Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards (ACRS) Future Plant Design Subcommittee

Docket Number: (n/a)

Location: Rockville, Maryland

Date: July 8, 2014

Work Order No.: NRC-900 Pages 1-207

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

FUTURE PLANT DESIGN SUBCOMMITTEE

+ + + + +

TUESDAY

JULY 8, 2014

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

COMMITTEE MEMBERS:

DENNIS C. BLEY, Chairman

SANJOY BANERJEE, Member

CHARLES H. BROWN, JR. Member

MICHAEL L. CORRADINI, Member

DANA A. POWERS, Member

HAROLD B. RAY, Member

STEPHEN P. SCHULTZ, Member

JOHN W. STETKAR, Member

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

THERESA CLARK, NRC

SARAH DiTOMMASO, Westinghouse

TOM FREDETTE, NRC

BOB HIRMANPOUR, Southern Company

TERRY JACKSON, NRC

RENEE LI, NRC

ANDREA VALENTIN, NRC

P-R-O-C-E-E-D-I-N-G-S

(8:30 a.m.)

CHAIR BLEY: The meeting will now come to order, please. This is a meeting of the Future Plant Design Subcommittee. I'm Dennis Bley, chairman of the subcommittee.

ACRS members in attendance are Ron Ballinger, Sanjoy Banerjee, Charlie Brown, Michael Corradini, Dana Powers, Harold Ray, Steve Schultz and John Stetkar. Did I miss anyone? I don't think so.

Christina Antonescu, of the ACRS staff is the designated federal official for this meeting. The purpose of this meeting is for the staff to brief the ACRS on results from several Design Acceptance Criteria, DAC, inspections completed for the AP-1000 Digital I&C using the new inspection procedures.

I'm going to divert from my printed notes for just a second. For people who weren't here four years ago when we wrote our last letter on DAC, I thought I'd just give a little abbreviated summary o how we got here.

We initiated our own look at DAC at that

time and wrote a letter. The letter had two recommendations. First, the DAC closure requires expertise, judgment and interpretation. It should be performed by NRC staff experts with an independent assessment by ACRS.

And, two, it's preferable that all DAC be resolved no later than the COL stage. However, whether the result is part of COL process or post COL, proper closure of DAC requires a consistent scope and depth of evaluation in accord with our first recommendation.

We had lots of discussions with staff at all levels at that time. They weren't quite in agreement and thought that we didn't belong in the --

MEMBER CORRADINI: In DAC land.

CHAIR BLEY: -- DAC land, in the inspection process at all. We wrote our presentation to the Commission and reminded them of a statement they'd made when they first started looking at Part 52, in the Statements of Consideration.

The Commission does not believe that it is prudent to decide, now, before, the Commission has even once gotten through the process of judging whether a plant built under a combined license is ready to operate, that every finding the Commission will have

to make at that point will be cut-and-dried proceedings according to highly detailed objective criteria entailing literal judgment and discretion in their application and not involving questions of credibility, conflicts and sufficiency.

And the DAC, if they're inspections as we normally think of when, caused us to wonder quite a bit about it, all right. After the meeting with the Commission, they didn't quite agree with us. But they didn't quite agree with the staff either.

And they suggested that we follow the first few DAC inspections and see if we're satisfied and we'd get back together and talk about it. Ron's going to tell us a bit later about what we're looking at.

Among the DAC we were most concerned with the Digital I&C DAC but wanted to watch the piping DAC as well, but thought that would go pretty cleanly. So we're at the point we finally have some inspection results the staff's going to share with us. And we'll continue that process now.

Today the subcommittee will hear presentations by and hold discussions with the NRC staff and other interested persons regarding this matter. The focus of the meeting is going to be on Digital I&C

DAC inspection results, piping DAC inspection progress and licensees' perspective on DAC inspection.

The Committee will gather information, analyze relevant issues and facts and formulate purpose, positions -- formulate and propose positions and actions as appropriate for deliberation by the full committee.

The rules for participation in today's meetings has been announced as part of the notice of this meeting previously published in the Federal Register of June 18, 2014. We have received no written comments or requests for time to make oral statements from members of the public regarding today's meeting.

Also, we have some people on the Bridge phone line listening in to the discussions. We know that several will be there, Rick Connolly and Kevin Durrwachter of Southern Nuclear Operating Company, Vogtle 3 and 4; Brian Bedford, Westinghouse Electric Company with V.C. Summers Units 2 and 3 and Anthony Masters, U.S. NRC Region II of Atlanta.

To preclude interruption of the meeting the phone line will be placed in the listen-in mode during the discussions and presentations and committee discussions. Also, the Bridge line will be opened at

the end of the meeting to see if anyone would like to make any comments.

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

The participants should first identify themselves and speak with sufficient clarity and volume where they can be regularly heard. We will now proceed with the meeting.

I'll call upon Andrea Valentin, Deputy Director in the Division of Construction, Inspection and Operational Programs in the Office of New Reactors to make an opening statement followed by Tom Fredette, Reactor Operations, Engineering, Construction and Inspection Programs Branch. Ms. Valentin?

MS. VALENTIN: All right, good morning. Thank you. Good morning, Dr. Bley and subcommittee members. I'm Andrea Valentin, the Deputy Director in the Division of Construction, Inspection and Operational Programs within the Office of New Reactors.

The staff is here today to provide the

subcommittee an informational briefing on our activities related to Design Acceptance Criteria or DAC inspection. We last briefed you in November of 2011 when we committed to provide periodic briefings for you as the DAC inspection program was implemented.

Mr. Thomas Fredette, from my staff, will provide today's briefing. And we also have Mr. Bob Hirmanpour from Southern Nuclear, a little later, who will provide perspectives from the AP-1000 licensees regarding Digital Instrumentation & Control System DAC inspections. Tom?

MR. FREDETTE: Thank you, Andrea. Thanks, Dr. Bley for allowing us to brief you this morning. As Andrea mentioned, it's been since November of 2011, was the last time we briefed you. That was, this will be the fourth time that we've actually briefed the subcommittee on the DAC inspection process and the procedures and the program as we've sort of gotten off the starting block.

This is our, we're into our fifth year right now of DAC inspection program and process, planning and implementation. A lot of things that we thought would happen over the past couple of years did not transpire on schedule. So we're a little bit behind

as far as implementation.

You mentioned that we would talk about implementation of DAC inspections in the piping and Digital I&C area. Well, there have not been any piping DAC inspections as of yet. We expect to have those start being conducted later this year, possibly into next year.

So, anyway, I'm here to provide a little bit of a briefing for your subcommittee. The objectives for today, I'm going to give you an overview of the working group activities with an emphasis on DAC inspection, our approach to AP-1000 DAC inspection, the results of the Digital I&C inspection activities to date.

And then we'll talk a little bit about some of the insights and lessons learned that we've compiled over the past couple of years. And then an overview of where we see DAC inspection going over the next 12 to 18 months.

CHAIR BLEY: Can I interrupt you here?

MR. FREDETTE: Certainly.

CHAIR BLEY: You know, we originally were all looking forward to the South Texas Project inspection where there was a little bit more in the

way of I&C DAC.

MR. FREDETTE: Yes, sir.

CHAIR BLEY: AP-1000 only had one. As you talk about that one, if there's anything you can relate of the staff's thoughts, having at least explored a little bit into South Texas where there was a little more meat, we'd be interested in hearing any thoughts that developed during that time as well as any ones you've actually been able to do here.

MR. FREDETTE: Yes, sir, Dr. Bley. Just to make a note here, when we did the, when we started out with South Texas, we only did one pilot inspection.

CHAIR BLEY: Mm-hmm.

MR. FREDETTE: I'll talk a little bit about that. But it was a very limited pilot inspection. And then when we were just about to embark on some real meaty type of inspections, that's when things got turned off with South Texas and we had to shift our focus to the AP-1000, so.

Some background, Dennis, you've talked about how we got here. But I sort of wanted to give a little bit of flavor for some of the other members here. I cannot remember who might be new from 2011 and who's still here from 2011.

I know Mr. Brown and Mr. Corradini and Mr. Stetkar. If there are any new faces, this slide is for you. It's basically to set the stage for how we got to where we're at today.

(Off-microphone comment)

MR. FREDETTE: The DAC Task Working Group was established in November of 2009 to do develop a viable inspection strategy for Design Acceptance Criteria. At the time, the main focus was, of course, Digital I&C.

The inspection process and procedure development was initiated for the South Texas Project, for the ABWR DAC. And we conducted a pilot inspection in June of that year, of 2010.

We committed that time to periodically brief ACRS on status. And then the Fukushima event occurred in March of 2011 and the South Texas Project development was basically suspended indefinitely.

Our focus, at that time, was to shift to AP-1000, recognizing that, for Digital I&C DAC, it was, the AP-1000 design had a very limited DAC scope.

We finalized the procedures we were going to use in September of 2011. We briefed the ACRS, our last briefing, on the AP-1000 approach. At that time,

most of our procedures were being finalized. And we committed, as you mentioned, to provide periodic briefings as the inspection process was implemented.

I want to backtrack here for a moment. You know, we're going to talk today about piping DAC and Digital I&C DAC. There is one other discipline that's involved here and that's human factors. We are not going to brief on anything having to do with human factors today. We want to defer that to another meeting.

There has not been any activity in the human factors area but the staff expects to conduct the first human factors inspection for AP-1000 later this year. So what we want to do is we want to wait until those inspection results are finalized and we have some fruitful things to basically report on to the subcommittee.

CHAIR BLEY: Let me ask you a little bit about that, okay?

MR. FREDETTE: Okay.

CHAIR BLEY: The design cert material on human factors was pretty much process oriented. Are they far enough along now that many of those programs have real meat or are we still going to be looking at

the process side of it?

MR. FREDETTE: No, they're at the point now, the AP-1000 simulator has gone through factory acceptance testing.

CHAIR BLEY: Mm-hmm.

MR. FREDETTE: They're at the point now where they're going to start doing integrated system validation.

CHAIR BLEY: Okay.

MR. FREDETTE: That's scheduled to start October of this year and run through until December. And we're going to do that inspection, that first inspection, of integrated system validation in that two-month time frame.

CHAIR BLEY: Okay, good.

MR. FREDETTE: So I expect that we will be able to report on inspection results in the spring of 2015.

CHAIR BLEY: Okay, that's good. We'll be very interested in that one because we've seen nothing much yet of substance. So that will be very interesting to us.

MEMBER SCHULTZ: Tom?

MR. FREDETTE: Yes, sir.

MEMBER SCHULTZ: Do you know what the inspection plan documentation is like for that activity and when it might be prepared for implementation?

MR. FREDETTE: I do not, Mr. Schultz. That's something we can certainly explore. Let me do some research and I can get back to the Committee on where they stand with all their documentation --

MEMBER SCHULTZ: Thank you.

MR. FREDETTE: -- if that would be suitable.

MEMBER SCHULTZ: Okay.

MR. FREDETTE: I should point out, we have some of the Westinghouse and licensee personnel in the audience today who might be able to speak to some of the details regarding where, exactly, they stand with the human factors development, so.

MEMBER STETKAR: There's actually some, I'm, because I don't have anything else to do, I decided to read the inspection procedures for HFE also. And there's some proprietary appendices that have been prepared that are reasonably focused on AP-1000 in the HFE area.

I'll use the term reasonably focused, not excruciating detail. But it's more than just a

general, you know, just a general high level procedure.

MR. FREDETTE: Yes, sir. I am not a human factors expert, and I don't claim to be. And, I'm looking around today, we don't, since we weren't going to talk about human factors today nobody from the staff has come down to talk about that.

MR. STETKAR: It's just, I just wanted to add that because there is, there has been, I think, a reasonable amount of thought, at least focusing it on --

MR. FREDETTE: Well, there were --

MR. STETKAR: -- on projected information that is or will be available for AP-1000 anyway.

MR. FREDETTE: Thank, Mr. Stetkar, for pointing that out. The HFE DAC for AP-1000, there's four different ITAAC that cover the DAC. And there is a procedure for each of those ITAAC.

That's the way that we sort of structured how we were going to do those inspections. And, as I mentioned, the procedures were pretty much finalized over the past, oh, I'd say in the 2012 time frame. The staff's just waiting for a chance to use them.

Okay, anyway, that's, that will conclude our discussion for HFE DAC for today. As I said, we'll

brief the Committee at a later date.

Back to AP-1000, some significant activities that have taken place over the past couple years, we'll go into some more detail on these. We did an initial inspection in April of 2012 of the AP0-1000 ITAAC. And this was for the Protection and Safety Monitoring System for AP-1000.

This is basically the reactor trip and ESFAS system for AP-1000. We looked at one life cycle element of that ITAAC. It was for the, basically the system and software development requirements phase.

The consortium, basically the licensees and Westinghouse, implemented some corrective actions over 2012 and 2013 as the result of that inspection. We've had some various public and working level meetings with the consortium over the past couple of years as the corrective action was being developed.

And we completed our one and only AP-1000 Digital I&C DAC inspection in January of this year. In the piping arena we had committed to conduct a walk-through exercise with the licensees and with Westinghouse to talk about out piping DAC inspection process. And we completed that tabletop exercise in July of 2012.

This gives you an idea of how things have sort of been delayed over the past couple of years. You know, July of 2012 was when we thought we were on the verge of actually getting some piping packages --

CHAIR BLEY: Yes.

MR. FREDETTE: -- to actually inspect. Here we are, almost, well, virtually two years later and we still haven't done an inspection yet. But it's coming.

Our inspection model, a DAC inspection is, of course, a subset of an ITAAC inspection. It's incumbent upon the licensees to perform and complete those ITAAC. And we verify through inspection.

Unlike the garden variety NRC inspection, we engage the technical staff to augment our inspectors in a pseudo-inspection role. The technical staff are not trained inspectors but the bring the subject matter expertise and the technical discipline expertise to help inspectors in the field with questions about, for AP-1000 purposes, some of the licensing insights that inspectors may not be aware of.

And then they're basically put, thrust, into an inspection role which they've performed pretty well at so far.

CHAIR BLEY: Are you going to tell us more about their participation later?

MR. FREDETTE: Yes, I will.

CHAIR BLEY: Okay, I'll wait for that.

MR. FREDETTE: As with a lot of things with construction inspection, we rely on the performance schedule for the ITAAC as the licensees go through it. We document all our results in an inspection report.

And you've been provided copies of the inspection reports today. And, of course, the inspection reports are archived to support our ITAAC closure verification process later on down the road.

In the area of piping DAC inspection, as I mentioned previously, our procedures were developed to address site-specific ITAAC for piping design and pipe rupture analysis. In the licensing phase for AP-1000 the process for piping design and the process for pipe rupture hazards analysis were taken and made site-specific ITAAC in both licensees' AP-1000 licenses.

There is an ITAAC, a site-specific ITAAC for design and a site-specific ITAAC for pipe rupture hazard analysis. We did author an inspection procedure for both. And they were issued in late 2011.

This is the, I pulled this out of the COLs. This is the site-specific ITAAC for piping design. Basically, it's stipulating that you will design your code piping in accordance with ASME Code Section III requirements. The acceptance criteria basically mirror the design commitment.

And the on the next slide, this is the site-specific ITAAC for pipe rupture hazard analysis and, as design pipe rupture hazard analysis report, will exist and conclude that analysis performed for your high-energy and moderate-energy piping systems confirms protection of systems, structures and components required for functionality during and following the design-basis event.

CHAIR BLEY: Let's use this one, as an example, in the acceptance criteria. I don't know the, I know your inspectors are trained on how to do inspections but this kind of an inspection says the report exists and it has a conclusion which is fairly straightforward for an inspector.

MR. FREDETTE: Yes, sir.

CHAIR BLEY: But, as we talked more on Digital I&C rather than piping, still, this is referring to a calculation, an analysis which, I suspect, is where

your staff, headquarters staff people, are helpful in figuring out, helping them figure out if the calculations meet the criteria. Is that --

MR. FREDETTE: That's --

CHAIR BLEY: Am I right?

MR. FREDETTE: That's exactly right, Dennis. These types of inspections require more than just field verification. So we rely on the technical staff who are the real subject matter experts in a discipline that's very specialized, like this --

CHAIR BLEY: Who would have reviewed this if the design had been complete.

MR. FREDETTE: That's exactly right. So the same people who would have done the technical review and licensing, and did do the technical review and licensing, are now pulled in to help with specific inspection criteria, to look at.

MEMBER RAY: But that's not with this says, of course. It says the report exists and concludes. That's something that's subjectively verifiable as an inspection function.

Those words themselves don't include what Dennis asked you and you said it would be included, which is that the, you might say the report is verified

as correct or is reviewed for correctness or something that goes beyond it merely existing and reaching a conclusion.

MR. FREDETTE: That's right. And we don't just rely on the actual report that exists. We look at all of the activities that were involved in formulating and developing that report.

The report that's listed here in this acceptance criteria is basically the final, as design pipe rupture hazard analysis report. There are several analyses that are put together as the facility is constructed to look at different rooms, different areas, different segments of the plant and doing a pipe rupture hazard analysis for those rooms, areas and segments of the plant.

The inspectors, augmented by the technical staff, look at the methodology that was used for it to basically develop those analyses. I've got two members of the technical staff, the engineering technical staff, here who are the, basically, the pull of resources that we would call upon to help with this type of detailed inspection.

They're in the audience today. It's Theresa Clark and Renee Li. Basically, they're the

subject matter experts for pipe rupture hazard analysis. And they can expound on any detailed questions regarding how we would actually perform detailed calculation verifications and analysis verifications of this type.

CHAIR BLEY: I think it's fair to say we're interested in the substance of how that's done. But we're also interested in the point Harold raised. And can you point us to, for our record, anywhere in the inspection procedure where is implies you have to do something more than check the box that a report exists and concludes.

MEMBER STETKAR: And I'll follow up on the same thing, the Digital I&C, but even to a greater extent. So it's a generic question. It's --

CHAIR BLEY: So ten years from now, whoever's doing it and wasn't here today or wasn't here on this first one --

MR. FREDETTE: No, I understand --

CHAIR BLEY: -- knows what they really ought to be doing here.

MR. FREDETTE: I understand the question, Dennis. And Mr. Ray and Mr. Stetkar, thank you for chiming in.

We've had this discussion before, okay? We are not relying on just the fact that a report exists that an inspector can go and check a box, yes, the report's here and it's a concrete, tangible report that I can put my hands on.

Our process, all along, has relied on the actual activities that went into developing the report. That's what we actually inspect. Renee Li, from the technical staff, is here. Renee, would you like to B

CHAIR BLEY: Yes, would --

MS. LI: Yes. I'm a Renee Li from the Technical Engineering Bridge. I kind of operate --

CHAIR BLEY: Can you talk into the mic?

COURT REPORTER: Just speak into it.

MS. LI: Okay. Different from piping design which is ASME, COL as described.

But that information --

CHAIR BLEY: Don't worry about us.

MS. LI: Okay. I want to mention that making, in a piping design report. And for the pipe break hazard analysis there is no standard that describe those information.

So for the staff's review that we put in

ITAAC because the PRHA report compares numerous information the detail is not possible to be improved in the ITAAC. But when we say it's a PRHA report, actually, during the design certification review, in the DCD there is a section, subsection, specifically describe the outline of all the information needed to be included in the report.

So that would cover, for example, there are a methodology of determining are the pipe rupture locations, what type of breaks, the configuration. It should even show the sketch of where the pipe rupture location and also include how the applicant or licensee evaluate the dynamic effects such as jet impingement, pipe whip restraint.

You know, they indicate the location of those details, including how they evaluate the environmental condition result from pipe rupture such as fretting, water spray. So even though there are certain criteria since a PRHA report exists.

But a corresponding subsection in the DCD power line, you know, all the information needed. So during the ITAAC inspection the technical staff will support that inspection and do through the report.

