Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, March 5, 2009

Work Order No.: NRC-2707 Pages 1-244

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

+ + + + +

560th MEETING

+ + + + +

THURSDAY

MARCH 5, 2009

+ + + + +

ROCKVILLE, MD

+ + + + +

The Advisory Committee 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 Mario Bonaca, Chair, presiding.

COMMITTEE MEMBERS PRESENT:

MARIO V. BONACA, Chair

SAID ABDEL-KHALIK, Vice Chair

J. SAM ARMIJO, Member-At-Large

GEORGE E. APOSTOLAKIS

MICHAEL CORRADINI

CHARLES H. BROWN, JR.

HAROLD B. RAY

COMMITTEE MEMBERS PRESENT: (CONT.)

OTTO L. MAYNARD

MICHAEL T. RYAN

WILLIAM J. SHACK

DANA A. POWERS

DENNIS C. BLEY

JOHN W. STETKAR

SANJOY BANERJEE

JOHN D. SIEBER

NRC STAFF PRESENT:

KARL STURZEBECHER

ERIC LEE

DEBRA HERMANN

CHRISTINA ANTONESCU

DAN SANTOS

JOHN LUBINSKI

MATTHEW MITCHELL

MARK KIRK

VERONICA RODRIGUEZ

GEARY MIZUNO

MARY DROUIN

GARETH PARRY

JOHN MONNINGER

DON DUBE

STEVE DINSMORE

ALSO PRESENT:

WILLIAM ARCIERI

RICK GRANTOM

TABLE OF CONTENTS

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

CHAIR BONACA: Good morning. The meeting will now come to order. This is the first day of the 560th meeting of the Advisory Committee on Reactor Safeguards. During today's meeting the Committee will consider the following; Draft Final Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities"; Draft Final Revisions to 10 CFR 50.61, "Fracture Toughness Requirements for Protection Against Pressurized Shock Events"; the final Revision 2 to Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of the Probabilistic Risk Assessment Results for Risk-Informed Activities"; and the preparation of ACRS Reports.

A portion of the session dealing with cyber security programs for nuclear facilities may be closed to discuss and protect information classified as national security information as well as safeguards information. This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Mr. Sam Duraiswamy is the designated federal official for the initial portion of the meeting. We have received no written comment or request for time to make oral statements from members

of the public regarding today's session.

A transcript of portions of the meeting is being kept and it is requested that speaker use one of the microphones, identify themselves and speak with sufficient clarity and volume so that they can be readily heard. I would begin with some items of current interest. I'm happy to announce that Mr. Harold Vander Mollen has been selected to receive the NRC Meritorious Service Award for his valuable contributions to the regulatory process. Well deserved.

(Applause)

CHAIR BONACA: Thank you for your good work. With that we will move now to the agenda and the first item on the agenda is Draft Final Regulatory Guide 5.71 "Cyber Security Program for Nuclear Facilities and Professor Apostolakis would take us through that presentation.

MEMBER APOSTOLAKIS: Thank you, Mr. Chairman. We had a subcommittee meeting last week Thursday and Friday where we had a number of presentations, not just on the cyber security issue that we would be hearing today. We also reviewed a few interim staff guidance documents, five, six and the committee will review those and there will be a

letter at the April meeting.

Today we're focusing on cyber security. We had a few comments that we made on the regulator guide or the draft that we had anyway, 5.71. The staff promised to address them today, I believe, and I don't want to take the thunder away from them so I'll let them, when the time comes, point out that the subcommittee had some questions on a couple of specific items and what their preliminary response is. So with that, I will turn it over to the staff.

MR. STURZEBECHER: Good morning. My name is Karl Sturzebecher. I'm from the Office of Research. I am the Project Manager for Reg Guide 5.71. With me today is my team; Eric Lee from NSIR, Debra Hermann from NRO. We have adjusted our presentation from the feedback we got from ACRS last week. This presentation goes through the guide. I'll start with the agenda. We're going to go over the development of RG 5.71, the technical approach, and our path forward. Then we have some backup slides to -- that have the response, the comments that we had from ACRS last week.

