- Data sets must be predefined and invariant
- ISG includes sample list (not comprehensive) of credible communication faults, including data storm and bandwidth problems
- Vital communications must include error-checking and must be direct point-to-point (not multidrop network)

Interdivisional Communications

(maintenance considerations)

- Prespecified parameters can be adjusted via shared memory
- Access to function processor is controlled via key-lock switch
  - Modifications must be to only one division at a time
  - No program modifications during safety operation



Command Prioritization

The process of selecting a particular command to forward to plant equipment when multiple commands exist

- Safety command from safety system always has priority
- Nonsafety command from safety system can be overridden by (nonsafety) Diverse Actuation System (DAS)
- Prioritization details must be determined individually for each safety function
- DAS used for D3 must bypass the digital system

Command Prioritization
Hardware-Based Priority Modules

- Physical device with inputs from safety and nonsafety sources via hard wire and/or data link
  - Must be fully tested
  - May contain software and digital circuits
    - Software used in safety function must be safety-grade
  - Includes both safety and nonsafety circuits, with appropriate isolation
  - Priority logic is nonvolatile & not alterable in-place
- Suitable for D3

Command Prioritization
Software-Based Priority Modules

- Code is executed by the function processor
- Code must be safety-grade
- Not suitable for D3

Multidivisional Control and Display Stations

nonsafety control station that has access to multiple safety divisions as well as to nonsafety devices

- Communications with safety divisions as described for interdivisional communications
- Control of safety devices via priority modules
- Cannot suppress or adversely affect any safety function
- Application & removal of bypasses only with the permission of the safety system

Multidivisional Control and Display Stations

- Plant safety analyses must be consistent with possible failure modes
  - Spurious actuations could affect initial conditions
  - Spurious stoppages could affect event progress
- Spurious events may be initiated by multidivisional stations, or may be initiated by failures in control processors
  - Safety analyses must accommodate what might happen, regardless of the source of the event

Multidivisional Control and Display Stations

- Hardware must be qualified for same design bases as safety systems at same location
  - Must demonstrate no spurious operations
  - Need not remain operable during / after DBE
  - Software need not be safety-grade
- Need at least 2 positive operator actions to command plant equipment
  - Protection from accidental contact with control station

Multidivisional Control and Display Stations

- Power loss/surge/interruption etc. must not produce spurious actuation or termination
- Operator workstation disable switch to prevent spurious event due to fire, flood etc. in control room

- Staff generally believes that all safety-related plant devices need to have safety-grade controls
- ISG recommends individual safety-grade controls, & requires justification if they are not provided

Multidivisional Control and Display Stations – Human Factors

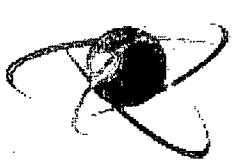
- Use of less familiar (safety-grade) control stations under accident conditions could lead to operator error
- Other HF concerns are addressed by HF TWG

Multidivisional Control and Display Stations – D3

- D3 considerations may affect the selection & type of priority modules
- D3 considerations may affect qualification requirements
- Other D3 considerations will be addressed by D3 TWG

Path Forward

- Work with industry to have ISG incorporated into industry standards
- Revise RG 1.152
- Revise the Standard Review Plan



Diversity and Defense-in-Depth (D3) Interim Staff Guidance

Ian Jung, NRO
Mike Waterman, RES
Paul Loeser, NRR

September 13, 2007

D3 Task Working Group

- Initial public meeting February 2, 2007
  - Five more public meetings
- NRC members from NRO, NRR, RES, and NMSS
- Industry contacts
- Purpose: Clarification for incorporating D3 in digital safety systems that will provide the nuclear industry with a high level of confidence that license applications will be reviewed in a consistent and predictable manner.

Seven Problem Statements

1. Adequate diversity
2. Manual operator actions
3. BTP 7-19 Position 4 challenges
4. Effects of common cause failures (CCFs)
5. CCF applicability
6. Echelons of defense
7. Single failure

Interim Staff Guidance

- **Problem Statements 1 and 2**

1. <u>Adequate Diversity</u>: Additional clarity is desired on what constitutes adequate D3. Determine how much D3 is enough.

2. <u>Manual Operator Actions</u>: Clarification is desired on the use of operator action as a defensive measure and corresponding acceptable operator action times.