MEMBER RAY: Why doesn't it say that here?

MR. FREDETTE: Yes, what are you looking at, Mr. Ray?

MEMBER RAY: Originally, what's on the screen up there.

MR. FREDETTE: Oh, okay.

MEMBER RAY: And I'm saying why doesn't it say what she just said, which is that the report will be reviewed for acceptability and compliance with the requirements in the DCD as well as merely that it exists.

MR. FREDETTE: Well, remember, the ITAAC is something that the licensee has to do.

MEMBER RAY: We're talking about inspection procedures, I believe.

MR. FREDETTE: Okay.

MEMBER RAY: And I'm asking why it is that nothing is said equivalent to what she just said.

MR. FREDETTE: In the actual ITAAC?

MEMBER RAY: Wherever you want to put it.

MEMBER STETKAR: No, in the inspection procedures. We don't care what ITAAC says.

MEMBER RAY: I don't care where you want to put it.

MS. LI: It says in the inspection report.

MR. FREDETTE: In the inspection procedure it does talk about this.

MEMBER RAY: It does?

MEMBER STETKAR: It does not.

MS. LI: Yes.

MR. Jackson: I'm sorry. This is Terry Jackson, I&C Branch Chief, NRO. And in the standard review plan, Section 14.3 which addresses ITAAC, it specifically talks about the phrase there about a report exists and concludes and what that means to the staff.

And during part of our review of the ITAAC during licensing we verify that the FSAR has that same understanding as in the SRP which is basically that it's not just the report exists but the report basically is consistent with what is in the Tier 2 information in the FSAR.

MR. FREDETTE: Sure.

MR. JACKSON: So then the inspection procedure, I think, points to some of the information you're going to use in the inspection is the FSAR itself which will then support that. Because this level of information here is basically a requirement. It's the regulation.

So to keep from putting a whole lot of

detail into the ITAAC --

MR. FREDETTE: Yes, I think, Terry, I think their question, though, is why doesn't the inspection procedure not go into the level of detail that, sort of paraphrasing what Renee basically talked about, in how we actually do the inspections.

And I believe that IP 65001.21, I mean, it --

MS. LI: Yes.

MR. FREDETTE: That inspection procedure has been vetted before. And if it, well, if it doesn't have that kind of detail that you're looking for we'll probably have to enhance it. But --

CHAIR BLEY: So you think it should be in the inspection proceedings?

MR. FREDETTE: Well, I --

CHAIR BLEY: I mean, you think it's there?

MR. FREDETTE: Yes, I think it's there.

CHAIR BLEY: Okay.

MR. FREDETTE: It's in the inspection proceedings.

MS. LI: Yes, because --

MEMBER RAY: Okay, but without trying to differentiate between the ITAAC and the inspection

procedure, maybe this is part of the problem I'm having, one would think that there would be some indication that not only something exists but that it was reviewed and found acceptable.

You're saying well, that latter part doesn't appear in the ITAAC but it does appear in the inspection proceedings.

MEMBER STETKAR: Let me give a specific example. And 21 is the one that I think gets closest to what we're asking about, of all the ones that I read in terms of an independent review of the technical elements, let's say, of the design rather than the process elements.

But the example I bring up only because I'm a risk assessment guy is there are many references in that particular procedure, 21, the pipe rupture hazard analyses, that use terms like review the as-design pipe rupture hazard analysis report to verify that each space containing structure systems and components important to safety is addressed.

You know, that's a technical review. That's not just confirmation that a box is checked off.

MEMBER RAY: That's a good point.

MEMBER STETKAR: So that's good. The

system selection criteria for inspection should consider risk significance, operating experience, new design, complexity of system transients and safety significance of the essential SSCs.

The inspector should review the design-appropriate risk insights document during the selection of essential SSCs and so forth. So those do point toward a more substantive technical review than simply confirmation that a document exists and it checks off the boxes.

One of the questions that I had is, to kind of probe the level of review. I focused on this risk significance stuff for two reasons.

One is that I don't know how that risk significance is determined, for example, because the design certification PRAs are, in many cases, simplified so that determination of risk significance based on PRA may have some relevance to risk significance after a more complete PRA is done.

Do the inspectors, now, supplemented by the staff, the headquarters staff, delve into those sort of interdisciplinary areas? In other words, do they question the fundamental basis for determining that this particular location in the plant is risk

significant and that other location is not risk significant?

Because that's part of what a more in-depth review would do. Not just accepting the fact that the applicant has identified this space as risk significant and now checking how you did the analysis within that constraint, but the more integrated analysis that sets the scope.

And one of the reasons I bring it up is because of the limitations of the design certification PRAs, as the plant progresses, by the time the fuel is loaded there will be a different PRA. I say different intentionally because it may build on the rudiments of what was created during the design certification.

But the scope and the level of detail is much more extensive so that by the time fuel is loaded in the plant there may be a very different picture of what is risk significant compared to the snapshot that you're taking today.

Now people, perhaps from the risk assessment branch might have some insights that could help you. But that's the type of sense that I'm trying to get from this, is how broad and how deep are these

reviews.

And, as I said, of all the procedures that I read, 21 is the one that comes closest to saying that the inspection needs to delve into those kind of details. So it's a good, yes, point.

MR. FREDETTE: Yes. Thanks for the question and the point, Mr. Stetkar. We've all had this discussion before. We had this discussion a lot when we were in the inspection planning process.

The inspection planning process is not a one or two-day effort. It's probably a six to eight-week effort as we lead up to each inspection. And we always try to pull in risk insights where they'll be helpful.

Now we rely on the engineering technical staff. But if there are other technical staff who are more expert in risk insights, PRA, other risk factors where we can use them to help us in the inspection planning process, we'll bring them in also.

They won't actually be in field inspection but they'll help us with planning and identifying our sample. So --

MEMBER STETKAR: Yes, I mean, that's essentially what I'm asking about --

MR. FREDETTE: Yes.

MEMBER STETKAR: -- is the scoping of the sampling process.

MR. FREDETTE: Yes.

MEMBER STETKAR: And the questioning of the applicant to have confidence that, indeed, the analyses that the applicant performed were, indeed, of the risk significant areas and not just a nominal subset of, you know, so-called safety related piping areas or something that's determined by some other --

MR. FREDETTE: No, we always --

MEMBER STETKAR: -- set of, you know, ASME piping standards criteria or --

MR. FREDETTE: Our sample always tries to bring in risk insights where possible. It's, we call it a risk-informed sample. Typically, inspectors in the field will use that term.

MEMBER STETKAR: Some, and kind of now that I've kind of led you into feeling good about yourself, I don't see any guidance in the inspection procedures that keys people, especially in these areas that use these terms, risk significant, important to safety, and they're used extensively throughout the procedures, that keys the inspection plan to reach out to these

other disciplines.

MR. FREDETTE: That's --

MEMBER STETKAR: I don't see anything that says, well, we need help in this particular area, not just people who understand piping but the risk assessment.

MR. FREDETTE: No, I understand. It's skill of the, I hate to use this term but I'm going to use it anyway, Skill of the craft. As trained inspectors know to look for risk insights, they know, inspectors in the field know that they have the entire agency backing them up.

And they can pull in expertise from just about anywhere within headquarters, with contractors --

MEMBER STETKAR: Yes.

MR. FREDETTE: -- with the labs. They're not limited. And they know that they're not limited.

MR. STETKAR: But knowing that I'm not limited and taking the initiative to bother a bunch of really busy people in areas that I feel confident in myself is one perspective.

Giving those inspectors direction to say you should reach out so that all inspectors, regardless

of which office they're sitting in or their own individual expertise or their own concept of their own knowledge is a different perspective. And --

MR. FREDETTE: Well, I --

MEMBER STETKAR: And in many other staff guidance that type of interdisciplinary guidance is given. When I look at the standard review plan, there's typically a section that says you need to engage people with the following disciplines when you do this review, outside of that specific narrow focus. I don't see that here.

MR. FREDETTE: Right. We --

MEMBER SCHULTZ: And here the general comments that John referred to earlier set that expectation, set that expectation that that engagement will, in fact, happen.

MR. FREDETTE: Well, I can assure you that the engagement does happen.

MEMBER SCHULTZ: All right, well --

MR. FREDETTE: We've had this discussion before and I sense that I'm going to be on the losing end of this battle. So what I'm going to do is we are going to, we need to enhance these procedures anyway.

So when we enhance them what we'll do is

we will make sure that we establish the direction that the inspectors would need to basically seek out the necessary insights that they need from the staff or from whatever resource they want to call upon so that 10 years from now, 15 years from now, inspectors know, and the direction is there and it's basically archived for us.

MEMBER STETKAR: That's right. There's two concerns. Obviously, we're expressing, or at least I'm -- we, I speak for me. I'm expressing my concern without the benefit of having any tangible inspection results other than the preliminary stuff that's been done on Digital I&C, which is primarily process oriented.

Perhaps if we had some of those inspection results, you know, they would, indeed, demonstrate the fact that all of this is implemented in the way you would see.

MR. FREDETTE: Right/

MEMBER STETKAR: So but that, again, as you just said, that might be today or next year or three years from now. It might not hold forth 10 years or 15 or 20 years in the future.

MR. FREDETTE: The Committee's brought

this concern up before. And, you, in particular, have brought it up before, Mr. Stetkar. You know, I don't want to battle --

MEMBER STETKAR: No.

MR. FREDETTE: -- over this. This is, it's not worth it. There are, the inspection manual contains hundreds of procedures. All of them could use enhancement of some sort or another. I mean, I don't have a copy of that procedure in front of me but I will, obviously, take your word for it.

MEMBER STETKAR: This one, it's the one when I read through them all --

MR. FREDETTE: No, but --

MEMBER STETKAR: -- came closest to looking at the technical stuff. But it still --

MR. FREDETTE: Risk. Risk insights are important. We, maybe because I've been an inspector for so long I know that, I know naturally what to do and how to plan an inspection. But we'll make sure that the direction gets incorporated.

CHAIR BLEY: Okay. Enough --

MEMBER STETKAR: One last little thing, Dennis. And I know that we need to move on.

CHAIR BLEY: That's okay. This

discussion was coming sometime or another, so --

MEMBER STETKAR: That's right. How do you, you know, in this inspection process, in practice now, let's presume that you have all of the disciplines involved.

How do you address the fact that if I were to do a piping inspection today or Digital I&C inspection or a human factors engineering inspection, all of which make reference to terms like risk significance, important to safety, those types of terms. How do you grapple with the fact that the metrics that you might be using are derived from something that is known, is certainly incomplete?

There's no, because none of the PRAs include, for example, an evaluation of seismic events. And most of them include very simplistic evaluations of shut-down modes and things like that.

So it's correct to say that they're not complete. The level of quality one can argue when you look at the details. But certainly metrics that are derived from a preliminary snapshot of risk developed for the purpose of Chapter 19 of the Design Certification, which is a very, very narrow focused purpose.

Yet you're doing inspections to give you assurance that the plant, as built, as operated, will meet our acceptance criteria.

MR. FREDETTE: That's right.

MEMBER STETKAR: And that's a pretty big burden, especially if you do these inspections rather soon after the COL is issued. If you do them very close to, prior to loading the fuel, you might have that more, that better developed risk assessment available to you.

But you can't afford to do that. You can't afford to wait until a year before a fuel load to close out everything.

MR. FREDETTE: Well, for areas like this, we try to do it early.

MEMBER STETKAR: Yes.

MR. FREDETTE: But we're using the best metrics and tools that we have available to us, recognizing that things may change later on.

But the inspection program will pick that up. In other words, once fuel is loaded inspection program doesn't stop. It continues on as an operating unit.

MEMBER STETKAR: Okay.

MR. FREDETTE: And the inspection program

will continue.

MEMBER STETKAR: Okay. That's fair.

MR. FREDETTE: Theresa Clark, who's the Branch Chief for the Mechanical Engineering Branch, has stepped to the microphone. Theresa, did you want to chime in on anything?

MS. CLARK: I don't know if I'm going to make this better or worse. This is Theresa Clark, Chief of Mechanical Engineering Branch and formerly of the Risk Assessment staff at NRO. So hopefully I can address a couple pieces of this.

MEMBER STETKAR: Theresa, because I'm behind the --

MS. CLARK: Sorry. I'll --

MEMBER STETKAR: -- column here. No, speak, speak into the microphone.

MS. CLARK: Okay.

MEMBER STETKAR: You'll come through.

MS. CLARK: You good?

MEMBER STETKAR: More or less.

MS. CLARK: I don't think I heard that. I don't know if it's turned on or --

MR. RAY: Smack it a couple times.

MS. LI: Speak into it.

MR. RAY: It's not --

MR. FREDETTE: Just speak up.

MEMBER STETKAR: Speak --

MS. CLARK: Sorry. Technical difficulties.

MEMBER STETKAR: -- like you were singing.

MS. CLARK: Better?

MR. FREDETTE: No, move it up so that you --

MEMBER STETKAR: There you go.

MS. CLARK: Better?

MS. LI: No, I think that you need to step up and talk into it from over there.

MR. FREDETTE: I'm not sure that was on.

MR. RAY: That was on before.

MS. CLARK: All right. Sorry about that.

MEMBER STETKAR: Much better.

MS. CLARK: All right, thank you. Just a couple of points that I was trying --

MEMBER STETKAR: You pulled the switch.

MS. CLARK: I'm not a microphone expert. A couple of points that I hope I can pay attention to from what I was listening to.

The first point I'd like to make is, yes,

I agree with the comments about the level of detail in the PRA and what's going to be updated later on and that sort of thing.

We, for example, the risk insights document that's referred to there was something we developed in about the 2007 time frame when we were still looking at the design certification. So the information in there is out of date or will be out of date by the time the plant is operating.

However, one of the important things that I think, and Renee can correct me when I get out of my DAC, is that these inspections, particularly in the piping area, while we look at the technical details and the procedures will say some very detailed thing about the details of what we expect to be in the report, it's a methodology inspection first and foremost to say did the licensee implement the methodology that the NRC certified in the design certification to say the piping analysis will be done this way, the pipe rupture hazards analysis will be done this way.

You know, we check and make sure it's not glaringly wrong as well because it would be unfortunate if we didn't do that. But we're making sure that the DAC, which is not just an ITAAC that you see in the

Table of ITAAC, it's all of the methodology that's described in the DCD. We're checking to make sure that that's implemented.

So the way that we do that, you know, you could call it risk informed. But it's unlikely that our sampling is going to go down to the sorts of systems that might swing between risk significant and not risk significant later on. It's possible.

But I'll give you an example. The piping procedure lays out particular lines that say you should look at these piping analyses packages. You should look at the pressurizer surge line because that's been a typically challenging thing to do a piping analysis of.

That's going to be challenging regardless of the outcome of the later risk assessment. So it's important that we include that in our sample.

There are a few Class 2 and Class 3 ASME code lines that are included. Those are probably going to come out as important regardless of the status of the risk assessment. You know, would a non-safety residual heat removal system go up a little bit if shut-down risks were included more? Maybe.

But the verification that the methodology

was used appropriately --

MEMBER STETKAR: Well, in terms of sampling, I understand this process but spending effort to look at the methodology for a particular pipe in a particular location is one part of the review. That's, for example, designing a pump.

Doing a more integrated review to make sure that people understand that they should do that analysis for a spectrum of piping sections is probably equally important in the overall integrated review. Because nobody has looked at that up to this point, have they?

Has anybody, during the staff, reviewed the pipe rupture hazard analysis from the perspective of did they appropriately identify the locations where they would then implement that detailed review that the piping inspectors -- or detailed analysis that the piping inspectors look at?

MS. CLARK: If I understand your question right, yes. During the DAC inspections we would be looking at, for example, a pipe rupture hazards analysis report that shows here's how we postulated where the pipe break locations are per whatever.

MEMBER STETKAR: Not the pipe break locations per section in this particular room, the

selections of rooms where I do that analysis.

MS. CLARK: Okay. And --

MEMBER STETKAR: Look at all of the piping. Conceptually, look at all of the pipe in the plant. Look at the risk assessment.

Identify first the risk significance systems and, therefore, the locations where those risk significance systems live and, therefore, the inventory of piping in those locations. And then do all of your detailed pipe rupture analysis.

MS. CLARK: Yes, and --

MEMBER STETKAR: Has anybody reviewed that at any point?

MS. CLARK: For the selection, again, sorry if I --

MEMBER STETKAR: For the selection.

MS. CLARK: -- have any misunderstanding. For the selection of which samples we inspect.

MEMBER STETKAR: No, no, no.

MS. CLARK: No?

MEMBER STETKAR: No. Not the selection of which samples, the fundamental process. And applicant presents to you a report and said I did a pipe rupture hazard analysis for the following pipe

sections in the following locations because I think that these are important pipe sections.

And I think these are important locations because if a pipe breaks in this room I'm going to have, it's going to be a bad day for the pumps and the valves and the electronics that live in this room.

Who and when reviews the because part of this? I understand how you may select piping sections for your sampling process for the piping review. I understand how you walk through the process of how they did an analysis for the particular piping section.

MS. CLARK: Okay, now I think I understand you. And I'd like Renee to correct me when I misspeak here if, I misspeak, is that I'm pretty that they don't analyze a subset of them. They analyze all of the spaces that include high-energy and moderate-energy line piping. Is that correct, Renee? Oh, and then we would inspect the subset of them.

MS. LI: It's on now?

MS. CLARK: Right. There we go.

MS. LI: Okay, the review process is as far as where to calculate pipe breaks or pipe length is described in SRP 3.6.2. And the approach is, we call it mechanistic approach that basically there are

two criteria.

One is the stress criteria, one is the fatigue usage factor. So using those guidelines the DCD described where would be the break location using those guidelines. So the break location, actually, would be determined first.

And then, for each postulated break location what the applicant need to do is identify all the nearby safety-related equipment. And then determine whether, if it's in case of jet impingement, they either construct a jet shear or they design that particular piping or component to accommodate the load from the break.

And as far as the ruptured pipe, they will have to design a pipe restraint to stop the pipe whipping. So all this information gets into the PRHA report.

CHAIR BLEY: Renee, I think that's good. The question was aimed a little differently.

MEMBER STETKAR: Let me try -- sorry, let me try something that --

CHAIR BLEY: Just, you get one more minute.

MEMBER STETKAR: Okay.

CHAIR BLEY: And then we move on.

MEMBER STETKAR: Something you said, and this dovetails with my concern. So let's presume that they look at every moderate and high-energy pipe regardless of where it is in the plant.

You said you look at effects on safety-related equipment. And the guidance in your procedures say things like risk significant, important to safety, those types of words. So that if you're, and believe me, in the AP-1000 plant there isn't a heck of a lot of safety-related equipment anywhere, safety-related.

There's a heck of a lot of risk significant equipment. So if you're only focusing your review on effects on safety-related equipment you're not doing an integrated review. And that's, rather than approaching it from space point I'll approach it from the equipment.

MEMBER RAY: Dennis, there's one thing I want to say and then I'll --

MEMBER STETKAR: Go ahead, Harold.

MEMBER RAY: -- continue being quiet. Is there anything, Renee, that you just described that is different than the review you would do under Part 50 at the OL stage?

MS. LI: Okay, the review --

MEMBER STETKAR: Open the mic.

MS. LI: The review is same as far as the content. But in Part 52 that during the design certification stage we will only review the methodology if that is proposed because the detailed calculation won't be there if we review the --

MR. RAY: No, I'm talking about the stage, the end stage that we're talking about here when we're implementing these inspection procedures. And you described very thoroughly the review that would be done then.

I'm just asking is there anything different between that review that you're doing in accordance with these inspection procedures and a Part 50 OL review that would be done?

MS. LI: It's same.

MR. RAY: The same? All right.

MS. LI: It's just different timing.