The Reg Guide is based upon the Rule 10 CFR 73.54 and the Rule's basic objective is to protect digital computers, communication systems and networks

from a cyber attack. The functions that those computers and communications systems carry are listed below, as you see, safety related, important to safety functions, security functions, emergency preparedness functions and support systems.

Now, the idea is to protect from -- the Rule basically states that you're supposed to protect from a cyber attack and when I say that, I mean an adverse impact to the integrity of the data or software, denial of service for any of this equipment that's running and an adverse impact to the operation of that equipment.

MEMBER APOSTOLAKIS: Well, just a question of clarification. There was a question, I believe, last time, what is the distinction between information technology and digital INC as it applies here?

MR. STURZEBECHER: Go ahead.

MR. LEE: Let me answer it. Hopefully, I'll answer your --

MEMBER APOSTOLAKIS: You can rephrase the question.

MR. LEE: The digital INC mainly talks about the safety systems, those systems that pertain to safety functions. Here in the 73.54, we are trying to protect the -- any system that could adversely

impact, meaning that could cause -- reduce the ability for -- so any system that could adversely effect safety and security or emergency preparedness functions of the nuclear power plant. So whether it's an information system or a control system or any system that could adversely impact it will --

MEMBER APOSTOLAKIS: So what I'm doing now with my computer is information, is it not?

MR. STURZEBECHER: Yes, sir.

MEMBER APOSTOLAKIS: Okay. If I control a system from here, I'm ready to do something, then that would be digital INC the way we talk about it here.

MR. STURZEBECHER: And that's where the modernization at the sites has gone to. They original -- in the `90s the fossil sites have been upgrading their digital INC. Information Technology comes in and makes that connection to the site controller, an engineer at a remote location, I've seen it, was able to disarm the safety system on the turbine and right away had to call the operator and say, "Well, look, the protection wasn't there".

MEMBER APOSTOLAKIS: So the information technology then supports the digital systems that are monitoring and controlling the safety functions. That's really what it is.

MR. STURZEBECHER: It can be --

MR. LEE: Safety, security, yes.

MR. STURZEBECHER: You can look at it that way.

MEMBER APOSTOLAKIS: Why can it be looked that way? I mean, you're --

MR. STURZEBECHER: Well, it depends which side you're on. There's two different mindsets.

MEMBER APOSTOLAKIS: I'm on the side of science.

MR. STURZEBECHER: Okay. All right, science. I kind of come from the art side, but I think it's a nice balance that you have to have. But I mean, I would go with a point that says what we discussed last week, where the mindset of IT people tend to be interconnect and use the full band width of whatever the highway, whatever communication network you're using. Well, the controls have a different perspective where you're limiting -- you're trying to limit the amount of traffic on your highway.

You want that safety point to make it. If it triggers and goes off, you want that information delivered with high assurance that it's going to make it to that point.

MEMBER APOSTOLAKIS: Okay.

MR. STURZEBECHER: There are situations like what happened last year where you make that tie between the information system to a digital system, and it happened to one of our plants in the US, and the mindset is not -- they're not compatible completely. That's why when we get further into the slides, you'll see level two and that concentric architecture showing.

MEMBER APOSTOLAKIS: Very good, thank you.

MR. STURZEBECHER: Okay. Okay, in the development of the guide, we went through the past Reg Guides we've had -- we've issued over the last 10 years. We've looked at NIST. We also got the industry perspective and we created a feature list and when I say features, these are a comprehensive set of methods that you could use or employ to protect your system. The Reg Guide or the Draft Guide at that time, was about 120 pages.

Some of the feedback we got from industry was that we were being very prescriptive, so we looked at the way we had that particular guide and realized we could narrow down these features into attributes and this is sort of a classic quality function of the employment method used that's a Six Sigma method, where you know what your attributes, higher level

attributes are, and the features that align to them, and the features are always changing because cyber security moves. The threat constantly changes. So does the good guys versus the bad guys kind of thing.

So we wanted something that was flexible and yet would also fit into the idea of being programmatic. So those were the steps we took to refine the Reg Guide to where it's at now.

