# Official Transcript of Proceedings

# NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Friday, February 27, 2009

Work Order No.: NRC-2691 Pages 1-137

**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

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

MEETING

+ + + + +

FRIDAY, FEBRUARY 27, 2009

+ + + + +

ROCKVILLE, MD

+ + + + +

The Subcommittee was convened in Room T2B3 in the Headquarters of the Nuclear Regulatory Commission, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, at 8:30 a.m., Dr. George Apostolakis, Chair, presiding.

Subcommittee MEMBERS PRESENT:

GEORGE APOSTOLAKIS, Chair

CHARLES H. BROWN, JR.

MARIO V. BONACA

JOHN W. STETKAR

DENNIS C. BLEY

JOHN D. SIEBER

CONSULTANTS TO THE Subcommittee PRESENT:

SERGIO GUARRO

MYRON HECHT

NRC STAFF PRESENT:

CHRISTINA ANTONESCU, Designated Federal Official

MICHAEL WATERMAN

STEVEN ARNDT

ALSO PRESENT:

RICHARD WOOD

RAY TOROK

TED QUINN

MIKE CASE

T-A-B-L-E O-F C-O-N-T-E-N-T-S

Opening Remarks, George Apostolakis................4

Review of Draft NUREG/CR "Diversity Strategies of Nuclear Power Plant Instrumentation and Control Systems," (Continued), Mike Waterman...............4

Comments by Subcommittee Member..................121

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

8:28 a.m.

CHAIRMAN APOSTOLAKIS: This is the second day of the ACRS Subcommittee meeting on the digital I&C. Mr. Waterman has the floor.

Please.

MR. WATERMAN: Thanks, George.

Just to bring us back to where we were yesterday, yesterday we talked about the issues that are to be addressed by the research, the diversity attributes and criteria that we are using. We then went into some operating experience considerations just briefly. We talked about the sources of data we're using and talked about some of the research assumptions that we used when we did the research.

And so today we'll pick it up from the data evaluation method by first recapping some of the research assumptions. And this will be on slide 23, for those of you who want to come up to speed on that.

The research assumptions were, we said we'd use diversity positions and designs used by other people on the basis that they probably used operating experience and judgment in developing those designs, that we would then try to correlate that information with NUREG/CR-6303, diversity attributes and criteria. And that by doing that, we should be able to develop an evaluation process that we could apply the design to. Well, the new design's in. You'll see how they stack up, if you will, against what the rest of the world is doing. And then we would try to capture some better perspectives out of industry and nuclear power plant operating experience and see if that could help us in developing this method.

So practically speaking, what we did was we took the NUREG/CR-6303, diversity criteria and attributes. And there's a circle here; the rest of them aren't, but that's all right. We transferred that data into a spreadsheet format. We used Microsoft Excel spreadsheet. And by taking those diversity criteria; they were ranked in 6303 as I explained yesterday, we developed a simple waiting system that would give more emphasis to more effective criteria and less emphasis on less effective criteria.

CHAIRMAN APOSTOLAKIS: So, you know, let me understand this a bit better.

MR. WATERMAN: I'll get into the actual weighting assumptions and stuff like and --

CHAIRMAN APOSTOLAKIS: But what's the

intent? Why are we doing all this?

MR. WATERMAN: We're doing this to develop a method of evaluating proposed diversity approaches. Say a licensee determines off of a BTP 7-19 analysis that they need a diverse low-pressure injection actuation system because the operator doesn't have enough time to respond to a large-break LOCA. And so they need to develop a diverse system to do the automatic initiation of low-pressure injection.

The question that's always come up is they propose a design and then they don't know whether that design is diverse enough to meet all the criteria it needs to meet, have sufficient diversity. Because there's been a lot of uncertainty, regulatory uncertainty as licensees propose designs and the regulator says well, I don't know if that's enough. Is it really diverse, and things like that. And we're trying to nail that down to where there's not all of that uncertainty, that when a licensee proposes a design using this method here, verifying it through this method here, that the NRC staff can also use this method to verify, yes, it looks like it's diverse enough and we, through our review process, confirm yes, all of those features are in the design.

And so, the easiest way to do that is if you have some numerical range to start out with, then you can screen out diverse designs that just don't fit into the range. They're way too low, for example. And designs that are within that range, the licensee has some, if you will, certainty that it's probably good enough.

CHAIRMAN APOSTOLAKIS: So essentially you are developing a metric called diverse --

MR. WATERMAN: Thanks. That's a very good way to put it.

CHAIRMAN APOSTOLAKIS: And if this is -- I mean, the scale is what, zero to one?

MR. WATERMAN: Well, the scale is zero to some number just slightly less than two.

CHAIRMAN APOSTOLAKIS: Okay.

MR. WATERMAN: When you plug all the Xs in, it comes up --

CHAIRMAN APOSTOLAKIS: Yes.

MR. WATERMAN: But 1.0 would represent the average diversity that we've seen in the applications that we've actually tried to address deliberately diversity strategy.

CHAIRMAN APOSTOLAKIS: So if I have to designs and one has a metric of 1.2 and the other .7, then I can claim the one with 1.2 is more diverse?

MR. WATERMAN: Yes, exactly. It is probably more likely to be accepted and approved in a review process.

MEMBER BROWN: There was another comment you made yesterday day though about effective. The higher the number, the more effective.

MR. WATERMAN: Yes, the --

MEMBER BROWN: Relative to whatever the diverse --

CHAIRMAN APOSTOLAKIS: Yes. Yes.

MR. WATERMAN: No, the thing I have to keep focusing myself on, and I hope everybody else does, the mission here isn't how much diversity is in the system, right? The mission is to address common-cause failures, not just to build diverse systems. The idea of a diverse system os to address some potential range of common-cause failures. That's where operating experience can help out and where engineering judgment can help out, is to identify the common-cause failures that have to be addressed. And so any diversity strategy should be focusing on we've got a common-cause failure microprocessor. Okay. We'd better do something about some diversity in that area so that if that occurs we're not affected in our diverse system.

MEMBER BROWN: So another way to phrase that, you're really trying to develop a ranking that would give you a numerical metric or a numerical ranking of how effective is the diverse system you've designed at combatting, or taking care of, or addressing common-cause failures?

MR. WATERMAN: That's correct.

MEMBER BROWN: So you have to add the add addressing and its effectiveness on doing CCFs, right?

MR. WOOD: I would add the caution, too, that this is more of a comparative tool than and absolute measure of diversity, because there's not a set of metrics that provide a comprehensive well-defended number. But this does provide a very systematic and effective tool for doing comparative assessment of the diversity strategies that might be proposed.

MEMBER BLEY: Now, the effectiveness of a particular strategy against a particular kind of common cause might be different than against another kind of common cause.

MR. WATERMAN: Oh, absolutely. Yes, you're right.

MEMBER BLEY: But that there's no way to -- you're not trying to track anything.

MEMBER BROWN: I don't think --

MEMBER BLEY: So it's just kind of the best thing that -- when you look at it and try to evaluate it, is this the best it performs against any common cause? It probably can't be on average, because who knows what that is?

MR. WATERMAN: Not any common cause. The real trick in doing BTP 7-19 analyses or NUREG/CR-6303 analyses is to identify which common causes do I have to address. Now one system may have a set of common causes that they've identified and another system may not be subject to that same set of common causes. And so those two diverse designs will be different because the idea of a diverse system is to address the common causes that have been deemed to be --

MEMBER BLEY: So this you have to apply to one specific area of the design?

MR. WATERMAN: You can have a design that addresses several different common causes all in one design.

MR. WOOD: And they might not all be implemented on the same system. You can implement some of these diversity strategies within your safety system, like the functional diversity is an example that's very common, and then implement some of the other diversities in a diverse actuation system as well. In the underlying rationale, and there's a great deal of it in chapter 6 of the NUREG report, it talks about the effectiveness or the effect, impact of these different diversities on those areas that I mentioned yesterday, the purpose, the process the product and the performance and whether or not you're dealing with the introduction of systematic faults or you're dealing with common responses to external stimuli or common demand space, things like that. So in applying this tool, it can't just be used as I'm looking at a number and that's all I need to know. You need to verify some assumptions and the way you characterize the diversities and also have tie to the application space that you're talking about. The caution really is this is still a subjective analysis. It's just a systematic rigorous way of looking at that subjective analysis. But we need a caution about losing sight, that it is still a subjective analysis.

MEMBER BLEY: I guess where I'm coming from is I see parallels between this and what we tried to do in safety analysis many years ago; more people are trying to do in proliferation resistance analysis and that's trying to see some intrinsic value to some, I'll call it a barrier or a system. The trouble was it really is dependent on the scenario you're focused on. In that case, that scenario is in common cause. So without that framework, there really is no particular intrinsic value to any --

MR. WATERMAN: Yes.

MEMBER BLEY: So I think we're on the way, but maybe this refines over time or application.

MR. WATERMAN: Mind you, licensees aren't require to put in -- if a licensee identifies that they need some diverse system, because, for example, the operator doesn't have enough time to respond to an event, say it's low-pressure injection actuation, that doesn't mean they have to put in containment isolation into that diverse system and containment spray and high-pressure injection, all that. They only need to put in diverse systems to handle the functions that an operator may not have enough time to address.

MEMBER BLEY: And then you evaluate against that particular --

MR. WATERMAN: That's correct. The example that comes to mind is the Oconee upgrade, they're putting in a diverse low-pressure injection actuation system and I believe a diverse high-pressure injection actuation system. They're not doing diverse containment isolation or any of the other engineer safety feature actuations. They're not putting in a diverse reactor trip.

CHAIRMAN APOSTOLAKIS: Who is doing the evaluation of the weights, the licensee or the staff?

MR. WATERMAN: The staff. Research right now has developed these set of weights.

CHAIRMAN APOSTOLAKIS: And then who's going to use them? I mean, the licensee or the staff?

MR. WATERMAN: It would be my hope that the licensee would use this tool and the staff would also use the very same tool with the exact same weights that everybody's working on the same sheet of music, if you will. So that when the licensee does an evaluation, identifies the common-cause failures they need to address and uses this tool maybe even to help them design the system, that once they design it and they come up with score of, say, .94, which should be well within the region of acceptability, when they submit it to the Agency and the Agency runs those same assumptions, the Agency should also come up with a score of .94. And, you know, if they don't, then there's something going on there that is causing licensing uncertainty, and licensing uncertainty is a safety concern.

CHAIRMAN APOSTOLAKIS: The licensee will

come here and say for low-pressure system actuation we calculated the weight and it's 1.1. They're not going to give you an alternate design. They will just say this is the design, we propose 1.1. What is that telling you? Are you going to have some standard that says for these kinds of things 1.1 is good enough?

MR. WATERMAN: I'm actually going to talk about that a little bit later in the presentation.

CHAIRMAN APOSTOLAKIS: Okay.

MR. WATERMAN: We haven't yet determined the region of acceptability, but I can guarantee it's not as tight as 1.01 down to .99. It's going to be a much broader region. And in order to use this as a screening tool to tell us this is within reason; let's take a look at what they did, or this just doesn't look reasonable at all. Let's take a look at what they did and we'll discuss it.

CHAIRMAN APOSTOLAKIS: Now, the other thing is you said earlier for these kinds of common-cause failures or, I guess, in all the presentations yesterday we avoided going into the causes. We were looking at the symptoms. But that's what you meant, too? We're losing, you know, two redundant parts of the system, for whatever reason.

MR. WATERMAN: For whatever reason.

CHAIRMAN APOSTOLAKIS: And then we are designing against that, how to protect it and mitigate it. That's what you meant. The symptoms?

MR. WATERMAN: Yes.

CHAIRMAN APOSTOLAKIS: Yes.

MR. WATERMAN: Exactly.

MR. WOOD: NUREG 6303 D3 analysis sort of can be characterized as a top-down approach of looking at the use and you can take a bottom-up approach. It's just very difficult to claim that you've identified all of the potential vulnerabilities.

CHAIRMAN APOSTOLAKIS: Okay. Now, we can move onto the details.

MR. WATERMAN: So, we gathered data from around the world, from organizations such as the IEC and the Federal Railway Administration and Federal Aviation Administration. We also looked at different industries like the rail industry, the chemical industry, aerospace and aviation. And then we also looked at what's going on in international nuclear power plants.

MR. WOOD: I want to add that we looked at other industries as well. It's just in many cases those industries don't specifically as a response to common-cause failure, and in some cases they don't identify common-cause failures.

CHAIRMAN APOSTOLAKIS: Do they even use the words?

MR. WOOD: In some, they don't. And they do rely on the first line of defense, which is high-quality process and very much rigor in their engineering approach.

MR. WATERMAN: So we took the data that we gathered and we populated our spreadsheet with the various, if you will, diversity strategies that we saw. And by doing that, we were then able to determine how many of these criteria were used in the data set; we summed them up here, and how many times a particular attribute was used out of all of the people that we looked at.

Doing that, we were able to determine a diversity attribute effectiveness weight, which is a weight sort of representative of -- for example, of the 14 designs that actually had deliberate application of diversity, it looks like all 14 of them use some design diversity approach. And so, 14 divided by 14, that would give us a value of 1.0 for the diversity attribute effectiveness weight for the design attribute. And we went through there. We'll get into all the assumptions underlying. That's very simple, simplistic. I realize that, but it's a step I think in the right direction to developing a metric.

CHAIRMAN APOSTOLAKIS: Can you walk us through an example here?

MR. WATERMAN: Right now?

CHAIRMAN APOSTOLAKIS: Pick one, yes.

MR. WATERMAN: I don't think I have any in my slides.

CHAIRMAN APOSTOLAKIS: Well, the first row here that says --

MR. WATERMAN: Well, but it only goes down to, you know, the function part. The first row here is we have -- this application, it's just labeled design 1. I could bring up the spreadsheet, if you'd like, but it's --

CHAIRMAN APOSTOLAKIS: No, let me tell you what I'm trying to understand. There is an arrow from the attribute design. Says different approach, same technologies, I guess. And you go to different technologies and you give it a rank of one. That's the first row, right?

MR. WATERMAN: You're talking about right here?

CHAIRMAN APOSTOLAKIS: The very first row.

MR. WATERMAN: The different technologies?

CHAIRMAN APOSTOLAKIS: Different technologies. The first row.

MR. WATERMAN: Yes. Oh, different technologies, and we've got line No. 2 using different technologies. And by using different technologies, in other words, we're probably backing up a digital with an analog system.

CHAIRMAN APOSTOLAKIS: Right.

MR. WATERMAN: Or maybe backing up an analog system with a digital system.

CHAIRMAN APOSTOLAKIS: But why is the rank one?

PARTICIPANT: That's just a number.

MR. WATERMAN: Because NUREG/CR-6303 ranked these diversity criteria according to their relative effectiveness compared to the other criteria within that attribute. So, using different technologies as a design diversity is considered to be more effective than using the same technology and just changing the architecture, which is down here at three.

CHAIRMAN APOSTOLAKIS: Okay.

MR. WATERMAN: So this is the best approach, second best approach for relative effectiveness, third best approach.

CHAIRMAN APOSTOLAKIS: Okay. So this is the judgment of the authors of 6303?

MR. WATERMAN: That's correct.

CHAIRMAN APOSTOLAKIS: Fine.

MR. WATERMAN: And for the most part when you read it, this sort of makes sense.

CHAIRMAN APOSTOLAKIS: The second column says DCE Wt.

MR. WATERMAN: And I'll get into the development of the diversity criterion effectiveness weight, and I'll talk about why I came up with those numbers, or how I came up with those numbers. Okay?

CHAIRMAN APOSTOLAKIS: Okay.

MR. WATERMAN: This is just sort of a recap of what we're going to be discussing in the follow-up slides.

CHAIRMAN APOSTOLAKIS: So we'll come back to a table like this?

MR. WATERMAN: Yes, I'll probably demonstrate how the tool actually works, but yes.

So after populating it and getting a diversity attribute effectiveness weight, now I've got my weights. I've got my diversity criterion effectiveness weight that I just developed off of the various relative effectivenesses of the criteria within an attribute; that's these weights right here, and I've got a diversity attribute effectiveness weight that's really representative of the frequency of usage of that attribute around the world, if you will, from the things that we looked at.

We transferred those weights and the criteria and the attributes into a new table such that we could populate that table in new designs that were proposed and from those designs we could then come up, if you will, with a score using the weights that we developed. And this is sort of the tool that will be looking at later on, if you want a demonstration of it. Charlie and I played around with it a little bit yesterday.

CHAIRMAN APOSTOLAKIS: So at some point you will give us a demonstration --

MR. WATERMAN: Sure.

CHAIRMAN APOSTOLAKIS: -- of how these numbers --

MR. WATERMAN: Absolutely. I'd love to.

CHAIRMAN APOSTOLAKIS: Okay. Jack?

MEMBER SIEBER: This really doesn't tell you where diversity is needed. This tells you where diversity is used by practitioners to overcome problems that they perceive could occur. Right?

MR. WATERMAN: Thank you, Jack. That's exactly right. This does not defend whether or not diversity is needed. It only says once that determination is made, you have to address it and how do --

MEMBER SIEBER: Yes, here's how people do it.

MR. WATERMAN: Yes.

MEMBER SIEBER: Okay.

MR. WATERMAN: Thanks, Jack.

MEMBER SIEBER: This is a history lesson.

MR. WATERMAN: This is sort of a history lesson, yes.

MEMBER SIEBER: Yes. Okay.

MR. WOOD: The tool provides an excellent mechanism for capturing those kind of experiences.

MEMBER SIEBER: Well, it also gives you the framework in which one thinks about how to achieve their goals. You know, without the framework, I'm not exactly sure what one would do.

MR. WATERMAN: We don't seem to have a good framework.

MR. WOOD: It's a multi-dimensional problem.

MEMBER SIEBER: Well, this is a good first step.

MR. WATERMAN: This is a first step.

MEMBER SIEBER: Yes.