MR. RAY: Okay. That's all I wanted to hear because that certainly isn't the impression that I get when I read this stuff. But I believe I you, and that makes it fine.

CHAIR BLEY: Okay. You're back and you've

just barely begun. But I think you'll go faster now.

MR. FREDETTE: No, in the past, when we've talked about piping and PRHA we've sort of blown through a lot of this --

CHAIR BLEY: Yes.

MR. FREDETTE: -- quickly. We appreciate the questions. And if there are holes or gaps within the inspection procedure we will, our intent is address them.

Hopefully we'll get a chance to actually use the procedures in the field and actually have some tangible results to report next time that will sort of maybe address some of the concerns that the Committee has.

CHAIR BLEY: We look forward to that. And the way Harold just expressed that is it begs our concern. And it's a comforting answer, and we hope, when we see the actual inspections we're, we agree. Go ahead, Tom.

MR. FREDETTE: I want to thank Theresa and Renee for basically bringing their expertise to bear the answers to some of those questions because they're beyond my area of expertise.

Theresa sort of stole my thunder here.

The DAC inspection objective for piping, basically we were going to, our intent is to verify that the methodology for pipe design and the methodology for PRHA basically conforms to the licensing basis.

For piping packages, there in the DCD, there is a list of all the piping packages that were intended to basically satisfy the pipe design DAC requirement. There are 13 Class 1 and 35 Class 2 and 3 code piping packages in the DCD.

Basically, that would be the sample from which inspectors would select which piping package they would look at. Theresa mentioned the pressurizer surge line which has historically been a problem area. We had intended that we'd have a chance to look at piping packages by now.

But the inspection process, we're basically going to wait and look at some Class 1 packages when they become available. These are some highlights from the tabletop exercise we did two years ago.

This was a public meeting in July of 2012 where we basically tabletopped and walked through the inspection procedures and the process with both Westinghouse and the AP-1000 licensees. At that time we used an actual Class 2 package from the Passive Core

Cooling system.

We outlined our inspection framework and we outlined all the attributes that inspectors would choose from which are outlined in DCD Table 3.9-19.

And then Renee has talked about this, but the procedure for PRHA basically reflects on DCD Section 3.6 which talks about dynamic environmental effects of pipe break, the pipe break cracks, breaks or cracks, and their type and location, leak-before-break, et cetera.

We anticipate that our actual availability for some of the Class 2 and 3, our Class 1 packages, will be later this year. We're going to wait until the Class 1 packages become available before we actually do an inspection.

We're always looking to align our inspection resources in accordance with the actual availability schedule for those packages. The AP-1000 licensees have license conditions, basically to notify us when piping packages become available before they actually do installation.

So it's up to us to basically be ready to go in and look at those pipe packages before they actually do any work.

CHAIR BLEY: Before the hard --

MR. FREDETTE: Before they're actually installed. It's incumbent upon us basically to be aware with those notifications and basically marshal the resources as necessary and put an inspection together.

And that concludes my presentation with regard to piping and DAC. I took an action item here. It's basically to address Mr. Stetkar's concern that the procedures don't provide the necessary direction for inspectors with regard to some of the other tools that they should bring to bear when doing an inspection planning, specifically, risk insights, PRA tools, other metrics and that type.

So, as I mentioned --

MEMBER STETKAR: I think it's like the Standard Review Plan. Typically, in a lot of sections, it says, well, to perform this review you may need to use resources from these other --

MR. FREDETTE: No, I understand.

MEMBER STETKAR: Or something on that line.

(Off microphone conversation)

MR. FREDETTE: Like, I said, it's not worth

battling over. We want to enhance the procedures any way we can. So that's one that we'll certainly address. And next time we come and report to the Committee, hopefully we'll have that procedure, an enhanced procedure in place.

MEMBER CORRADINI: Can I ask a different question?

MR. FREDETTE: Yes.

MEMBER CORRADINI: I'm trying to figure out how you do your job with all these procedures, I wonder. So, long ago, when you were doing inspections at these 1st generation of plants were the procedures this complex? Because I'm going somewhere with this. I'm curious about --

MR. FREDETTE: I can only speak to certain areas of procedures. Specifically --

MEMBER CORRADINI: But, as an inspector, my question really comes down to, my impression is, in looking through the background we were given much more complex in your procedures.

But I'm kind of curious in terms of how the inspectors are trained and how they go about doing what they need to do to look at, like, a new plant construction. Has is really changed and, if so, what

are the most important changes that have come about?

Do you know what I'm trying to get at? I'm trying to understand --

MR. FREDETTE: Well, they get, as the new plants have come along, we're in Part 52 space here which is a little different from the typical inspection environment.

MEMBER CORRADINI: Well, the only reason I linked it is because he asked, Harold asked a question and I was comforted by the fact that substantively you'd look at it as if it were a 50 OL compared to a ITAAC and DAC 52, which made me feel like, okay, then we really have some sort of historical connection.

So then my next question is the how you do it and what things have improved and --

MR. FREDETTE: As an inspector, I do my job the same for Part 52 and I do for a Part 50.

MEMBER CORRADINI: Okay.

MR. FREDETTE: The inspection planning process is generally the same. Bringing ITAAC into the fold is a nuance.

MEMBER CORRADINI: Right.

MEMBER RAY: Can I respond to Mike this way? In Part 50 the OL review isn't part of the

inspection process that Tom's talking about right now.

MEMBER CORRADINI: Oh.

MEMBER RAY: The inspection process, it's very important it takes place. But the OL review is an OL review. Now they're embedded.

MEMBER CORRADINI: Oh, they're folded together?

MR. FREDETTE: They're, well, ITAAC forces us to fold them together.

MEMBER RAY: Right, yes. And the question that ultimately we're concerned about is the judgment that takes place during a Part 50 OL review. Has it been eliminated and replaced by DAC? That's the question.

MEMBER CORRADINI: Yes, yes.

MEMBER RAY: And because nobody, and I was on the other side of the table when this was all created some time ago, but nobody ever imagined that DAC could substitute, written down design acceptance criteria, could substitute entirely for the exercise of judgment in the review that would take place at the OL stage under Part 50.

So we're dealing with something that isn't, it isn't something that is an unknown, as you've said

many times. It's been an issue that we've talked about repeatedly.

MR. FREDETTE: That's one reason why we bring the technical staff. We sort of bring them into the fold --

MEMBER RAY: Exactly. And we're trying to understand how you do that and, et cetera.

MR. FREDETTE: Okay.

MEMBER RAY: So --

MEMBER CORRADINI: But I guess what you're saying is what I was expecting, which is that the complication is that you're folding them together. And it's how you fold them together, not that, substantively, you don't do the same sort of review?

MEMBER RAY: Well, the danger is that you eliminate something and you only have an inspection. Dennis outlined that in the beginning. I don't want to repeat it.

MEMBER CORRADINI: Right.

MEMBER RAY: That, we're being told, isn't the case. And that's why we're having this discussion.

MR. FREDETTE: You know, we've only completed, in strictly speaking of DAC terms, we've only completed one inspection that really has looked

at DAC. And that's in Digital I&C. We'll talk about that a little bit later.

MEMBER CORRADINI: Okay. All right, thank you.

CHAIR BLEY: We had scheduled a break at this point. But I think, since we're going to 12:30, we'll let you go about a half an hour until we find a decent place to break.

MR. FREDETTE: Okay.

CHAIR BLEY: And then we'll take a break, around ten.

MR. FREDETTE: Okay. We're going to shift gears and we're going to talk about the other major DAC discipline, another major DAC discipline, and that's Digitial I&C.

As you mentioned in your opening remarks, Dennis, this was the real primary focus of the DAC Working Group that was formed back in 2009. Our efforts at that time were to basically establish a process and a framework to do a DAC inspection.

And our pilot effort in that regard was with South Texas Project. We completed that pilot inspection in 2010. We've shifted our focus to AP-1000 in 2011.

We had our first meetings with the AP-1000, at that time they were applicants, in October of 2011. The AP-1000 Digital I&C design includes one design acceptance criteria. It's the protection and safety monitoring system component interface module, which is a subassembly of the PMS.

And we were looking at the CIM planning, life cycle planning phase activities. The working group had written an inspection procedure, a generic inspection procedure, IP 65001.22, which we issued in 2011. This is a generic procedure basically intended to look at any design efforts using any typical Digital I&C system or software life cycle process.

The procedure borrows from guidance that's established in the SRP, all the industry standards, NUREGs, staff expertise. It generally mirrors an I&C development life cycle. There's guidance for sampling of life cycle attributes and design outputs.

And then our focus is on process, configuration management, verification validation, traceability throughout all elements of the life cycle. The procedure is front-loaded.

We typically would provide more effort in the inspection process in the planning and requirements

phases. It's not saying that we won't also have suitable inspection resources when they get to integration and testing.

We conduct inspections for each safety-related I&C platform at various development milestones. We rely on early and continuous engagement with the licensees and their design agent, Westinghouse, for optimum deployment of our inspection resources.

Our resources are limited. As everyone knows, an NRC inspection relies on, in the Digital I&C area we rely on two things. We rely on the fact that licensees are going to take a rigorous approach to development in this area and they'll have a robust V&V process.

MEMBER STETKAR: Tom, since you mentioned resources I wasn't, we don't normally get involved in that. But in the Digital I&C inspection procedure there's a resource estimate. And the estimate is 660 person hours. That's to review all of the Digital I&C.

That, to me, I can spend 660 hours here muttering about nothing, as you well know. That, to me, sounds to be either a woefully low estimate or it's indicative of the fact that this is, indeed, a fairly

process-oriented review.

MR. FREDETTE: Yes, your first instinct was correct.

MEMBER STETKAR: Okay.

MR. FREDETTE: It's a woefully low estimate.

MEMBER STETKAR: Okay, that's what I was hoping because the second question was how much time have you spent so far on what you've done.

MR. FREDETTE: A lot.

MEMBER STETKAR: Okay. Okay.

MR. FREDETTE: Later on I'll talk about some of the lessons learned.

MEMBER STETKAR: Okay. That's fine, thanks. Thanks.

MR. FREDETTE: When I had mentioned earlier that there are a lot of procedures that always need enhancement, well, that's one of them.

MEMBER STETKAR: Yes.

MEMBER BROWN: I would argue that it's not just -- what were your two points? It's woefully low, to which you said yes?

MR. FREDETTE: Yes.

MEMBER BROWN: And the other point that

it's process-oriented.

MEMBER STETKAR: Well, but I mean if --

MEMBER BROWN: It is process-oriented. That's why our big emphasis in our recent, you know, was that we've learned is we've got to focus on these new designs on the architecture type aspects which don't get brought out in the process reviews.

I mean, it's all that a guy, you know, that they developed the software okay. Did they do this okay, did they do that okay. And that's what the inspectors look at, and the V&V that they go through.

That's all process. They cannot do code reviews. They cannot do verification, that code comments are verified. They can't go through and see that, did they actually execute code functions properly. They can't do that. They do not have the staff to do that.

And that's why the architectural focus that we've tried to provide is far more important now. You used to get that in the old Part 50 world when you did stuff because you got the design upfront. Here you don't. Here you get a bunch of blocks and then the process says okay, I've filled in the blocks properly.

So I think this DAC aspect is far, it just

doesn't accomplish anything from the architectural point. If I had to go do DAC again, based on since we did this four years ago or five years ago, whatever it is, I would have tried to incorporate some type of DAC that focuses on the overall architectural functionality that was done at some stage of the thing.

But it's, you know, we're passed that now. So I just wanted to get that point out on the table for people to understand that if we, if we, it was brought to us for a review I think you would find the focus and emphasis would be a lot different from my perspective, not necessarily, I can't speak for the Committee.

I can only speak for myself in that circumstance. So, anyway, I'm sorry. I didn't --

MEMBER SCHULTZ: This diagram shows that the DAC process is I don't know if this is ideal or, Tom, is this the way it worked?

MR. FREDETTE: This is --

MEMBER SCHULTZ: But the way you're showing it --

MR. FREDETTE: This is a notional diagram. Okay, this is --

MEMBER SCHULTZ: Okay, because it seems

to reflect what Charlie said should happen. And the question is it happening or is it --

MR. FREDETTE: Well, this would be --

MEMBER SCHULTZ: -- developing sufficiently?

MR. FREDETTE: This would be our intent, if DAC carried through other phases of a typical system life cycle. This was the strategy that we would have employed for ABWR and South Texas.

MEMBER SCHULTZ: Mm-hmm.

MR. FREDETTE: And what we would have, what we'll employ for future designs if they, in fact, do come in with a lot of DAC. The ESBER design has a sizable number of DAC ITAAC. And that carried all the way through to the validation testing and installation. And this is the kind of diagram that we would employ, okay?

CHAIR BLEY: Let me ask you a question. Now Charlie just gave a speech that I mostly agree with, but not 100 percent. The left five blocks on your diagram are process over and after. So that's the design process and the testing process and all that.

When we get to installation, after that, we've got a real design that's going in the plant.

MR. FREDETTE: That's right.

CHAIR BLEY: The DAC inspection that occurs at that point, I think there is one or would be --

MR. FREDETTE: It would be.

CHAIR BLEY: -- if the design were complete.

MR. FREDETTE: It would be for installation, yes.

CHAIR BLEY: That's the one that I would hope we could hear something like we heard from Renee about the piping DAC, that, in fact, at that point, once that inspection's done, we would be where we would have been with the Part 50.

MR. FREDETTE: That's the intent.

MEMBER BROWN: The same, I'm going to disagree slightly with Dennis because --

CHAIR BLEY: I would expect no less.

MEMBER BROWN: Because I think once you get passed those five boxes, okay --

CHAIR BLEY: It's perfect by definition.

MEMBER BROWN: Yes, well at that point you're verifying people who hook up the wires right, if the cabinets are in the right place. But they're

not verifying some fundamental overall architectural view of the thing, COL issued, over there on the left, that little yellow dot.

That's all done, if you don't get that before you're not going to get that out of this. You cannot change that architecture. That says I've got the vendor's design. Now, when I put it together with all the wires and all the connections and all that other kind of stuff --

MEMBER STETKAR: In some sense it's at least one box back on the validation and testing because that's part of that process. But it comes back to a lot of the requirements phase, but not, the documentation specifies the requirements. It is, from a technical perspective, are the requirements specified appropriately.

So not reviewing that I have a software requirement specification and that I've referenced the appropriate IEEE standards and reg guides and all that kind of stuff in the specifications, but does it make sense from a design.

MEMBER BROWN: Yes, but you're, fundamentally, before that yellow dot, you've got to say do I need independence? For instance, does the

functional architecture do that? Now you get out here and during that process you should be seeing does the architecture meet that. That's got to be already agreed to upfront B

CHAIR BLEY: No --

MEMBER BROWN: In the DCD.

CHAIR BLEY: That's right.

MEMBER BROWN: And that's missing right now, relative to our DAC, the focus we placed on DAC, in ESBER or even some of the AP-1000 or what have you.

MEMBER STETKAR: That's right, in those two particular instances.

MEMBER BROWN: Now, am I bent out of shape about that whole thing? Yes, a little bit, but just didn't know it. But it's in the DCD. It's in the DCD and I suspect that the staff will pay attention to that. You've got to have some confidence.

MR. JACKSON: This is Terry Jackson. And I think the slide, and actually Tom's further slide will probably clarify a little bit more, and I'm talking specifically about AP-1000. The DAC inspection is really just associated with the planning phase.

The other phases are ITAAC inspection. And the reason I say that is because when you get into

requirement specifications this is not just automatically standard. There's probably 10,000 plus requirements for the reactor protection system for AP-1000.

And so the staff is going to go in, when they do an inspection, and sample those because there's no way we can inspect every single one of those. It's the same thing with design implementation. When you get to that stage it's actually code. So the inspection staff is going to look at the code.

We haven't gotten to that stage yet. We haven't performed those inspections at this time. We have looked at requirements and I think we did, we did find some process issues which I think were troubling to the staff because they had, the licensee had committed to do, to develop the software a certain way. And Tom's probably going to explain those findings.

But we did find some, I would call them project issues where there some missing requirements as well. So the planning, you have the planning phase today is more process oriented.

But I would say that what was done on the one DAC inspection that was performed is consistent with what we did on the comparable license review as

well. So it was more process oriented.

And maybe to go to Charlie's issue about the architecture, yes, in the license review we do try to focus on those architectural issues so that when it comes to an inspection then, really, it's just verifying that the architecture is set up the way it is.

But they, I don't think that we necessarily have any, at least high-level, architectural requirements that the inspection staff needs to be able to address or determine its adequacy. That should be determined in the DCD.

MEMBER STETKAR: But, Terry, you said during the license review. And I'm assuming by that you mean the review that's done for the DCD, that you look at that architecture.

In the couple of instances that we're familiar with the level of information that's available, at least the stuff we've seen, it's really, really difficult. You could put that level of information at a very high level and build anything under it because it just specifies very generic criteria.

Some place between there and the lines of

code and the actual configuration of each card that you slide into a slot in the cabinet, which, obviously, are things that can be sampled and inspected, is how the general very high level stuff is implemented and practiced.

And where is that level of review done? Not from a programmatic sense that, yes, indeed, you have a software requirement specification and you have some general hardware design specification and there's some general integration specification but an actual engineering review as would be done, as Harold has mentioned, in a Part 50 type review to say that, indeed, the design as, I don't want to use the word conceived, as it will be developed, satisfies those high level requirements.

Because you couldn't do that at the design certification statement. You could just say yes, indeed, it seems like they specified the high level requirements, okay.

MR. JACKSON: Yes, and I think some of those things, like, for example, if you have to look at the, say, a hardware diagram or something of the circuit board or if you had to look at the software code, then, yes, that would be something that would

fall under the inspection.

MEMBER STETKAR: But we're asking when in this process because you said you're front-end loading it. I'm stealing some of your thunder here. You're front-end loading it and admitting that a lot of that is process related.

And then in the back-end, because it's simply inspections, you're just sampling to say well, we'll take a look at a sample of code and make sure that it was written according to the specification and we'll take a sample of the hardware and make sure that it was, indeed, wired together correctly.

Where is that real technical meat of the review done?

MR. JACKSON: That's basically done --

MEMBER STETKAR: Yes, on this slide.

MR. JACKSON: -- on that slide there. It would begin at requirements.

MEMBER STETKAR: Okay.

MR. JACKSON: But it would get heavier and more involved in the design and implementation --

MEMBER STETKAR: Okay.

MR. JACKSON: -- the integration.

MEMBER STETKAR: Okay.

MEMBER JACKSON: And then the testing should be, there should be tests to verify this --

MEMBER STETKAR: But, as Charlie mentioned, at that point it's starting to get pretty late in the design --

MEMBER BROWN: Yes.

MEMBER STETKAR: -- to make any substantive changes.

MEMBER BROWN: To your point, if you've got the architecture specified upfront you would look where in that line? Does somebody say, okay, here's the design that he's taken. Does the way he interconnects the card.

Don't look at the design of the card or the design of the software. It's how does the design match up with that architecture that we have specified, that was specified prior to the --

MEMBER STETKAR: Yes, is anything missing or is there some extra junk in there?

MEMBER BROWN: Yes, but they've done something there that crosses the line.

CHAIR BLEY: There's one thing we ought to say to be fair. We refer back to Part 50 OL. Hence, we have never done a Part 50 OL on one of these complex,

highly integrated digital systems so we don't know what that would have been.

(Simultaneously speaking)

MEMBER STETKAR: Right, trying to do it with some relay technology.

CHAIR BLEY: Yes, I mean, if you've written it in analogue and relays we'd know how you do it. But if you were doing it here we're kind of, you'd have to be inventing a similar process to do that.

MEMBER STETKAR: The only reason I ask is I wanted to sort of get my mind oriented, and Terry's discussion helped, about where in this process I would expect to see more of that review come in and use that as a gauge when Tom talks about what they've done so far to see where they are on this line.