MEMBER APOSTOLAKIS: But what you just said is a high level statement which, you know, nobody can disagree with. The question is, how far did you go? I mean, that's where the subcommittee had their problem. We felt that the Guide, at least the one we saw, did not -- did not provide sufficient guidance so that the user will know what is expected of them.

So, you know, I mean, it's okay to talk about trying not to be very prescriptive and so on. I mean, these high level statements we all agree to, but the question is, is this guide supplying sufficient information to the licensees, to our reviewers, to the public, so that they will know what they are supposed to do to meet the requirements of the Rule. So I hope you're going to address that a little later.

MR. STURZEBECHER: Slide 12.

MEMBER APOSTOLAKIS: I'm just alerting the

Committee to the fact that this was a point of concern.

MR. STURZEBECHER: And it was well taken and we adjusted to show an actual scenario, a rough scenario, using the set of features.

MEMBER APOSTOLAKIS: When you say you adjusted it, I mean, you will have a slide, but did you actually revise the Guide?

MR. STURZEBECHER: No, no.

MEMBER APOSTOLAKIS: Okay. Very good. Very good, I mean -- (Laughter).

MR. STURZEBECHER: So this is sort of -- this is the history that we used and I'll go briefly through this. We had participation from NERC, FERN, DHS, NIST, Joe Weiss, vendors, licensees, and NEI. The first meeting was in July and as I mentioned, we had a 120-page document with about 208 comments and the majority, I'd say half were again, that we were being too prescriptive actually listing out the features and telling them to do -- how to set up a firewall was one of the examples, which you don't necessarily want to do because the technology continues to change and you're also putting yourself in a liability perspective.

So we worked on the Guide. There were

some comments here like in December there was a request for -- you can see the different lists and my favorite was the graded approach. We had one statement in the original Guide and we kind of -- we beefed up and used -- referred to NUREG/CR 6847 to assist in providing that graded approach.

When you look at the progression of the technology over the last almost 40 years, the first time frame from the `60s to `70s you may have had a network that was in the office. The second set, from the `80s to the `90s, you may be going between buildings and today the -- because of the global economy, the way the web works, you are literally connected to the outside world right from where you're at. It's kind of introspective in that way.

Right here we have a listing of the paradigm that you used to adjust to the particular situation and we're using a management controls, operation controls and technical controls as our main part of the program in the Reg Guide and this is based off of NIST.

MEMBER APOSTOLAKIS: This -- the bottom paragraph is something that is new to us? There was a request at the subcommittee meeting that you guys define cyber security. So this is a new thing that

the staff wrote. So shall we see what it is? Maybe you can read it so we buy time.

MR. STURZEBECHER: "Cyber security is a combination of inherent technical features, functions that collectively contribute to a system, system of systems and enterprise achieving and sustaining confidentiality, integrity and availability." The second part, "The implementation of a standardized operational and management controls that define the nature and frequency of interaction between users' systems, system resources, the purpose of which is to achieve and sustain a known secure state at all times, prevent accidental and intentional theft, destruction, alterations or sabotage to a system resources".

MS. HERMANN: I think the important thing to note here is that if you look in the early paradigms, security engineering was only focusing on the technology. Now we have to focus on the management and operational controls as well.

MEMBER APOSTOLAKIS: And I see you're using fashionable terms here, system systems. Everybody is using them. You seem to be surprised. It was there. That's a Department of Defense. People are talking about system of systems all the time, but I don't think anybody knows what to do with them.

Okay. It's like convergent properties of complex systems, people love to talk about them, but if anybody knows what to do with them, I never met them.

MEMBER BANERJEE: Self-assembly.

MEMBER APOSTOLAKIS: Pardon?

MEMBER BANERJEE: Self-assembly.

MEMBER APOSTOLAKIS: Self-assembly is another. Let's go on, Karl.

MR. STURZEBECHER: So knowing what the environment is and the input that we received, this is basically the purpose of our Reg Guide and it's -- the main point here is to establish a performance-based requirement with the licensee or Applicant. And as you can read here, to insure the functions of these systems are protected from a cyber attack.