Draft ISG

- **Staff Guidance on Problem Statements 1 and 2**
  - The methods described in this guidance are not the only methods that the staff may find acceptable. The staff may also find other methods acceptable, but other methods may require more in-depth staff review.
  - There is no distinction in D3 guidance for digital Reactor Protection System (RPS) designs for new/future nuclear power plants and current operating plants.
  - While CCFs in digital systems are beyond design basis, the digital RPS should be protected against CCFs.

Draft ISG

- **Staff Guidance on Problem Statements 1 and 2 (continued)**
  - A D3 analysis should be performed to demonstrate that vulnerabilities to CCFs have been adequately addressed.
  - Where the protective action that should have been automatically performed by the system subject to CCF is required in less than 30 minutes to meet the BTP 7-19 acceptance criteria, an independent and diverse automated backup, achieving the same or equivalent function, should be provided.
  - This automated backup guidance does not apply to follow-on actions that are handled in a manual fashion.
  - In addition, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual actuation and control of safety equipment to manage plant critical safety functions.

Bases for 30-minute Operater Action Time

- Minimizing operator burden under the conditions of a digital system CCF
- Past regulatory decisions
- Regulatory practices applied in the international community
- Engineering judgment

Draft ISG

- **Problem Statement 3**

3. <u>BTP-19 Position 4 Challenges</u>: Further clarification is required for whether credit can be taken for component-level versus system-level actuation of equipment.

Draft ISG

- **Staff Guidance on Problem Statement 3**
  - Clarification of BTP 7-19 Position 4
  - It no longer specifies whether the diverse displays and controls be used for component-level or system-level actuation of equipment, as long as the criteria are met.

Draft ISG

- **Problem Statement 4**

4. <u>Effects of CCF</u>:

– BTP 7-19 guidance recommends consideration of CCFs that "disable a safety function." Additional clarity is required regarding the effects that should be considered (e.g., fails to actuate and/or spurious actuation).

– Industry also requested that the staff determine whether spurious actuations should be considered when evaluating software CCF.

Draft ISG

- **Staff Guidance on Problem Statement 4**
  - In general, spurious trips and actuations are of lesser safety concern than failures to trip or actuate.
  - There may be plant and safety system challenges and stresses; however, these challenges are not as significant as failure to respond to a Chapter 15 event.
  - Software CCFs resulting in a spurious trip or actuation of a safety-related digital protection system do not need to be considered in the single failure analysis.

Draft ISG

- **Problem Statement 5**

5. <u>CCF Applicability</u>: Clarification is required on identification of design attributes that are sufficient to eliminate consideration of CCFs (e.g., degree of simplicity).

Draft ISG

- **Staff Guidance on Problem Statement 5**
  - Diversity: If sufficient diversity exists in the reactor protection system such that CCFs within the channels are considered to be fully addressed, then no additional diversity would be required in the safety system.
    - What constitutes "sufficient diversity" should be evaluated on a case-by-case basis, considering design and process attributes that preclude or limit certain types of CCFs. It should then reference the ISG on Problem Statements 1 and 2 for additional guidance.
  - Testability: If a system is sufficiently simple such that it is fully tested and found to produce only correct responses, then no additional diversity would be needed in the safety system.

Draft ISG

- **Problem Statement 6**

  6. <u>Echelons of Defense</u>: Additional clarification is desired regarding how the echelons of defense for maintaining the safety functions should factor into D3 analyses. A particular concern is that the current BTP 7-19 guidance does not consider plant design characteristics and operating procedures that affect how D3 is actually used to maintain the safety functions.

- **Staff Guidance on Problem Statement 6**

  - The RTS and ESFAS functions may be combined into a single digital platform if the criteria of the ISG on Problem Statements 1 and 2 are met.

Draft ISG

- **Problem Statement 7**

  7. <u>Single Failure</u>: Additional clarification is required regarding the acceptance criteria for CCFs versus the acceptance criteria for single failures in safety system designs.

- **Draft Interim Staff Guidance on Problem Statement 7**

  – A software CCF does not meet the criteria for a single failure in single failure analyses (defined in 10 CFR 50, Appendix A).

  – A software CCF, even when caused by a software error, is considered a failure that is beyond design basis.