MR. WATERMAN: So, in summary, we developed a spreadsheet using the 6303 guidance as a framework to capture diversity designs and positions from other organizations, industries and companies, countries. And the data and the guidance was in use to develop weights and the weights were used to store the designs and positions. And this is sort of a breakdown of how the attribute usage came out for the designs we looked at. You can see that there's about 20 percent of the applications. From this slide you it can be seen that the distribution of diversity attributes is approximately 20 percent usage for life cycle; here, the orange, logic in the red. And signal diversities, it varies between seven percent and 13 percent for the remaining diversity attributes. And this is not surprising in that life cycle diversity and logic diversity have been used extensively in response to licensing uncertainty rising from incomplete guidance on the use of diversity.

People just said, well, we'll just build it as good as we can and we'll try different algorithms and things like that. And since the signals are already in the plant, you know, they just used what they could.

MEMBER BROWN: So this is the fraction of all those existing systems you looked at and how they approached dealing with -- they had to design a diverse system and this is the approach that the various you look at took, just a breakdown of those.

MR. WATERMAN: Yes.

MEMBER BROWN: Okay.

MR. GUARRO: Have you tried to make a judgment as to -- you know, because you have looked at different industries, right?

MR. WATERMAN: Yes.

MR. GUARRO: You tried to make judgment as to whether there is a difference in usage between industries that have more awareness of the problem of diversity versus industries that have less awareness of them, because that's a little bit of a concern that comes to mind. Because I mean from my personal experience I know that there are certain industries that they don't even, as George was saying, the word "diversity" isn't even in their vocabulary.

MR. WATERMAN: And actually, when I do the summary plot of how everything scored out using this particular score, you'll see that arise. Sometimes industries don't look at diversity simply because they don't have enough room to put another rack, for example. Or the domain space in which they're operating doesn't lend itself to diversity.

MR. GUARRO: You know, in the space system industry where I work there's no room for diversity for that very reason.

MR. WATERMAN: Exactly.

MR. GUARRO: And there is no material and room.

MR. WOOD: In the examples from NASA there was some usage of diversity, although it's not the primary response and a lot depends on whether it's a "human rated mission" or a "deep space mission."

MR. GUARRO: Yes. Right.

MEMBER SIEBER: How much of a function applying diversity is the fact that some malfunctions or accidents that you could have really just don't mean that much from the standpoint of economic cost, or danger to people, or what have you? Is that a function that's hidden all of this?

MR. WATERMAN: There is some cost benefit functions in there. You know, it would be great if everybody chose different technologies. Sometimes there's just not a cost benefit in going with completely different technology and so somebody might back off and say well, instead of different technologies where we can't get the analog parts, for example, let's try FPGA's backing up microprocessors. We'll ramp it down a little bit and we'll go with that. And I think that cost benefit is sort of implied by how many of these different criteria were selected overall.

MEMBER SIEBER: Yes, if you're control system messes up and the result is you burst some tank some place it doesn't hurt anybody, doesn't cause environmental damage, can be repaired, you know, why would I put in an expensive diverse system to deal with it?

MR. WOOD: The application of diversity, whether or not it's applied addresses the issue of is it important. There are faults and I don't care that they exist because they don't cause a failure that I'm concerned about. This looks at when it's been decided diversity is needed, when the industry or the application decided what kinds of diversity were applied.

MEMBER SIEBER: You face the same thing in a nuclear power plant. Depending on what the system is and what function you're performing at a given time, you may decide I don't need to spend money on diverse instrument and control systems because if it breaks, it's not going to lead to core melt, it's not going to lead an off site --

MR. WATERMAN: Yes, as a matter of fact, Branch Technical Position 7-19 addresses that very point.

MEMBER SIEBER: Yes.

MR. WATERMAN: When it says look at your potential common-cause failures. For each one you see, run it through your pseudo design basis analysis and look at the consequences. Now the consequences don't rise to some level of significance; for example, 10 C.F.R. 100, 10 percent of 10 C.F.R. 100, you're done. But if you do exceed those, then put in a diverse system to address it. And that last thing, put in a diverse system to address it is where this would come in.

MEMBER SIEBER: Well, what defines the boundary? Part 100?

MR. WOOD: For the D3 analysis.

MR. WATERMAN: For the D3 7-19, yes. Well, part of this part 100, part of it's how much fuel damage you get and those limits are less than the 10 C.F.R. 100 limits.

MR. WOOD: But they're addressed as criteria in 6303.

MEMBER SIEBER: Okay.

MR. WATERMAN: So 7-19 essentially says, okay, look, you need some diversity. And what this research is doing is saying, okay, now that you determine you need it, how much is enough? Are you really diverse enough?

MEMBER SIEBER: So if you're getting close to some limit, then your first thought as a designer is I'll put in a diverse system and hopefully avoiding hitting that limit. But you never really know for sure because of the complexity of the situation whether you do or don't, right?

MR. WATERMAN: Yes, that's right.

CHAIRMAN APOSTOLAKIS: So, what kind of complexity are we talking about here? I mean, if I have a simple actuation system, would I have to do all this?

MR. WATERMAN: Well, if you have a simple actuation system and you run it through your BTP 7-19 analysis and you do not exceed those threshold limits that are described in BTP 7-19 and the SRM to SECY 93-087, then you don't need diversity.

CHAIRMAN APOSTOLAKIS: But it's a scram

system?

MR. WATERMAN: Yes.

CHAIRMAN APOSTOLAKIS: That probably exceeds those limits, doesn't it?

MR. WATERMAN: Well, on a large-break LOCA I don't know that you need to scram the reactor. I could have scrammed it anyway.

CHAIRMAN APOSTOLAKIS: So now what you're saying is that I have to look at the actuation system in the context of an accident sequence?

MR. WATERMAN: Yes. That's right.

CHAIRMAN APOSTOLAKIS: And then, I mean, do I have to worry about all this? I mean, are these systems simpler than day -- the example that always brought up, you know, the control system of the Arianne rocket in Europe where people give you, you know, weird things that happen and they say, well look, you nukes don't worry about these things. Well, that was a system that controlled the whole damn rocket. Here, all I have to do is insert the rods. I still have to worry about all this? I mean, is there an issue of complexity here and utilization of the system? Is it overkill, on other words?

MR. WATERMAN: Well, keep in mind, this doesn't address whether or not there's a need for diversity.

CHAIRMAN APOSTOLAKIS: You're right.

MR. WATERMAN: This addresses the question that once somebody determines there is a need for diversity, how do you make sure you've got enough? And like you say, this is like a metric that helps you screen somewhat and get a comfort level, if you will, of licensing certainty and safety.

MR. WOOD: There are some differences in the decision making in Europe. Let's say in Britain they tend to use a risk based argument for determining which functions need to be backed up by a diverse system.

MEMBER SIEBER: Yes, I can't think of any other way to do it. Are we going to require the same thing? You know, you put in a diverse system and you say I've reduced my chances, but you have to do a specific analysis to determine the extent to which you've reduced your chances. And so are there boundaries on -- you know, no one can guarantee that you aren't going to have a series of screw-ups that eventually are going to lead to disaster. Is there a limit as to what the risk is after you've applied various diverse techniques in order to determine whether you've done enough or not, other than a cost benefit?

MR. WATERMAN: That's looking at the space of the common-cause failure and determining their credibility.

MEMBER SIEBER: Yes.

MR. WATERMAN: Right? And then addressing the ones that are most credible. Now, this research here did not address the area of what's credible and what's not credible.

MEMBER SIEBER: Yes, but where do we from here? Because this then doesn't define the total answer. It doesn't tell me what to do, right, without additional work.

MEMBER BONACA: How do you deal with other attributes? What I mean is that, here you have alternatives focused on diversity. They measure how much diversity you get. But each one of these engineering solution, they have other attributes. Which is more desirable than other of these solutions? How do you weigh that?

MEMBER SIEBER: That's another way to ask the question.

MEMBER BONACA: What?

MEMBER SIEBER: It's another way to ask the same question.

MR. WATERMAN: You mean attributes in addition to the seven attributes here, Mario?

MEMBER BONACA: Yes, in addition to the diversity, measuring that, but each one --

MR. WOOD: There are two ways of characterizing a response to a common-cause failure vulnerability. One is to prevent the potential posed by that vulnerability. The other is to mitigate the fact that that's there. Diversity tends to lead toward mitigation. Design tends to lead toward prevention. And like I mentioned, some industries that aren't reported, that don't discuss diversity tend to focus on the design, the rigor of the design, the ability to identify hazards and address those hazards in the design and following that through with a very rigorous review process and confirmation process. But even in those industries they can't claim that they've avoided the common-cause failure. They can only say that they've done what was reasonable or practical to address it through design.

CHAIRMAN APOSTOLAKIS: Several times, Mike, you had to, or you felt that you had to say, you know, that you started with BTP such-and-such. I think and the questions you got from Jack from Mario seems to me would help your cause here to have some sort of a block diagram that sends a message of what really is happening in real life, that the analyst will start by doing an evaluation according to this BTP. If the analyst finds this, then he or she determines that there is a need for this. If he finds something else, then this will be placed in its right context. It seems to me that's an important thing. Because every time that you get a question, both you and Richard have to go back and say but, we don't determine the need, we don't do this, we don't that. So if you have one picture that will show that and say now, here, down here is where we are working today, then I think that will communicate better what you're trying to do.

MR. WATERMAN: That's a great idea. I like pictures, so thanks, George.

CHAIRMAN APOSTOLAKIS: Okay.

MR. WATERMAN: I put a little note right here. You never know what will happen --

CHAIRMAN APOSTOLAKIS: Why is little note? I said a lot of things.

MR. WATERMAN: I write small.

MEMBER SIEBER: To do what George is suggesting is not trivial.

CHAIRMAN APOSTOLAKIS: What? What did you say Jack? I'm sorry.

MEMBER SIEBER: To do what you're suggesting is not trivial.

CHAIRMAN APOSTOLAKIS: Is not trivial, but it seems to me that's why we have this discussion, because people try to think at that higher level and evaluate what these gentlemen are --

MEMBER SIEBER: I think it can be done, but it's a lot of work.

CHAIRMAN APOSTOLAKIS: Yes. Yes.

MEMBER SIEBER: The way I picture it.

CHAIRMAN APOSTOLAKIS: Okay.

MR. GUARRO: Just to complete a little bit the question that I was asking before, were you able to look at a pie chart like that by different industries and industries and see if there was a substantial difference in the relative use of the different attributes.

MR. WATERMAN: You know, I didn't think of that, but it's not hard to do.

MEMBER BROWN: You mean within an industry or between industries?

MR. GUARRO: No, between industries.

CHAIRMAN APOSTOLAKIS: Why are you interested in this, Sergio? I mean, I know you are interested, but --

MR. GUARRO: Well, because I don't think all industries are equally aware of the relevance of this issue in the same way. And so, you know, in other words, to adopt a criterion of goodness based on an industry that doesn't do diversity very well seems to -- and diluting the -- an industry that does it well doesn't seem to be the right thing to do.

MR. WOOD: If I could make an observation. We did that, not through pie charts, but for example, the aerospace industry, the NASA examples, which show very low on these scores, they have a context issue because of size, power and weight limitations. That's a constraint that we had to consider in determining whether or not it needed to be factored into determining this region. The aviation industry, on the other hand, they also have some size and weight limitations, but they also are dealing with a problem space that's different. They're an active control system with a very immediate indication of a failure.

MR. GUARRO: I understand, but for that very reason, because the contexts are different and, you know, so maybe you don't see, you know, that the distributions change much and that would be a confirmation that everybody does more or less the same thing. But otherwise, if you see a difference, then you should ask yourself why the difference and make a judgment as to who has the better solution, rather than mix them together blindly.

MR. WATERMAN: Skipping ahead on the presentation, this shows the breakdown. Boy, this is way ahead, this slide 47. The public handouts, it's all bad, but you guys have the really good handouts. The applications of positions that we use to develop the weights and the normalized score are shown between these two red lines here. We screened out applications that had either size, weight or functional domain restrictions to them. They weren't useful, like you said. They just weren't representative of what the nuclear industry faces. For example, the nuclear industry uses a design system. They got plenty of space for another rack. They can put in a different system. You go off on international space station or space shuttle, you don't have that luxury.

So we pretty much screened all the aerospace and aviation application. Additionally, we screened out one of the applications out of non-nuclear industrial applications. We screened out one of the international positions and we screened out one of the plant designs that we gathered, because they were using minimal diversity. And so what we're looking for is how much is enough, so we just screened it out of this calculation here. And then what was left were fairly energetic, if you will, diversity approaches that we then used to score the normalized value of 1.0 and develop all the weights just on these here. So we didn't use pie charts or anything, but we did sort of look at what they were doing and decide well, is this really something that the nuclear industry can benefit from? And it was like no, not really, because you know, we're talking apples and oranges.

MR. WOOD: But I want to note that just because they were screened out of the use and the tool didn't mean that we through away the insights that can be gained. For example, in the aviation industry, even with the size and weight limitations, there's a use of different microprocessors to provide some diversity. And we consider that very significant because it sort of flew in the face of size and weight limitations. And we looked at the rationale that was provided on why they did that and also considered those things. In the report there are some baseline strategies or groupings of strategies that factor those kind of considerations in and they assess very well using the tool.

MEMBER SIEBER: Another factor that I think is there that we haven't fully evaluated is the tolerance of the public for mishaps in various industries. For example, the public is sort of satisfied with killing 40,000 or 50,000 people a year in automobiles. They may take 500 to 1,000 in aircraft.

MR. WOOD: Aircraft, yes.

MEMBER SIEBER: You do one thing to one person at a nuclear power plant and that changes your value system.

MR. WOOD: And we did look at like braking systems and other things in automobiles to see if diversity was used and didn't find specific instances of that.

MEMBER SIEBER: Right. On the other hand, the fact that the public and the law, our law, is sensitive to danger to people from this industry, that increases the demand for diversity over and above what you would find in other industries.

MR. WOOD: The guidance that we cited for the chemical industry came about as guidance in response to calls for regulatory oversight after the

Bho Pal incident.

MR. HECHT: Mike, can I ask a question about basically you're weighting on the basis of industrial experience. But earlier here on chart 18 you have some very interesting data related to the relative proportion of I guess --

MR. WATERMAN: Defects. Common defects.

MR. HECHT: Yes, of common defects or basically important defects. Why did you choose the industrial rating rather than just using the defects weighting?

MR. WATERMAN: Because the industry itself was struggling with this issue back when we started this research. None of that had been done at the time. And we felt, and I think the ACRS supported the approach, that we ought to take a look at what the rest of the world is doing. And so that's what we did, is we went out and we wanted to see what experts in other industries, how they approached this whole idea of how much diversity is enough. We wanted to look at what evolutionary nuclear power plants who had a lot of digital systems going and how were they approaching it? And our nuclear industry didn't really have a lot of experience in the safety arena with digital systems being backed up by analog systems. They had some, but we just felt we needed to look outside the industry to get a clearer more global perspective, if you will, on this.

MR. WOOD: There's actually another consideration to that. Those defects that had been reported are what you're seeing and the response typically to those is to improve your design. Diversity is really there for the things that you haven't seen but anticipate might be there. And so basing the decision making tool on what you've seen leaves you wide open to the things you haven't seen, the unknown unknowns.

MR. HECHT: Well, that's always the case no matter what decision you make. But I would just say that you've made the comment earlier, and that's been reflected also in here, that the aerospace industry has different, not only constraints, but they also have different failure modes. And the same thing would be true of other transportation industries. Even here, what I saw on slide 47, a lot of that seemed to be nuclear industry. NPPs in other countries seems to be the dominant shade on there, pink.

MR. WATERMAN: Well, the shading is not pink because it's nuclear power plants.

MR. HECHT: Yes.

MR. WATERMAN: The shading was pink by my choice.

MR. HECHT: Right, I understand. But the point is that that seems to be where most of your experience is coming from, so implicit in that is the fact that people that you're using data based on what other people have seen and how they've responded. It could be that, if you will, I don't know much you gain from adding yet more multiplications and normalizations. Including a third factor just based on the experience becomes an important thing to consider. Because one of the things that I see in this chart; and by the way, this is common with space, is incorrect parameter values. One of the things that you spend more time on at any point prior to launch, and this is where people spend a lot of time, is the 40,000 or 50,000 parameters that go into the launch vehicle, making sure that they're all exactly right.

CHAIRMAN APOSTOLAKIS: Forty-thousand, Myron?

MR. HECHT: Yes. Yes, I was amazed.

CHAIRMAN APOSTOLAKIS: Well, I am, too. Gee, 40,000.

MR. WOOD: By comparison, nuclear power

plants are very simple, well-behaved things.

MR. HECHT: yes, it keeps a good portion of the overhead paid so that people like us can mess around.

But that's reflected here. That's this peak right there. So I guess my point is that if parameters are the major issue here, then anything you do in terms of an alternative life cycle process or a different manufacturing process would not be relevant.

MR. WATERMAN: I don't follow that, Myron, it wouldn't be relevant.

MR. HECHT: Well, let's just say that you have one version implemented in eta and another version implemented in C, and they're both dependent on the same parameter database, then the diversity that you might get or the score that you might get for that eta and C, which might take you over a threshold, actually is less effective in this application domain.

MR. WOOD: Or for that specific common-cause failure instance I would agree that there would be perhaps some design approaches and some other diversity attributes that would be effective whereas different software implementations would be. I would agree. But we tried to factor those things in. In chapter 6 of the report it goes through each diversity and talks about what is that diversity's impact on these sources of common-cause failure, these triggers of common-cause failure, these locations of common cause failure.

So the tie to the experience is two-fold. One is through the approaches that have proven effective in the international plants that have a significant amount of digital systems used. And the other is through the rationale used in determining the effectiveness of different diversity applications.

MR. HECHT: Okay. But what you're really selling here is you're selling a score, you know, kind of like a FICO score on a credit report or something like that, right?

MR. WATERMAN: Well, what we're trying to sell, if you will, is a metric for evaluating diversity approaches.