MEMBER BROWN: Let me just, one, Terry, let me give one example, an AP-1000. No, it was ESBER. I'm sorry. That's where there's a lot of DAC.

MR. JACKSON: That's right.

MEMBER BROWN: Okay, I had a little subsequent discussion with the I&C guy, Butler, yesterday after they went through their shafafa.

Because it took us two years to get into the DCD, all right, the functional architectural layout

plus a, call it what you want, a processor monitoring, watch it all the time or whatever you call it, that actually executes if it locks up a trip in a particular channel.

You would expect now in this DAC process or wherever it falls that somebody would say, okay, now that's what's in the DCD, how does this design actually execute? That's a high level review, okay, of saying did they compromise that as part of their development of the hardware and the software to perform that?

If the hardware function monitor is a separate unit it executes a trip with its own software. It's not controlled by -- hardware, excuse me. It doesn't have any software that sets it up operationally or for functionality in terms of its trip.

Those are the types of things that I'm worried about, after the DAC aspect of this thing, particularly on the ESBER. Now we have a lot of words in the DCD that they incorporated. They developed those words. We didn't do that. They developed, brought them back, and they were pretty descent.

AP-1000 has a nice functionality laid out. So I just, my point is how, I keep hearing process.

But I'm looking for specifics --

MR. JACKSON: On DAC --

MEMBER BROWN: -- on this architectural -- that's not a process issue. That's making sure the process has delivered what's specified in the DCD.

CHAIR BLEY: And I think we've just hit the guts of that. I think jumping to this was good. This has us set up.

MR. FREDETTE: It wasn't on ten, but --

CHAIR BLEY: But I'm going to call a recess now. And the only one that doesn't get a complete recess is Tom because you've got to finish by 11:30 because we have a separate meeting that starts at 12:30 so we have to wrap everything up by then.

I know we're going to be especially interested in results and corrective actions and your plans for the future. We're going to recess for now until 10 after 10:00. At this point, the meeting is in recess.

(Whereupon, the foregoing matter went off the record at 9:55 a.m. and went back on the record at 10:10 a.m.)

CHAIR BLEY: The meeting will come to order. Tom, you're back on.

MR. FREDETTE: Yes, sir. Thanks, Dennis. I think we've, my intent in putting this slide up was just basically to give everybody sort of historical perspective of what our approach was in mirroring a typical life cycle.

It does not fit well with what we've done for DAC inspection and AP-1000. Dennis, over the past couple of years, we've become aware that the Committee has been interested in what kind of inspection expertise we've been able to bring to bear in these type of inspections.

And this is sort of a profile of our core inspection team. This is not everybody, but these are the core people who have been involved in every inspection since we started.

The lead Region II inspector is an industry V&V expert formerly employed by AREVA, involved in a lot of different upgrades in the Digital I&C arena, including the Oconee RPS/ESFAS project, author of various planning documents for some of those software upgrades and failure modes and effects analysis.

The Region II, the real Region II expert is a 20-year industrial automation professional experienced in a lot of different distributive control

system and PLC platforms and man/machine interfaces and an experienced code review type person who can look at C++, visual C++, things like that.

Our technical staff expert who we brought in from the tech staff was a former employee of Terry Jackson's, 20-year experience with development and design installation validation programs and he was the lead reviewer for the AP-1000 design. He also sits on the IEEE Standard 1012 Working Group.

As you know, a lot of things happened between Rev 15 to Rev 17 to Rev 19 of the AP-1000 DCD, a lot of it very convoluted with regard to how Digital I&C evolved.

This technical staff expert was there for all of it and was basically able to give the staff, the inspection staff, all the insights needed as to how things were done by Westinghouse, by some of Westinghouse's sub-suppliers with regard to the AP-1000 I&C platforms.

We had the opportunity back in April of 2012 to validate our inspection process in a real ITAAC inspection. This was the inspection conducted for the PMS life cycle requirement space and some of the high level planning documents which include the software

management plan for PMS, the configuration management plan and the V&V plan.

These were ITAACs 2.5.2.11.bravo and 2.5.2.12. The inspection scope here was the requirements phase design output which is basically the software requirement specification for the PMS.

We did a sampling of the PMS reactor trip and ESFAS signals to do traceability and vertical-slice looks at the functional requirements. And then we looked at independent V&V result and then basically, overall compliance with the AP-1000 licensing basis.

I should point out here, and I don't have a slide that talks to this, but our sampling of the reactor trip and ESFAS signals was risk informed. We brought in the PRA expert from Region II at the time to basically identify some of the reactor trip and ESFAS signals that carried the most risk weight from a preliminary PRA standpoint. And that's how we developed, basically, the sample we were going to look at.

The inspection part here highlights our inspection results. There was a notice of violation that came out from this inspection in the area of design control which was Criterion 3 of Appendix B.

Basically, detailed some deficiencies in the IV&V tasks that were not performed for the software requirements DAC.

There was no independent verification and validation. It's supposed to be independent. In this case, Westinghouse was taking credit for some design activities as part of their V&V which was a pretty significant issue.

They did not do software hazard analysis for the software requirements DAC. The life cycle basically prescribes that they'll do a software hazard analysis at each phase.

There were some custom software elements that were basically outside the V&V process, custom software things like reusable software that they would use for different applications, like pressurizer density compensation, pressurizer level density compensation.

Some of the more complex algorithms which they've used in the past, for instance, the reactor trip setpoint for overpower or over-temperature Delta T. Those were basically outside the mainstream process for V&V. They were in their own little process. So they were given a violation for that also.

And then, finally, their software requirements specialist was basically incomplete. There's some requirements and licensing, basically that their software will be fully complete. In this case, they had a couple of requirements that were not identified or not detailed enough in the software requirements spec, things like recovery from a loss of power to the system and a couple other miscellaneous requirements that we identified.

CHAIR BLEY: So in this inspection process the notice of violation is to the utility to the licensee, even though they may be vendor oriented or would have been focused on the vendor if there had been a design original?

MR. FREDETTE: Yes, and you bring up a good point, Dennis. This being our first inspection opportunity with AP-1000, we did this against the Vogtle docket.

CHAIR BLEY: Mm-hmm.

MR. FREDETTE: So it was an inspection of Vogtle's ITAAC. In the subsequent couple of years since that inspection we basically have rolled the inspection effort over into the vendor arena.

Because all the activity is being done at

Westinghouse and if fit better as a vendor inspection. So the subsequent DAC inspection, and actually every inspection in this area going forward will be a vendor type inspection.

MEMBER STETKAR: So that explains the 2014 non-conformances at Westinghouse.

MR. FREDETTE: At Westinghouse.

MEMBER STETKAR: Okay. Okay.

MR. FREDETTE: Yes, you're getting a little ahead of me here, Mr. Stetkar but --

MEMBER STETKAR: Okay.

MR. FREDETTE: Yes, what you'll see in the future is notices of non-conformance written against Westinghouse as opposed to a notice of violation against Vogtle's docket.

CHAIR BLEY: Just for the regulatory side of it, which isn't our real focus but it's a curiosity for me, is that some kind of agreement among the licensee, NRC and Westinghouse or?

MR. FREDETTE: No, it was basically us taking a step back.

CHAIR BLEY: Mm-hmm.

MR. FREDETTE: Us, in the staff, taking a step back and saying what's the best fit --

CHAIR BLEY: Okay.

MR. FREDETTE: -- for these types of inspections. Since Westinghouse is doing all the development work and the licensees really haven't taken ownership of the system yet, it's, the best fit was for us to do this as a vendor inspection.

CHAIR BLEY: Okay.

MR. FREDETTE: That's another lesson learned.

CHAIR BLEY: I just didn't know how that really works.

MR. FREDETTE: Yes, that's --

CHAIR BLEY: That makes a lot of sense to me. I didn't know you could do that, so.

MR. FREDETTE: Yes, we learned, that was just a lesson learned, okay. In this particular case, since this is --

CHAIR BLEY: So that was a broad thing if it's not yet belonging to the plant, it makes sense to do the inspection where the, where there is ownership.

MR. FREDETTE: That's correct.

CHAIR BLEY: Yes, okay.

MR. FREDETTE: Now we'll think back to

piping --

CHAIR BLEY: Yes.

MR. FREDETTE: -- piping DAC for just a moment. Since licensees have taken ownership of those piping packages --

CHAIR BLEY: Right, they give you the package, yes.

MR. FREDETTE: -- they actually have the packages and they've reviewed them. And they are now the owner --

CHAIR BLEY: Owner, okay.

MR. FREDETTE: -- of those packages. So those inspections would revert back to typical ITAAC inspections.

MEMBER STETKAR: Okay. HFE, more vendor or more --

MR. FREDETTE: HFE is more vendor also.

CHAIR BLEY: Is it really? Okay. That's interesting.

MR. BROWN: Since I was a little late coming back, I kind of would have expected that you all would be doing this at the vendor, not with the COL. I mean, that just never made sense to me. I didn't even think about it in that sense.

MR. FREDETTE: We just did --

MR. BROWN: I mean, that's what you're all now doing. You're --

MR. FREDETTE: Yes.

MR. BROWN: Is that 2going to be kind of your game plan?

MR. FREDETTE: That's our game plan going forward.

MR. BROWN: Going forward?

MR. FREDETTE: That's right. This was our first time out of the box for AP-1000 and we hadn't, you know, the Construction, Inspection and Operational Programs Division really hadn't thought through how best to conduct these inspections.

So, at the time, it looked like we would do inspections of both licensees together. Well, Vogtle basically took the brunt of this particular inspection. And they took the onus of all the corrective action stemming from this inspection also.

MR. BROWN: So what, let me ask one other question related to that. I presume you still would be executing an inspection or an evaluation of the licensee's oversight of what he should be -- I mean, he should be doing that himself.

MR. FREDETTE: That's right.

MR. BROWN: And while you all should be hoping that they're doing their job, you're also checking at the vendor level as well to make sure that they are performing in accordance with the requirements?

MR. FREDETTE: Yes, and when we talk about the corrective actions here in a minute we'll go through some of the gaps that existed between Westinghouse's philosophy and Westinghouse's perspective and what the licensing basis really called for, so.

MEMBER STETKAR: Tom, one last question. And this is, probably not the last question, but how much outreach does the staff do with other vendors, other design centers to communicate what you're doing and how you're doing it and what you're finding in these inspections so that we don't have the same process when you do the ESBER DAC or when you do the ITAAC inspections for the active plants that have less DAC, for example?

MR. FREDETTE: The answer's --

MEMBER STETKAR: Because a lot of this stuff is proprietary, is the problem. I mean, you can't share the details.

MR. FREDETTE: Not the details, but the

overarching stuff we do share with, and we do have a lot of outreach --

MEMBER STETKAR: Okay.

MR. FREDETTE: -- that goes on. We have public meetings approximately every two months or so with all the design centers. The ESBER design center is very well represented. Skip Butler's at some of those meetings. And there are other design centers involved.

MEMBER STETKAR: Good.

MR. FREDETTE: Since most of the work is AP-1000 we tend to gear our focus and path forward and future activities with regard to what AP-1000's doing. But the other design centers are involved.

MEMBER STETKAR: Good. But the only point is I hope they're learning because you don't want to have to --

MR. FREDETTE: I hope so.

MEMBER STETKAR: -- a similar experience. Thanks.

MR. FREDETTE: Okay, so as a result of this first inspection there was some pretty extensive corrective action that stemmed from this. And --

MR. BROWN: Can I backtrack for just a

second?

MR. FREDETTE: Certainly.

MR. BROWN: I'm sorry.

MR. FREDETTE: No.

MR. BROWN: But go back to Slide 18 for a minute. Relative to my discussion earlier, before we broke, I would have viewed your second bullet where you talk about traceability of system signals, functional requirements, that that would, you would then take your cue back from the DCD and the architectures and things like that. Is that a valid assumption?

MR. FREDETTE: That's a valid assumption. Yes, sir.

MR. BROWN: So you would, that's where you would bring in the, I'll say it again, bring in the did they meet the functional architectural requirements --

MR. FREDETTE: Yes, sir.

MR. BROWN: -- that are shown and are those specified as requirements in their development of their requirement schedules?

MR. FREDETTE: Yes, that's exactly right. And we go all the way back to reactor safety

requirements, regulatory requirements and then specific system or plant requirements. And we trace those all the way through.

MEMBER STETKAR: One of the examples someone brought up, and I don't know whether you're here, is they identified a problem with, the requirements were deficient --

MR. BROWN: I missed that, so --

MEMBER STETKAR: -- in terms of identifying the requirements for loss of power and re-powering the system. So that's a real --

MR. BROWN: Yes.

MEMBER STETKAR: That's a real engineering type thing that came out --

MR. BROWN: Yes, yes, that's -- okay.

MEMBER STETKAR: -- came out of this.

MR. BROWN: All right, thank you. That's what I was looking for.

MR. FREDETTE: Okay. I mentioned the corrective actions that stemmed from that particular inspection. This is basically a summary of them, you know, a lack of regulatory guidance in some of the procedures that Westinghouse was using, management enforcement of corrective action, inclusion and

verification of process requirements in IOT development.

They took a bunch of different corrective actions in, you know, over a fairly long period of time. Some were short-term where they had mandatory stand-downs including some Part 52 training.

And I'll just provide a little anecdote here. Middle management at Westinghouse was not quite sure what the ITAAC really meant in the AP-1000 space. And I was questioned one day about what does ITAAC really mean and where can I find the ITAAC.

So just things like that, which sort of --

MEMBER STETKAR: Gives you pause for thought.

MR. FREDETTE: -- got our attention.

MR. BROWN: Well, Tom, relative to this, isn't the COL responsible for passing those ITAAC and those requirements down? I mean, he's not going to invent those out of thin air.

MR. FREDETTE: No, and at the management level within Westinghouse they were certainly cognizant of the ITAAC. But this did not trickle all the way down to the working level and middle management level,

so.

MEMBER STETKAR: Is this because a lot of the work was being done, is being done at CSI rather than --

MR. FREDETTE: Well, that's a different --

MEMBER STETKAR: I mean --

MR. FREDETTE: That's a different --

MEMBER STETKAR: Different issue? Okay.

MR. FREDETTE: -- a different issue that we'll, I'll talk about later --

MEMBER STETKAR: Okay.

MR. FREDETTE: -- when we talk about the actual DAC inspection --

MEMBER STETKAR: Okay.

MR. FREDETTE: -- Mr. Stetkar. But Bob Hirmanpour is here from Southern Company. And he can talk, he'll talk a little bit about some of these issues. And we also have some Westinghouse people here in the audience who can talk, speak to some of these systemic issues and some of the corrective actions that went on over quite a long period of time.

MEMBER STETKAR: As best as I can read twice --

MR. FREDETTE: I'm sorry?

MEMBER STETKAR: As best as I can read twice, are still going on.

MEMBER STETKAR: That's right. And they'll probably be going on for quite a while. But the net result here at the bottom of this slide, this was a real setback for Westinghouse. You know, their completion, their schedule for completion of these Digital I&C ITAAC was basically pushed back as much as, I would say it's fair to say, about 18 months for some of these.

MS. CLARK: Wow.

MEMBER SCHULTZ: Tom, I can understand the focus now being understood to be more toward the vendor than to the licensee. But the licensee involvement is also critical --

MR. FREDETTE: Yes.

MEMBER SCHULTZ: -- in terms of the findings of the audit and the expectations for the licensee and the vendor's interaction.

MR. FREDETTE: Yes, and the licensees understand that, that they are really the oversight champion for everything that goes on with their facility, whether it's, regardless of what vendor it's

been developed at. They bear the brunt of the oversight.

And our process, I don't have a slide that talks to this, but our process now is even though we do vendor inspections, when the vendor gets a letter from us with an inspection report and they get a notice of non-conformance associated with that, the licensees also get a letter, a corresponding letter that basically alerts them that their ability to complete that ITAAC and subsequently close that ITAAC may be impacted.

So licensees, you'd better take appropriate action whether it be be involved in the corrective action or beyond, the involvement of more oversight.

MEMBER SCHULTZ: The latter, I was looking for in terms of their oversight and their responsibilities and such.

MR. FREDETTE: Yes, and we reinforce that with every inspection.

MEMBER RAY: Does Appendix B apply to this?

MR. FREDETTE: To what, Mr. Ray?

MEMBER RAY: Well, what you were just speaking of.

MR. FREDETTE: Yes.

MEMBER RAY: Yes? It does?

MR. FREDETTE: Yes.

MEMBER RAY: And so --

MEMBER STETKAR: Safety and Safety-related stuff.

MEMBER RAY: They do.

MEMBER STETKAR: No. No, I mean the safety-related stuff, that's the --

MEMBER RAY: I ask -- I know, but I --

MR. FREDETTE: Yes, Appendix B and --

MEMBER RAY: I was trying to ask it a different way which was not which is safety-related and what's not but does Appendix B apply --

MR. FREDETTE: Yes.

MEMBER RAY: -- to what you were just saying?

MR. FREDETTE: Yes, and along those lines, I'm going to go back a couple slides here. The notice of violation that's written here, it's written in the design control area of Appendix B.

MEMBER RAY: I understand, Criterion 7.

MR. FREDETTE: In the regulatory deliberations, I'll say, there is a lot of talk about whether this should be a notice of violation written

against Criterion 7, which is oversight of contractors and suppliers.

MEMBER RAY: Yes, well the thing I've noticed is that, although the citations are written against the various criteria in Appendix B, the review of engagement doesn't seem to be as programmatic as I would expect given the applicability of Appendix B.

In other words, the issue is whether or not deficiencies are found or not, not are you implementing an oversight program that complies with Appendix B. If deficiencies are found on the citation it's always to Appendix B.

But the question is to what extent is Appendix B itself evaluated in terms of, we were just talking about the licensee's oversight of the vendor.

(Off microphone conversation)

MEMBER RAY: And that seems to be a big gap as compared with my past experience anyway in which are you implementing Appendix B was the question. If not, are the deficiencies as a result of not implementing Appendix B, if that makes any sense to you.

MR. FREDETTE: I'm trying to understand.

MEMBER RAY: The issue that I'm trying to

say, and I know that time is of the essence so I'll just say it and shut up, the emphasis doesn't seem to be in the current time frame evaluating whether the licensee is fully implementing Appendix B from a programmatic standpoint.

Appendix B only enters the picture when a deficiency has been found, like you've been talking about. Then we point back Criterion 3 or Criterion 7 or something like that and write a citation. And I just don't see any priority put on are the licensees implementing Appendix B.

MS. VALENTIN: This is Andrea Valentin. I can help with that. There are separate key way inspections overall even outside of DAC, just overall of the licensees for all of the inspections that we do. So that is a separate consideration that applies to this as well.

MEMBER RAY: Well, it should. That's fine. That's a perfectly good answer. I just, I see a disconnect between, if you understand my point, people finding problems and then they say, well, what did you not do on Appendix B.

But I never hear anybody talk about we're not implementing Appendix B the way we should. It's

always just the reason why this deficiency was allowed to exist or came into being. With that, let's go on.

MR. FREDETTE: Oh, okay.

MEMBER RAY: I mean, there's a separation in the Agency between, as she just said, who's looking for the implementation of Appendix B versus who's looking to see if there are any technical discrepancies.

MR. FREDETTE: Well, the technical discrepancy is that we identify, basically point back to implementation --

MEMBER RAY: It does, but then it never results in anything that says we've got to do something about Appendix B implementation. That's my point.

MR. FREDETTE: Right, okay.

MEMBER RAY: All right? Let's move on.

MR. FREDETTE: Anyway, just to recap, there are a lot of corrective actions that were put in place by Westinghouse and the licensees, or with the licensees' help to basically correct some of these deficiencies from this 2012 inspection.