Longer-term Activities

- Work with industry to have ISG refined
  - Adequate diversity strategies
- Staff assessment of ACRS recommendations on operating experience and inventory/classification
- Revise the Standard Review Plan

Inventory/Classification and Operating Experience for Diversity and Defense-in-Depth

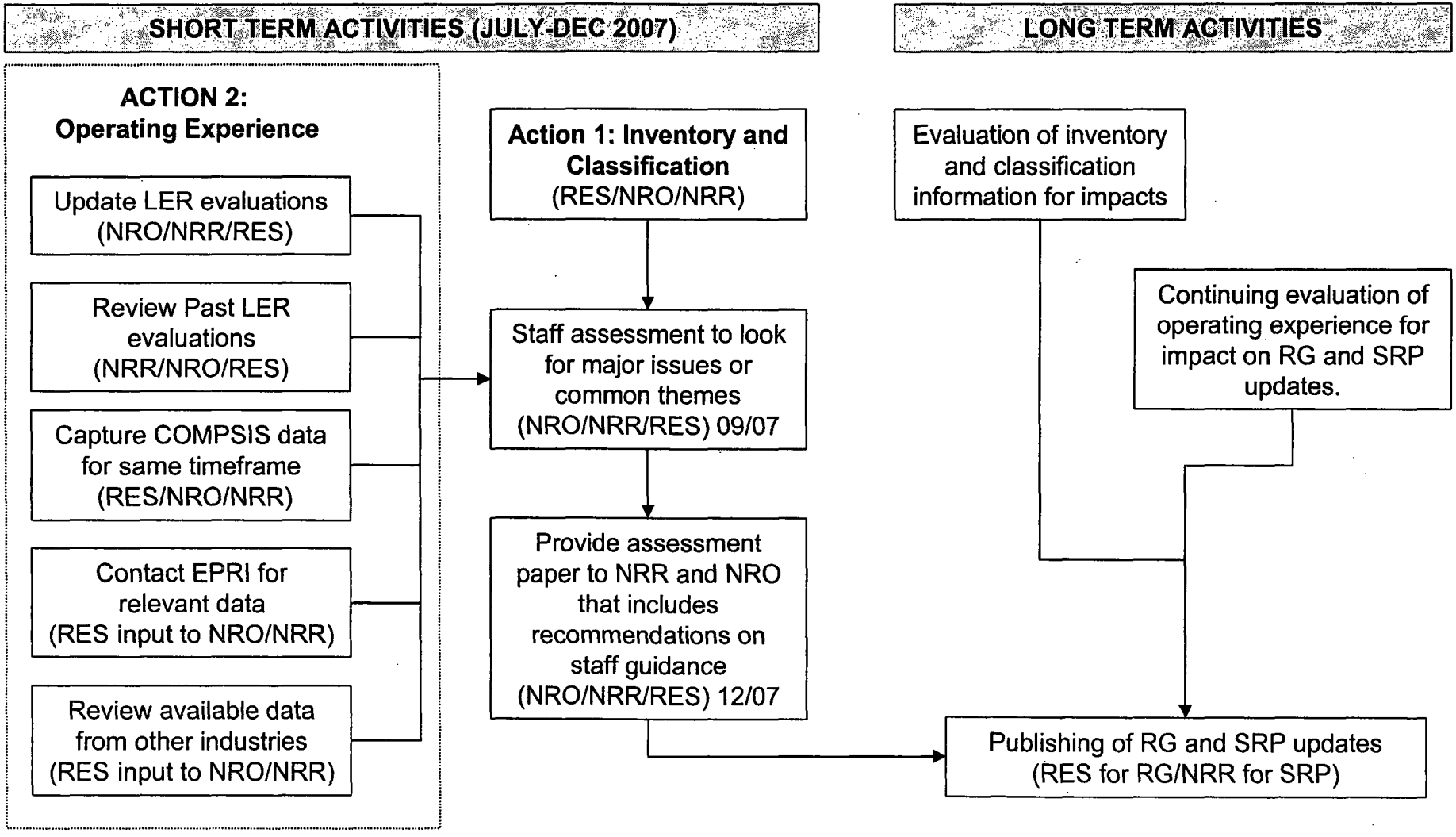
Ian Jung, NRO
Russ Sydnor, RES
Steve Arndt, RES