MR. HECHT: Okay. I call it a score, which it's easier for me to --

MR. WATERMAN: I'll use George's definition. It probably sounds better.

MR. HECHT: Okay. Fine. That metric.

MR. WOOD: I like to look at the score and the tool that gives the score as a way of informing your decision, but not the sole basis of your decision.

MR. HECHT: Okay. Well, I guess the point is that once you look at a number like that, a number has a compelling value and the reason why I use the word "score" is precisely because, you know, you want to determine whether you've won the game. So if you say this score is only a partial weight and you also have to consider the application of the particular diversity problem that you're addressing, then why not take it one step further and say include that particular problem that you're addressing in the way, or in the metric?

MR. WATERMAN: The particular problem you're addressing determines whether or not you need diversity.

MR. HECHT: All right.

MR. WATERMAN: What this does is assesses once you've determined that need, okay --

MR. HECHT: Fair enough.

MR. WATERMAN: -- and you've designed to address that need, have you really hit all the things you need to hit?

MR. HECHT: Okay.

MR. WATERMAN: Okay. You're getting into

need again, and I don't want to get into need. We've already done the research on that. We got a regulation that says sometimes it's needed. You have to determine where it's needed. None of this research identifies that, but this research identifies it as once that need has been determined, by whatever process is used, how much diversity is enough? And when a design is proposed so that we can evaluate a design, do a quick screen and then dig into the design to make sure all the things that are credited are really there.

MR. HECHT: Okay.

MR. WATERMAN: They're appropriate.

MR. HECHT: You've said that, or I think what you basically said is that because BTP 7-19, that filter has pretty much eliminated the question of need and --

MR. WATERMAN: In some applications, not all.

MR. HECHT: Okay. All right. So like I said, that was the point. I'm not sure that can completely get away from that even afterwards.

MR. WATERMAN: Okay.

CHAIRMAN APOSTOLAKIS: Shall we move on beyond slide 26? I think we beat that to death.

MR. WATERMAN: And slide 27 just broke it out by various attributes. A very busy slide, you know? Okay. That's the data.

CHAIRMAN APOSTOLAKIS: So what is the message here?

MR. WATERMAN: It just shows some of the results of the data. There's no big message there.

CHAIRMAN APOSTOLAKIS: So it's the percentages in terms of --

MR. WOOD: We've seen instances of each criterion being employed.

CHAIRMAN APOSTOLAKIS: Right. Right.

MEMBER BROWN: And it's not concentrated. If you look at this, it's not concentrated in one particular --

MR. WOOD: There's no magic bullet.

MEMBER BROWN: There's 20 different, or whatever the number is, and it's a relatively --

CHAIRMAN APOSTOLAKIS: And most of them are low now, two, three, four percent.

MEMBER BROWN: Sure.

CHAIRMAN APOSTOLAKIS: Different logic processing versions in same equipment architectural, zero.

MR. WATERMAN: Yes, didn't seem to see any

-- let's see here. I can't hardly read it.

CHAIRMAN APOSTOLAKIS: Oh, well it is on the right.

MR. WATERMAN: Yes, I see where it is.

PARTICIPANT: It's a blue box.

MR. WATERMAN: Yes. It's one of the blue ones, yes. It's different logic processing versions in same equipment architecture. Somebody using an Intel and a Pentium. There are different versions made by the same manufacturer to get diversity. We just didn't see any cases where people opted for 486s and 286s or --

MR. WOOD: We did see one instance in aerospace in an Airbus application where they used I think a 286 and then a 386, but because of the context considerations, that was screened out as a tool.

MR. WATERMAN: This is the data that went into developing the weights.

CHAIRMAN APOSTOLAKIS: I mean, what impresses me here is these very low numbers.

MR. WATERMAN: Add them up. They add up to 100.

CHAIRMAN APOSTOLAKIS: No. Yes, but, I mean one or two, three, four percent. There doesn't seem to be something that most people seem to like.

Is there a message here or am I missing --

MR. WATERMAN: I think the message here is that --

CHAIRMAN APOSTOLAKIS: What is the message?

MEMBER BROWN: The message is it's not clear.

MR. WATERMAN: No, I think there's another message here.

MEMBER BROWN: It's not clear.

CHAIRMAN APOSTOLAKIS: Well, I understand that, but I mean --

MR. WATERMAN: I think the message that really comes through loud and clear here is that just selecting one of these is probably not going to be enough. The real diversity approach takes advantage of a lot of different criteria in a particular combination to address a set of common-cause failures.

CHAIRMAN APOSTOLAKIS: Well, look at the --

MR. WATERMAN: We had the software languages thing here, six percent. What that six percent represents is that if somebody just wanted to go with different software languages, you'd get a score of maybe six percent or nine percent, or something like that where you apply all the attribute weights, right?

CHAIRMAN APOSTOLAKIS: Different algorithms logic --

MR. WATERMAN: So if somebody says, yes, my diversity involves I'm using C instead of eta 85 or whatever, some other language. You know, I'm using that and therefore I have enough diversity. Well, if go look at this kind of information here, you go, wow, that doesn't seem diverse to me. What are you doing about functional diversity, you know? What if you got the wrong requirements and you're just programming the wrong requirements in two languages? You haven't addressed diversity at all.

MEMBER BLEY: The troubling thing here for me is that these tell us the variety of things people are doing, have tried and they don't tell us anything about how effective they were or are they repeating these and continued applications, or in one area? Are they using six of these or two of them? It's just a count. And I have real trouble seeing how that relates to any measure of goodness or effectiveness.

MEMBER BROWN: The other thing it doesn't show is, you know, did you start out, you know, 20 years ago using software -- down and some of those have been thrown away and people aren't doing them anymore.

MR. WOOD: We looked at it some in the --

MEMBER BLEY: Since this is just the total for all time.

MR. WOOD: We looked at it for the Airbus because you had a progression of examples. We looked at it in the nuclear industry because we had an evolution of starting -- I guess Darlington may have been one of the earliest examples we used. And then through Sizewell and then to Olkiluoto and Lungmen as the current examples. So we did look at things. What we didn't see is a narrowing down to a limited set of responses or application of diversity. We saw still a multi-faceted use of diversity in most applications.

MR. WATERMAN: There are a couple of things with time experiences. The diverse systems that go in are going in to handle an unusual accident. So you don't see a lot of challenges where they actually have to respond to anything. The other area you see is that the fact that we go out and we collect this data from plants, if the systems weren't very diverse or weren't very affected, they would have changed them. Right? Until they get something that works for them, and that's reflected in the data that we gathered. This isn't theoretical stuff. This is we went out and looked at what are people using? And remember the assumptions are was that there was engineering judgment applied in the application of those particular diversity strategies along with cost benefit, operating experience and things like that. The fact that they actually exist in plants and exist in different industries and also that they're addressed in different positions by agencies and organizations reflects some judgment went into actually selecting those particular combinations of diversity attributes --

MEMBER BLEY: I guess what I don't see is a place here where -- I don't know anything else you could have done, where you've applied your judgment of yes, seeing people have used these, I know a little bit about how effective they are, I don't, but where you overlay on that your knowledge of our systems and some measure of -- usually we like to see something on risk-informed, performance-based, something about is there performance, anything about this related to our industry that would tell us one of these is any better than any other in particular applications?

MR. WATERMAN: Well, you can pull example systems out of the U.S. we applied after the fact.

Actually use sort of benchmarks of, you know, what are we doing. These systems have been approved. This is -- forgive me, this is an ATWS, generic ATWS, as we've been told not to mention ATWS because -- but this is just a generic ATWS system of one particular vendor design. Went into the technical information, dug out all of the features that they use in the ATWS system, stuck it into that little tool I described and it calculates up I think at 1.01 or something like that, Some value like that, which gave me some reasonable assurance that here's a system that the NRC reviewed, licensees have applied and we found it acceptable. And how does it score out and --

MEMBER BLEY: They're using the same kind of things that other people are using.

MR. WATERMAN: Right. And this here is the Oconee diverse low-pressure injection actuation system scored out. Okay? And it's well within this pink region of warm, fuzzy feeling about, you know, is it really important?

MEMBER BLEY: Right.

MR. WATERMAN: Of course we reviewed that one. So an answer to your question is, is this stuff applicable to the U.S. industry? It would appear just from these limited examples, yes, it can.

MEMBER STETKAR: But, Mike, this still comes back to you assigned weights to each of those seven attributes based on what the world, an amalgam of a mushy world, has done.

MR. WATERMAN: Full of experts and people --

MEMBER STETKAR: No, no, no. An amalgam of a mushy world has done. Suppose, for example, that the Oconee engineers thought about a specific set of common-cause failure modes and made the determination that all three specific attributes were the most important ways to address those failure modes. So they effectively discounted the other four, the work that the amalgam of the mushy world has done and they assigned, you know, 33 percent weight --

MR. WATERMAN: They can't find a weight. What are you saying?

MEMBER STETKAR: No, no. You've assigned the weight based on the multi-amalgam and I'm saying that weight doesn't mean anything to me. If I always leave my driveway and turn left because I'm worried about a common-cause failure to the right side of my street, you would identify turning out of the driveway as something that a technology always does. That's mean my practice applies to a nuclear power plant.

It's just my decision for my particular common cause on my street. I wouldn't assign that a weight of anything to a nuclear power plant and yet I might assign it a weight of 100 percent, the most effective technology that I could use in my particular application to battle that common cause.

MEMBER BROWN: Unless your neighbor parked their car on the other side.

MEMBER STETKAR: All right. Yes, that's variability. But my point is that assigning pre-defined weights to the attributes as if they are universally applicable to any industry and any common-cause failure mode constrains that number. It means that comparing that nice 1.01 for the one bar to the, you know, .895 or .925, or whatever the heck it is for the other bar, doesn't mean anything because you're looking at the problem from a different -- you're trying to protect perhaps against different types of common-cause failure modes.

But I finally see where you're going with this thing. What I'm concerned about is the a priori numerical weights for the seven attributes.

MEMBER BROWN: Just a question. Why is that any different than -- and I don't know if this is the right analogy or not; I understand the point and I actually agree with you. But when you look at a PRA world and you look at the assignments of probabilities to some of the events in the trees that are developed, low numbers, and try to come up with a basis for ten to the minus six or ten to the minus four --

MEMBER STETKAR: Oh, looking for a valve failing?

MEMBER BROWN: I don't agree with that. I think there's a relationship there when you're making a judgment, you're using a judgment.

MEMBER STETKAR: Because I'm not making a judgment about the valve.

MEMBER BROWN: Oh, well you know the population of all the valves in the entire industry and how many have failed each year and under what circumstances, and this has been calculated out?

MEMBER STETKAR: Yes, but I'm not using pump data for that valve as a generic piece of equipment.

MEMBER BROWN: Well, I agree. I agree with that.

CHAIRMAN APOSTOLAKIS: You are not using valve data from some industry that has nothing to do with nuclear.

MEMBER BLEY: Or even pump data or logic

card data, which is --

CHAIRMAN APOSTOLAKIS: Well, but I mean, this is a perennial problem it seems to me of the generic information's applicability to a specific -- which comes back to Sergio's comment earlier, it seems to me. If I had a pie chart like this from high-hazard industries, ideally only from nuclear, then this would be much more meaningful.

MEMBER STETKAR: I was sitting here and because of the time, I was starting to draw an analogy to some of the stuff that some human reliability methods use. If you think of these as performance shaping factors and for a particular human performance scenario certain performance-shaping factors are move important than others. The time may be more important than the availability of procedures, for example. Man-machine interface might be more or less important. That's a scenario specific. The weights that you assign to those performance-shaping factors vary given the context of the scenario. So they're not fixed weights.

Now within each performance-shaping factor, you may have different attributes which you haven't even gotten there yet. You know, your different rankings of the effectiveness within each of those categories. Those might be relatively fixed.

MEMBER SIEBER: Yes, on the other hand there's no way for the staff to reach a conclusion without putting numerical values on these things, whether they're right or wrong. I mean, to me I consider this just an advancement.

CHAIRMAN APOSTOLAKIS: I really think it comes down to whether you can take the information from all industries. Because look at this purple on 27, slide 27, because that tells me a lot. It's one of the higher numbers, is different reactor or process parameter sensed by different physical effects? Eight percent.

MR. WATERMAN: Sure.

CHAIRMAN APOSTOLAKIS: The reason it's eight is if you did it only for the nuclear industry, that would be very high. The reason why it's eight is because the other stuff pulls it down.

MR. WOOD: Actually no, it's very high because of nuclear.

CHAIRMAN APOSTOLAKIS: And I think that is along the lines of John's comment and back to Sergio's. In other words, I know that in the nuclear industry we use a multiplicity of parameters to monitor and all that. I know. I mean, if I limit myself to nuclear, that would be, I don't know, 90 percent or something. It's eight. It still stands out, because everybody else is two and three. But the reason why it's eight is because the denominator is artificially large.

MEMBER BROWN: I think he's going to disagree with you, yes.

CHAIRMAN APOSTOLAKIS: Well --

MEMBER BROWN: No, he just said -- go ahead.

MR. WOOD: The nuclear industry has the most predominant use of alternate measurements.

CHAIRMAN APOSTOLAKIS: Right.

MR. WOOD: Because of the application of functional diversity --

CHAIRMAN APOSTOLAKIS: Right. Right.

MR. WOOD: -- compounded with signal diversity. And those have a heritage in some of the traditional approaches to diversity that derive from the general design criteria and are not specific to digital or --

CHAIRMAN APOSTOLAKIS: That's true. Absolutely. Yes. Yes.

MR. WOOD: Some of the other industries that were factored out don't have signal diversity because they're limited on the sensors that they can apply. The chemical industry does highly recommend different measurements to support the decisions for shutting down different reactions or chemical processes. So I think the industries that were included that are not nuclear have more in common with nuclear power than the ones that were excluded and don't use some of the diversities that were seen.

MEMBER BONACA: I got to understand one number. still don't understand it, so take the box on the left. Different manufacturers, fundamentally different equipment designs, two percent. What does it mean, two percent? Could you explain to me? Does it mean that the diversity has been improved by two percent?

MEMBER BROWN: No, only two percent of the people have taken that approach.

MEMBER BLEY: Can I try to see if I understand it?

MEMBER BONACA: And I would like to have an answer.

CHAIRMAN APOSTOLAKIS: Only two percent are using it. I think that's what it means.

MR. WATERMAN: Of your average strategy that might make up the two percent.

MEMBER BONACA: Okay. All right.

MR. WOOD: And that's related to how many instances where different manufacturers supplied. It's constrained by other instances where the same manufacturer provided a diverse system.

MEMBER BROWN: That's another box in here though.

MR. WATERMAN: So there are some inter-relations among the attributes.

MEMBER BLEY: I want to really understand this one because I kind of lost it twice. When you looked at all the different industries, you kind of counted up out of all of these things they could do, they either do them or they don't them. If they do them, you counted it.

MR. WATERMAN: Yes.

MEMBER BLEY: You didn't have any kind of count of how many times they do these things.

MR. WATERMAN: No.

MEMBER BLEY: It was just industry A uses 10 of these, something like that?

MR. WATERMAN: Well, yes, in a way you --

MEMBER BLEY: And then you had a total of all the industries that were whatever number.

MR. WATERMAN: Actually, that was --

MEMBER BLEY: This is a fraction of the industries that used these particular --

MR. WATERMAN: For developing the weights, I only used those industries and positions and plants that were between the red lines.

MEMBER BLEY: Right.

MR. WATERMAN: We screened out the other stuff there. And then we took an aggregate of those, if you will, for determining well, what's the average usage on design diversity? What's the average usage on, you know, each of those attributes and scored it out and --

MEMBER BLEY: But each industry kind of gets one count for each of these things.

MR. WATERMAN: Yes, but I think we're getting wrapped around the axle about numbers in the second decimal. Right? And we're getting wrapped around the axle about 1.01 versus .94, when really what the metric says is, is it good enough? Right? Does it matter if it's one or .94? Not really, because does it address the common cause?

MEMBER BLEY: I don't think that's where we're hung. We're --

MR. WATERMAN: Well, that's what I'm getting is --

MEMBER BLEY: -- hung up somewhere else.

MR. WATERMAN: Yes.

MEMBER STETKAR: Mike, let me make sure I understand. When you were talking about different industries as if you have thousands of sample points. The railroad industry has precisely three things that you looked at.

MR. WATERMAN: Yes.

MEMBER STETKAR: The aerospace industry has two.

MEMBER BLEY: But they're not inside the red line.

PARTICIPANT: Four.

MEMBER STETKAR: Four. Okay.

MR. WATERMAN: But yes, I know what you mean, is they --

MEMBER STETKAR: Well, so those two percents and one percents are sort of fractions of a population of --

MR. WATERMAN: Of a small population. Really a small population.

MEMBER STETKAR: -- that's highly weighted toward the nuclear business because they have about, I don't know, 12.

MR. WATERMAN: Since that's where we're

trying to, you know, apply this, yes.

CHAIRMAN APOSTOLAKIS: One other thing that I think you had discussed but I want to make clear for me, when Dennis raised the issue of effectiveness, I think part of your answer was, well, one of the reasons they are using it is because they have judged it to be effective. In other words, effectiveness is to some degree included in these numbers.

MEMBER BLEY: That seems to be the crux of the argument here.

CHAIRMAN APOSTOLAKIS: Right.

MEMBER BLEY: These are done by smart people who probably are going --

CHAIRMAN APOSTOLAKIS: Who have already decided that this is --

MEMBER BLEY: So that's our basis for thinking it's a reasonable thing.

CHAIRMAN APOSTOLAKIS: Okay. Okay. Good.

MEMBER BLEY: That's correct.

MR. WATERMAN: Well, that's why I brought to you guys.

CHAIRMAN APOSTOLAKIS: I think --

MR. WATERMAN: I'm going after more smart people.

CHAIRMAN APOSTOLAKIS: I think -- yes? What? Oh, I'm sorry. Ray.

MR. TOROK: Just a little --

CHAIRMAN APOSTOLAKIS: Identify.