MEMBER APOSTOLAKIS: The issue of performance based requirements is interesting here. I think it's worth pointing out to the Committee that we have seen those words a lot in the last eight, nine years. If I have a performance requirement that is, say, like in the maintenance rule, the availability or unavailability of this system should be less than this number, I understand that. Here, of course, we don't have numbers like that and we shouldn't, but is it really a performance based approach to say produce a

plan to do this? I mean, I think we're stretching the concept of performance based approach if we just say produce a plan.

Yeah, produce a plan so I perform? Don't I have to have something more? That was something that really struck me as being odd about the Regulatory Guide, that essentially it was asking people to do things in the sense, you know, "Give me plan that will make sure that this thing is protected and leave it at that." I wouldn't call that a performance based requirement. I think we're really stretching the concept too far.

MR. STURZEBECHER: Well, part of the expectation is that they continue with the life cycle review of whatever plan or the program they set up. A lot of sites have health, system health reports.

MEMBER APOSTOLAKIS: but that's the point, you just said of whatever program they have set up. So there's tremendous flexibility in this kind of thing, right?

MR. STURZEBECHER: That is correct.

MEMBER APOSTOLAKIS: Well, I am a little bit --

MEMBER POWERS: I hate to parse to language a little bit, George. Let me parse some

language here. I'm a little bit puzzled by what you mean when you say graded approach. If you're doing a graded approach, that means that there must surely be some activities that you've identified whose worth -- whose cost does not equal their worth and they'll get done. That means that you are allowing a certain amount of vulnerability to exist in systems because you think it's unlikely that somebody will try to exploit those vulnerabilities.

MR. STURZEBECHER: Right.

MEMBER POWERS: Okay, well, why is that compatible with insure. Shouldn't your sentence say "Requirements that the functions of critical systems and critical digital assets are protected adequately from cyber attack throughout the systems engineering life cycle using a graded approach"?

MR. STURZEBECHER: Well, when you're saying a graded approach in one particular item and if that system is selected, say it's a waste water site, that could have impact because the tied has with the main DCS, the Digital Control System. So whatever vulnerabilities that you look at on that particular system and you would have to make sure, insure that that -- that you're using a graded approach. How far do you need to put the firewalls on that particular

system, the connections between the two or if it's just a read-only input, then -- or it wouldn't have an effect necessarily if somebody were to compromise the controls at that waste water facility that's connected to the power plant.

MEMBER POWERS: It seems to me you either have a graded approach or you don't.

MR. STURZEBECHER: I'm not sure I understand.

MS. HERMANN: The graded approach applies to the level of protection to the assets. The critical assets get a higher level of protection. The less -- the ones that aren't critical get a lower level of protection. So the solution is tailored to the risk and the risk communication priority.

MEMBER POWERS: Then you have a threshold approach, not a graded approach.

MS. HERMANN: It's graded to the thresholds.

MEMBER POWERS: You're determined to use graded approach here.

MS. HERMANN: Actually, that was -- industry is comfortable with that term, but I understand what you're saying. There are tiers, thresholds corresponding to the level of protection.

MEMBER APOSTOLAKIS: Okay, so the performance based thing -- I mean, I'm a little bit uncomfortable using the words here. As an example, I mean, under system and service acquisition, the advice is, "Develop procedures to facilitate and maintain the implementation of procurement policies associated with vendor security and development life cycles". That's a performance criteria. It's a policy statement, yeah.

Okay, let's go on.

MEMBER BANERJEE: Are these critical systems primarily safety systems you're talking about here?

MR. STURZEBECHER: They can vary.

MR. LEE: Yes, well, some are and most of them -- definitely the safety systems are and a whole bunch of other control systems will be included as critical systems because any system that could bring down the mutual portion, we consider that as a critical system.

MEMBER BANERJEE: And these are sort of pertaining to these digital platforms that are being offered as well by the industry?

MR. LEE: Any system that has a computer in it. When I meant computer, I mean, able to store

data and process information.

MEMBER BANERJEE: I think I've got it.

MR. LEE: Thank you.

CHAIR BONACA: All right, let's move on.