September 13, 2007

BACKGROUND

- In a May 18, 2007, letter to the Commission the ACRS recommended that the Staff
  - Develop an inventory and classification of existing and potential NPP digital and software systems
  - Evaluate digital system operating experience in the nuclear and other industries to obtain insights regarding potential failure modes
- Use this information in the development of diversity and defense-in-depth (D3) regulatory guidance

Overview


SHORT TERM ACTIVITIES (JULY-DEC 2007)
LONG TERM ACTIVITIES
ACTION 2:
Operating Experience
Update LER evaluations (NRO/NRR/RES)
Review Past LER evaluations (NRR/NRO/RES)
Capture COMPSIS data for same timeframe (RES/NRO/NRR)
Contact EPRI for relevant data (RES input to NRO/NRR)
Review available data from other industries (RES input to NRO/NRR)
Action 1: Inventory and Classification (RES/NRO/NRR)
Staff assessment to look for major issues or common themes (NRO/NRR/RES) 09/07
Provide assessment paper to NRR and NRO that includes recommendations on staff guidance (NRO/NRR/RES) 12/07
Evaluation of inventory and classification information for impacts
Continuing evaluation of operating experience for impact on RG and SRP updates.
Publishing of RG and SRP updates (RES for RG/NRR for SRP)

INVENTORY AND CLASSIFICATION

- The inventory and classification research will provide
  - A framework for collecting operational data
  - Guidance for evaluating operational data
  - A process for translating operational data into D3 regulatory guidance

INVENTORY AND CLASSIFICATION

- Classification systems
  - Regulatory-based
    - Safety versus non-safety
    - Category A, B, and C (primarily a European system)
    - Risk-informed grading systems (50.69)
  - Design-based
    - Rashly's aspects associated with timing, safety, and fault tolerance requirements
    - Perrow's interaction and coupling
    - Aldemir's Type I and Type II interactions

INVENTORY AND CLASSIFICATION

- Classification systems (cont.)
  - Operational-based
    - NASA classifies failures in mission critical software-intensive systems as
      - Type A failures – Translation-based errors
      - Type B failures – V&V-based errors
      - Type C failures – Specifications-based errors
  - NRC reviews of operational data have revealed that nuclear system failure classes are similar to failure classes in systems studied by Rashly, Perrow, and NASA

INVENTORY AND CLASSIFICATION

- A proposed failure-type classification expands on the work done by Rashly, Perrow, Aldemir, and NASA
- The proposed classification consists of three attributes
  - Complexity (including hardware and software complexity and testability of the system)
  - Interactions/inter-conductivity (including inter-system communications and the importance of timing and feedback with other systems)
  - Importance (including risk importance, how important the system is for maintaining defense-in-depth and the consequence of system failures)

INVENTORY AND CLASSIFICATION

- The proposed classification system will address
  - Failure modes
  - Failure history
  - Potential failure consequences
- Once the classification system structure is sufficiently complete, a systems inventory will be conducted to identify the population of the failure data

OPERATING EXPERIENCE ASSESSMENT

- Assessment of operating experience in nuclear and other industries:
  - Internal assessment of operating experience and LER failure data ('87-'06)
  - I&C digital system failures in nuclear power plants ('94-'99)
  - COMPSIS database
  - Contacted EPRI and NEI for similar operating experience failure data
  - *Survey of Digital I&C Failures* (ORNL)
  - *Risk Informed Safety Assurance and PRA of Mission-Critical Software-Intensive Systems* (NASA)

OPERATING EXPERIENCE ASSESSMENT

- Preliminary findings
  - Availability of quality data is limited
  - Exact causal data is particularly difficult to locate
  - CCFs are credible
    - Other industries use diverse systems to mitigate the effects of CCFs
  - Ongoing NRC programs (e.g., operating experience program) are valuable in that they collect, analyze and distribute information providing lessons learned to staff, applicants, vendors, and licensees.

Preliminary Conclusion

On the basis of an assessment of existing classification systems and operating experience data,

No changes to the proposed D3 ISGs are required.