MR. TOROK: Oh, I'm sorry. I'm Ray Torok from EPRI. I just wanted to offer a little clarification, maybe a suggestion. If we go back to Mike's slide 18, which is the one where Mike looked at the OE evaluations we did and showed how they fit into the wheel there.

CHAIRMAN APOSTOLAKIS: Okay.

MR. TOROK: One of the thing that's interesting to note there is that if you add up all those orange bars, it shows that for the NRC industry experience that we were looking at, those things dominate. And so if you're talking about diversity measures or other kinds of measures that go after those things, then it shows, you know, what is probably of value in the nuclear industry. It's roughly two-thirds of it.

Now if and when we come back later, we can talk more about that, why it comes out that way based on the OE and so on, but I don't want to take any more time right now. Thanks.

CHAIRMAN APOSTOLAKIS: You will come back later.

MR. WATERMAN: Thanks, Ray.

CHAIRMAN APOSTOLAKIS: You can request the time and it has been granted.

MR. WOOD: When we gathered the data, the usage of the data was to inform the development of some strategies. Concurrently, the tool was developed as a way of systematically looking at and comparing a proposed strategy to examples that were chosen that were representative. But also, baseline strategies that were developed based on the understandings derived from the examples and also of engineering judgment on how effective or what's the effect of different diversities. So in chapter 6 there are 10 baseline strategies grouped in three families. And one approach is to adopt one of those strategies and they'll show up very high for the tool.

Another approach is to use the tool to help inform your design and then the staff can use the tool to determine whether or not it fits within this region of acceptability and that helps them understand how much more detail they need to investigate.

CHAIRMAN APOSTOLAKIS: I think that maybe we should move on. But seems to me a lot of the questions have to do with how you plan to use this.

And especially, you know, since this is generic information, at which point in your decision making process do you bring into that process the fact that you are dealing with a specific system in a nuclear power plant. So I get this generic, you know, .95 that Mike mentions, .98. I will not forget that this is generic.

Now what do I do to make sure that the conclusions I'm going to draw and the decision I'm going to make is in fact system-specific? So that, I think, would be a very crucial step in the methodology.

MR. WATERMAN: That was probably on slide 47 or --

CHAIRMAN APOSTOLAKIS: Well, we're still on 27, so in 20 slides we're going to get that answer.

MR. WATERMAN: Yes.

CHAIRMAN APOSTOLAKIS: Very good. So move onto 28 then. How about that? Is this running it with an iron hand, or not? I'm asking you. I'm asking you.

MR. WATERMAN: So what kind of weights have we got here? We've already hammered on this. We have diversity criterion effectiveness weight, which represents the criterion's relative effectiveness within the diversity attribute. And we use the NUREG/CR-6303 guidance as a basis for the attributes we've put in there.

MEMBER STETKAR: I have to admit I didn't read NUREG/CR-6303. Did they weight things just qualitatively A, B, C or did they --

MR. WATERMAN: Yes.

MEMBER STETKAR: You assigned the numbers?

MR. WATERMAN: And I assigned the numbers, because I was looking for a way of -- on the strategies that were developed in the research, I wanted some way of saying well, did that really capture the conclusions appropriately?

MEMBER STETKAR: They rank ordered them, but you assigned --

MR. WATERMAN: They rank ordered them. They said this is more effective than this, which is more effective than this.

MEMBER STETKAR: Thanks.

MR. WATERMAN: And so forth and so on. And we'll talk about my assumptions and the way I did that, yes.

MEMBER STETKAR: Okay.

MR. WATERMAN: The diversity attribute effectiveness weight represents attribute effectiveness. That's design, function, equipment manufacturer, etcetera based on operating experience, engineering judgment and positions of other organizations, industries and countries and the standards, and common position. And if you will, that weight was derived from a frequency of usage weight. Okay? We looked at how often is this particular attribute used? How often is this particular attribute used?

And while not absolutely true, the criterion effectiveness and the attribute effectiveness are relatively orthogonal such that both weights could be applied multiplicatively. In other words, the DAE, the diversity attribute effectiveness, if you will, modifies the value of the diversity criteria effectiveness for those criteria that are used in particular strategies, keeping in mind that the intention is to use this as a screening too. I don't care whether the value is 1.01 or 1.03. I just want to know is the value within a range of reasonableness for what we would expect.

Now, the diversity criterion effectiveness assumptions are first that the criteria within a diversity attribute can be weighted according to the ordering of the criteria within that diversity attribute. That came out of NUREG/CR-6303 where they said this criterion is more effective than this one. We read through those criterion. It seemed like we didn't have any bones to pick about their assumption, you know, that different technologies for diversity tend to be a little bit more effective than using just digital technology to back up digital technology, using FPGAs to back up microprocessors would appear to be a more effective approach than using AMDs to backup, that type of thing.

MEMBER BLEY: I'm not quite sure how or why -- when do you need to need to claim it and how in the world can you even make the claim that those two effectiveness measures are orthogonal?

MR. WATERMAN: I said relatively orthogonal.

MEMBER BLEY: Based on the argument you made about the diversity attribute effectiveness weight, being that these experienced people applying judgment are using suitable and effective systems has probably got the same judgments in there that we have in the other set of weights out of 6303. There are different levels, I'll acknowledge that, but that they're orthogonal just seems -- do you need that assumption for any reason?

MR. WATERMAN: Well, I think you do if you're going to multiply them together.

MEMBER BLEY: If you do, I think that's hard to claim.

MR. GUARRO: If they are hierarchical. In other words, the first set of weights is applied to the broad categories and the second to the subcategories. They don't need to be orthogonal, just the different -- I think that's what you're seeing.

MEMBER BLEY: That's what I think.

MR. WATERMAN: Okay.

MEMBER BLEY: But, you know, I'm not sure what this measure really means. But you are multiplying.

MR. WATERMAN: Well, the criterion effectiveness simply says how effective is this particular criterion relative to the other criterion. It has nothing to do with what the world does with it.

MEMBER BLEY: That makes --

MR. WATERMAN: The design -- wait. No, just a second.

MEMBER BLEY: I don't think that's true.

MR. WATERMAN: You don't think it's -- okay. Let's --

MEMBER BLEY: I think the world does with it --

MR. WATERMAN: I think we're ready to get into a really lively discussion here. What you're saying is that despite --

MEMBER BLEY: If those guys are really smart, it does.

MR. WATERMAN: Yes, they're really smart, but it has nothing to do with is analog backing up digital more effective than FPBs backing up Intels.

MEMBER BLEY: Sure it does.

MR. WATERMAN: Okay. Then it doesn't matter whether the world uses it or not, does it? It is more effective, and so I can weight one over the other. Right?

MEMBER BLEY: If you believe that.

MR. WATERMAN: If you believe that. Well, I believe that.

MEMBER BLEY: But if you believe that the industries are doing it on a logical and smart basis, then I don't see how the orthogonal would be the same.

MR. WATERMAN: Well, scratch the orthogonal. What I'm trying to say is that the diversity criterion effectiveness weights are measuring something different than the attribute weight measured. The attribute weight simply says how many people are using design as an approach toward diversity?

MEMBER BLEY: I'm just going to say this once more and then I won't --

MR. WATERMAN: Okay. Okay.

MEMBER BLEY: But we've argued that that's a useful measure because the people making those decisions can understand they're picking things that are effective in each of their experiences, I think.

MR. WATERMAN: Yes.

MEMBER BLEY: So I don't seem them as really -- but let's go ahead.

CHAIRMAN APOSTOLAKIS: What's an FPGA, Mike?

MR. WATERMAN: FPGA is a field-programmable gate array. Thanks. And a field-programmable gate array is a different way of instantiating digital logic. It's a different type of complex electronic --

MEMBER BROWN: Like that word, "instantiating?"

CHAIRMAN APOSTOLAKIS: I don't understand.

MEMBER BROWN: Yes, that's because nobody else does either. Software engineers love that word.

I've sat through more --

CHAIRMAN APOSTOLAKIS: Stantiate?

MEMBER BROWN: They stantiate everything.

MR. WATERMAN: The real answer here is an FPGA is effectively hardware logic. It's combinational logic as opposed to microprocessors which have software logic. If you're running a program, a step program where you're looking at memory and pulling stuff out, all you've done is take individual transistors that you would burn to make a logic diagram. You put it on a chip in an FPGA and you cut lines to make sure you now have that hardware logic burned in. It's not software. So it's really an analog system once you've done it. Now if you can program it separately and un-program it, that's another issue you have to deal with. Some of them you build, once you burn it, it's burned.

MR. WOOD: FPGAs don't necessarily have to become notarial logic. They can include --

MEMBER BROWN: But it's still more of an analog approach because it doesn't change all the time. And we can argue about that. I was just trying to --

MR. WATERMAN: The way I look at it in layman's terms is a microprocessor fetches data, fetches instructions, does the instruction on the data, stores the result and repeats. And that's how it goes through its process. An FPGA, the data comes through the FPGA and the data flows simultaneously through the FPGA without any fetch instructions, without any fetching data or anything else like that. And what comes out the other side is either a zero or a one, that tells something to trip. They're different animals. That's very simplistic and an FPGA expert would probably --

CHAIRMAN APOSTOLAKIS: The *Webster's New Riverside University Dictionary* does not have the word instantiate.

MEMBER BROWN: That's because they made it up.

MEMBER BLEY: It came out of the expert systems 20 years ago. And it's a neat word.

MEMBER BROWN: What does it mean?

MEMBER BLEY: It means you took a concept and you applied it in a particular --

MEMBER BROWN: Why don't you just say that?

MEMBER BLEY: You are. You're getting old and cranky.

MEMBER BROWN: Yes, right. I'm getting

old and cranky. I just hate that stuff.

MEMBER BONACA: Well, he's getting the big dictionary now.

CHAIRMAN APOSTOLAKIS: Well, if this doesn't have it, then --

PARTICIPANT: Wait until you see the next definition.

CHAIRMAN APOSTOLAKIS: But we shouldn't complain, because the word "exceedance" does not exist either.

PARTICIPANT: Well, it does now.

MEMBER BROWN: It's not a word, that's why.

MEMBER BLEY: I think English evolves.

CHAIRMAN APOSTOLAKIS: Michael, will you please continue?

MR. WATERMAN: Thank you.

CHAIRMAN APOSTOLAKIS: We are exploring the --

MR. HECHT: Why don't you go to Google?

CHAIRMAN APOSTOLAKIS: No, no, no.

MR. HECHT: Type in the word and --

MEMBER BROWN: That's like Wikipedia. It's made up facts. Okay?

MR. WATERMAN: Moving right along.

CHAIRMAN APOSTOLAKIS: Yes, moving right along. Yes.

MR. WATERMAN: DCE weights are based on the NUREG/CR-6303 relative effectiveness discussions.

MEMBER BLEY: I'm sorry. It's in the *OED*. Enough said.

MR. WATERMAN: The *OED*.

MEMBER BLEY: *Oxford English Dictionary*. It's the authority on the language.

CHAIRMAN APOSTOLAKIS: Here it is --

MEMBER BLEY: One-oh-six volumes.

CHAIRMAN APOSTOLAKIS: Instantiate. To provide the instance of or concrete evidence in support of a theory, concept, claim, or the like. That's what it means.

MEMBER BONACA: It doesn't say substantiate. It says --

CHAIRMAN APOSTOLAKIS: It says to provide an instance of or concrete evidence in support of a theory, concept, claim, or the like.

MEMBER BONACA: Yes, instantiate.

MEMBER BLEY: Is that concrete evidence?

PARTICIPANT: No, it's an instance that's concrete --

MR. WATERMAN: An object --

MEMBER BROWN: Concrete is very firm.

MR. WATERMAN: Making something --

CHAIRMAN APOSTOLAKIS: Instance of or concrete evidence, yes.

MEMBER BROWN: Yes, concrete evidence. That's firm.

CHAIRMAN APOSTOLAKIS: What does that have to do with instantiate?

PARTICIPANT: Or. Or. There's and "or." So instance of or --

CHAIRMAN APOSTOLAKIS: Concrete evidence. Or, O-R.

MEMBER STETKAR: George, what does this have to do with DCE weights?

CHAIRMAN APOSTOLAKIS: Instantiate is a word that we heard yesterday and today and Charlie said that this word is --

MEMBER BROWN: It's just made up.

CHAIRMAN APOSTOLAKIS: -- made up.

MEMBER BLEY: It's in the *OED*. It means represent as or by an instance.

CHAIRMAN APOSTOLAKIS: What, instantiate?

MEMBER BLEY: Yes.

CHAIRMAN APOSTOLAKIS: Mike, can you go on?

MR. WATERMAN: I'd love to, but I got a note here, never use instantiation.

MEMBER BLEY: Oh, please do. You've got half-and-half.

MR. WATERMAN: Now, the DCE weights, the criterion effectiveness weights are based upon that discussion in NUREG/CR-6303 about what would be considered more effective than something else, in each of those attributes. And the *95421 relative effectiveness, well we accepted that. I mean, after all we published the NUREG. And that's essentially been accepted by the nuclear industry since it was published in 1994. So, you know, those relative effectiveness things, I felt, well, they've been around for 15 years. It seems like I should be able to, you know, take their word for it that one is more relatively effective than another.

And we haven't gone back in and revised that relative effectiveness, so it seemed like, oh, okay, I can use those relative effectivenesses. Now, mind you, when they were described in the NUREG, it was all qualitative discussion. This is more relatively effective? Then how much more relatively? Well, nobody ever defined that. And maybe that would be a good research project.

MEMBER STETKAR: You've never defined how much more relatively more effective. You've said that different logic processing architectures are twice as effective as different compound and integration architecture.

MR. WATERMAN: Yes, I've just --

MEMBER STETKAR: They're precisely effective.

MR. WATERMAN: I'll get into that in a second. Thanks.

MEMBER STETKAR: Okay.

MR. WATERMAN: Where am I at here? The second assumption was that, okay, if we're going to have weights, they ought to be different for each criterion within the attribute. And the underlying basis for that assumption is that the authors of NUREG/CR-6303 did not ever equate two adjacent criteria within a diversity attribute as being equally effective. It was always this is more effective than this, which is more effective than that. So if we're going to weight those criteria, well it seems like the weights ought to be different, too.

And diversity criteria within a diversity can be distributed uniformly according to the order and number of criteria within a diversity attribute.

Okay. I didn't have any data that said different technologies was 27.5 percent more effective than fundamentally different approaches within the same technology. I didn't have any of that information. So I had to make some assumptions. Well, if we're going to weight this, what's an easy way to weight it, keeping in mind that I was going to apply those weights uniformly across the full set of data. Any differences in relative effectiveness, everything would be treated the same. And so that's what I did. And furthermore, I felt that -- yes, John?

MEMBER STETKAR: Yes, let me ask you a specific question then. I didn't notice in your handouts. You don't have the table of weights, do you?

MR. WATERMAN: Yes. No.

MEMBER STETKAR: Okay. Okay. Let me ask you a specific question, because you said you didn't have any evidence. So I'm looking at the design attribute for which you've assigned weights of .5 for different technology, .33 for different approaches --

MR. WATERMAN: Three-six-two-six-one-six.

MEMBER STETKAR: Three-six-two-six-one-six. Different architectures receives a weight of

.167. I notice though that the infinitely wise people who actually do these things, within the design slice of your pie chart applied different architectures five percent of the time, different approaches within a technology two percent of the time and different technologies two percent of the time, meaning that the people actually doing it have made the decision that different architectures must be more than twice as effective as either of the other attributes.

MR. WATERMAN: Within a cost-benefit basis. Maybe part of their decision I'm sure was driven by, well, how much more is it going to cost us to go with completely technology? Well, we can't afford that. Okay. Well, let's take the second alternative.

MEMBER STETKAR: Okay.

MR. WATERMAN: That's a usage consideration --

MEMBER STETKAR: Okay.

MR. WATERMAN: -- versus a relative effectiveness.

MEMBER STETKAR: But you'd argue that the cost and efficacy and --

MR. WATERMAN: Well, I can't control that, you know?

MEMBER STETKAR: Yes.

CHAIRMAN APOSTOLAKIS: So, maybe I missed it, the weights you're deriving now, how are they related to the fractions, to the percentages that we saw earlier?

MR. WATERMAN: Those percentages were strictly off of what we saw --

CHAIRMAN APOSTOLAKIS: Okay. So these are not your own evaluations or judgments?

MR. WATERMAN: Yes.

CHAIRMAN APOSTOLAKIS: And I was wondering, this is, as we've said many times, this is a judgment thing. One way of structuring the solicitation of judgment is to use methods like the analytic hierarchy process. Have you thought about it at all?

MR. WATERMAN: No, I haven't.

CHAIRMAN APOSTOLAKIS: Would you like to think about it? Because that helps also when -- it helps you to make self-consistent judgments. And also you can use to elicit the judgments of a number of stakeholders, not just your own. I mean, say Michael and Richard are two stakeholders. Do your own thing and then compare. But you can to other people, too. And that might be a way of addressing questions like

Dennis' regarding orthogonality and Sergio's hierarchy, because it is a hierarchical approach. So, I don't know. Steve, are you familiar with the method?

MR. ARNDT: Very much so.

CHAIRMAN APOSTOLAKIS: Okay. And you work for this Agency that work for this -- you talk to each other? Just a suggestion. I mean, is what you are presenting cast in stone yet?

MR. WOOD: No.

CHAIRMAN APOSTOLAKIS: Okay.

MR. WOOD: No, this is all still draft stuff and then, you know, the threshold --

CHAIRMAN APOSTOLAKIS: Very good. Well, that's the purpose of Subcommittee meetings, actually.

MR. WOOD: Okay.

CHAIRMAN APOSTOLAKIS: Occasionally be helpful.

Okay. Please. I think we should stop here. Take a break. Because this is now our numbers. I mean, quantities. I see plus and minus.

MR. WOOD: Only one page. Originally, I was just going to show this equation, not do all the assumptions.

CHAIRMAN APOSTOLAKIS: Where are now,

slide 32?