MEMBER APOSTOLAKIS: Sorry, what?

CHAIR BONACA: I said, let's move on.

MR. STURZEBECHER: Okay. This slide shows a mapping of how you would actually start to review a system by going over the vulnerability and then reviewing what the threat assessment is and finally coming up with a risk mitigation or a security risk assessment is the bottom line.

MEMBER STETKAR: Karl, this slide, and I don't think we saw this in the Subcommittee meeting, this slide implies that there is some threat assessment which, in fact, there isn't. So this slide shows a nice neat --

MR. STURZEBECHER: Sequence.

MEMBER STETKAR: -- whole sequence of doing a risk assessment. There really is not a cohesive risk assessment because there is no treat assessment. The treat is presumed. Any threat is presumed with equal likelihood as far as I can understand, but it's really a vulnerability assessment. It's not a risk assessment and there is

no threat assessment. I don't see anything in the process. I don't see anything in the NUREG that the process refers to that says we evaluate the frequency and types of threats that may, indeed, try to compromise our system so that we can assess our vulnerability of the system to those threats and the consequences would be those threats are successful if they bridge --

MEMBER SIEBER: It's a moving target.

MEMBER STETKAR: It's a moving target but this implies that this is a complete risk type based approach which would have a frequency of various types of threats and assessment of the vulnerability to those threats and assessment of the consequences if the threats were successful and, therefore, establish some sort of barriers against threats. That would be a more integrated graded approach to the process but, indeed, the process doesn't say anything about threat assessment.

CHAIR BONACA: You're referring to the text.

MEMBER STETKAR: I'm referring to the actual -- no, this is the technical approach. I'm referring to the technical approach.

MEMBER APOSTOLAKIS: Yeah, we are

reviewing the Regulatory Guide that we have.

CHAIR BONACA: That's right.

MEMBER APOSTOLAKIS: And John is right, the Guide we have says nothing about this.

MEMBER STETKAR: Neither does the NUREG as far as that goes.

CHAIR BONACA: We have commented already on this issue in fact.

MEMBER APOSTOLAKIS: Huh?

CHAIR BONACA: We commented last year.

MEMBER APOSTOLAKIS: Yeah, that was my next comment, that our letter from April of `08 specifically recommended that the threat assessment be done.

CHAIR BONACA: Right.

MEMBER APOSTOLAKIS: And we have never really received a response to that. I mean, the Guide is silent.

CHAIR BONACA: Well, we would like to see this --

MEMBER APOSTOLAKIS: At least if you would tell us why you disagreed.

CHAIR BONACA: -- in the guidance, but it's not there right now.

MEMBER APOSTOLAKIS: Huh?

CHAIR BONACA: We would like to see this in the Guidance but it is not there now.

MEMBER APOSTOLAKIS: It is not there now, that's correct.

MS. HERMANN: This diagram is actually going to be added. This is one of the diagrams we're going to add into response to the comments and I'd like to -- if you'd look under the definition of threat, where it says "it's a function of the operability mode of expertise and resources available", that's where we're getting into the security threat assessment. Yes, there's a vulnerability. Yes, it can be exploited, but in order to be exploited, the attacker has to have an opportunity. They have to have sufficient expertise which could be very high, very low.

They also have to have certain resources available which could be a $5.00 piece of equipment or a $5 million piece of equipment. And there are metrics where you measure the opportunity, motive, expertise and resources. And that is the security equivalent of the threat assessment that you're talking about. And then that feeds into the risk mitigation priority. And the risk does get into the severity of the consequences but it's tied to -- this

gets into the intentional exploitation as opposed to an accidental, because the intentional is totally driven by the OMER model.

VICE-CHAIR ABDEL-KHALIK: If that is the logic, if one goes through the first block, which is the vulnerability assessment, the second time you cycle through this diagram, what would you know that you didn't know the first time?

MS. HERMANN: Well, initially what you do is you find out what vulnerabilities are there, inherent. Remember, this starts at the requirements phase. This isn't after. We do this at each life cycle phase. So it's like the hazard analysis. What could go wrong, what are the vulnerabilities? And then you characterize your adversary using the OMER model.