FUTURE PLANS

- September 28, 2007
  - Complete short-term staff assessment
- December 31, 2007
  - Provide white paper that details potential impact upon staff guidance
  - Capture assessment results of inventory/classification and operating experience
- 2008 and beyond
  - Provide inputs for proposed long-term activities to refine guidance
  - Continue ongoing operating experience program reviews

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

Cyber Security Interim Staff Guidance (ISG)

Presentation to the ACRS Subcommittee on
Instrumentation and Controls

Mario Gareri, NSIR

September 13, 2007

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

Agenda

- Background
- Draft ISG
- Status
- Path Forward

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

Background

- Industry requested clarification of differences in guidance associated with implementation of cyber security programs at nuclear power plants as it relates to protection of safety-related digital instrumentation & control systems.
- Specifically, Task Working Group (TWG) was established to address industry concerns that Regulatory Positions 2.1-2.9 in RG 1.152 Rev 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" conflict with NRC-accepted NEI 04-04 Rev1, "Cyber Security Program for Power Reactors."

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

Background (cont)

- Problem Statement:
  - Regulatory Positions 2.1 – 2.9 of RG 1.152 and NEI 04-04 provide conflicting guidance for implementing cyber security requirements for safety systems at nuclear power plants.

- TWG staff developed a gap analysis to identify areas where the two documents may be inconsistent or overlap.

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

Background (cont)

- Gap analysis revealed some guidance overlap but no inconsistencies/conflicts between RG 1.152 Rev2 and NEI 04-04 Rev1. Rather, the two documents are complementary.

- Industry committed to revise NEI 04-04 Rev1 to better incorporate cyber security guidance for safety-related systems so that criteria from RG 1.152 Rev2 would be addressed.

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

Background (cont)

- Following the revision, draft NEI 04-04 Rev2 would be submitted to NRC for review and official acceptance so that industry can then use NEI 04-04 Rev2 in lieu of RG 1.152.

- Industry agreed to provide a cross-correlation table to the TWG to demonstrate how the topical elements within Regulatory Positions 2.1-2.9 map directly to the provisions within draft NEI 04-04 Rev2.

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

Draft ISG

- Draft interim staff guidance (ISG) will clarify the NRC staff's guidance with regard to implementation of cyber security requirements for nuclear power plant safety systems.

- To facilitate licensing process using NEI 04-04 Rev2 the ISG will include an enclosure of a cross-correlation table to clearly show how criteria from Regulatory Positions 2.1-2.9 map directly to draft NEI 04-04 Rev2.

- Pending formal acceptance of NEI 04-04 Rev2, licensees, permit holders, and applicants involved in the design, construction, implementation, or upgrade of safety-related systems should adhere to RG 1.152 Rev2.

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

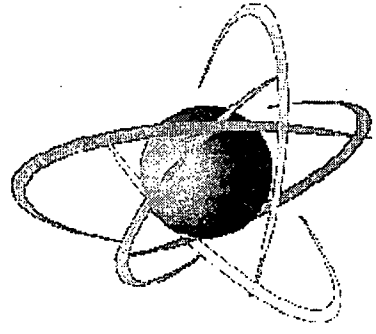
Status

- Last public meeting with Industry – 09/10/2007
- Current draft ISG will be revised to incorporate a cross-correlation table.
- ISG on cyber security is currently planned to be issued by end of October 2007

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

Path Forward

- TWG staff will complete review of most recent cross-correlation table that was submitted by industry and the current draft ISG will be revised as appropriate by staff.
- Revised draft ISG will be provided to industry for review/comment.
- TWG staff will consider industry comments
- NEI will submit NEI 04-04 Rev2 to the NRC for review and official acceptance separately soon after the draft ISG can be finalized by TWG staff.



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Interim Staff Guidance DI&C-ISG-05 Highly Integrated Control Rooms-Human Factors: Computer-Based Procedures

Presentation to:

Advisory Committee on Reactor Safeguards

September 13, 2007

Michael A. Boggi, CHFP
Human Factors Engineer
Division of Risk Assessment and Special Projects
Office of Nuclear Regulatory Research

Purpose of this Briefing

Inform the ACRS of the basis and state of the Interim Staff Guidance (ISG) regarding computer-based procedures.

Basis for the ISG

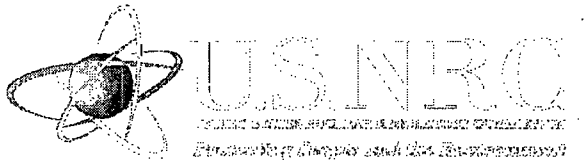
Problem Statement: Review existing NRC regulatory guidance, positions, and acceptance criteria, and make necessary changes, to facilitate consistent and efficient licensing of computerized procedures and soft controls in highly integrated control rooms. Develop guidance and acceptance criteria, if necessary, to minimize the impact of degraded digital instrumentation and controls associated with computerized procedures and soft controls on human performance.