MR. WOOD: I'm on 32.

CHAIRMAN APOSTOLAKIS: Yes, but that's what you think you're going to do. There may be questions.

MR. WOOD: Yes.

CHAIRMAN APOSTOLAKIS: So we'll be back at 10:15, there about.

(Whereupon, at 10:0 a.m. off the record until 10:19 a.m.)

CHAIRMAN APOSTOLAKIS: Okay. Are you ready, Mike?

We're back in session.

Mike, how are you?

MR. WATERMAN: I'm great. I'm getting a lot of good feedback here, real positive feedback.

CHAIRMAN APOSTOLAKIS: Very good. So then, slide 33.

MR. WATERMAN: Before I jump into this slide, I would like to point out that this is still a work in progress. You know, none of this stuff is draconian yet.

CHAIRMAN APOSTOLAKIS: No, no. Actually, this is the kind of Subcommittee meeting that most of us like. When you guys are still in the process of doing things to come here so in case you get some insight or whatever, you will have time to respond. I mean, if you come with a finished product, it's always a problem.

MR. WATERMAN: Yes, it certainly is.

CHAIRMAN APOSTOLAKIS: So we appreciate your willingness to come while this thing is still evolving. Okay.

MR. WATERMAN: And the purpose of this metric; I really like that term, George. The purpose of this metric is that there's a lot of really good engineers out in the industry and each one of them brings their own set of judgments to the table when they're designing a system. And then they submit those systems to the NRC and we have a lot of different judgments within the NRC, even between reviewers. And what I was hoping with this type of a metric would be that we would help reduce that variability and judgment. Because really, when a licensee submits something to the NRC, it really shouldn't matter who's doing the review, right? If you've got two different reviewers, they should both come to the same conclusion. And I'm hoping that this metric will help us arrive at that position such that we do a consistent licensing process and the industry knows what to except and then bring in their variability and judgments also.

MEMBER BLEY: One thing that's going to be crucial there, I see two applications. If I need some way to get confidence that this measure, metric behaves the way one would like it to behave is really important, after you apply it do the things make sense the way they rank afterwards? Do they stack up the way you think they should? Is it transitive? If you do the evaluations backwards or something, does it come out the same? Things like that.

MR. WOOD: Sensitivity studies on the weights would be useful.

MEMBER BLEY: I think so. I think you need a probative -- that to gain confidence that when you get results from it, they really mean --

MR. WATERMAN: Yes, and that was part of using that ATWS system, because I wanted something that what have we approved, what have we accepted, what are people using out in the industry? How does that stack up against all this metric? And it seemed to stack up like it came out. Well, it's about average.

MEMBER BLEY: It would be nice to see something that you didn't approve first. You know, look at earlier versions in time, see what it looks like with this metric. Was it bad at first and then got better with respect to the metric?

MR. WATERMAN: Good point, Dennis. I usually try to do that stuff. Think of what doesn't work and figure out why.

Okay. DCE weight. Wow, how did I get to there? Okay. Here we are. This is was the algorithm. All I did was the sum of the digits, if you will, and because I wanted to preserve that ranking one, two and three, one being the best and two being second-best, I had to do the little numerator thing up there so that number one would get the heaviest rank. And so for an attribute that only has three criteria in it, it splits out a 3.6, 2.6 and 1.6 for the weights, right?

MEMBER STETKAR: Is that for logic? Is that for logic or --

MR. WATERMAN: Well, for four, it would be .4, .3, .2. Four-tenths, three-tenths, two-tenths. They all, four, three and two and one add up to ten, right? Very simply. You know, in the absence of having a lot of time to dig and determine some finer scale of weighting, I thought well, this is probably pretty good for me to be able to, you know, do a back-of-the-envelope judgment on various strategies.

MEMBER STETKAR: I think table A3 you might have left a line off of.

MR. WATERMAN: A3.

MEMBER STETKAR: Table A3 is the basic weight table. Continue. We don't have a lot of time. Just check table A3.

MR. WATERMAN: A3?

MEMBER STETKAR: Yes.

MR. WATERMAN: Thanks, John.

On the diversity attribute weight assumptions, the first assumption was that the frequency of attribute usage is consistent with the assumed or observed effectiveness of a diversity attribute in addressing common-cause failures. In other words, things that work people tend to use. And so if a lot of people are using a particular attribute, it looks like a lot of people decided, you know, hey, that's a good attribute to use and so that attribute should have a pretty good weight.

The second assumption on slide 34, design constraints specific to a particular industry. The use of a diversity attribute should be reflected in the determination of the diversity attribute effectiveness weight for that attribute. In other words, if there are industries out there that just can't apply a particular attribute, well they ought to be screened out before we determine a weight for the diversity attribute usage. And that goes back to us screening out aerospace and aviation, because that domain there just isn't applicable to the nuclear power industry, right? I mean, they have to keep the plane flying, they can't shut down the engines, things like that. And they really don't have a lot of room for putting in diverse designs and diverse systems, another rack and stuff like that. So, this assumption here is the thing that helped us screen out things that really aren't applicable to the nuclear industry.

MEMBER STETKAR: But another way to think of that is that we do know the particular industries. Those other design attributes ought to be assigned a weight of zero when you look at the effectiveness of diversity strategies for those industries.

MR. WATERMAN: Yes, for those industries. But since I was only interested in the nuclear industry --

MEMBER STETKAR: Fine.

MR. WATERMAN: Yes. The next assumption was the decision to use a diversity attribute is sufficiently independent of the decision to use other diversity attributes, which isn't totally true, right? Because, for example, if you go with the design diversity attribute, that's going to do an inherent credit toward other types of diversity attribute usage. I mean, if you're using analog to back up digital, that automatically implies that your logic attribute is going to be also affected, right? Because the way the logic is instantiated. It may also affect different manufacturers over in equipment manufacturing attributes, but for doing frequency of usage, I thought well, I'm willing to live with doing that to come up with a relative effectiveness.

And the other thing about developing the weights is that if you have an attribute where each of the criteria within the attribute are mutually exclusive, when you go out to look at frequency of usage you should account for that type of things when you're doing the weight calculation. So there were three different ways of calculating diversity attribute weights. The first way was for things that are not mutually exclusive. You just sum up the usage of; well, you can see it, the number of criteria. You sum up the number of criteria in I used in attribute J by the systems that are used to develop the weight. And you sum up that number of usages and you divide by the number of system designs an agency position is evaluated; that was that between-the-red-lines thing, times the number of opportunities people had to use all of those weights. For example, for the equipment manufacturer, things have modified, because equipment manufacturer is one of those mutually-exclusive things.

For function, where you could use all of the criteria within function for a particular design, that value would be three up in here. So because people could use one, two or three of those criterion when selecting that attribute, which all we're interested in is what do people think about using that attribute. And so that's how I did the scoring on that.

MEMBER BLEY: Can I just toss you an idea?

MR. WATERMAN: Sure.

MEMBER BLEY: On the surface this looks pretty reasonable and, you know, the test will be how well it works, but I just wanted to relate something that I saw happen. And I don't fully understand -- I haven't chased the arithmetic of why it happens. But there's a human reliability method called SLIM that was developed for NRC that in an odd sense is similar, as John said, but it does weights and rankings for each characteristic, each performance shaping factor and then your sum. Well, some people that I was associated with, you know, were -- a couple of these really, it shouldn't be a sum. It seemed to me they ought to get multiplied together and then there ought to be three more and then you ought to divide by another one, because it just makes kind of sense. And it did kind of look reasonable. What happened was when you expanded it and did all that stuff, your answers all complex to be almost exactly the same thing. Didn't matter what you came in with, you almost always get the same answer. So something weird goes on in these kind of equations.

MR. GUARRO: Is the theorem of tendency to the mean?

MEMBER BLEY: There's a central tendency to --

MR. WATERMAN: Almost. But it's not exactly right, but that's what's happening.

MR. GUARRO: That's it. I've seen it happen.

MEMBER BLEY: But be a little careful, especially if you start tweaking with these and trying to things out, and do test them pretty thoroughly on --

MR. GUARRO: Which is why certain people actually argue that when you assign weights, you should use geometric progressions instead of try to separate out more, if you really believe that there is a different.

MEMBER BLEY: In fact that was the basis for SLIM, although it hasn't always been used that way.

MR. WATERMAN: What I found by using this tool is the first time I input all the data I made some mistakes and so I thought, ah, the weights are wrong. So I went back and I fixed the mistakes that I found that time and the weights changed a little bit. But when I started looking at the average, that number in that region, it really didn't change a lot. The average moved up and down a little bit.

MEMBER BLEY: Maybe you're already there.

MR. WATERMAN: Yes. And I thought, well, gee, you know, and so I went back in and scrubbed a little bit more and found some other stuff. And the weights have been changing; it's a work in progress. The weights have been changing, but really everything stayed kind of relative to -- you know, all the strategies stayed pretty much relative to each other, you know. Some were higher scores than others and it remained that way no matter how I changed those little weights by making corrections to the data. And I thought, geeze, does this mean that if I go get more data, I'm really just, you know, marginal return on the effort?

MEMBER BLEY: And like what you just said, I think you need to make sure that in cases where clearly you don't have enough diversity that you get an index out of this thing that says so.

MR. WATERMAN: Yes. And this just talks about design. There's also some equipment manufacturer criterion in it. It was just a little bit different way. On the mutually-exclusive, when I looked at frequency of usage for that attribute, say equipment manufacturer, if you look at those criteria, it's really -- you can only select one of them. I mean, you've got four options, but if you select one you can't do the other, you know? Different manufacturers of fundamentally different equipment, if you say that's the way I'm going, you can't also say they're same manufacturers of the same equipment. Right? So they were mutually exclusive, so the number of choices that you had for using criterion in that was equal to one. And then that came out like that. You notice at times $N_C$-something there, down on the bottom, is equal -- so that weight was calculated a little bit differently. And if you look at the weight per design especially, it's weighted 1.0 because in the diversity approaches that we looked at to determine the weights, one of the criterion design was used by everyone of them. In other words, every one of those examples, somebody decided we need design diversity in here. We either need different technologies or different approaches in the fundamental technology or we just need different architectures, AMD-versus-Intel-type thing.

And for logic processing equipment what we found was that that was a mix of mutually-exclusive and not mutually-exclusive. The first two criteria in logic processing equipment or mutually-exclusive, but the other two criteria could be used with either of them. And so that came up with a little bit different thing there. Instead of having four choices in logic processing equipment, you'll really only have three if you're going to design a system. You can pick one of the first two and both of the second two, but you can't pick both of the first two. They just exclude each other. And so therefore you only a total of three possible choices in one strategy.

And then we used those weights that we are starting out with to score all of the strategies to come up with an average score, if you will. And that was just the diversity criterion and times of diversity attribute effectiveness weights for the criterion attribute used in a particular design.

And then those things usually came out to be some number and a fraction, like 2.38 or 1.96. And me, I relate more to numbers in the hundreds that are integers and so I just scaled it by hundreds so when I looked at the scores I had, you know, a different feel. But it's just linear scaling.

And then I averaged up the scores and then use that average to normalize all the scores, because it's always easier to compare something to 1.0, the average, than it is to compare a number like 259 to 275. What does that mean? And so that's the general algorithm that I used. And the spreadsheet does it, so it's not really onerous. The spreadsheet just goes through and adds up all these Xs and Is and comes up with a score using the weights.

MEMBER BLEY: I see later in this you have a reference to the tool, so if we go to that we'll get the spreadsheet? Is that what that is?

MR. WATERMAN: Yes, I've got the spreadsheet on here and I thought I would demonstrate it and put in some different views. It's kind of hard to see on these screens because you have to scroll a lot. Charlie and I, we worked through an example yesterday and I'll show you how it works.

And then we normalize the scores with a normalizing concept. Then this ought to look familiar. This is 47, or 46 on yours, in which we screened out aerospace and aviation applications. We also screened out some various other applications that just had minimal diversity usage, so it wasn't really telling us how much diversity is enough. And then we used the rest of these things in here to come up with our weights.

MEMBER BLEY: Now once you get these weights; I mean, you did all of these, the ones that did come out low, how do you spin back to see why it's coming out low?

MR. WATERMAN: Well, we went back and actually looked at the design. We screened it out originally because they just weren't using a lot of diversity.

MEMBER BLEY: Okay.

MR. WATERMAN: I mean, they were just backing up a system with a different function. It's like that's it? You know, what about a technology approach? Aren't you worried about common-cause failure in a microprocessors or an instrument, or something like that? And they just weren't doing that, you know? As a matter of fact, the report documents which ones were screened out. I don't want to call anybody and make them feel awkward here.

And then we had a couple of examples. We've approved, as far as I know, I've been told we've approved the Oconee low-pressure injection actuation system, diverse low-pressure injection actuation. So I don't know if that's gone out yet. So that's pre-decisional, but anyway in talking to the branch chief, he says yes, they found it acceptable. I don't know what the status is on Oconee anymore. I'm not involved in that. And so I scored it just to say oh, really? Well, let's take a look at it. And actually the first time I scored it they were still down at the plant reviewing the system and Bill gave me a call and said, "Hey, could you score this real quick for me and see how it shakes out?"

MEMBER BLEY: So as you score one of these, take one of those examples from another industry that didn't score high, you kind of know as you're scoring it that it's not good. The score just gives you something to compare it to other things with and say I noticed it didn't have all of these and look, here the scores comes out.

MR. WATERMAN: Yes, that's right, Dennis. Thank you for bringing that up, because this is not a draconian measure, thou shall reach the threshold or else. This is more of a, look, their score is really low. Maybe we ought to take a second look at this when it comes in and really understand why the score is so low. Maybe the score is so low and it's appropriate. In that case there, well, it would still be approved. But what it does do is if a licensee addresses typical common-cause failure space that we're all familiar with, their score is probably going to end up in this red region. And that gives us some comfort level, if you will, from the metric that, yes, looking reasonable so far. That doesn't mean we're going to just blindly rubber stamp it and say, well, you made the score and you passed. But what it does do is it tells us looks like we're all working on the same track here. And so it reduces some of that variability and judgment.

MEMBER BLEY: I just want to come back to something you said earlier. If a design that -- essentially from everywhere on your wheel they'd get a two, or something about a two.

MR. WATERMAN: Yes.

MEMBER BLEY: So if it's higher than it's not extreme. That's about it.

MR. WATERMAN: Yes, if they get that, but that doesn't mean we don't review it.

MEMBER BLEY: Sure.

MR. WATERMAN: It just means it looks like -- it gives us a comfort feeling, if you will, and it gives the licensee a comfort feeling about their certainty of getting approval that they don't have right now. So that's why I've got this little arrow out here that as the score goes up, the licensing uncertainty will probably go up, too.

So now we're getting into the part that I should have put up at the beginning of this, was the implementation constraints. And the first is that potential common-cause failure should be used identified using operational experience, NUREG/CR-6303 and the BTP 7-19 analysis. All of those things go into helping determine is there really a need for diversity? So the first constraint is to determine whether or not you have to address, you know, diversity. And the second thing is when a design is developed the design should identify, you know, should address those identified common-cause failures.

Somebody shouldn't just go willy-nilly into the table picking up Xs to get a good score. And licensees, you know, they've got a bottom line to worry about, so they're going to design against common-cause failures that they think are credible. But the design should address each of the identified common-cause failures.

And on the flip side of that is all credited diversity criteria should be in the design. In other words, if somebody says these are the things that give us the score, all of those things ought to be in the design submitted for review and that the staff should verify our actioning there. And I'll show you how that creeps into here when we talk about intentional selection of diversity criteria and the inherent selection of diversity criteria as a result of selecting certain criteria. And you'll see in the demonstration about how things --

And the resulting diversity score should fall within a yet-to-be-determined range of acceptable scores. Now, we haven't determined that range yet. I just through a shaded area on the plot there to give you some concept. We're not looking for 1.0 or .95 anymore. We're looking for are you within a range of acceptability. And part of that range is we go out and we look at things that have happened in the past and what other people are common-cause failures and determine, you know, these are the things that ought to be addressed. Here's a research project right there. These are things that ought to be addressed. And so if they are addressed, scores should fall, you know, above that limit, at that limit or above that limit. So if we look at the things that ought to be addressed, you should be able to calculate up a diversity strategy to address that minimum set of common-cause failures. That will give you the bottom line and then we put in the pink area into that. And that has to be worked out with industry. It has to be worked out with the public, obviously, with you gentlemen here and among the staff. We don't know what that range is right now and it's just a conceptual idea and we realize we've got a lot of hammering to do on that one, too.

And then all the information that went into justifying that strategy should be submitted to the NRC so that we can plug it into our own metric, right, and verify, yes, it's there. And so we can start doing the reviews. When somebody says this is how we're addressing design common-cause failure, we can verify, yes, they did it. That's the way it is.

I suspect there's going to be some

research on refining what those criteria mean. I would hope we do more research, because just in working with the staff in NRR they've come up with some very interesting questions about what those diversity criteria really mean. That's like, I didn't think of that. So we probably need guidance to the industry and to the staff about when somebody says they're going to use different equipment manufacturers for the same design, what does that mean? If one vendor, for example, procures equipment for the diverse system, is that a different manufacturer just because the equipment is different, or is that the same manufacturer? So we have to resolve those things, too, we can give credit where credit is due.

And what's our path forward? Well, obviously we want stakeholder feedback, and I'd just look for as much feedback as I can. I realize that some of the digits weighting is very subjective. It looks quantitative, but it's subjectivity hidden underneath quantification. But if somebody's got a better idea for a better set of weights, you know, we would really like to pursue that, if we can, and keep refining this particular type of metric.

So what we've done is the evaluation tool is available now publicly in ADAMS. I thought it was publicly all along. We put that into ADAMS, the first version of that tool, back in December of last year. A draft version of the NUREG, which you all have, is also publicly available in ADAMS for the industry and the public to review and provide comments on. And the intention is to get those comments, weed through them and incorporate all those good ideas into the NUREG to make the NUREG that much more usable. And then eventually as that NUREG gets polished off, we want to incorporate that evaluation method into our licensing process.