And if you're expecting a high level of expertise and a high level of resources like state-sponsored cyber terrorists, then you need a high level of mitigation. If you're worried about the high school kid around the corner, you don't need a high level of mitigation.

MEMBER APOSTOLAKIS: But isn't that saying, though, that the threat assessment --

VICE-CHAIR ABDEL-KHALIK: Comes ahead of

the vulnerability assessment.

MEMBER APOSTOLAKIS: -- comes before the vulnerability?

MS. HERMANN: No.

MEMBER APOSTOLAKIS: You have to have some threat in mind before --

MEMBER BLEY: I mean, that's a key point that I was going to bring up, too. The vulnerability is really --

MEMBER APOSTOLAKIS: Is what?

MEMBER BLEY: Dependent on the threat.

MEMBER APOSTOLAKIS: Correct, so the threat has to be up front.

MEMBER BROWN: No, I wouldn't agree with that. I mean, if you have an isolation, okay, or a strictly one-way path, the vulnerability is, you know, from exterior, is not very much at all, if anything. So there's levels -- I agree with you to a certain extent. You've got to have some idea of the threat, but there are certain methods of security that really reduce the threat from anything. That's the only point I'm trying to make, nothing more complicated.

MEMBER APOSTOLAKIS: It's like trying to find the accident sequences without considering the initiating events.

MEMBER BLEY: And people have tried and --

MEMBER APOSTOLAKIS: There is no question that you're right, Charlie. Some of them you can find.

MEMBER BROWN: Thank you.

MEMBER APOSTOLAKIS: Some of them you can find, but in a systematic approach, it seems to me you have to have a threat in mind and then you go and say, "Well, this is how this" -- it doesn't have to be very specific but some -- like state sponsored, I mean, these guys have capabilities that a graduate student doesn't. So you know, you approach the program of vulnerability identification differently.

I'm sure when they actually do it, they will do these things. It's just --

MEMBER BANERJEE: What is a concrete example, a hacker or a virus or what is this?

MS. HERMANN: We actually have a slide on that coming up with all sorts of --

CHAIR BONACA: But I think, in my judgment, I mean, you can make the sequence work.

MEMBER APOSTOLAKIS: What?

CHAIR BONACA: What I mean is that you do an assessment. You have a risk mitigation determination that you make and then we characterize

the vulnerability because you take into consideration the threat and the mitigation capability.

MEMBER APOSTOLAKIS: It doesn't -- I don't think you can do the risk assessment.

CHAIR BONACA: Okay.

MEMBER APOSTOLAKIS: Okay, especially the probability of attack. The analysis has to be conditional. I mean, you have in mind, of course, how maybe how likely it would be that I would have the whole state attacking me. But what it says there, likelihood of vulnerability being exploited, I mean, there is a lot behind it. I don't think it's going to be as straightforward as a PRA, for example, because a lot of this is intentional.

To bear in mind the likelihood and somehow include it in the calculations is a good idea. To expect that we will quantify explicitly like we do in PRAs is not a good idea. So risk assessment, risk mitigation, priority, I mean, risk here I would say is used in the everyday meaning.

MEMBER SHACK: Well, I think here the risk is really looking more at consequences than the likelihood.

MEMBER APOSTOLAKIS: But also the likelihood plays a role because --

MEMBER SHACK: You might have -- you know, you might be happier if it said consequence assessment.

CHAIR BONACA: I'm not sure that --

MEMBER APOSTOLAKIS: It's not exactly consequences either because, you know, the threat part is important.

MEMBER BANERJEE: Is there a design basis threat?

MEMBER APOSTOLAKIS: Yes.

MEMBER BANERJEE: So is this sort of like -- this is a more probabilistic approach or what is this?

CHAIR BONACA: Well, I mean, I'm not sure they intend this all in a quantitative mode.

MEMBER APOSTOLAKIS: No, they cannot.

CHAIR BONACA: No.

MEMBER APOSTOLAKIS: But would you comment on that? I mean, is this beyond design basis threat or is it below or what is it?

MS. HERMANN: It's up to is our requirement.