Problem Resolution

Short term - prepare Interim Staff Guidance

Long term - deeper dive

- update NUREG-0700, Human System Interface Design Review Guidelines, May, 2002



Purpose of Computer-based Procedures

To guide the operators' actions in performing their tasks in-order-to increase the likelihood that the goals of the task are safely achieved. NUREG-0700

Interim Staff Guidance

Computer-based Procedure Systems

- General
- Plant Data
- Automation
- Soft Controls
- Modernization

Computer-based Procedures

- General
- Backup Procedures

Interim Staff Guidance

Staff Rational:

- Content and development of paper and computer based procedures can be essentially the same.
- Both can and should be easy to use.
- The differences (e.g. automation) possible with computer-based procedures should not limit the control or situation awareness of the procedure user.

Review Criteria, examples:

- Automation should not select nor initiate the procedure to be used.
- The computer-based procedure should not initiate control actions without first receiving a command from the operator to do so.
- Computer-based procedure systems do not change the procedure.
- Hold points should be established to effectively monitor automation progress.

Review Criteria, examples:

When soft controls are used:

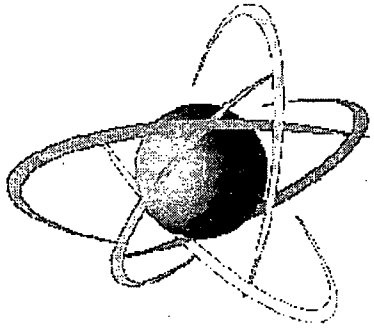
- The computer-based procedure system should contain a concise set of soft control whose meaning is obvious to the user.

- Soft control display properties should not violate stereotypes of hard or soft controls already in place in a Main Control Room.

- The control of plant equipment should take at least two discrete actions.

Conclusion

- ISG is a good interim measure.
- Industry and stakeholders were actively involved in the process.
- Long-term guidance will require an update to NUREG-0700



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Interim Staff Guidance DI&C-ISG-05 Highly Integrated Control Rooms-Human Factors: Minimum Inventory

Presentation to:

Advisory Committee on Reactor Safeguards

September 13, 2007

J. Persensky
Senior Technical Advisor
Division of Risk Assessment and Special Projects
Office of Nuclear Regulatory Research

Purpose of this Briefing

Inform the ACRS of the basis and status of the Interim Staff Guidance (ISG) regarding minimum inventory.

Basis for the ISG

- Problem Statement: Review existing NRC regulatory positions and acceptance criteria, and make necessary changes, to better define minimum inventory of alarms, controls, and displays needed to implement the emergency operating procedures and bring the plant to a safe condition ..... consider development of a process approach to the development of a plant-specific minimum inventory.

- Multiple stakeholder meetings to discuss ISG.

Problem Resolution

Short term - prepare Interim Staff Guidance

Long term – consider applicability to operating plant modernization

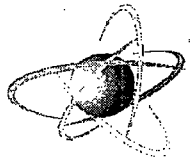
– consider additional guidance for readily accessible, spatially dedicated, and continuously visible

Purpose of Minimum Inventory

Assure that operators have the minimum inventory of alarms, controls, and displays needed to implement the plant's emergency operating procedures, bring the plant to a safe condition, and to carry out those operator actions shown to be important from the applicant's probabilistic risk assessment both in the main control room and at the remote shutdown panel.

Interim Staff Guidance

- Process Development, e.g.,
  - D3 evaluation for coping with common cause failures
  - Credited operator actions
- Minimum inventory list, e.g.,
  - Containment pressure
  - Manual containment isolation
- Verification, e.g.,
  - Risk-significant operator actions
  - Use of full-scope simulation



Interim Staff Guidance

Two Step Process:

- Review process used to identify the list of alarms, displays, and controls that would constitute the minimum inventory and the list

- Verify the implementation of minimum inventory

Conclusion

- ISG is an acceptable means of meeting Commission requirements as an interim measure.

- Industry and stakeholders were actively involved in the process.