So, what I talked about today is that we correlated experience and engineering judgment, if you will, with the diversity attributes in NUREG and we used that correlated data to develop a method for evaluating diversity in I&C system design. And we have a spreadsheet tool available in ADAMS. There's that number again. And the draft is available for the public and industry to comment on.

And the bottom line is that this licensing uncertainty is just stifling the industry and it's really tying up us in knots, too, over in regulation. I'm just trying to address that issue. We are trying to address it.

MR. HECHT: Mike, can I ask a question?

MR. WATERMAN: Sure.

MR. HECHT: On slide 41 --

MR. WATERMAN: Oh, that's right. I'm one slide ahead of you.

MR. HECHT: Oh, okay.

MR. WATERMAN: This one here?

MR. HECHT: No, I guess it would be slide 42.

MR. WATERMAN: How about that one right there?

MR. HECHT: Yes. Right.

MR. WATERMAN: Okay.

MR. HECHT: I don't understand $N_{C3}$-1.

MR. WATERMAN: Okay. Okay. That was the one where I was talking about in the logic processing equipment, if you take a look at those diversity criteria --

MR. HECHT: Yes.

MR. WATERMAN: -- criterion 1 and criterion 2 are mutually exclusive.

MR. HECHT: I see.

MR. WATERMAN: You see? So whatever diversity strategy you're using; I think it's criterion 1 and criterion 2, whatever strategy people use, they can only pick one or the other of those.

MR. HECHT: Okay.

MR. WATERMAN: And so if I'm looking at frequency of usage, I have to account for that when I weight it out.

MR. HECHT: Right. Right. Okay.

CHAIRMAN APOSTOLAKIS: Any other comments or questions from the members?

MR. HECHT: I do notice that you use the word "score."

MR. WATERMAN: Score? Yes, I know. I like metric better. I'm going to adopt that.

CHAIRMAN APOSTOLAKIS: The public has a comment? Ted?

MR. QUINN: Sure. Yes. Ted Quinn, representing Diablo today.

We're familiar with this report from last summer and we honestly like it and we expect to use it in our processes going forward. So there's two comments to you.

One is related to software failures. I think it's important to look at the old data and the new data in relation to the importance of software failures and their contribution to the potential for CCF. And the old data is Bob Brill and Eric Lee that came from years ago and it said that greater than 50 percent of the errors were caused by -- in the requirement space, or due to the thing. And you know that from -- well, I think looking at the industry data that they have, I just recommend it, that I think you might see -- and you know, the old data was where Nancy Levinson drew some of her conclusions. I think the new data may change her conclusions and some of the importance of where you may show it. It may give you some benefit and robustness of your factors. I think it's something to consider. Okay?

CHAIRMAN APOSTOLAKIS: You think it's not 50 percent anymore, Ted? Is that what you're saying?

MR. QUINN: I think; and I'll leave to the experts who have done this hard work, I think it's less. And that's number one.

Number two, I think it's important to ask you to look at the DAS and the importance of the DAS. And I'll just give an example. In General Electric, I spent the last two-and-a-half years -- and were you to this, Mike, up there today with the GE RPSS DAS, which is, all four echelons are separated and there is a full backup DAS, I think it would be a two on this thing. Okay? It would be a number that is large. But it has a full backup DAS. And the DAS has pluses and minuses. And you know, the best lecture I know is

Steve Hanauer on the benefits or the lack of benefits of adding complexity to this. No mater what we do -- and I think your analysis is tremendous. What you're doing is great work. Maybe it's a separate task to look at DAS, I don't know. But I really think if you could factor or look at where if the results of this are X, then thing that I think George said awhile ago was, well, what do you do with this? Where does this number go in our D3 analysis, or explicit D3 analysis? Well, part of it is the evaluation of a non-safety DAS that I'm adding and the real benefits for it.

MR. WATERMAN: Thank you for bringing up that point, Ted. The other area where you can use the tool is actually when you're looking at your primary system and determining do I have enough diversity in the system that I don't need to worry about common-cause failures and another system added onto it.

MR. QUINN: Agreed.

MR. WATERMAN: I think the GE system is one, as I recall; it's been a while since I looked at it, where they've got a ton of diversity with the system itself.

MR. QUINN: They do.

MR. WATERMAN: Yes.

MR. QUINN: They do actually, between

vendors and -- so your comparison of that would be great, but again, number one is we're going to use your work. Thank you.

MR. WATERMAN: And incidently, I did not demonstrate the tool. So if you wish, I can do that.

CHAIRMAN APOSTOLAKIS: Demonstrate what?

MEMBER BLEY: The tool. Put in some numbers, get an answer. Is that what --

MR. WATERMAN: What I did was, I've got the tool here. I can't click to clear the worksheet. There's a macro in the tool, so if anybody gets it out of ADAMS, that macro allows you to clear all the Xs and Os by clicking on that thing there. This computer here has a security level too high, so I can't run macros. So it's kind of a drag going through and doing it manually. But in the case of just talking about inherent credit and intentional credit, intentionally selecting some criteria, like different technologies, inherently credits other criteria in there without the person actually consciously going in and clicking those. For example, let's just say we have a design that's using analog to backup digital, which is easy. And by clicking an X there, then inherently, because you have analog versus digital, the architectures of those two systems are really going to be radically different. Right? I mean, if you look at it here, you're going to have relays strung together with wire versus software in a digital.

John's over there. He's making me nervous now.

There's an inherent credit that if you're backing up a digital with an analog, you probably have different manufacturers of those fundamentally different designs. You've got one company who's producing digital equipment, you've got another company that's producing analog equipment. That's not the case. Say you've got a company that can do it all, you know, you could always put an N in there, negate that. You could say it's the same manufacturer, fundamentally different designs and you could credit it like that. And these little weight out in here, these are their criterion effectiveness weights just transferred over to here and for the boxes that aren't used, they stay zero so that I can adding them up down in here in these subtotals.

MR. GUARRO: Mike, just one quick question on that that I should have asked before, but I know that your chart 30 said that, you know, you assumed that you had to have different ways for the categories there, because what the NUREG-6303 did.

MR. WATERMAN: Yes.

MR. GUARRO: Have you looked at whether, you know, that's still something you agree with, that it was not allowing two factors to be equally weighted? I mean, I don't know it's important. Just as a conceptual point of view.

MR. WATERMAN: Yes, I went through and read it real carefully, I just went out looking, how can I weight this stuff? And so, I got into the NUREG/CR-6303 and I noticed the relative effectiveness. And so I went through there and sort of verified for myself, yes, they're all different, yes.

MR. GUARRO: Yes, because, I mean, you know, from a conceptual point of view it seems that, you know, depending on whether a certain major category has more or less subcategories, it creates more or less distance between your scores, which is somewhat artificial in some cases.

MR. WATERMAN: Yes, it is.

Backing off there, just by selecting intentionally different technologies we get a lot of inherent credit for other types of diversity attributes. For example, if you're going analog versus digital, way over in logic, you know, do you have different languages? Yes, of course you do. Because the way you described your analog system and laid out the logic for that is totally different than what you would do if you were writing a digital system in C. So those are really different languages. Do you have different algorithms? The actual algorithm itself is going to be different, right, because of the way the components are laid out. And so the tool automatically credits things. Remember one of the constraints is all of this credit that's given, the licensee or the vendor and the staff have to ensure, yes, those things do in fact exist in there. And the one example I gave is if it's a different manufacturer, well you don't get credit for different manufacturers because it's the same manufacturer. But you do get credit by checking an X in there and that changes the score a little bit.

MEMBER BROWN: Just one comment on some of the inherent ones. Dennis brought up the thought process; I don't understand your orthogonal, I know you're all orthogonal, non-orthogonal, whatever, but once you select a different technology and then you go down and you credit the different -- wherever it's -- down in the -- where it's a different language.

MR. WATERMAN: Here we go. Yes.

MEMBER BROWN: And you say it's inherent. You said one thing and I'm trying to pick up on whichever one it was. Do you run the risk of adding in some additional goodness that may -- you're counting it twice, only maybe at a different level. And when you hit one of those, it just happened to hit me that, yes, maybe that might be one.

MR. WATERMAN: Yes.

MEMBER BROWN: For instance, in another case where you give a differentiation at the top between different architectures, which was .167, and the different approaches within a technology, which is .333. I think this is possibly a case where you could assign equal weights almost, because there are some fundamentally different architectures in the microprocessor world that you can apply where you get a benefit. Because all microprocessors themselves do not have the same architecture. They're are inherent differences included in their designs on the chips. So you get different failure mechanisms. I just wanted to try to provide an example based on the discussion we had; that's all, since we've been talking about it. I understand that, you know, you've got to make some decisions about what to do. It's just it's not always real crisp that that applies, that they're always less, none of them are equal, and that you're not double counting somewhere. I think some refinement in that thought process over and above whatever you drive out of 6303 or 6033, whichever -- what is it, 6303 --

PARTICIPANTS: Sixty-three-oh-three, yes.

MEMBER BROWN: -- needs to be thought about in terms of how you apply the thing.

MR. WATERMAN: Well, that double accounting, it was more of a step back and really thinking about that effects. You know, the whole software thing is -- when it to be called software you could say that's an analog system, no software, no credit for different algorithms, no credit for any of that stuff, and so your score comes out real low. And I thought, you know, this reasonableness thing, is that right? And so Richard had developed the whole process of inherent and intentional selection, the intentional drives some of the inherence. And so while it appears to be double counting, for most of that stuff you --

MEMBER BROWN: I'm not saying anything new, Mike. I'm just saying that the issues are one.

MR. WATERMAN: The other issue on

different -- I keep giving an example of Intel versus AMD and, boy, if you look at an AMD microprocessor and an Intel microprocessor, those are different animals. You know, one's --

CHAIRMAN APOSTOLAKIS: I think you should explore a different way of setting the weights, as I suggested earlier, which address some of these questions. But it's not really AHP itself. It just occurred to me that the staff had a contractor, ISL, develop a methodology for prioritizing the ITAACs. And that's a fuller methodology than the AHP in the sense that -- but it's very similar to what the committee does in evaluating the quality of research reports. It's exactly the same. It has relative weights of attributes, but then within each attribute you score how good it is, how well it is achieved. So I have that report electronically. I can email it to you, or you can dig it up. It was sponsored by the Office of Research. But it is being used, I understand, by the Atlanta office of NRO.

MR. CASE: I know of that report, so I can get to it.

CHAIRMAN APOSTOLAKIS: Oh, wonderful.

MR. CASE: I'm Mike Case. I'm the director of the Division of Engineering and Research.

And so I know that --

CHAIRMAN APOSTOLAKIS: Oh, okay.

MR. CASE: -- about construction inspection, so we'll get that to Mike.

CHAIRMAN APOSTOLAKIS: Yes. Very good. But that might give you a different perspective. Maybe if you ask the questions while you're looking at it that Charlie and Dennis and others have asked, maybe you can get some insights that would be useful. Because the whole point of that approach is to actually help you structure this kind of judgment. Plus, then you can say we used this method which has a name.

MR. WATERMAN: Well, the metric is obviously the Apostolakis method.

CHAIRMAN APOSTOLAKIS: Hey.

MEMBER BLEY: You might run into some trouble.

CHAIRMAN APOSTOLAKIS: And also, the ACRS, you can look at the ACRS view. In fact, that's a much simpler description of the methodologies, the ACRS evaluation of the quality of research, which I believe we're going to do for 6303, aren't we, Charlie?

MEMBER BROWN: Oh, is that one of them?

CHAIRMAN APOSTOLAKIS: Of this one.

MR. WATERMAN: Oh, you're doing it on this?

MEMBER BROWN: This one.

CHAIRMAN APOSTOLAKIS: Or do it on this?

MEMBER BROWN: This? Yes.

CHAIRMAN APOSTOLAKIS: But it's not the finished product.

MR. WATERMAN: Yes. Well, I tried to explain that.

MEMBER BROWN: That gives you ample opportunity to make some astute and erudite observations.

CHAIRMAN APOSTOLAKIS: We'll raise it next week. I mean, we're supposed to review finished products.

MEMBER BROWN: And this is not finished.

CHAIRMAN APOSTOLAKIS: No, this is not finished.

MS. ANTONESCU: Well, Research offered it, so --

CHAIRMAN APOSTOLAKIS: Well, the Research made a mistake. Why? Because it's unfair to Richard or to Mike. If we make a comment and then they say, but we're thinking about it, then what do you do? It's really unfair to review in that context work that is in progress. To have a Subcommittee meeting is completely different, yes. No, I hadn't realized that. I'm glad I haven't started.

MEMBER BLEY: Sixty-three-oh-three, that's --

CHAIRMAN APOSTOLAKIS: Sixty-three-oh-three is a NUREG. It's out. It's fair game.

MEMBER BROWN: One other point on the assessment.

CHAIRMAN APOSTOLAKIS: Sure.

MEMBER BROWN: I mean, the weights, my concern; and whether this is valid or not, I'm not analytical enough to say, but the concern is you get the wrong order. I mean, so you assign numbers to the weights; a=-alf, .33, .167, if the order is correct relatively, even though you may have slightly different numerical assignments, you can kind of still use it for relative judgments a little bit better. If you get the order out of rank, if you get the order out of order, okay --

CHAIRMAN APOSTOLAKIS: Wrong. If you get it wrong?

MEMBER BROWN: You just get it wrong, yes, and you're really compromising your ability to draw conclusions from it. Again, it's just a thought that you're going through 6303 over to this and if those guys thought about it and it was 15 years old and therefore it's got to be right --

MEMBER BLEY: But they didn't think about how much of it you need, kind of. They looked at each thing.

MEMBER BROWN: Yes, although --

MEMBER BLEY: A is better than B, but this one's doing a different thing.

MEMBER BROWN: Well, they ranked --

MEMBER BLEY: Out of A through Z, how many do you need?

MEMBER BROWN: Yes, somebody determined the order and they assigned a number.

CHAIRMAN APOSTOLAKIS: I think the order is taken care of automatically in this hierarchical approach, but I maybe misunderstanding what --

MEMBER BROWN: The order's been predetermined based on 6303.

CHAIRMAN APOSTOLAKIS: Right.

MEMBER BROWN: And that's how old? When was that written?

MR. WATERMAN: Fifteen years old.

MEMBER BROWN: Fifteen years old, and things change.

CHAIRMAN APOSTOLAKIS: If they go to this new approach, I think that it will be a systematic --

MEMBER BROWN: What's AHP? Analytical hierarchical process?

CHAIRMAN APOSTOLAKIS: Right. Yes, that's what it is.

MEMBER BROWN: Okay. That's very academic. I'm way down the --

CHAIRMAN APOSTOLAKIS: Which means it's useless?

MEMBER BROWN: No. It just means I have to learn about it, that's all. I suspect I'm going to have to since it's in that study report.

CHAIRMAN APOSTOLAKIS: You guys in the real world sometimes have to get out of our cocoon.

CHAIRMAN APOSTOLAKIS: Vice-versa.

CHAIRMAN APOSTOLAKIS: And go to the unreal world --

MR. WOOD: Pay a visit to the ivory tower every now and then.

CHAIRMAN APOSTOLAKIS: Mike, do you have anything else to say that is of great interest?

MR. WATERMAN: No.

CHAIRMAN APOSTOLAKIS: Thank you very much.

I think there was a comment on this presentation, right? If you're talking about your 10 minutes, that will come later.

We're done. Thank you very much.

Now, the public, NEI has requested some time, so they will get 10 minutes or so. In fact, my understanding is that it will be EPRI making the presentation, correct?

But one important thing is as you know we have postponed a presentation or two presentations that were supposed to take place today. I suggest we take 5-10 minutes to go get our calendars and decide on dates here in session after Ray finishes his remarks. Because we're talking about a June time frame, maybe one week before, one week after, but essentially that time. I think that's what Mr. Grobe said yesterday, around June. Yes?

MR. ARNDT: I'd have to check collective calendars, but the two obvious challenges for the staff are the Commission meeting, which will probably be the first week in June, the 2nd or 3rd of June, on this same general area, I&C.

CHAIRMAN APOSTOLAKIS: So you want the Subcommittee meeting to be before or after?

MR. ARNDT: I don't think it matters so

long as it's not that same week. Preferably a week or two after for our preparation time.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: And of course a number of the Committee and probably some our prep people will be --

CHAIRMAN APOSTOLAKIS: Why we have to stop the process and at least identify a couple of --

MR. ARNDT: Yes.

CHAIRMAN APOSTOLAKIS: Because, you know, some of our calendars are pretty full, too.

MR. ARNDT: Correct.

CHAIRMAN APOSTOLAKIS: So why don't we do that? Come back in about 10 minutes and bring whatever information you can bring regarding your commitments and then we'll give the floor to Mr. Torok.

(Whereupon, at 11:04 a.m. off the record until 11:14 a.m.)

CHAIRMAN APOSTOLAKIS: Okay. I think we should start. Okay. Shall we resume? Okay. We're back in session and we have a request for some time by Mr. Ray Torok of the Electric Power Research Institute.

So, Ray, you have about 10 minutes.

MR. TOROK: Okay. Thank you. Thank you

for the opportunity. Yes, as you know, at one point we were planning to give a presentation here today and that didn't happen, but I wanted to follow up and talk a little about, you know, what we would like to come back and talk about and why we think it's a good idea to do that. And, by the way, after listening for the last couple of days, I am more convinced than ever that it's a good idea for us to come back and talk about these things some more, and I think I can explain more why.

A couple of areas that we were going to talk about have to do with the operating experience evaluations that we did and you saw them referenced in what Mike was talking about a few minute ago. And also, PRA methods for digital, and, you know, that came up several times yesterday. So those are important topics. But also, there's another one that's related to both really, which has to do with failure modes, and failure mechanisms, and failure effects for digital equipment. And it plays into both really, because, you know, there's a question of what we see in the operating experience that we looked at. There's also the question of what does that mean relative to PRA? So it's tied to both. So we want to talk more about failure modes and mechanisms and that sort of thing.