MEMBER CORRADINI: Is there, let me ask you a practical thing. Is there any indication that this will then cascade to Summer so they won't do it again?

MR. FREDETTE: Well, we haven't, you know, Summer is involved in all of discussions.

MEMBER CORRADINI: So they see and they're aware of all of this anyway?

MR. FREDETTE: Yes, we tend to look at the two AP-1000 licensees monolithically.

MEMBER CORRADINI: Okay, sorry. Okay.

MR. FREDETTE: If one of them is implementing something one of our first things is to see if the other licensee is also doing the same thing.

So that was a 2012 inspection. And our DAC inspection took place in January 2014. So in that two-year runup we basically were monitoring all the corrective actions and basically the PMS and the CIM schedule for development, trying to align our inspection resources.

And then we have a new tool at our disposal. It's the Virtual Reading Room. Westinghouse has made documents available to the inspection staff on a SharePoint virtual site that we can access and look at documents ahead of time.

It's been a pretty valuable tool for us as from an inspection planning standpoint. We don't have the days, the old bag-man-trip days where we would

send somebody to Westinghouse and they would come back with a big suitcase of procedures.

Now we can look at the procedures just about in real time. If there's something new that's been developed, Westinghouse is kind enough to post that for us and we can take a look at it and discuss it.

CHAIR BLEY: And that's on their system? You can, you have access?

MR. FREDETTE: We have access. And they've got protocols for us to basically access it, yes.

This is the ITAAC 2.5.2.14. This is the PMS component interface modular ITAAC. It's not particularly well worded. If you look at the design commitment it says that this design commitment is designed acceptance criteria.

But if you read the AP-1000 SER, really, the only area where DAC applies is for the CIM life cycle stage, Alpha, which is the design requirements or planning phase activity. So the CIM was never adequately addressed during design certification. Hence, it remained its own DAC.

It's a field programmable gate array platform. It's a subcomponent embedded within the PMS

system and serves as an interface between safety components and various safety controls.

Beyond the life cycle planning phase the rest of that ITAAC, Bravo, Charlie, Delta and Echo, which is system definition, development and design implementation, integration and testing and, finally, installation, that will all be addressed as standard ITAAC.

MR. BROWN: Now let me ask one other question.

MR. FREDETTE: Sir.

MR. BROWN: This is, and I may be off-base with this, so just let me know. I know that's the only formally defined DAC. But one of the ITAAC that we had before also addressed the use of commercial grade hardware and software, if I remember correctly.

MR. FREDETTE: Yes, that's right.

MR. BROWN: I've got it, I've pulled it up. That's not a DAC.

MR. FREDETTE: No.

MR. BROWN: It's still, it's just an ITAAC. Is that right?

MR. FREDETTE: Yes, sir.

MR. BROWN: Have you all gotten there yet?

MR. FREDETTE: Yes, we have. That's been within the scope of, it was within the scope of an interim inspection that took place back in March of this year, Mr. Brown. I don't have the inspection report number but I can get it for you.

We're not finished with that ITAAC. There are going to be some subsequent inspections that are going to address some elements of commercial grade dedication.

MR. BROWN: Okay, so you all have not left that one where the other --

MR. FREDETTE: No, we have not.

MR. BROWN: That's what I get out of it.

MR. FREDETTE: No, we have not. That inspection's underway.

MR. BROWN: Is part of that inspection, and this is, I hope that's not too far down in the detail, commercial, typically the commercial grade computer hardware and its associated software is pretty complex. They have large amounts of, huge amounts of code because they're trying to meet multiple desires so they can market their product.

Do you all have any specific criteria that you've developed relative to how that ancillary or

miscellaneous code that's not useful relative to the reactor? You know, our application is either dumped, not processed or is it part of the normal operating cycle and you just have to live with it?

MR. FREDETTE: I could not speak authoritatively --

MR. BROWN: Okay.

MR. FREDETTE: -- on that particular issue.

MR. BROWN: All right.

MR. FREDETTE: The vendor inspectors are doing inspections of commercial grade dedication basically aimed at that particular ITAAC. And that will be taking place over time.

They just did their first one back in March, as I mentioned.

MR. BROWN: That's, you said that's the vendor's side of it. But you all haven't gotten any of that yet?

MR. FREDETTE: No, we have not.

MR. BROWN: Okay.

MR. FREDETTE: But I understand your point. In other words, you've got a lot of software that really doesn't apply for your safety application.

And how do you address it so that, to make sure that it doesn't interfere with safety functionality.

MEMBER STETKAR: Well, fundamentally the, if I can insert something here, it might help. I thought I remembered something. I just looked up the inspection report from the Vogtle inspection a couple of years ago.

And there were a couple of lines in there when you looked at whatever the acronym, RSED, Reusable Software --

MR. FREDETTE: Reusable Software Element Testing.

MEMBER STETKAR: -- that, indeed, the inspectors looked at. As examples, the use of RSEDs for software requirements introduces extra software code that is not necessary to implement the system requirement.

Extra software code does not -- the extra code, dead code, has the potential to expose the PMS from an unexpected fault condition. So that says the inspectors are looking for that.

MR. BROWN: Yes, my concern --

MEMBER STETKAR: But whether they're looking for it, you know, in commercially dedicated

software, but at least in this context they were.

MR. BROWN: My concern with that non-used code is the potential for locking up the stuff.

MEMBER STETKAR: Sure.

MR. BROWN: Because it's not totally consistent or tested. You can't just normally test that as well as you'd like relative to the main path code that you want. I mean is it, it's not being, I mean, at this point is not being called but it's still residing in memory somewhere where it's what subject --

MR. FREDETTE: Can it interfere with --

MR. BROWN: Exactly. It's just, we haven't had an opportunity to talk about this anymore for the last two or three years. And it would be interesting sometime, Dennis, to get just maybe a discussion of the results of the review of that to see --

MEMBER STETKAR: And in fact this came out from inspectors looking at the software hazards analysis and identified this as a deficiency that the hazards analysis hadn't --

MR. BROWN: Didn't find it.

MEMBER STETKAR: -- hadn't found it. So

all I'm saying is that at least this little snippet says within the context of that particular inspection, they're sensitive to, how they're doing it in terms of how the commercial grade stuff is folded in isn't clear yet, as Tom said, when we were looking at it.

MR. BROWN: One anecdotal comment on that is that there was a specific project back when I was still working with NR where we attempted to take the Microsoft operating system which was being adapted to a particular platform for a monitoring function that was going to be used in one of the aircraft carriers.

And after we looked at it we had to step back and say, look, I mean, there's so much of this stuff floating around in there. How can you take that out? Okay, is there a way to dump, identify.

The problem we got into was there were so many tendrils from the code you did need that touched, in some way, shape or form, touched all these other non-useful sets of sub-routines and everything else that it became just cumbersome and we just, we quit trying.

It was, but the Microsoft code is a really spaghetti code to start out with as you're well aware from your computers. It's not well controlled in all

circumstance. And that's all. It was just, that's an anecdotal point. This is very difficult to do and not have that code interfere with your normal mainline stuff. It's a tough operation.

MEMBER STETKAR: And this, Tom, are these inspection reports public or?

MR. FREDETTE: They're public, yes.

MEMBER STETKAR: They are? Okay, because this particular one, and I've lost the place and time, sites something like they identified, during this part of the review, they identified something like 485 additional software requirements that hadn't been analyzed.

MR. BROWN: Oh, geez.

MEMBER STETKAR: Just, so that kind of supports what you're saying.

MR. BROWN: Yes.

MEMBER STETKAR: And that's just from this part of the report. But what it does, from our perspective, it says they're looking for that.

MR. FREDETTE: Yes, we have a sense --

MEMBER STETKAR: And that's good.

MR. BROWN: By the way, that's one of the reasons I've been as anal as I have been on terms of

processors being monitored, lockup, communications from one thing, you know, then mixing all the fold-in units on the rest. When you've got this complex a code, you just can't keep yourself straight. So that's --

CHAIR BLEY: Well, we were looking at the one that actually had code to generate interrupts but it was supposed to be bypassed and not used.

MR. BROWN: Yes.

CHAIR BLEY: But it's been years since I wrote code. But even when you do a good job you have some overarching things that lay out. And that has links. And if the links aren't there it doesn't work anymore.

MEMBER STETKAR: Yes, well, there was another example I couldn't find that was similar to that, bypasses and just maintenance bypasses.

CHAIR BLEY: Accounting.

MEMBER STETKAR: Overrides that a chunk of code was left in there that supposedly wasn't going to be used. But if it somehow got invoked you could bypass two or three channels at the same time.

CHAIR BLEY: Sorry for the diversion. Go ahead, Tom.

MEMBER STETKAR: Yes, that's all.

MR. FREDETTE: This is all a good discussion. I captured an action for the staff to provide our perspective on commercial grade dedication results of commercial grade dedication inspection of a digital system in the future that we can present basically some results about that.

CHAIR BLEY: Tom, do you know, and I don't, because this example that I brought up is a good example, was found through the inspection of the software hazards analysis, I think.

Is, does that software hazards analysis extend out through the integration of commercial dedication software into, let's call it the mainstream --

MR. FREDETTE: Mainstream system?

MEMBER STETKAR: Well, the PMS.

MR. FREDETTE: Well, yes. In fact, they're supposed to, there's a requirement to update that software hazard analysis every time they complete a phase of the life cycle.

MEMBER STETKAR: Okay.

MR. FREDETTE: In other words, so they start out with their preliminary hazard analysis. When they develop software requirements they're supposed

to --

MEMBER STETKAR: Okay.

MR. FREDETTE: -- enhance the, or revise the hazard analysis to include hazards that were identified when they developed those requirements and what those requirements may or may not impact.

MEMBER STETKAR: Okay.

MR. FREDETTE: So in every phase they'll update. Anyway, as I was mentioning, we'll pick an action to present on commercial grade dedication inspection results at a later forum.

MR. BROWN: Is that okay, Dennis?

CHAIR BLEY: Yes, that's sounds awesome. Is that okay?

MR. BROWN: Yes, I mean, I think it was, well I introduced that and it's your meeting. So I just wanted to make sure I didn't overstep my bounds here.

CHAIR BLEY: What you did was fine, Charlie.

MR. BROWN: Thank you. I appreciate it.

MEMBER STETKAR: A little help for the future.

MR. BROWN: Thanks, Tom.

MR. FREDETTE: All right, this was our DAC inspection scope for the January 2014 inspection. Again, this was the CIM planning phase. So we looked at the software management plan.

This is Westinghouse's software management plan. But the CIM, because it was developed, originally developed by one of Westinghouse's sub-suppliers, CS Innovations out in --

MEMBER STETKAR: Lake Forrest, California.

MR. FREDETTE: Scottsdale, Arizona.

MR. BROWN: Oh, I thought it was in Phoenix now.

MR. FREDETTE: Scottsdale, Arizona.

MR. BROWN: Yes, Scottsdale.

MR. FREDETTE: The CIM had its own project plan. We looked at the software safety plan including the FMEA and the hazards analysis, the hazard software development plan and QAP. And we took a look at the integration testing and installation plans, configuration management and finally the V&V plan.

We looked at all of these plans for the PMS when we did our inspection back in 2012. I just don't have a slide that reflects that. But all of these

sort of factored into some element of every inspection that we do for these systems.

This was a vendor inspection. It's documented with that ML number. There were two notices of non-conformance issued to Westinghouse this time for design control deficiencies, the CIM project plan, compliance with the licensing basically, these IEEE Standards 1074, 1012 and 828 and incomplete CIM configuration items.

There were some more details in the inspection report that talked about some of these inadequacies. And then, finally, an inadequate V&V plan. They never fully translated the 1012 requirements to the lower tier documents.

They didn't address CIM software hazards. This has been a reoccurring theme with every inspection. It does not seem to me that software hazards are fully captured as they advance their design.

And, in fact, several of these items that were identified in these notices of non-conformance were repeat issues that we had previously identified. In other words, the long-term corrective action that Westinghouse had implemented hadn't fully taken effect and/or they had not extended to the CS Innovations

development team out in Scottsdale.

In the interim, since 2012, CS Innovations has been brought back into the fold within Westinghouse at their Warrendale facility outside of Pittsburgh. But they are still going through some of the corrective action pains of getting their sub-supplier personnel and processes fully up to snuff to where they actually meet what's called for in the AP-1000 licensing basis.

CHAIR BLEY: I'm going to ask something again. You might not want to answer it. Maybe a licensee or maybe even a vendor, if they're available to speak, one would want to answer.

These, especially these repeated items, are they things that were just missed or are they things that the vendor thought they were doing that didn't quite agree with you on what the requirements met or something else?

MR. FREDETTE: Well, I'm going to attempt to answer, Dennis.

CHAIR BLEY: Mm-hmm.

MR. FREDETTE: And we have a representative from Westinghouse who's here. And she can chime in here, okay?

CHAIR BLEY: Okay.

MR. FREDETTE: Early on the inspection team used to have arguments with the vendor about what's really committed to in the licensing basis.

CHAIR BLEY: Okay.

MR. FREDETTE: A lot of discussions back and forth, sometimes heated discussions, as part of the inspection. We don't have those arguments anymore.

Westinghouse has taken it upon themselves to basically address all of our concerns, all of their deficiencies in their corrective action program. My sense is that they have just not followed through completely yet.

And as we advance, as they advance their design and as we go through more and more inspection iterations, my sense is that they're going to bring their processes into full compliance with what's called for in that licensing basis.

CHAIR BLEY: And let me ask you just a slightly different way. Was it thinking the licensing basis didn't fully invoke what's in the IEEE Standards or was it interpretation of the IEEE Standards?

MR. FREDETTE: I think it's interpretation that -- I'm sorry. Interpretation is not the right word. A thinking, a school of thought that the

licensing basis was really guidance for implementation and not really a compliance issue.

CHAIR BLEY: Okay, go ahead.

MR. FREDETTE: Mr. Hirmanpour is going to talk a little bit more about that when he gets to his --

CHAIR BLEY: Okay.

MR. FREDETTE: -- discussion. The Westinghouse corrective actions from this inspection area are still in progress. They're committed to have them in place fully by February of 2015.

We have a regular ITAAC inspection coming up in August and we're going to look at the interim corrective actions at that time. Or at least that's the plan right now.

MEMBER STETKAR: Tom, one little question that popped out, and it's a little bit relevant to what Dennis brought up. I was reading the Westinghouse response to their inspection on the CIM. And part of the response says an evaluation will be completed to determine if the CIM IV&V team should adopt the work constructions developed by the PMS IV&V team or develop additional work constructions to address IV&V gaps.

That, to me, says that, for some reason,

independent verification and validation is that that basic process or concept is tailored depending on what part of the design you're working on. That strikes me as a bit odd.

It says that different parts of the organization are still thinking about this differently. Or am I reading too much into that statement?

MR. FREDETTE: No, I, that may be true. I'm going to call on Westinghouse. Sarah DiTommaso's here from Westinghouse. Sarah, can you address Mr. Stetkar's question from a vendor perspective?

MS. DITOMMASO: I don't want to talk in this anymore. Hi, I'm Sarah DiTommaso from Westinghouse. I'm the manager of AP-1000 Instrumentation and Controls Licensing.

In general, from an IV&V perspective, the majority of our IV&V documentation process plans and procedures were focused on the Common Q system in the past. And so we developed the work instructions for the Common Q, performance of activities for IV&V. Those were focused there.

For the component interface module, because it was developed at CS Innovations under their program, they had developed their separate IV&V process.

So when CS Innovations was brought to Westinghouse, or when CSI Innovations was closed and the CIM, the component interface module system was fully brought into the Westinghouse program as part of the corrective actions we determined we want to keep the CS Innovations processes or fully develop the Westinghouse safety system processes.

Currently, the Common Q system is our main safety system that we use for the AP-1000 and for a number of other operating plants we also have another AP-1000 -- I'm sorry, another safety system in development that uses very similar, if not the same, processes as the IV&V for the Common Q.

We need to understand that there's some differences in technologies. So, relative to very specific requirements for what IV&V activities need to be performed, there are going to be some nuances at the very lower levels, like the work instruction level.

MEMBER STETKAR: That I understand.

MS. DITOMMASO: Yes.

MEMBER STETKAR: But from a fundamental IV&V process, how it ought to be run, how the --

MS. DITOMMASO: And that's where we use

the, our standards --

MEMBER STETKAR: Okay.

MS. DITOMMASO: -- to drive our processes. We use the IEEE 1012, IEEE, I mean, we bring into the fold IEEE 1028. That's really how we develop our overarching processes.

MEMBER STETKAR: I guess that helps. Thanks.

MS. DITOMMASO: Does that help?

MR. FREDETTE: Thank you, Sarah. This is our status to date. And it's the DAC inspections, complete, pending verification of those corrective actions.

We expect to conduct the next ITAAC inspection for the CIM which would be the requirements phase sometime late 2014. We continue to monitor progress of the corrective actions through working meetings and dialogue with the licensees and Westinghouse.

I have a bi-weekly call with the licensees and Westinghouse every, well, every two weeks to discuss progress, status, schedule. And our inspection schedule's tailored to their status as best we can get it, as best we that we can pull inspectors together.

CHAIR BLEY: Just for me, in this inspection process, violation is the name of what we do to identify the problems. They don't imply any other penalties beyond corrective action, right? Or they could.

MR. FREDETTE: Well, they could depending on how severe they are. But for a vendor inspection it's always going to be notice enough.

CHAIR BLEY: Yes.

MR. FREDETTE: There are other, if the penalties are --

CHAIR BLEY: These aren't operating as yet, so, yes.

MR. FREDETTE: If the penalties are severe, if the discrepancies are severe enough then our recourse with vendors is basically -- Andrea, help me out here. For vendor inspection, beyond normal notices of non-conformance, there are other mechanisms we use, but --

MS. VALENTIN: Sure, this is Andrea Valentin. If, we always have the option if there is enough -- now, we haven't done this, but if there is enough non-conformance at a vendor we could theoretically issue notices of violation to the

licensing.

I mean, we have that in the toolbox. Again, didn't need to do that, haven't done it. But typically for vendors it's notices of non-conformance, a lot of interaction, a lot of corrective action.

MR. FREDETTE: Yes, so the notice of violation for the licensee probably would be in the area of oversight.

CHAIR BLEY: Mm-hmm.

MR. FREDETTE: We haven't reached that point yet, but --

CHAIR BLEY: I understand.

MR. FREDETTE: -- from a regulatory, our regulatory envelope is quite, there are a lot of tentacles that reach out.

CHAIR BLEY: I see. Well, this is, well, I mean, we're still exploring this process right now, so.

MR. FREDETTE: Throughout all the inspections that we've conducted, again, this goes back even to the South Texas days, I've been compiling insight and lessons learned that will aid us going forward, I hope.

Achieving a common understanding on what

the ITAAC or what the DAC really say, you know, for long time the staff, we, if you take the letter up the way that ITAAC for the CIM is written, it looks like the entire process for the CIM is design acceptance criteria.

We have to go back and use the other documents that are official records, like the SER, you know, staff insights and things like that, to come up with what the intent in AP-1000 design certification was, to really come up with what you have achieved aas a common understanding.

Dedicated inspection planning, we have limited resources, as I've mentioned many times. The Tech staff involvement has really been an aid to us. We looked at this in the early days as this was the best way for us to get the best snapshot of design implementation.

But, really, they've brought a lot to the table with regard to all the different insights and all the different nuances of the design certification process which, in AP-1000 space, was pretty convoluted in the I&C platforms.

CHAIR BLEY: So this is the place I have to ask this one. Do you view their participation as

kind of something permanent that's always going to be needed because of the characteristics of these things we call DAC or as training of the inspection team so that the inspection team won't need their help so much in the future?

MR. FREDETTE: No, I think it'll always be a part of it, yes. They, it's just they've been pretty invaluable from my standpoint. And things like HFE and Digital I&C, they are very, very technical, very complex. And so we don't want to ignore a resource that's at our fingertips, really.