MEMBER APOSTOLAKIS: Up to the design basis threat but not beyond? Why do we go beyond design basis everywhere else and not here?

MS. HERMANN: That's just the language in the Rule.

MEMBER APOSTOLAKIS: The Rule says that?

MS. HERMANN: Up to and including.

MEMBER APOSTOLAKIS: Yeah, I remember those words.

MEMBER BANERJEE: Is there analogy in this with other things that we do? The standard approach is a design basis threat and you're asked to assess the consequences and you protect against these. There are several -- I don't know the field at all.

MEMBER APOSTOLAKIS: Up to.

MR. LEE: When we developed -- worked on that NUREG-6847, it was back in 2003, we used this approach, a baseline approach that was developed by PNNL and actually it took us more than a year and we had a volunteer, a full volunteer of plants and also we have industry participation to develop this process about what we're talking here, assessment method.

And using the three nuclear power plants, what we did was we fine-tuned this baseline method, then we validated it at the fourth plant and the approach that we took, we took certain assumptions. The way we did it was, when we did a vulnerability assessment, initially we were trying to see whether a

person can -- outside people coming into the specific system and when we look at that approach, it was impossible for us to protect because it was continuously changing and you will never know who might be coming in.

So we looked at it differently. We had some research done and the -- we found out that the -- it might be better if you looked at it from inside out, meaning we -- what we did was whatever the system that we have identified as a critical system, let me go back to what -- how we define critical systems. We said that the critical system is any system that could adversely impact safety, security, emergency preparedness system. That critical system is identified by a team of experts or a team of people who has expertise in cyber security, information security, plant computer system, plant operations and plant design and engineering.

Those folks get together because they know the plan. They know there was consequences associated with it, so they identify a particular system and see whether they have a digital system or not. If there are any digital systems, we identify that as a critical digital asset and that, if -- then what we do is we -- taking this inside out approach, we draw a

circle around it and we say that any connection, either it is a --

MEMBER APOSTOLAKIS: Is that 14, Slide 14? Is that what it is? So we'll come to that. This is Figure 1. Go to 14 and complete the argument.

CHAIR BONACA: Yeah, let him finish the argument.

MEMBER APOSTOLAKIS: Slide 14. Complete the argument here.

MR. LEE: Actually, why don't you go to the -- may I go to the last slide, backup slide? Yes, when we do vulnerability assessment, we drew a circle around it and we say that the -- we assume that any connections you have, either is a direct or indirect, meaning it could be a sneaker -- a sneaker connection or the direct connection. So we identify all those connections and we say that if we have connections, there's a vulnerability. So we have to address those issues.

And the next thing that we do is we are trying to identify the -- here we called it a threat assessment, but I think in the paper we called it a susceptibility analysis. That's how likely that the vulnerability you have or how likely that critical asset or critical system that you have is vulnerable

to be exploited. We have a couple of experts in the PRA. His name is Dr. Glantz. He assists us in doing this and also we had participation from all the --

MEMBER APOSTOLAKIS: Wait a minute. Why would an expert from PRA assist you in that task? That task you need somebody who understands digital systems I would --

MR. LEE: Well, I'm getting to that, sir. What I'm saying, sir, it's not just him but he was helping us looking at the -- how we could tell of this and also we had a team of I&C folks and also all the people that were involved with this project. And we got together and see how we could make it realistic and the -- we have identified that susceptibility is how many vulnerabilities that you have and also what type of vulnerability you have and then what type of measures you already have and that's how we determine how likely that it could be exploited.

So when we did that, when we tried to identify how susceptibility it is, we had a cyber security expert. We had a plant operational expert and we had a PRA expert getting together and we inject ideas and see how likely it is and we --

MEMBER APOSTOLAKIS: Let me understand this now. You say, "We did this, we did that". You

are writing the Regulatory Guide.

MR. LEE: No, this was --

MEMBER APOSTOLAKIS: Are you sending a message to the industry that they have to do this?

MR. LEE: They are actually doing that. They --

MEMBER APOSTOLAKIS: No, but when I read it, it didn't say that. The Guide didn't say that. So you say they are doing it. They are doing it because they're nice people? I mean, when you read the Guide, it does not say do the stuff you're -- I didn't see that listed.