CHAIRMAN APOSTOLAKIS: Well, as you probably know, this Committee has been very interested in failure modes.

MR. TOROK: I read your letter. That's right.

CHAIRMAN APOSTOLAKIS: Well, somebody --

MR. TOROK: And we agree that it's a good thing to keep --

CHAIRMAN APOSTOLAKIS: Very good. Very good. Okay.

MR. TOROK: And I guess really in the area of OE, we're talking about, in some sense, picking up where we left off when we talked to this group back in March and April last year, and where we were just getting into this subject of failure modes and whatnot when we ran out of time.

So we want to follow up with that discussion and there are a number of things that we can get into there. One of course is what we were seeing in the data in terms of modes and mechanisms, but also I think that leads us into more discussion of specific events that we looked at and what the OE said about it, and what the LER says about it, and how we extracted our conclusions from that sort of thing.

And I heard a lot of discussion in the last day around that kind of issue, so I think that would be useful and you guys will want to ask more questions about it.

Another thing that comes into play here is the root cause analysis practices that utilities use, and that's a very interesting exercise by itself. And our guy, Bruce Geddes, our consultant here, has a fair amount of experience in that and can enlighten us in that area, and I think that's very useful.

Also, the notion of FMEA analysis as is practiced today by vendors of the digital equipment, you know, of the equipment going into the plants. I think that's a real useful topic to get into more.

And with that, what I would characterize as the realistic behaviors of digital systems, especially systems being used for 1E applications. There is this whole issue of realistic behaviors of actual systems being used in the plants and being proposed for the plants, because you know, there's a difference between what's theoretically possible with a digital system and what's possible in systems as they're designed because of various design characteristics that the vendors incorporate in them and, you know, their impact on the actual failure modes and effects and those kinds of things. And that's a very interesting discussion by itself.

And then finally, where does that leave you in terms of modeling these things in PRA, you know, in terms of failure mechanisms versus modes versus effects and so on? And that brings me to the PRA subject, right? In the area of PRA, a number of questions have been raised here in previous meetings, in letters and so on, in regard to the state of the art of PRA and whether that's good enough for digital equipment in terms of questions about level of detail that you need for digital equipment is one, in terms of possibly new failure modes and how those need to be handled, in terms of establishing or estimating failure probabilities. Right? These are all wide-open questions.

But the fact of the matter is, the PRA analyses are being done right now for new plants. They're being done in some cases by operating plants. They're being done by national labs on these systems. They're being done by overseas utilities. So it's happening. And the fact that it's ongoing now while there are these big questions surrounding it means we should be talking about it more. That's the way I look at it.

Now, we sent you a report. We sent you

two reports, right? One was our final OE report that was published in December. The other was on an example of applying PRA methods to a particular digital issue.

MEMBER BROWN: Is that the risks and benefits?

MR. TOROK: That's right. That's the PRA one. And that describes how we applied PRA to a particular issue to extract insights.

Now, in my mind what's important about that report is not the specific conclusions of that analysis. What's important is that it demonstrates I think the usefulness of PRA in that we were able to extract useful insights and the insights were insensitive to the assumptions made in the analysis and we did that without what I would call precise knowledge of the failure modes or the probabilities of failure. And that's interesting, I think. And to the extent that you can do that with PRA, I think we should be looking at it more and recognizing the limitations of it, obviously. But it's a great example, I think, of what you can extract right now. So that's what we wanted to talk about.

Now, another thing was that, I guess yesterday there was some question raised or a reference to industry continuing R&D, you know, on digital issues, whether or not we are doing it or not doing it. So I wanted to mention a few things that are still ongoing.

In the area of common-cause failure in D3, we are working this year on guidance on what we call protecting against common-cause failure. Now I think of that as sort of a more holistic broader version of what Mike's got going on with his diversity deal. Because the way we view it, the issue that you really care about is not how diverse are you. The issue is how good is your protection against common-cause failure? And when you're protecting against common-cause failure, diversity is not your only tool here. Right? Because there are methods for prevention of failures and there are also methods for mitigating failures, and all of it should come into play. And when you start talking about for digital system failures in particular -- and by the way, we usually don't say software common-cause failure, we say digital common-cause failure, which is a little broader and we'll explain that when we come back. Okay? But the idea, I guess, is that you can talk about design attributes and process attributes and so on that are intended to prevent faults, for example, and others that are intended to prevent triggers. And these are both useful in protecting against common-cause failure. Now, if I talk about diversity, I'd say, well, if I apply diversity within a system, then I would call that a preventive measure because it helps prevent common-cause failure. If I talk about diversity between two different systems; for example, in terms of a diverse actuation system, the so-called DAS, that's a mitigated measure because it waits until the primary system had its common-cause failure, then it helps, then it backs it up. Right? So diversity enters in both those contexts, I think. Right?

Now another thing that comes or is related to that I think is of interest here, when we start talking about design measures that can be useful in protecting against common-cause failure, it's interesting to see how that might flange up with what Mike's doing. And I'll give you an example just so you don't think I'm making this stuff up. One design attribute of I guess a high-integrity digital system would be that if there's a operating system, it's used in the device in such a way that it's what we would call blind-to-plant transients. Which means every time step -- the operating system does certain stuff. It looks at the inputs, it puts the inputs some place so the application code can pick them up and run with them, it issues outputs, maybe it resets a watchdog timer, those kinds of things. But every time step it does exactly the same thing. So the operating system can't tell what's going on in the plant; it doesn't care. And that's a very interesting feature.

MEMBER BROWN: Hold it. But that's all you're talking about is a main operating loop that always does the same thing with every piece of data every time.

MR. TOROK: Yes.

MEMBER BROWN: And nobody's dictating. It makes absolute sense what you're saying.

MR. TOROK: But not every system does that.

MEMBER BROWN: If you want a deterministic system, then it has to do that.

MR. TOROK: And that's something --

MEMBER BROWN: And that's not addressed. I mean, I've looked at three different systems and I can't get anybody to define and show that they're doing that. I keep asking about main operating loops and that's the guy, oh, yes, they shake their heads up and down, but there's nothing written in their descriptions of their systems to do that. And all you've done is say that -- the way I read that is somebody ought to be coming down and say, look, guys, every digital -- and I'm using the broad term, although it really applies in this case to software-type systems for the --

MR. TOROK: Yes.

MEMBER BROWN: -- not combinational logic, because that is pretty -- once you go, it flows.

MR. TOROK: Okay.

MEMBER BROWN: That it always does -- it picks up every parameter, it executes every algorithm, it goes through whatever partial test sequence in the sample time that's left and it reiterates and it finishes some sort of, you know, in-sequence testing that you can do of the system while you're doing that. And then it finishes and it strobes a watchdog, and then it goes back and starts over again. It does everything every time.

MR. TOROK: Right.

MEMBER BROWN: Now, that sounds good, doesn't it?

MR. TOROK: Well --

MEMBER BROWN: Come on. I'm waiting for a response.

MR. TOROK: Yes, it sounds good.

MEMBER BROWN: Okay.

MR. TOROK: I'll go along with that.

MEMBER BROWN: But I don't see anything that tells the vendors or the manufacturers or the designers of these systems that that's what's expected. I address that by talking about determinacy, because that's the only way you can get determinacy.

MR. TOROK: Okay. And I guess I would say that's a characteristic that you would certainly want to see in, you know, a 1E system in a nuclear plant, right?

MEMBER BROWN: Yes.

MR. TOROK: Fine. And I would expect that the plant, the licensees are making sure that their vendors are doing that. Now, you're not going to read about that in the brochures that come with the equipment.

MEMBER BROWN: No, but --

MR. TOROK: You have to sit down with the guys who design the box and look inside it and make sure it's doing that.

MEMBER BROWN: You don't want a Bill Gates operating system that does all kinds of things besides -- oh, this time I'm going to do this, this cycle I'm not.

MR. TOROK: Right.

MEMBER BROWN: You know, and makes executive decisions or evaluates the data. You just want it to process.

MR. TOROK: That's right. And in evaluating the systems you want to be pretty sure that it's doing those things correctly, right?

MEMBER BROWN: Can we have you back? I like this.

CHAIRMAN APOSTOLAKIS: We will have him back, yes.

MR. TOROK: But we can go on all day on this subject.

CHAIRMAN APOSTOLAKIS: No, no, no, no. Are you approaching the end of your comments?

MR. TOROK: Yes. Yes.

CHAIRMAN APOSTOLAKIS: Okay.

MR. WATERMAN: Yes, this is Mike Waterman, Office of Research. What you describe, Charlie, has been a philosophy of the NRC's for as far back as I can remember. For example, the Teleperm TXS system does exactly what you described. I believe the Common Queue does the same thing, too.

MEMBER BROWN: Well, I've been told MELTAC does also, but if you look at the DCD it doesn't say that.

PARTICIPANT: It's not written down.

MEMBER BROWN: It's not written down anywhere and how they accomplish that is not stated, you know, because it has to literally be the main operating loop, not a commercial-type non-real time operating system.

MR. WATERMAN: And if you look at like the safety evaluation or the Teleperm XS system that was done in 2000, it goes into great detail about exactly what you were describing. And we've been emphasizing thou shalt be deterministic to the industry for, oh, gosh, ever since I've been with the NRC. So those particular features are in some of the major platforms. I don't know about MELTAC.

CHAIRMAN APOSTOLAKIS: I think we had some good --

MR. TOROK: I know Common Queue does it and --

MEMBER BROWN: You just said everybody doesn't do it. Now, I've only heard words.

CHAIRMAN APOSTOLAKIS: We've had some good signs here that it will be an interesting meeting when you come back, Ray.

Now, you described a lot of stuff. Roughly how much time will you need, do you think?

MR. TOROK: Well, I tell you, I sat here and I've listened to, you know, the discussion of Mike's topic and I think we're pushing four hours on that. And when I add up all the stuff we have, it's certainly more than four hours. So what I'd like to ask for is a day on that, please.

CHAIRMAN APOSTOLAKIS: A day? The staff will need how much time for their own presentations?

MR. ARNDT: It depends a little bit on what you want to hear. There's a number of things that we would like to present on. Certainly the research plan, which I think the Committee is very interested in hearing.

CHAIRMAN APOSTOLAKIS: The research plan is absolutely important, yes.

MR. ARNDT: There's the final close-out of the Brookhaven risk work that I believe Alan wants to come back and talk about.

CHAIRMAN APOSTOLAKIS: Yes.

MR. ARNDT: I believe we wanted to talk about ISG-07.

CHAIRMAN APOSTOLAKIS: So you're talking about a day-and-a-half at least?

MR. ARNDT: Probably. I'd have to go back and add it all up. Probably in that ballpark.

CHAIRMAN APOSTOLAKIS: Well, then -- what?

MS. ANTONESCU: The I&C plan takes about a day.

CHAIRMAN APOSTOLAKIS: The plan is one day?

MS. ANTONESCU: Yes. Yes.

CHAIRMAN APOSTOLAKIS: Really? You're planning a lot of things, huh?

MS. ANTONESCU: I don't know, it's up to you.

CHAIRMAN APOSTOLAKIS: Well, the point is this: The reason why I'm asking is because, first of all, I think this is interesting work that Ray is talking about. There is interest from the members. Judging from past experience it's always good for the Committee, Subcommittee and then the Committee to hear from the industry because you have a different perspective, especially in the old days of developing the Regulatory Guide 1.174. It was very, very valuable for us to hear the views of South Texas and so on. So I think we should be generous and give as much time as we can to the industry.

The bottom line is, is this becoming now a three-day meeting?

MS. ANTONESCU: Yes.

CHAIRMAN APOSTOLAKIS: Well, since we're coming here, we might as well do something useful.

MS. ANTONESCU: Yes.

CHAIRMAN APOSTOLAKIS: What is the --

PARTICIPANT: Why now?

CHAIRMAN APOSTOLAKIS: -- point of coming, you know, especially for you.

PARTICIPANT: Why now?

PARTICIPANT: Yes, for a change.

CHAIRMAN APOSTOLAKIS: For you guys to come all the way from California, you know, might as well get something out of you. That didn't come out right.

I think, by the way, that we should be off the record now. We are talking about planning the meeting and the dates. There is no reason to have a record, so unless Ray wants to add something.

MR. TOROK: The only other thing I was going to say is we would like to do this in such a way that we can support the detailed technical discussion at whatever level you want to go. So we'd be bringing our technical guys, which means people from California and Atlanta and Paris. Okay?

CHAIRMAN APOSTOLAKIS: And Paris?

MR. TOROK: Paris.

CHAIRMAN APOSTOLAKIS: Okay.

MR. TOROK: I'm sorry, we've got some people in here from EDF who didn't get to speak today, but he's got plenty to say later.

CHAIRMAN APOSTOLAKIS: Okay.

MEMBER BROWN: We should have at least two-and-a-half days to let the guys get out --

CHAIRMAN APOSTOLAKIS: The official part of the meeting is over. We're off the record now.

(Whereupon, the meeting was adjourned at 11:32 a.m.)

# Digital I&C Licensing Process
# Task Working Group-6

Lois James, Lead
Task Working Group 6
Office of Nuclear Reactor Regulation

February 26, 2009

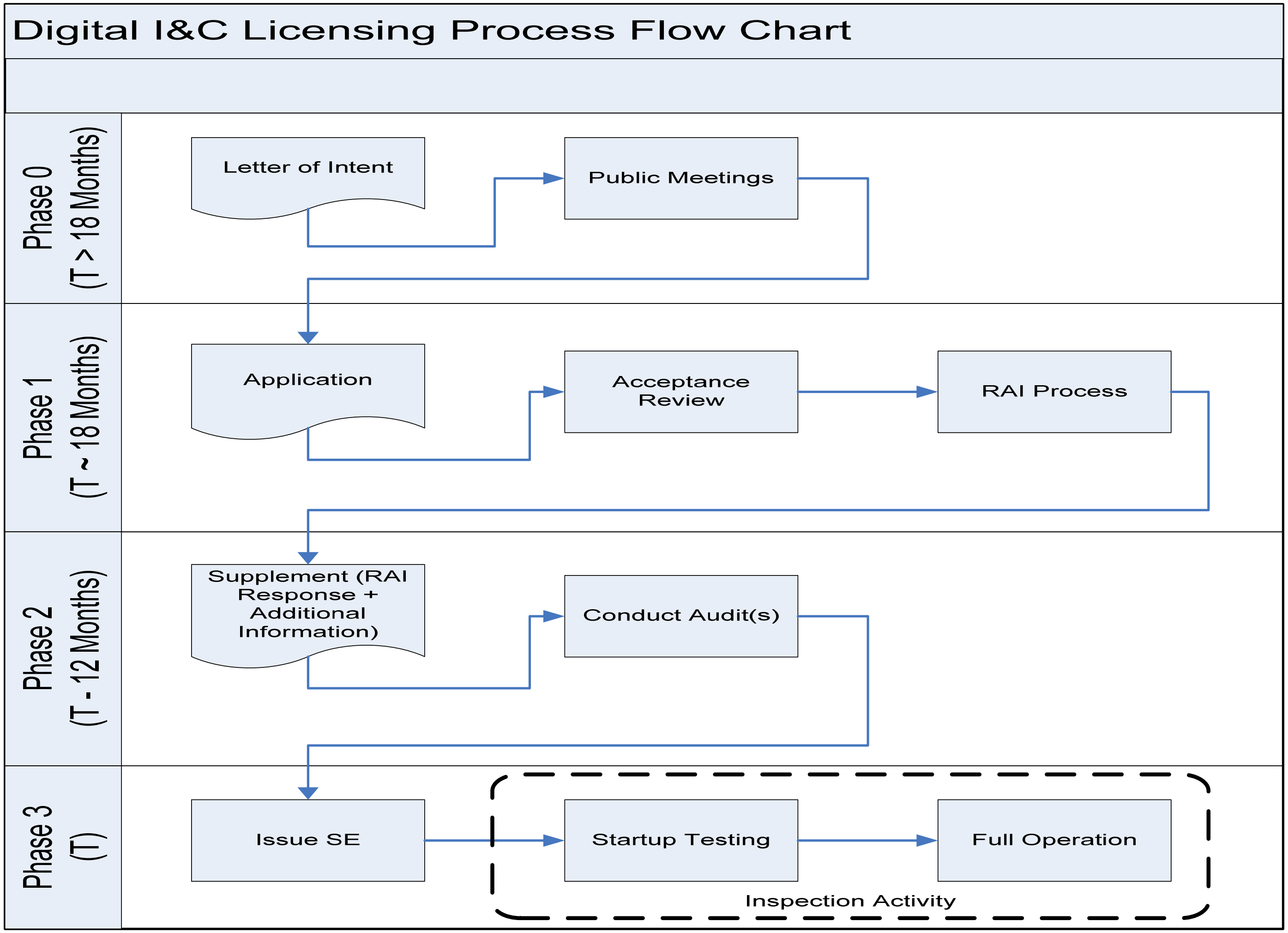
# Agenda

- Introduction
- Process Overview
- Format of ISG-6
- Tiers of Complexity
- Phases of Process
- Areas of Review
- Path Forward
- Summary

# Introduction

- Purpose of ISG-6
  - Refined licensing process
  - Expectations for documentation
  - Knowledge management
- Lessons learned from recent I&C amendment reviews

# Process Overview



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

# Format of ISG-6

- Introduction
- Purpose
- Licensing Process
  - Process Overview
  - Pre-Application Meetings
  - Initial Application
  - Continued Review and Audit
  - Implementation and Inspection
  - Review Areas
    - Scope of Review
    - Information to be Provided
    - Regulatory Evaluation
    - Technical Evaluation
    - Conclusion
- Appendices (Example Formats)

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

# Tiers of Review

- Each Tier corresponds to an expected review complexity:
  - Tier 1:  Previously approved system, no deviations from topical report, review to focus on plant specific aspects, least review effort expected.
  - Tier 2: Previously approved system, with deviations, moderate review effort expected.
  - Tier 3: Totally new system, extensive review effort expected.  Thorough review of all technical areas.