CHAIR BLEY: Thank you. Go ahead.

MR. FREDETTE: I mentioned this, the use of the Virtual Reading Room. This is a tool that we've put in place now. It's been, it's really saved us a lot of time in inspection planning efforts.

CHAIR BLEY: Are there expectations that this will be the process with other vendors, or is there any way to tell?

MR. FREDETTE: Well, it's difficult for me to tell at this point. That's something we would always explore with that. Our fallback is we'll go back to the --

CHAIR BLEY: The Stone Ages.

MR. FREDETTE: Understanding organizational and document hierarchy is really, this is really where the Virtual Reading Room has really paid off because there are hundreds of documents that come into play with regards to one of these inspections.

Understanding how they relate to each other and how the organization relates to each other saves us a lot of time on the front end. I mentioned here pre-briefs. Sometimes vendors are kind enough to give us a pre-brief when the inspection team shows up to give us sort of an overview of how they're set up.

Not always necessary and it's not required, it's something that they do on their own. In general, and I think I'm safe in saying this, but time will tell if we ever get to ESBER, okay. The inspection effort that we've achieved had, in my view, has matched the level of technical review that would have been undertaken if this had been provided during licensing.

I'm not going to say that that's always been the case or it will always be the case. We'll find out when we get into more substantive DAC environments like ESBER.

The tech staff's adapted pretty quickly to the inspection environment. We have typically used

a pretty large inspection team for some of these inspections. Our feeling going forward is we'd like to make the inspection teams a little smaller and have more time to do more focused review.

One of the challenges we face is maintaining continuity. Some of our inspectors have moved on. The AP-1000 tech reviewer, he's not got a new job so we're bringing a new AP-1000 tech reviewer into the fold for future inspections.

And then this goes back to our procedures. Where I wrote this procedure three, four years ago now for Digital I&C. Every time I use it or every time I pull it out I always seem to see stuff that I think needs to be enhanced.

So, and it's due for enhancement, it's due for revision anyway so we're going to take some licensing, some editorial licensing and do some enhancements.

CHAIR BLEY: When do you expect to have a revision out?

MR. FREDETTE: It's due to go into the pipeline in November, Dennis. I don't, it's a little beyond my area of expertise as to how long it takes to get that through and get comments back and

everything, so.

MEMBER STETKAR: Tom, you mentioned the Digital I&C. Are you doing that for the other inspection procedures also?

MR. FREDETTE: The other inspections also.

MEMBER STETKAR: So the whole suite?

MR. FREDETTE: The whole suite. I can't, I don't want to say any, for the HFE procedures yet, Mr. Stetkar. I'm not sure when they're due for a revision. But I can say for the piping and the Digital I&C they are due for revision at anyway. They've been out on the street for a while now.

MEMBER STETKAR: It's Sanjoy's phone. God, I won't go into his bag.

MR. BROWN: Drop it in there.

MALE PARTICIPANT: It was working.

CHAIR BLEY: Go ahead, Tom.

MR. FREDETTE: Our expectations for the rest of this year and into 2015, we expect to conduct our first piping DAC inspection sometime later this year, hopefully.

The first HFE inspection we already talked about will start, well, it'll take place in the October/December 2014 window. We continue to enhance

the process where we feel it's necessary.

Preparation for other design centers, you know, we all know that the ESBER has a sizable Digital I&C DAC population. We haven't really looked in any great detail as to how we're going to address those yet.

I've had enough on the AP-1000 plate that I haven't really had time to look into ESBER. But our sense is that it may be coming. So we are going to start to take a look at it and how we're going to tackle it.

And then, as always, our commitment is to brief you and your committee as appropriate. So we'll set the stage for future forums. One thing we know we want to brief on is the results of HFE inspection when that's complete. So we're looking at that sometime in 2015.

CHAIR BLEY: All right.

MR. FREDETTE: And then just in conclusion, we feel like we've demonstrated our process. We're positioned to do the necessary piping DAC inspections. We feel like we provide the appropriate technical rigor for these inspection efforts with the technical staff's help.

And our process is pretty flexible. We can adapt on the fly for different circumstances at different inspection environments. And, in short, we feel like we're in a position to verify adequate design implementation as these designs advance and to make sure they conform with the licensing basis.

And, with that, I'll open it up to discussion or any other further questions.

CHAIR BLEY: I think we've done that. I think we can thank you very much. That was very helpful and we'll talk more at the end of --

MR. FREDETTE: Okay.

CHAIR BLEY: And we can go to Bob then.

MR. HIRMANPOUR: Okay. Good morning. I'm Bob Hirmanpour, down at nuclear Vogtle 3 and 4 at part of the Digital Systems Group and also licensing.

CHAIR BLEY: Do you want to put your slides up?

MR. HIRMANPOUR: Yes, let me --

MR. FREDETTE: I should mention that throughout all our inspections, Bob here, he's been our primary licensee focal point and point of contact with regard to --

MR. HIRMANPOUR: That's right.

MR. FREDETTE: -- the Digital I&C systems progress. So we have worked pretty closely over the past couple years on, as we implement the program.

MR. HIRMANPOUR: Thank you. Good morning again. How much time do we have?

CHAIR BLEY: You've got more time than you thought you had because we finished a little early there. Finish by noon, I think.

MR. HIRMANPOUR: Okay. Well, I'll at least report it and so many questions you ask. Again, I'm Bob Hirmanpour. Also as part of the audience we have Sarah DiTommaso. You already met Sarah.

Also Mr. Andy Underwood is a supervisor for I&C for V.C. Summer 2 and 3. And Mr. Ryder Thompson is the ITAAC manager for V.C. Summer. So if you have any questions they can back me up.

So before we get started, as far as my history, I know some of you may remember I was with NuStar for four years. I was at Southern and it was what I called AP-1000 Standard COLA which included Chapter 7, Chapter 8, Chapter 18 and also Chapter 19 which is PRS. Since I was the only one who could spell PRS so I became responsible for that.

And after completion of the NuStar I joined

Southern Company as part of the ITAAC team. And here I want to address one of the, one of Mr. Ray's concept, what I can speak.

I got a call around February 2012. And the first inspection we had was the PMS inspection. It was basically two months after we received our call. So we had not done at that point much oversight of the Westinghouse.

We were involved in the design certification and we had also attended some of the what we call interning or final design reviews. But there was no work, our review of the documentation. So when we did get that violation part of that was what they call a cross cut-in aspect which was major oversight.

So as a result of that we put a team together. We increased our oversight and we started reviewing all the documents basically to some point. Some of them we do samplings, some of them we do added person reviews.

So toward the end of 2012 we realized that Digital has life of its own and it's very important. So we formed a new group at Vogtle called Digital Systems Group. So for the past year and a half we had a new team. And that team has grown to about eight

to nine people right now, and it's still growing.

So as far as answering that, and it's big question, yes, we do provide lots of oversight, specifically in the area of I&C. Now our confidence monitoring program, I mean, there's over a hundred people in there. And that's mainly to making sure that when they are, do licensing basis including all the ITAAC requirements. I hope that answered your question on that one, Mr. Ray.

MEMBER STETKAR: I had another one. And I thank Carol for teeing me up on it. I understand Appendix B applies to all the safety-related stuff. Part of the digital I&C system includes non-safety related I&C equipment and it includes the Diverse Actuation System.

And the Diverse Actuation System is identified in the DCD as a so-called RTNSS system, Regulatory Treatment of Non-Safety Systems.

MR. HIRMANPOUR: Correct.

MEMBER STETKAR: And I noticed that when the staff went up to Westinghouse they actually observed some of the testing of the DAS, some of the DAS cabinets.

So I got curious. I looked up in the DCD and I said, gee, I wonder what kind of quality assurance

they're applying to DAS. Because it was my understanding that RTNSS-type equipment would have some intermediate, enhanced, less rigorous, for example, than the Appendix B, less onerous, but more rigorous than perhaps normal non-safety related equipment.

What I found in the DCD, at least, there's a Table 17-1. And under quality, and this applies, there's statements in the DCD that says, "For systems, structures and components included in the regulatory treatment of non-safety systems, the quality requirements are identified in Table 17-1."

And I go to that and it says, Quality Assurance Program. It is expected that the existing body of suppliers, procedures or practices will describe the quality controls applied to the subject equipment. A new or separate QA program is not required.

So does that mean that the same QA requirements apply for the DAS cabinets and system as would, oh, you know, a local space heater out in a room because those are equally non-safety related pieces of equipment?

MR. HIRMANPOUR: So basically DAS has what they call a graded approach to Appendix B. It is

included in DAC in Chapter 17 of the DCD. Also we have a section in our Southern Company, QA manual or QA program, that includes.

So it is not 100 percent Appendix B. But what the statement is saying is you are following almost the same process as Appendix B. So the same --

MEMBER STETKAR: And that's the way I'm supposed to --

MR. HIRMANPOUR: -- procedure and processes are used.

MEMBER STETKAR: Okay.

MR. HIRMANPOUR: Now there are some differences. So DAS has two requirements, one that's Chapter 17 requirement. Then that also is a ATWS system. So it has a generic, like, I believe it's AB 401 applies there.

So some of the aspects, all of the documentation and independent review is the same as Appendix B, 100 percent the same.

MEMBER STETKAR: Okay.

MR. HIRMANPOUR: So those controls are applied.

MEMBER STETKAR: Okay.

MR. HIRMANPOUR: However, there are

additional requirements put in place, like the IV&V of the DAS, even though it's not required by regulations. But we do the IV&V, so IV&V, that's the independent testing of the DAS system.

MEMBER STETKAR: There is? Okay.

MR. HIRMANPOUR: So there's additional requirement put on top of it, what we would a non-safety system.

MEMBER STETKAR: Thanks. Now let me ask the staff, does the staff in the inspection process audit that element of the IV&V? Because it's not safety related now. How does the -- okay, you do?

MR. FREDETTE: Yes, if you look at, there's a specific, well there's several ITAAC just for DAS.

MEMBER STETKAR: Yes.

MR. FREDETTE: And one of them is, talks about the development process, the testing and installation for the DAS hardware or software or any software. And we treat it just like any other safety related system.

MEMBER STETKAR: Okay. Okay, thanks.

MR. HIRMANPOUR: Yes, and the staff did look at that during inspection.

MEMBER STETKAR: Okay, thank you.

MR. HIRMANPOUR: Okay, anything else? Okay, I'm going to basically put the next slide. I'm going to put the next slide and talk about the ITAAC.

So Tom already mentioned the PMS. So, as some of you may recall, we had four DACs in the DCD amendment process. There were two on the DAS, that was Actuation System. There were ITAACs A and B, which was the planning phase and requirement phase.

Those were closed. Similarly, we had the ITAACs, what I called 11.a and 11.b, for the PMS planning and requirement phases. Those two DACs were also closed during the DCD Amendment 17. There were used none.

Initially ITAAC 12.a or 11.a was removed from the ITAAC by part of the SDRSD request that was added back on as not used. Plus you added probably about 15 documents to DCD to show how the ITAAC, what the DAC was addressed.

And remaining out of the was ITAAC 11.b. The DAC part was closed because at that point we provided the requirement specification, a number of diverted caps on communication and system architecture.

There was FMEA provided. There was software hazard analysis. So based on those, basically

SER concluded that the DAC portion of the requirement phase is closed. However, the ITAAC remained open for further inspection and especially on the design gets finalized.

Okay, so when ITAAC 11.a was closed CIM, which was a component of the PMS, we still did not have adequate planning documentation. Initially the intention was to use the same planning documentation that was used for the Wolf Creek.

That was FPGA process. That was used for feedwater isolation system. However, at that point the staff found that that's inadequate. Especially, that was the same timing that ISG-4 was developed and calling the FPGA basically a software process.

So as a result of that a new ITAAC or DAC was born, which is 252-14. So if you go two slides forward, okay, so 14 basically covered almost the same software life cycles as the PMS did.

Now some of the technology that was here, maybe a design requirement and culture system definition phase, these are basically the same as the IEEE one which is planning and requirements. Everyone does and uses its own terminology.

And as a result of that the staff concluded

that the Part A of that ITAAC, which is the planning phase, it is a DAC. And that's basically all the inspections and the new inspection procedure has been addressed in the 14.a at this point.

Now going back to, again, going back to the Appendix B and oversight requirements, when this inspection changed from Region II, it was a PMS to the CIM. And that's when the vendor branch came in. Now, at that point, we had not done our, basically the oversight of the planning documents.

So all the planning documents actually got ready one or two weeks right before the CIM inspection. And that was probably some of the reasons we ended up with the CIM findings and notice of non-conformance.

MEMBER STETKAR: Mm-hmm.

MR. HIRMANPOUR: Now the goal is, going forward, is to hopefully do our oversight and our due diligence before the inspections happen. So that's something we have talked with the inspection branch. And we are doing that.

The next inspection is basically August, the week of August 24th. And that's going to be the PMS testing, DAS testing and also probably BCIS which is the blank control system. And right now we are in

the process of reviewing those procedures and the test results.

MR. BROWN: So is your goal with that to ensure that you don't have notices of non-conformance issued to Westinghouse?

MR. HIRMANPOUR: No, our goal is the oversight. I mean, we are a oversight process.

MR. BROWN: Well, I mean, hopefully --

MR. HIRMANPOUR: I mean, intended of inspection.

MR. BROWN: But that's, you're doing that from the licensee's standpoint, right?

MR. HIRMANPOUR: Yes.

MR. BROWN: I mean, hopefully your goal would make sure that your oversight is ensured that Westinghouse is doing what they need to do so that they don't get hit with these is entirely, I mean, that's --

MR. HIRMANPOUR: Yes. I mean, and the concern is not the, I mean, that's the outcome or that's a by-product. But the goal is to make sure we meet the licensing basis --

MR. BROWN: Oh, no, I understand that. I wouldn't --

MR. HIRMANPOUR: -- the COL, the safety and all the key words, you know? Yes.

MR. BROWN: I was not trying to down, of course, that's the goal. But, obviously --

MEMBER STETKAR: Their goal is to catch it before the inspectors catch it.

MR. BROWN: That was my point, that they're sure they meet the licensing requirements as well as ensure that you've got the rest of the world covered as well. That's it.

MR. HIRMANPOUR: Yes, and some of that came up, I talked the NRC inspection branch. They wanted to make sure that the due diligence is done and the products are final and quality before they do a review. They don't want to come findings and keep coming back again. As I said their resources are tight there.

MR. BROWN: I didn't mean that as a negative comment though. That was --

MR. HIRMANPOUR: Yes, but --

MR. BROWN: That was not meant that way.

MR. HIRMANPOUR: But hopefully there are no NONs. If we've done our job and there will be no NONs.

MR. BROWN: Okay.

MR. HIRMANPOUR: Okay, so CIM, so we already talked about that briefly. Component Interface Module is basically a small module. Some other design centers call this priority module.

All it does, provide priority between non-safety and safety. So every safety related component that required for ESFAS or reactor trip gets a CIM. So it's like there's like over 200 of them practically. So altogether, with V.C. Summer Project, close to 1,000 CIM. And then we have the trainees.

So CIM originally, it was, I believe, an analogue we changed into an FPGA and then FPGA, as Ms. DiTomasso said, there's the software has to follow the software processes.

And the way the ITAAC is worded and the way the IEEE and reg guys are retained, that created some challenges for us. As an example, you go into the integration and the installation phase, well, installation generally, for IEEEs are when we install the system in the plant.

Well, actually this is, first of all this CIM is not a system. It's just a compound BNS. So that makes it difficult. And also we don't install it in the plant. So it's manufactured and installed

inside a larger system.

Now if you try to meet the IEEEs verbatim that creates challenges both for us and the inspectors. And when I see a DAC, DAC is a whole media CD which means you really don't have our licensing basis defined except high level.

You got your 10 CFR and the reg guys. Of course if you go to the DCD Appendix 1.a, all it talks about is like here it's all the reg guides as we conform. So that has created some, I said that has been problematic at this point because when the inspectors show up they won't have anything else and they are trying to approve your plans, going through verbatim confines of the IEEE.

And, as some of you may be aware, trying to meet some problematic or administrative IEEEs, like 1074, which is like the software life cycle, 10.20 or 10.28, that will be very, very difficult to do.

So overall we are in the process of basically have they looked in your software program and not foreseen the result of the findings and violation also. Plus the CSI got bought by the, got intake with as part of Westinghouse.

So there is some new documents, new

planning documents. And at the same time we are trying to actually establish licensing basis for CIM.

So that's probably the main challenge with dealing with planning phase and DACs. That's something that was not probably in Region before. Because inspections tend to look at the implementation but not here. Through inspection we are trying to do approval of the planning documents. And most of the inspectors don't have anything to go by, except for reg guides and IEEEs.

Any questions there?

MEMBER STETKAR: Yes.

MR. HIRMANPOUR: Yes?

MEMBER STETKAR: This comes out from something Harold mentioned earlier. And I want to make sure I understand what I'm hearing and ask you a question.

Harold brought up the notion earlier that if an integrated review was done for a Part 50 application we didn't have DAC. There are elements of judgment that are imposed by the technical reviewers as part of that process.

Am I hearing you to say that some of those elements of judgment have been lost from your

perspective because the inspectors are simply taking a list of -- an extensive list of IEEE requirements and reg guides and doing a check-off to say yes, you did satisfy this one, yes you did not satisfy this one?

MR. HIRMANPOUR: Yes, I will say with some inspectors, not all inspectors.

MEMBER STETKAR: Not all inspectors? But some inspectors? Okay, yes, that's a big problem.

MR. HIRMANPOUR: Yes, and, again, the problem is that do you see these void out licensing basis?

MEMBER STETKAR: No, it's not --

MR. HIRMANPOUR: That's not a program. So it is, so we are trying to address that. So part of that, part of the criteria, actually Westinghouse has done, they've gone through great pain operating on every IEEE, line by line, identifying how they comply.

MEMBER STETKAR: But see, expending a heck of a lot of time on check-off boxes to say that you meet, line by line, IEEE requirements is not a technical review.

It's counting jelly beans in a jar. And if we're implementing the DAC inspections by counting jelly beans in a jar we're not accomplishing what Harold

was saying earlier, which was an integrated technical review of the design.

MR. HIRMANPOUR: In the planning phase that seems to be the case that we are looking at the line, the IEEEs. And technical IEEEs, I mean, no issue there. I mean, we do have to do a verbatim compliance.

We cannot mix not 603. But then it goes like the 1074. And, you know, some of those IEEES that you see, the older versions, they have been improved and there are conflicting information in there.

So that, that's been, again, problematic. And the way we are trying to address then is actually put the document in front of the inspector and say here's how we're going to meet the reg guides. Now reg guides is the way for the NRC to approve what you have. However, we are going to have some, okay, you have alternate ways without doing some of that stuff as I'll give you an example.

Generally IEEEs require that we do upfront feasibility study based on the customer requirement spec. Well, actually, there is no real customer the way the new plans work because the vendors they own customer. Their requirements come from a mechanical section, safety analysis section, 10 CFR.

So they really, they will not assume there was no real feasibility study. However, there was a specification. There was prototyping done. So you knew that your product is going to meet the customer needs.

However, IEEE says you go to feasibility study, verbatim compliance. There is no paper that says here is the result of my feasibility study. And that's where we get in trouble. That's why, based on meeting those line by line.

What we are going to do, we're going to propose, okay, here is our kind of alternative ways to the reg guides that a staff needs to review and approve and say, look, I don't do feasibility study but I did this. And that's what we need to going at.

CHAIR BLEY: Let me turn John's question around just a little bit. I had asked staff earlier a similar question. But for the inspections that have occurred there were findings, there were violations cited, corrective actions that ostensibly were agreed to and carried out.