# Pre-Application (Phase 0)

- Encourage discussion of significant topics (defense-in-depth & diversity, variances from guidance, unique or complex aspects, etc.)
- Document meeting summaries
  - Can provide initial assessments and understanding of system concepts
  - Will document aspects that are important to the NRC staff decision
- Phase 0 ends with submittal of an LAR

# Initial Application (Phase 1)

- Staff will perform acceptance review in accordance with NRR Office Instruction, LIC-109
- Allowances are made for promised information
  - Appropriate to align staff review with system development lifecycle
- Staff can use RAI process to communicate those areas where the staff has no further questions
- Phase 1 ends when licensee submits all promised information
  - May overlap with Phase 2

# Continued Review & Audit (Phase 2)

- Staff will continue the in-depth review
- Staff will perform audit(s) of licensee design development process implementation
- Phase 2 ends with the conclusion of the NRC staff review

# Implementation & Inspection (Phase 3)

- Phase 3 begins with the issuance of the amendment and associated Safety Evaluation.
- Licensee implements upgrade
  - Installation of system
  - Amending of Technical Specifications
  - Procedure changes
  - UFSAR update
- Licensee will conduct startup testing
- Inspection of activities is governed by IP-52001, “Digital Instrumentation and Control Modification Inspection”

# Draft Review Areas

- The staff is developing a concise list of topical review areas to group the large number of criteria (IEEE Stds, GDC, BTPs, etc)
  - Review areas will be influenced by experience from current reviews
  - The list will also help knowledge management by allowing new reviewers to conceptualize the review process

# Path Forward (Working Group Activities)

- Monthly Public Meetings
  - Anticipate 1~4 Review Sections to be discussed
- Monthly conference calls on status

# Path Forward (Deliverables)

- Full Draft of ISG for Public Comment
  - Summer, 2009
- ISG-6 Issued
  - Fall, 2009
- Pilot application encouraged

# Summary

- Tiers of review address differences in complexity
- Phases of review adapt licensing process to digital I&C system development lifecycle
- Review areas identify major aspects of a digital I&C review
- Path Forward

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

# Digital Instrumentation Control Steering Committee Overview of Activities

John Grobe
Associate Director for Engineering and Safety Systems
Office of Nuclear Reactor Regulation

Stewart Bailey
Deputy Director for Digital Instrumentation and Control
Office of Nuclear Reactor Regulation

# Agenda

- Background on Steering Committee
- Digital I&C Project Products
- Other Key Digital I&C Issues
  - NRR Ongoing Reviews – ISG Usage
  - Operational Issues
- Path Forward

# Background on Steering Committee

- Digital I&C Steering Committee formed January 2007
- 7 Task Working Groups formed to address specific issues
  - TWG-1 Cyber Security
  - TWG-2 Diversity and Defense in Depth (D3)
  - TWG-3 Risk-Informing Digital I&C
  - TWG-4 Highly-Integrated Control Room – Communications
  - TWG-5 Highly-Integrated Control Room – Human Factors
  - TWG-6 Licensing Process
  - TWG-7 Fuel Cycle Facilities
- Industry established counterpart groups
- Over 100 public meetings to define, discuss and resolve issues

# Background on Steering Committee

- Status of Activities
  - Interim Staff Guidance (ISG) documents have been developed for technical issues related to power reactors
  - ISG is being developed for the licensing process
  - ISG is being developed for fuel cycle facilities
- Ongoing Work
  - Updates to Regulatory Documents

# Digital I&C Project Products

## TWG-1: Cyber Security

- Problem: Perception of Conflicting Guidance between NEI 04-04 and RG 1.152
- Resolution: ISG-1 Issued 12/2007
  - No Conflicts Identified – Gaps/Different Scopes
  - ISG has Table Cross Referencing Requirements in RG 1.152 vs. NEI 04-04
- ACRS Review: Letter dated April 29, 2008
- Next Steps: Update SRP and RG 1.152 following Rulemaking and RG 5.71

# Digital I&C Project Products

## TWG-2: Diversity and Defense-in-Depth (D3)

- Problem: SRM/SECY 93-087 Policy on D3. This TWG Provided Guidance on What Constitutes Sufficient D3 (6-part Problem Statement)
- Resolution: ISG-2 Issued 9/2007
  - Clarified when to Consider Common-Cause Failures (CCFs)
  - Guidance on Adequate D3, including Manual Action
  - Guidance on System vs. Component Level Actuation
- ACRS Review: Letter dated October 16, 2007
  - Recommends Process to Evaluate < 30 Minute Operator Action
- Next Steps: Complete NUREG on Diversity, Update SRP

# Digital I&C Project Products

## TWG-3: Risk-Informing Digital I&C

- Problem: Need Guidance for (1) PRAs required by 10 CFR Part 52 for New Reactors, (2) How to use Risk Insights to Address Issues, and (3) State-of-the-Art PRA Methods
- Resolution: ISG-3 Issued 8/2008
  - Provided Guidance on New Reactor Applications
  - Defer Risk Insights and State-of-the Art PRA Methods
- ACRS Review: Letter dated April 29, 2008
  - Recommends emphasize failure modes vs. sensitivity studies
  - ISG-3 was revised to incorporate recommendations
- Next Steps: Risk Insights and State-of-the-Art to be Addressed in 5-year Research Plan

# Digital I&C Project Products

## TWG-4: Highly-Integrated Control Room - Communications

- Problem: Guidance Needed on Separation, Inter-divisional Independence
- Resolution: ISG-4 Issued 9/2007
  - Guidance on inter-divisional communications (safety-to-safety or non-safety-to-safety
  - Guidance on Command Prioritization
  - Guidance on Multidivisional Control and Display Stations
- ACRS Review: Letter dated October 16, 2007
- Next Steps: Update SRP, RG 1.152, and IEEE 7.4.3.2

# TWG-5: Highly-Integrated Control Room – Human Factors

- Problem: Guidance Needed on (1) Minimum Inventory, (2) Computerized Procedures, (3) SPDS, (4) Graded Approach to Human Factors, (5) Manual Action for D3
- Resolution:
  - (1) and (2) ISG-5 Issued 9/2007
  - (3) Requires Rulemaking
  - (4) Dropped
  - (5) ISG-5 Issued 11/2008
- ACRS Review: Letter dated October 16, 2007
  - Present ISG on Manual Action today
- Next Steps: Rulemaking, NUREG, Reg. Guide, SRP

# TWG-6: Licensing Process

- Problem: Need Guidance on (1) Level of Detail in Submittal, (2) Applicability of SRP Chapter 7, (3) Process Protocols, and (4) Licensing Criteria for Cyber Security
- Resolution: ISG-6 Under Development
  - Inspection Procedure Issued 10/2008
  - Audit Procedure Issued 12/2008
- ACRS Review: Letter Dated April 29, 2008
  - Present update today
- Next Steps: Complete ISG, Add Cyber Security, Final Documents

# TWG-7: Fuel Cycle Facilities

- Problem: Need Guidance on (1) Cyber Security, (2) Diversity, (3) Independence of Control Systems, (4) Isolation, and (5) High-quality Software
- Resolution: ISG-7 Under Development
- ACRS Review: Request Review End of Summer
- Next Steps: Complete ISG, Update NUREG-1520, new NUREG

# Ongoing NRR Reviews ISG Usage

- <u>Wolf Creek</u>
  - Field Programmable Gate Array (FPGA) use for Main Steam and Feedwater Isolation System
  - Staff using ISG-2 and ISG-4
  - Staff Conducted Audits at Vendor Facilities
  - Draft Safety Evaluation is in Peer Review, Completion by April 2009

- <u>Oconee</u>
  - Microprocessor-based Teleperm XS (AREVA) use for Reactor Protection and Engineered Safety System (combined), Submitted 1/31/08.
  - Staff Acceptance Review/Letter Identified Six Issues to Resolve
  - Staff using ISG-2 and ISG-4
  - Staff Conducted Audits at Licensee and Vendor Facilities
  - The Review is Progressing, and Pathways to Resolve Issues have been Identified

# Operational Issues

- Issues Identified to Date
  - Provisions for hardware/software changes (10CFR50.59)
  - Dealing with the evolution of previously-approved platforms in licensing
  - Assessing findings using the Significance Determination Process
  - Handling risk-informed licensing issues
    - Risk-informed technical specifications initiatives
    - Previously-approved risk-informed submittals
    - Allowed outage time extensions
  - Implementing the maintenance rule (10CFR50.65(a)(4))
  - Monitoring shutdown risk
  - Evaluating the safety significance in Licensee Event Reports (10CFR50.73)
- Plans for Resolution

# Path Forward

- Complete ISG for Licensing and Fuel Cycle Facilities
- Update Regulatory Documents
- Address Operational Issues
- International Cooperation
  - MDEP - Bilateral Work
  - COMPSIS - IAEA and Other Interactions
- Ongoing Research Activities

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

# Digital I&C Highly Integrated Control Room Human Factors Task Working Group #5

# Interim Staff Guidance for Crediting Manual Operator Actions in Diversity and Defense-in-Depth Analyses

David R. Desaulniers
Office of New Reactors

February 26, 2009

# Topics

- Overview of TWG-5 and activities
- Manual Operator Action Background
  - DI&C-ISG-02
  - Industry white paper
  - Challenges
- Overview of ISG for crediting manual operator actions
- Path Forward

TWG-5

Task Working Group

- Michael Junge, NRO (Manager)
- George Lapinsky, NRR*
- Larry Vick, NRR*
- J. Persensky, RES*
- David Desaulniers, NRO*
- James Bongarra, NRO
- Barry Marcus, NRR
- Jack Zhao, NRO
- Jonah Pezeshki, NRR
- Paul Pieringer, NRO

*Principal contributor to ISG for manual operator action

# TWG-5

Areas of Expertise

- Human Factors
- Instrumentation and Controls
- Plant Operations
- Operator Licensing
- Plant Simulation

# TWG-5 Highly Integrated Control Rooms – Human Factors

Key areas

- Minimum Inventory
- Safety parameter display system
- Computer-based procedures
- Graded approach to human factors
- Manual operator actions

# DI&C-ISG-05 Topics

- Computer-based procedures
- Minimum inventory
- Manual operator actions

# Background

DI&C-ISG-02, Interim Staff Guidance on Diversity and Defense-in-Depth Issues, September 26, 2007

- Provided acceptable methods for implementing diversity and defense-in-depth (D3) in digital I&C system designs
- Clarified use of operator action as a diverse defensive measure and established corresponding operator action times

# Background

DI&C-ISG-02:

- The D3 analysis may determine that one or more reactor protection system (RPS) safety functions could become subject to a common cause failure (CCF)
  - use realistic assumptions to perform analyses of licensing basis plant responses
  - identify back-up systems or actions necessary for accomplishing the required safety functions

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

# Background

DI&C-ISG-02 states:

"Manual operator actions may be credited for responding to events in which the protective action subject to a CCF is not required for at least the first 30 minutes and the plant response is bounded by BTP 7-19 recommended acceptance criteria."

# Background

DI&C-ISG-02 further states:

"The licensee or applicant should demonstrate through a suitable human factors engineering (HFE) analysis that manual operator actions that can be performed inside the control room are acceptable in lieu of automated backup functions."

# Background

- Industry sought flexibility and guidance to credit manual operator actions in less than 30 minutes
- Scope of TWG-5 action plan expanded to develop guidance for crediting manual operator actions
- Public interactions between TWG-5 and industry counterparts
- Industry developed white paper methodology for crediting manual operator actions
- Staff considered and incorporated, as appropriate, white paper methods in developing an amendment to DI&C-ISG-05

## Summary of Industry-proposed Methodology

- Analysis
  - Time required for operator action calculated using a modified ANSI/ANS 58.8, 1994 methodology
  - Time available calculated using T-H models
- Verification
  - Operator action times confirmed through table top exercises
- Validation
  - Conducted using part-task, limited-scope, or plant reference simulator and captured as an ITAAC or license condition
- Human Performance Monitoring
  - On-going operator training

# ANSI/ANS 58.8

ANSI/ANS 58.8, Time Response Design Criteria for Safety-Related Operator Actions, 1994

- Provides a methodology for analyzing an action sequence and decomposing the task into discrete time intervals
  - e.g., diagnosis, response selection, manipulation
- Developed as a means to establish the minimum allowable response times for operator actions in response to design basis events
  - Uses specified time values for task intervals that are aggregated to calculate total response time
- Method has not been endorsed by NRC

# Industry White Paper

## Technical Issues/Challenges

- Analysis
  - Use of modified ANSI/ANS 58.8 methodology
  - Use of unique prompting alarms to significantly reduce time allotted for diagnosis
- Verification
  - Lack of specificity regarding purpose, scope & implementation
- Validation
  - Adequacy of simulation
    - Fidelity of facility
    - Number/scope of scenarios
    - Crew size
- Human Performance Monitoring
  - Lack of specificity regarding scope & implementation

# Industry White Paper

## Key Issues

- Focus on feasibility with little emphasis on reliability of operator actions
- Process weighted toward integrated system validation activities which occur late in the licensing process

# DI&C-ISG-05 (Revision 1)

## Manual Operator Action ISG

- Scope
- Staff Position
- 4-Phase Methodology

# Overview of ISG

## Scope

- Manual actions credited in D3 analyses for coping with abnormal operational occurrences and postulated accidents (AOO/PAs) concurrent with software CCF of the digital protection system
- New and existing reactors

# Overview of ISG

## Staff Position

Credited actions should be:

- Included in emergency operating procedures (EOPs)
- Executed from within the main control room
- Demonstrated to be feasible and reliable
- Addressed in the human factors engineering (HFE) program consistent with NUREG-0711

# Overview of ISG

## Method

4-Phases:

- Analysis
- Preliminary Validation
- Integrated System Validation
- Long-term Monitoring

# Analysis

## Objective

- Estimate *time available* and *time required*
- Identify critical assumptions and credible operator errors
- Establish adequate *margin*

# Analysis

## Method

Time Available

- Use methods and realistic assumptions consistent with BTP 7-19.

Time Required

- Use a documented sequence of actions (from task analysis, EPGs, EOPs)
- Use one of several acceptable methods for developing estimates of time required to perform action sequence

Margin

- Time to recover from credible errors

# Overview of ISG

## Analysis

Examples of Acceptable Methods

- Operator interviews and surveys
- Operating experience reviews
- Software models of human behavior, such as task network modeling
- Use of control/display mockups
- Expert panel elicitation
- ANSI/ANS 58.8, *Time Response Design Criteria for Safety-Related Operator Actions (task decomposition)*

# Analysis

Review Criteria Topics

- Time required
- Time available
- Use of alarms, controls, and displays
- Use of symptom/function-based EOPs
- Staff size, composition and augmentation
- Level of detail
- Identification of credible operator errors

# Analysis

Example Criteria

- The estimated time response of operators is sufficient to allow successful execution of applicable steps in the symptom/function-based EOPs
- The initial MCR operating staff size and composition assumed for the analysis of time required is the same as the minimum MCR staff defined in the unit's Technical Specifications

# Preliminary Validation

Objective

- Independent confirmation of analysis results

Applicability

- Only required for those vendors/applicants who are using the 10 CFR Part 52 process

Method

- Use diverse methods that are as realistic as maturity of design allows
- Submit analysis and results for NRC review as part of D3 submittal(s)

# Preliminary Validation

Examples of Acceptable Methods

- Tabletop analysis
- Walkthrough/talkthrough analysis
- Software models of human behavior, such as task network modeling
- Use of control/display mockups
- Man-in-the-loop prototype testing
- Real-time validation using part-task simulator

# Preliminary Validation

Review Criteria Topics

- Independence from Phase 1
- Validation team qualifications
- Use of two or more methods
- Validation of time required

# Preliminary Validation

## Results

- Shall be documented in the D3 analysis for NRC review
- Should support high confidence that the time required for manual operator actions will satisfy the success criteria for the integrated system validation

# Preliminary Validation

Unacceptable results

- Should result in modification of the D3 coping strategy

Acceptable results

- Provide basis for a safety determination conditioned upon the completion of any HFE open items, ITAAC, COL open items

# Integrated System Validation

Objective

- Confirm operators are able to perform credited actions in real-time using as-built design

Method

- Use plant-referenced simulator capable of realistically representing AOO/PA with CCF
- Validate time required using both nominal and TS minimum crews
- Accomplish as part of HFE program activities per NUREG-0711

# Integrated System Validation

Plants licensed under 10 CFR Part 52

- Implement and document as an ITAAC item or COL action item

Operating plants

- Review as part of license amendment

# Integrated System Validation

Review Criteria Topics

- Integration with HFE program
- Simulator
- Personnel
- Operational Conditions
- Performance Times

# Integrated System Validation

Performance Time Criteria

- For each AOO/PA, the *mean performance times* of the crews is less than or equal to the estimated *time required* derived from the analysis phase.
- For each AOO/PA, the *performance time* for each crew, *including margin* determined in the time required analysis, is less than the analyzed *time available*.

# Integrated System Validation

Unacceptable results

- Should result in modification of the D3 coping strategy

Acceptable results

- Provide the basis for meeting the license application or amendment request approval requirements
- Shall be submitted for final NRC review and closure of any HFE open items, ITAAC, COL action items, or License Conditions

# Long-term Monitoring

Objective

- Ensure credited actions remain feasible and reliable

Method

- Design and configuration controls ensure discrepancies from D3 assumptions and constraints are identified and corrected
- Training keeps performance within assumptions of the analysis

# Long-term Monitoring

Review Criteria

- A long-term monitoring strategy is capable of tracking performance of the manual operator actions to demonstrate that performance continues to support the associated D3 analysis
- The program is structured such that corrective actions are formal, effective, and timely

# Path Forward

- Develop draft Regulatory Guide
- Support future development and revision of ANSI/ANS 58.8, Time Response Design Criteria for Safety-Related Operator Actions