Among the kinds of things we saw there and the process we heard described by the staff this morning, are there places where, in your thinking, this

verbatim compliance didn't allow addressing the technical issues as they would have been in, say a Part 50 review?

Now are there corrective actions there you don't think were necessary? And if so, kind of why? Or in the end did you and the staff come to reasonable close agreement on how to deal with these issues that were found during the inspection so far?

MR. HIRMANPOUR: Under PMS we reached agreement it was a violation of the implemented corrective actions. On the CIM I would say that is a work in progress and that's part of the path forward we are taking.

Overall, as far as comparing the DAC inspection versus Part 50 --

CHAIR BLEY: Mm-hmm.

MR. HIRMANPOUR: I would say it is comparable, probably more comprehensive. This is probably, they done it, I mean, that's one of my summary, the first bullet said it was comprehensive and thorough. I mean, they did look at the requirements. They did look at the compliance in much more depth than I would say an ISG-6 process. But that's, I think it's definitely been more than I can --

CHAIR BLEY: I mean, I heard the staff say that whatever kind of review we were doing, if it were a Part 50 or if it had been, if you had a complete design when we did the Part 52, design cert, this expression of judgment doesn't bypass the requirements.

I mean, they are always requirements. And there might be matters of interpretation. Is there something there you disagree with? Are they somehow over-interpreting or is this working out? Are we getting to the place we want to be as it's moving forward?

MR. HIRMANPOUR: For the planning phase it's been challenging. The other phases, requirements, detailed design, I don't see any issues there. I mean, they are to the point they are reviewing the right information and right documents. Also they are not just limiting the documents they have. They are pulling the strings all the way out to safety analysis calculations. It's the planning that --

CHAIR BLEY: Are you in any way surprised that the first time through Part 52 things have been challenging?

MR. HIRMANPOUR: Well, no. But I was surprised as far as the level of review.

CHAIR BLEY: Okay.

MR. HIRMANPOUR: And, again, that's probably a problem that got created through DAC the way that we were planning to address it. Now there are a few ways to close the DAC. One of that being during the design certification. The other one, I mean, look at the second one there it talks about maybe during the COLA , which of course, we can do that.

The other one was after COL and one metric was actually a topical report. If I was going to go back two years they probably would have shown me that topical report. And because there is a judgment element in there, and some with subject to interpretation.

And, I mean, you look at the IEEE 830 on the software requirement inspection, it says software requirement spec shall be complete, accurate and ambiguous, okay. So --

(Simultaneous speaking)

MEMBER STETKAR: Well, that happens. But, again, your point is well taken because if the staff writes an SER on a topical report they reach a conclusion of reasonable assurance that the design, as specified in that topical report, will satisfy the

requirements.

It's reasonable assurance. It's not absolute unambiguity or absolute completeness or absolute correctness.

MR. JACKSON: It's Terry Jackson. Maybe if I could add something. I think what we're seeing is a difference in the processes within the staff's review. If we had to review a planning phase or a software program manual we would basically go through the standards and stuff that they said they've conformed to and compare that to what they're commitments are in the DCD.

Now the different process, if we have questions or we see issues, then we work it through RAI, through public meetings and then the applicant resubmits over the a revision and so forth.

In the DAC process there's not that type of process. It's basically, if you don't meet it, it's part of your licensing basis. So it's a non-conformance in this case.

And the remedy to it is either if they catch it early and say, well, this is a difference, this design change processes, it's like 50.59 or license and then they can come in and say we're actually going to do

something different here.

MEMBER RAY: Well, wait a minute. Let me interrupt you right there. I'm sorry to do this but the problem isn't so much, as I see it, did you or did you not comply with the requirements we established earlier but are those requirements the right requirements given the design that we are now looking at.

MR. JACKSON: Right. And I think with the DAC the issue with the DAC is that there is such a high level. So, for example, when they do 1000 they just basically say, okay, we commit to all these IEEE standards, to do them. So when the inspection staff go out they look at them and then say, okay, it doesn't.

MEMBER RAY: Yes.

MR. JACKSON: Whereas if it's in the licensing form then they say okay, we conform to these but here is additional information on specifics about okay, this is a nuance or something here.

MEMBER RAY: Right.

MR. JACKSON: And the staff gets to understand it. And then when we write the SER then it's a lot more clear. So we haven't run into those kinds of issues when we reviewed or did inspections

on the Common Q software like we had on CIM, and that's part of the reason why.

It's because the criteria that CIM, that DCD for CIM is at such a high level that they haven't really spelled out, okay, these are really how we interpret.

MEMBER RAY: If you're writing an SER it's different than writing an inspection report. I mean, just inherently that's true. You could try and make them be the same by making the inspection report more encompassing than an inspection report would normally be. And I think that's what you're doing.

But they still aren't the same. And I think what we're trying to do is figure out if there's anything we can do as input to the Commission's thinking about this right now and that's why we're asking the questions that we are.

MR. JACKSON: So kind of what we're doing right now, as the licensing staff, in the current reviews we're doing is we're asking questions about why can't certain information be provided at the licensing stage. Now the CIM is an artifact from the original AP -- well, the CIM DAC is an artifact from the original AP-1000 certification.

It was a DAC at that time so when it came in and we found that the plain document wasn't sufficient in the amendment then they just referred it back to the DAC again. But on the current designs we're asking questions on the planning phase and saying, okay, we've committed to certain standards but exactly how are you implementing them.

Because within the standards there's a lot of flexibility and you really have to understand what you're doing. So that's why we're not really seeing these same kind of DAC issues on, like EPR or USAPWR because we're challenging them now on this --

MEMBER STETKAR: But you guys see them on ESBER.

MR. JACKSON: Yes, the ESBER we do but that, yes.

MR. FREDETTE: But those won't be planning phase issues. Those will be more requirements and development done the line.

MR. JACKSON: That may well be.

MEMBER BROWN: It could be a lot more functional design stuff you get involved with because it's --

CHAIR BLEY: Well, that'll happen when it

happens. I want -- do you have a question?

MEMBER STETKAR: Yes. Well, actually I did for Tom. I was curious because when I went through the non-conformances on the Westinghouse inspection that the, whatever it was, the one that you talked about, the CIM. They were grouped into, there were two non-conformances written.

And I tried to read through between the lines. And they seemed to be grouped -- one of them seemed to focus more on the issues that Bob was talking about. In other words, compliance with, verbatim compliance with line by line IEEE standards.

And the second one seemed to address what I would call somewhat more substantive issues. Was that a conscious decision?

MR. FREDETTE: I couldn't speak to that. You know, the vendor branch, it was a vendor led inspection.

MEMBER STETKAR: Yes.

MR. FREDETTE: So the vendor branch inspection lead, he has responsibility for how he bins these together. You're right though.

MEMBER STETKAR: Okay.

MR. FREDETTE: All inspectors, we tend to

look at compliance. We look at implementation of certain requirements and then we look at compliance. And I think this was, the fact that some of these are more compliance issues versus process --

MEMBER STETKAR: In some sense, you know, moving forward if this can, is a point of contention, that type of process might help it at least. Because if you can bin together the strictly compliance oriented findings from an inspection versus the more technical related issues, I think you will --

MR. FREDETTE: And I'll be honest, I would, if it was me I would not have agreed with some of these compliance --

MEMBER STETKAR: Yes, but that's individuals. You know, that's not --

MR. FREDETTE: The point is Bob, he mentioned an example, a feasibility study, okay. In my mind, when we did this DAC inspection I would have, I was more concerned with the fact that software safety, hazards analysis wasn't captured once again. And that's what's, that's the other bin. That's not just portions of it.

MEMBER STETKAR: That's the other, that's the second bin.

MR. FREDETTE: Yes.

MEMBER STETKAR: Yes, that's the second bin. You're right.

MS. VALENTIN: This is Andrea Valentin. Going back to your question, Mr. Stetkar, that was a conscious decision. The person that led that inspection is planning to do that here on out.

MEMBER STETKAR: That could help to at least organize the way that both the licensee and the staff gets to resolution on this stuff going forward.

CHAIR BLEY: Mr. Hirmanpour, I'm sorry. I let this move back to staff, but back to your presentation if you want to finish up here.

MR. HIRMANPOUR: Okay, so overall going forward, right, we're saying we're going to do verbatim compliance which is impossible on those programmatic type of IEEEs. It's basically define our position and say what are the alternatives to the reg guides. So, okay, that's acceptable but here's how we did it.

Now, again, back to what inspection is, as Terry mentioned, when you have the software program manual and you have the card-to-card reports you get RAIs. Now if something the staff doesn't agree with that generally becomes findings and non-conformances

which is one of the by-product the inspections compared with a topical report.

All right, then we are completing the work on that. We are doing the oversight. The way this ITAAC is set up, ITAAC-14 and a similar ITAAC on, I believe on ESBER is what, like 220 DAC and ABWR is like 15 pages.

14.a is basically the planning phase. Now even though we're going to finish and the inspection is going to happen, we won't be able to complete that. You won't see any DAC completion package. We have to complete the whole ITAAC which includes installation. Now, again, that's something we need to finalize, what installation means, because if we can conclude that installation means installing the CIM inside the PMS. That's the end of CIM and the effort that PMS takes over. We should be able to probably complete that ITAAC next year.

If part of that is install the PMS in the plan that's going to take another two or three years. Again, the work doesn't change. It's a matter of timing when your start your ITAAC completion notice.

That is all I had. Again, my suggestion is that for the planning phase DAC definitely keep the

people from the I&C branch involved because, especially, I&C has been involved over the past 20 years, most of it because of Charlie.

But, nonetheless, you need to, the bar keeps moving. That's probably one of the challenges we have right now. I mean, the SBN, that's right now you see for CIM it's more comprehensive than any other SBN you've seen, combined with all the other plants. But the bar is moving every day and that's the nature of the business now.

CHAIR BLEY: Okay. Well, at least the first time through. Okay, we thank you very much. And thanks to the staff. Those were great presentations.

We'll go around the Committee in a minute but can we get the --

MS. CLARK: Yes.

CHAIR BLEY: -- phone line opened up? Is there any member of the public or anybody else here who would like to make a comment at this time? The mic's open? This is open? Is the phone line open? Would somebody please say hello so we know you're there?

MALE PARTICIPANT: Hello, and no comment at this time.

CHAIR BLEY: Okay. Is there anybody on the phone line who was not among the people we mentioned at the beginning? If so, I would like to have you introduce yourself so we have you on the record as participating in the meeting.

Are there any other comments from people on the phone line? Given not, I guess, personally, I look forward to the piping inspection reports and the HFE inspection procedures and results. We want to see where that's headed.

As we do that, I'm going to ask the subcommittee, do we need to follow things the way we've been following, the way we've just followed this one or do we need to do something different or see something different as we proceed? We want to follow this through, then comes the question later as to whether or not it's one look or more looks, the first few, for the ACRS.

At this point, I guess I'd like to go on around the table, and I'd start with Mike Corradini for any comments from today's meeting.

MEMBER CORRADINI: I have no comments.

CHAIR BLEY: Charlie.

MEMBER CORRADINI: I pass to Charlie who

has comments.

MEMBER BROWN: Well, I found this particular DAC briefing very, very good. It's much, this is, it's, I guess emblematic of having some real results from which to draw conclusions to see how this stuff is being executed and what you're finding and how you intend to do so.

Because it opened the door to a number of questions and I've found the responses very informative and I actually thought this was a pretty good brief relative to where we are.

I'm not quite sure where we go from here. I do know on the commercial grade thing it's, I'd just like to have some idea of what's involved with that, how it's going to be executed, largely from an information standpoint.

I'm not quite sure how to resolve this issue of verbatim compliance. And it's kind of a, I think the staff and the licensees are going to have to work that out. If judgment has been lost, how do you get it back?

I mean, you really kind of operate in a world where if you didn't have exceptions you wouldn't need rules. That's kind of one way of looking at it,

but you've got to be really careful about that. So I don't know how to resolve that forum other than to work out the details as they go.

CHAIR BLEY: Ron?

MEMBER BALLINGER: This is not my area but I found it very, very informative. I was sitting here feverishly downloading documents. I have about 20 documents which I'm going to go read tonight so that the next time we have one of these meetings I'll be a little bit smarter.

MEMBER BROWN: No, you'll them all by then. It's a two-year cycle. I'm just kidding.

MEMBER BALLINGER: I'm not as old as you are.

MEMBER BROWN: Oh, man, that hurts. It's true though. I won't disagree with that.

CHAIR BLEY: Yes, but you're probably in better shape, Charlie.

MEMBER BALLINGER: That I'll agree with.

CHAIR BLEY: Dr. Powers?

MEMBER POWERS: Well, again, I really appreciate the staff's presentation. And I don't envy you your job at all. I think it's formidably difficult. It's also one where we owe diligence to the Commission

because I think they are absolutely dependent on our good foot and bad, especially as we go through the first few plans, new plans.

So I think, in answer to your question, should we do more? Yes, I think we absolutely have to because I think they're absolutely dependent on us to do, to plunge into the details on this.

CHAIR BLEY: Okay, thank you. Harold?

MEMBER RAY: Well, I want to echo what Charlie said, the compliments about the presentation. And I think that one of the things that concerns me is that we have AP-1000 here as the active exemplar. We have staff and applicant, or licensees and DCD holder, vendor, all of whom are, I think, working together as well as they could.

And I just don't know if that's a good basis on which to build confidence about how this would work in the future with other applicants, other licensees, other DCD holders and other circumstances.

Therefore, I tend to look more at whether the requirements literally, although it's important how they're being implemented at this point in time, I also know, having gotten a CP, built a plant and gotten an OL that you have to have something that is, that can

replicate itself reliably.

And I would share what Dana has expressed which is I just don't know how to proceed other than by continuing to be involved and assess the situation.

The topical report approach, I think, is an excellent example, one that I would like to see, particularly in areas like Digital I&C and so on, that would allow rather than an inspection, would allow a staff-written SER to be used to reach the conclusion that John described, which is reasonable assurance, rather than a verbatim compliance inspection which is more or less what we're going to wind up with, I think, at the end of the day.

Because at the end of the day this will be routinized so that people will do what the procedures call for to be done. And so I think we've got to be concerned about that, not just how acceptable the current process is.

And it appears to be, I mean, I don't find any significant fault with what's described to us as taking place. The real question is is it, will it last under more difficult circumstances that may emerge in the future.

And so that's about all I want to say,

Dennis. I don't want to be, having been an advocate for Part 52 in years past and realizing that his was going to be a problem that we would face. Now we're facing it. I would just say it's a work in progress.

CHAIR BLEY: Thanks. Steve?

MEMBER SCHULTZ: Yes, I'm in agreement with all the comments that have been made by the committee members so far. And this is my first time into the topic in terms of the subject as a member.

So I was a bit concerned with the discussions earlier this morning and the materials that were being discussed there as well, having reviewed them.

I felt a lot better about the process and how it was going, Tom, by what you presented and what we've heard from Southern Nuclear, from Bob's presentation with respect to what has been learned, what has been completed and done in the examples shown.

For the reasons that Harold presented, it's really important, given the insights and lessons learned that you presented, Tom. I thought the findings were, in fact, substantial, and they were numerous. The findings should be very helpful in terms of improving the process and its implementation.

So you expressed that that's going to be an improvement opportunity that will be followed through upon. And I certainly hope that that is something that you, you and your staff, have enough time to work on.

With regard to the overall capture of lessons learned, with additional guidance, I really would be looking for that follow through. I didn't find that the outcomes in relationship to the process that was set out in Part 52, I didn't think the outcomes that we saw in the evaluations that have been done were surprising or unexpected.

And I wouldn't necessarily use those to jump to conclusions about how the process should be improved from here with regard to the inspection procedures, guidance and documentation, which I believe needs improvement. And I'm saying that because I think the tendency would be to jump to conclusions about how improvements might be based upon the way we've done things in the past.

And I do think we have to look to the future and think both in an integral sense about how that would be accomplished. It's worthwhile thinking about it hard before we make quick changes and improvements.

And we need to reflect on what intention of the process, the Part 52 process is before we jump to patchwork improvements.

CHAIR BLEY: Thank you very much, Steve. Mr. Stetkar?

MEMBER STETKAR: Yes, I, again, thanks to the staff and Southern for, I think, really good presentations. I viewed this meeting as, for my personally, mostly confidence building. And I think that's good.

As to the question, should we continue, I think absolutely, yes. I think that, from my perspective building of the confidence in terms of the effectiveness of the DAC inspection process to achieve the equivalence of design review won't be proven until we actually follow through the entire inspection process.

I'm cautiously optimistic given what I'm seen in terms of programmatic elements for Digital I&C the early part of the process which, admittedly, is mostly programmatic. Remain curious about the other, both the piping and the HFE and the follow-on through the completion of the DAC inspections for Digital I&C.

And because of that I think we need to

follow it on. But the staff needs to have some board inspection results, I think, available so that we can kind of compare what they've actually found and how they found it.

CHAIR BLEY: Thank you. Mr. Banerjee.

MEMBER BANERJEE: Thanks. I came to this meeting just to see what was being done about the piping DAC. But unfortunately nobody else knew I was at this meeting so they kept calling me and I was called out just when that was being handled.

The concerns there had been, if you recall back in the AP-1000 days, that we were worried about gas binding so that there had to be a certain slope and things in this.

And how those are being factored in, I think, is something which we need to follow. That's really all I have to say right now. But you probably recall that, don't you, Bob?

MR. HIRMANPOUR: Yes, there was a generic letter or something that came out and B

MEMBER BANERJEE: Yes, so we were concerned that you are progressing this in some way. Okay. I was away, unfortunately, out of the office.

CHAIR BLEY: That's all right. The real

piping DAC inspections will be the next time around.

MEMBER BANERJEE: Yes.

CHAIR BLEY: But be sure you have a strong invitation to come.

MEMBER BANERJEE: Yes, all right. Thanks.

CHAIR BLEY: Okay, well I, too, would like to thank the staff and Southern Nuclear for being here, and supporting the meeting. And I probably shouldn't say this but I really had trouble with this whole concept when I came across it.

But after today's meeting I would finally say I think the emperor actually has some fine clothes. And I hope we get to see the whole wardrobe. We do need to follow this and I'm looking forward to that process.

I'm much encouraged by what I hear today. And I really like Dana's point. And I've highlighted it for myself. We owe the diligence to the Commission on this one. We've been talking about it since its origins in about 1992, I think.

We've talked to them about it and now it's at the point we're going to be able to begin to say something substantive. But we've just begun. I'm not

sure, I kind of think we're also going to have to look at somebody who has more substantial amounts of I&C DAC before we gain the full confidence we're looking for.

So we really are looking forward to this. I guess, personally, I'm looking forward to reviewing the transcript, making note of all the commitments I heard made today. And I appreciate them very much.

I agree with all my colleagues on this and we look forward to continuing this process. Thanks very much to all of you and --

MEMBER BROWN: When you're done.

CHAIR BLEY: Mr. Brown, I'm done enough for you to go ahead.

MEMBER BROWN: I just wanted to make -- you're right. We have not done ESBER yet. Lots of DAC, lots of I&C DAC. In spite of what was done during our development of the license and our panel letters and stuff.

CHAIR BLEY: There's always the first one. So we can have as much impact there as we --

MEMBER BROWN: Yes, I know we didn't have any. And all I kept getting hit with was the well, we got to have the Part 52 and the DAC because the pace

of, the rapid pace of technology development in the I&C world is so rapid and so vast and so complex that there is no way that we can define these I&C systems well enough, functionally, in order to come to a licensing conclusion. And therefore we must depend on this new way.

Fundamentally, still, based on what we've done is I disagree with that. And I think it is, if we're going to do due diligence, my opinion again, for the Commission is that we really ought to evaluate that tenet, because I think it's wrong, and that we should try to develop a better approach relative to how we specify and do this at the licensing stage, that we can eliminate the DAC.

Because I don't think you get as good an overall integrated review via the staff and the Committee by having to resort and then depend on DAC coming down three, four, five years hence for licensing. So that was just, I wanted to get that on the table a little bit relative to some of the other discussion. I mean, we talked about the due diligence.

CHAIR BLEY: No, I think that's coming. And I think the Chapter 7, the small modular reactor, is going at the direction for that for future reviews.

And I think that'll lead it. I wouldn't be surprised to see people not wanting to go through this process again and maybe seeing something at COL stage.

In any case, thanks to everyone.

MEMBER BROWN: SRS, by the way, is an approach. We've taken those steps.

CHAIR BLEY: That's right. And we think that's going to be applied to the next development but we don't know for sure.

MEMBER BROWN: We'll keep working at it.

CHAIR BLEY: So thanks again to everyone. This was a great meeting for us and we appreciate all you've done and look forward to the future. This meeting is adjourned.

(Whereupon, the meeting in the above-entitled matter was concluded at 11:58 a.m.)

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

Presentation to the ACRS

Design Acceptance Criteria Inspection

Progress and Status

Thomas Fredette, PE
NRO/DCIP/CIPB
thomas.fredette@nrc.gov

July 8, 2014

Objectives

Provide the Committee:

- **Status of Working Group activities, with emphasis on DAC inspection implementation**
- **Overview of staff's approach to AP1000 DAC inspection**
- **Results of DI&C inspection activities**
- **Insights and Lessons Learned to date**
- **Overview of future activities**

Background

- Task Working Group established 11/2009 to develop viable inspection strategy for DAC
- Inspection process and procedure development initiated w/ STP for ABWR DI&C DAC; pilot inspection 6/2010
- Staff committed to periodically brief ACRS on status (10/2010)
- Focus shifted to AP1000 after Fukushima event
- Initial engagement w/ AP1000 DCWG (Piping, DI&C); inspection procedures finalized 9/2011
- Briefed ACRS on AP1000 approach 11/2011; committed to periodic briefings as inspections implemented

Significant Activities

- **Initial inspection conducted 4/2012 for AP1000 ITAAC (Protection & Safety Monitoring System (PMS) life cycle requirements phase)**
- **Consortium (licensees and WEC) corrective actions (2012 - 2013)**
- **Various public and working level meetings w/ consortium**
- **AP1000 DI&C DAC inspection (1/2014)**
- **Piping DAC – conducted walk-through (tabletop) of piping DAC inspection process (7/2012)**

Inspection Model

- **DAC inspection is ITAAC inspection**
- **Incumbent on Licensee to perform and complete ITAAC – Staff verifies through inspection**
- **DAC inspection engages NRC technical staff to augment inspection activity**
- **Reliance on construction and ITAAC performance schedule**
- **Results documented in Inspection Report; archived to support ITAAC closure process verification**

Piping DAC Inspection

- **Procedures developed to address AP1000 site-specific ITAAC (DAC) for piping design and pipe rupture hazards analysis (PRHA)**
  - **IP 65001.20 (design)**
  - **IP 65001.21 (PRHA)**
- **Both procedures issued in late 2011**

AP1000 Piping Design
Site-specific ITAAC

Design Commitment	Inspections, Tests and Analyses	Acceptance Criteria
The American Society of Mechanical Engineers (ASME) Code, Section III piping is designed in accordance with ASME Code, Section III requirements.	Inspection of the ASME Code Design Reports (NCA-3550) and required documents will be conducted for the set of lines chosen to demonstrate compliance.	The ASME Code Design Report(s) (NCA-3550) (certified, when required by ASME Code) exist and conclude that the design of the piping for lines chosen to demonstrate all aspects of the piping design complies with the requirements of the ASME Code section.

AP1000 PRHA
Site-specific ITAAC

Design Commitment	Inspections, Tests and Analyses	Acceptance Criteria
Systems, structures, and components (SSCs), that are required to be functional during and following a design basis event shall be protected against or qualified to withstand the dynamic and environmental effects associated with analyses of postulated failures in high and moderate energy piping.	Inspection of the as-designed pipe rupture hazard analysis report will be conducted. The report documents the analyses to determine where protection features are necessary to mitigate the consequence of a pipe break. Pipe break events involving high-energy fluid systems are analyzed for the effects of pipe whip, jet impingement, flooding, room pressurization, and temperature effects. Pipe break events involving moderate-energy fluid systems are analyzed for wetting from spray, flooding, and other environmental effects, as appropriate.	An as-designed pipe rupture hazard analysis report exists and concludes that the analysis performed for high and moderate energy piping confirms the protection of systems, structures, and components required to be functional during and following a design basis event.

Piping DAC Inspection Objective

- For piping design – verification of the methodology for piping design through sampled piping packages (13 Class 1, 35 Class 2/3)
- For PRHA – verification of the methodology through a sample of room/area PRHA reports
- Goal is verification that the methodologies are sound and conform to licensing basis

Piping DAC Inspection Planning Tabletop Exercise

- **Public meeting July 2012 to walk through inspection approach and procedures for piping design and PRHA**
- **Utilized sample Class 2 package for passive core cooling system (PXS)**
- **Outlined inspection framework**
- **Outlined procedure attributes, generally mirroring criteria in DCD Table 3.9-19**
- **Outlined procedure for PRHA (DCD 3.6- dynamic and environmental effects, pipe break/crack type, location, etc.)**

Piping/PRHA DAC Inspection Planning

- Anticipated packages would be ready for inspection in 2013
- Actual availability- early 2014 for Class 2/3, TBD for Class 1
- Inspections are deferred until Class 1 packages become available
- Goal: align inspection resources to availability schedule
- Similar approach for PRHA reports

Digital I&C DAC Background

- Initial primary focus of DAC working group
- Pilot inspection for STP in 2010
- Focus shift to AP1000 in 2011
- First meetings w/ applicants in Oct 2011
- AP1000 DI&C ITAAC includes one DAC (PMS-CIM “Planning” Phase)
- Generic procedure – IP 65001.22 issued late 2011

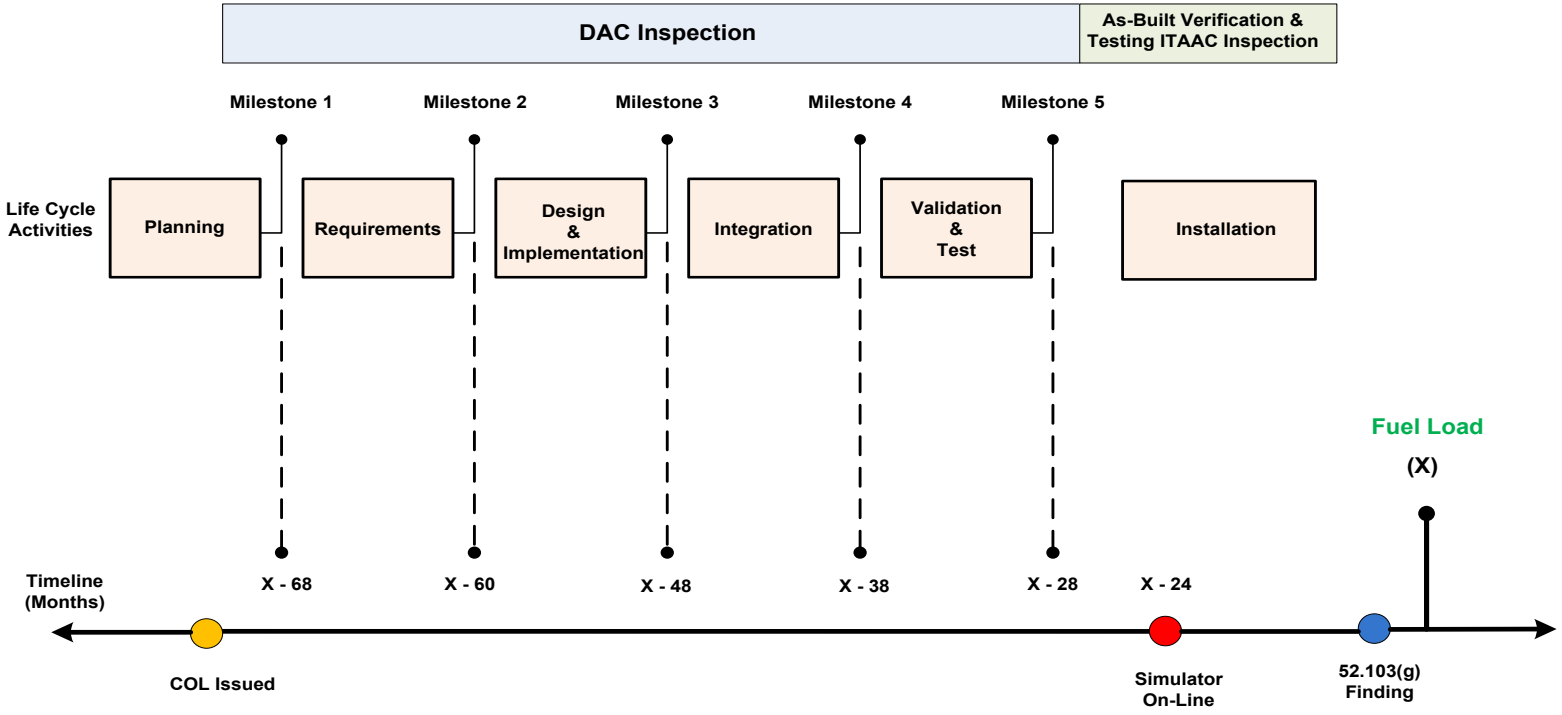
DI&C DAC Procedure

- **Guidance borrowed from SRP, industry standards, NUREGs, staff expertise, etc.**
- **Generally mirrors typical DI&C system development life cycle**
- **Guidance for sampling of life cycle attributes and design outputs**
- **Focus: process, C/M, IV&V, traceability throughout the development life cycle (requirements to system/software design to code to system integration to testing)**

DI&C DAC Inspection

- **Front-loaded effort for the life cycle Planning and Requirements phases**
- **Inspection conducted for each safety-related DI&C platform at development milestones**
- **Early and continuous engagement w/ licensees allows for optimum deployment of inspection resources**

DI&C DAC Inspection Strategy



Digital I&C Development and Inspection Chronology (Notional)

DI&C Core Inspection Expertise

Lead RII Inspector: Industry IV&V expertise for various digital upgrade projects, including Callaway feedwater pump control and the Oconee RPS/ESFAS project (TELEPERM platform). Authored CMP, SSP, IVVP and developed FMEA for these projects. Design engineer for Callaway Flux Mapping System digital upgrade (SIMATIC PCS7 platform)

RII Inspector: 20+ years professional industrial automation experience in human machine interfaces, SCADA, robotics, and PLC and DCSs.

Tech Staff Expert: 20+ years experience with the development, design, installation and validation programs for digital instrumentation and controls equipment as I&C design engineer; technical lead for AP1000 I&C licensing and review engineer; NRC rep for IEEE STD 1012 (V&V) working group.

AP1000 DI&C ITAAC Inspection

- **Opportunity to validate inspection process and procedure in real DI&C development setting**
- **Inspection conducted March-April 2012 at WEC**
- **Focus: AP1000 Protection & Safety Monitoring System (PMS) life cycle "Requirements" and high level Planning documents (ITAACs 2.5.2.11.b/2.5.2.12)**

ITAAC Inspection Scope

- Requirements Phase Design Output – PMS Software Requirements Specification (SRS)
- Sampling of PMS reactor trip and ESFAS signals (traceability of system and functional requirements)
- Independent V&V activities and results
- Compliance with the AP1000 PMS licensing basis (software and configuration management)

ITAAC Inspection Results

- **Inspection Report (*ML12171A058*)**
- **Notice of Violation (Design Control) for the following:**
  - **IV&V Tasks not performed for the SRS**
  - **Lack of V&V independence**
  - **No hazard analysis for the SRS**
  - **Custom software control (outside process)**
  - **Incomplete SRS**
- **WEC/Licensees initiated extensive corrective actions (*ML12205A298*)**

Corrective Actions

- **Licensees/WEC conducted RCE and identified I&C organizational issues:**
  - **lack of regulatory guidance in procedures**
  - **lack of management enforcement of corrective action program to resolve systemic I&C issues;**
  - **lack of inclusion and verification of process requirements in I&C development project documents**
- **<u>Short-term</u>: mandatory stand downs at WEC, including Part 52 training, and QA audit at sub-vendor CSI to raise level of awareness associated with DI&C projects.**
- **<u>Intermediate</u>: correct NOV examples identified by inspection, gap analysis between licensing basis and process, update processes and procedures, training, and update of work products (project outputs).**
- **<u>Long-term</u>: new/revamped processes for training oversight, review of procedures, standards, work products, etc. to ensure regulatory compliance, and project-based licensing plans.**
- **Full compliance achieved in 2013- verified through follow-up inspection**

Result - Setback for Licensees/WEC with respect to schedule for completion of DI&C ITAAC and DAC

Preparation for DAC Inspection

- **Monitoring of Licensee/WEC corrective action progress and PMS-CIM schedule**
- **Alignment of inspection resources**
- **Use of WEC virtual reading room for document review, detailed inspection planning**

AP1000 DI&C DAC Inspection
PMS Component Interface Module
ITAAC 2.5.2.14

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
The Component Interface Module (CIM) is developed using a planned design process which provides for specific design documentation and reviews. {Design Acceptance Criteria}	An inspection and or an audit will be performed of the processes used to design the hardware, development software, qualification and testing.	A report exists and concludes that CIM meets the below listed life cycle stages. Life cycle stages: **a. Design requirements phase, may be referred to as conceptual or project definition phase** b. System definition phase c. HW and SW development phase, consisting of HW and SW design and implementation d. System integration and test phase e. Installation phase

PMS Component Interface Module

- **PMS-Component Interface Module (PMS-CIM) design requirements (aka Planning) phase was never adequately addressed during certification, hence it remained as DAC (ITAAC 2.5.2.14.a)**
- **Field Programmable Gate Array (FPGA) platform**
- **CIM is a sub-component embedded within PMS and serves as an interface between safety components and controls**
- **Beyond life cycle planning phase, remainder of CIM development (ITAACs 2.5.2.14.b/c/d/e) is treated as standard ITAAC**

DAC Inspection Scope (January 2014 Inspection)

PMS-CIM

- Software Management /Project Plan
- Software Safety Plan; FMEA and Hazards Analysis
- SQAP and Software Development Plan
- Software Integration/Test/Installation Plans
- Software Configuration Management
- CIM IV&V Plan

DAC Inspection Results

- **Vendor Inspection Report (*ML14058A995*)**
- **2 Notices of Nonconformance issued to Westinghouse for Design Control deficiencies related to:**
  - **CIM project plan compliance w/ licensing basis (IEEE Stds 1074, 1012 and 828)**
  - **Incomplete CIM configuration items**
  - **Inadequate IV&V Plan; failure to translate IEEE Std 1012 requirements, and failure to adequately address CIM software hazards**
- **WEC corrective actions in progress- staff will verify during August 2014 inspection**

PMS-CIM Inspection Status

- DAC inspection is complete pending verification of corrective actions
- Expect to conduct next ITAAC inspection (CIM life cycle “Requirements”) late 2014
- Staff continues to monitor progress through working meetings/dialogue w/ licensees and WEC

Recent DAC Inspection Insights

- Achieve common understanding on interpretation of the DAC
- Dedicated inspection planning is essential; resources are limited, technical staff involvement aids the planning effort and selection of inspection attributes
- Use of virtual reading room for planning
- Understanding organizational and document hierarchy can streamline the inspection effort (pre-briefs are valuable)
- Inspection effort has matched the level of technical review
- Technical staff has adapted quickly to inspection
- Smaller inspection team and more inspection time is optimum
- Challenge – maintaining continuity among inspectors
- Continuous ID and implementing procedure enhancements

Expectations for 2014/2015

- Conduct first piping DAC inspection – TBD 2014
- Conduct first HFE DAC inspection – Oct 2014
- Continue to enhance process where necessary
- Prepare for other design center DAC (ESBWR)
- Brief ACRS as appropriate

Conclusion

- Staff has demonstrated process for DI&C DAC inspection (on limited basis)
- Staff is positioned for piping DAC inspection
- Process applies appropriate technical rigor (breadth and depth of expertise) to inspection efforts
- Process is flexible and adaptable
- Process will verify design implementation to licensing basis

Discussion/Committee Questions

AP1000 I&C Design Acceptance Criteria (DAC)

Bob Hirmanpour
Vogtle 3&4 Regulatory Affairs
July 8, 2014

Background – PMS DAC

- AP1000 Design Control Document Tier 1 included two (2) Design Acceptance Criteria (DACs) described in Protection and Safety Monitoring System (PMS) ITAAC 2.5.2.11 (parts a and b corresponding to planning and requirement phases).
- The above PMS DACs were completed during the AP1000 design certification. Part b of the ITAAC remained open but it is not considered a DAC.

Note: AP1000 PMS provides reactor trip, engineered safety features actuation and post-accident monitoring functions.

COL Appendix C Table 2.5.2-8
Inspections, Tests, Analyses, and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11. The PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages: a) Not used b) System definition phase c) Hardware and software development phase, consisting of hardware and software design and implementation d) System integration and test phase e) Installation phase	Inspection will be performed of the process used to design the hardware and software.	A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management controls for the following: a) Not used. b) Specification of functional requirements. c) Documentation and review of hardware and software. d) Performance of system tests and the documentation of system test results, including a response time test performed under maximum CPU loading to demonstrate that the PMS can fulfill its response time criteria. e) Performance of installation tests and inspections.

Background – CIM DAC

- ITAAC/DAC 2.5.2.11a was specific to planning phase of PMS software life cycle development.
- During the completion of this ITAAC/DAC, the NRC staff requested the addition of a similar ITAAC (ITAAC 2.5.2.14) for the Component Interface Module (CIM).
- CIM was a new product under development at that time. Since CIM is FPGA (Field Programmable Gate Array) based, NRC imposed safety system software development processes for CIM development.

COL Appendix C Table 2.5.2-8
Inspections, Tests, Analyses, and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
14. The Component Interface Module (CIM) is developed using a planned design process which provides for specific design documentation and reviews.	An inspection and or an audit will be performed of the processes used to design the hardware, development software, qualification and testing.	A report exists and concludes that CIM meets the below listed life cycle stages. Life cycle stages: a. Design requirements phase, may be referred to as conceptual or project definition phase b. System definition phase c. Hardware and software development phase, consisting of hardware and software design and implementation d. System integration and test phase e. Installation phase

CIM Development

- CIM is a component of PMS and serves as an interface between the safety components and safety / non-safety controls. CIM also provides priority control function.
- CIM was developed by CSI, an Appendix B company. CSI was later acquired by Westinghouse.
- CIM was developed as a stand alone product to be used on future safety system digital upgrades and AP1000.
- CSI used a defined process for FPGA development including Independent Verification and Validation (IV&V)
- Similar processes were previously used for a digital upgrade at Wolf Creek Nuclear Plant and approved by the NRC.

DAC Inspections

- Regulatory Guides, DCD and CIM ITAAC/DAC are geared more toward a digital system rather than a digital component embedded in a safety system.
- Planning phase Industry Codes and Standards (i.e., IEEEs) are focused on digital safety systems upgrades rather than new plants and digital safety components development.
- AP1000 DCD requires full conformance to the Regulatory Guides that endorse IEEE Standards for safety system/software development.
  - This has created challenges during CIM development and NRC inspections.

Summary

- CIM ITAAC / DAC inspections have been comprehensive and thorough.
- Licensees are continuing work on the completion of AP1000 I&C ITAACs/DAC.
- CIM DAC will be closed as part of the overall ITAAC 2.5.2.14 once all associated activities have been completed.

Questions?