MS. HERMANN: I think it just refers -- it refers to 6847 without repeating the information.

MEMBER APOSTOLAKIS: But, I mean, you know, when you refer to a NUREG report, it's you pick and choose really. I think a diagram like this in connection with Figure 1, for example, the existing Figure 1 and some discussion and then say, "Now, if you want this case, go to the NUREG". At least you are telling people, "This is what we want you to do". Then I think, you know, with some massaging of the words, that would be a useful contribution it seems to me.

Let's -- I mean, just to say, "Go to the

NUREG", I mean. The NUREGs usually have a lot of stuff.

VICE-CHAIR ABDEL-KHALIK: Where, within this process, would you take advantage of the experience accumulated since the last time you cycled through this process, both experience within and outside the nuclear industry?

MS. HERMANN: Well, that gets into the vulnerability environment changes, the threat environment changes, and so when you get into the -- one reason you constantly look through this because the things are changing and you may have installed a security control that was effective and now it's no longer effective. So that's why you're constantly also verifying the effectiveness of the security controls.

VICE-CHAIR ABDEL-KHALIK: But is there sort of a storehouse of information that this team can go to?

MS. HERMANN: Yes. Yes, DHS maintains a site, UScert, which has all the latest and greatest on vulnerabilities, threats, successful attacks, and they have one area that's specifically dedicated to control systems.

VICE-CHAIR ABDEL-KHALIK: Okay.

CHAIR BONACA: Let's go back to the presentation. But the point that Professor Apostolakis makes well-taken. What I mean is these are elements which are not in the Reg Guide right now and so it's hard to know what to comment on. I mean, these are positive steps.

MEMBER BROWN: One of the things I saw was missing, I guess, even as you go through this, is that one of the -- my opinion again, is one of the key elements of trying to have cyber security is in the initial system design to not set yourself up to have vulnerabilities. Before you ever get to this, you ought to be putting in a system that doesn't do all bells and whistles that you don't need. You ought to only do the specific function.

Yet there's no -- there's no comment or statement in here that the initial system design shouldn't be just whatever people want to do and then we'll go fight it off with 1,000 IT people and cyber security folks. You ought to design a system that minimizes the necessity for a lot of effort like this or complicated cyber security protections and firewalls. And there are ways to do that with many of the systems that you look at, because you get into this computer based data system, you can do anything

you want to.

Data is flying all over the place. Everybody wants to look at it and modify it and you know, chomp on it and analyze it and trend it. You don't need that. In 99 percent of the cases, there's a limited set of functionality that you want to achieve, yet we don't consider that in saying what's the fundamental basic approach to security? Don't set yourself up for it. It's not in the Reg Guide at all. It's not even in the 73.54 guidance. It doesn't have to be there. It's, you know, the implementing. If you want to get real guidance in RG, in this particular Reg Guide, it seems to me that's right up front. That ought to be the first statement.

Don't set up a system that gives you vulnerabilities. Don't wait for the system to get there and then assess what's going to happen. You want to put in a system that minimizes the vulnerabilities that have to be dealt with. That's one of my major --

MEMBER BANERJEE: They have to isolate it, I guess.

MEMBER BROWN: Well, fundamentally, the best of all is you don't allow any connection to the outside world. Then you don't -- you know, you've

only got internal threats where people coming in and putting a key on the thing and then put it in the shift supervisor's pocket and --

MEMBER BANERJEE: But is there a design basis threat? I asked this question before. I mean, how do they -- did I get an answer? I'm not clear. What is that design basis threat? Are there design basis threats, let's say, more than one?

MR. LEE: There is a rule, I think that just became effective not too long ago, 73.1, 10 CFR 73.1, states that we need to protect against cyber attacks from the external force on the cyber attack.

CHAIR BONACA: We need to move on at this stage, but still, I mean, I have a concern that when I look at your presentation, it has a lot of elements responding to the feedback to the Subcommittee and they would be valuable inside the Reg Guide but we're reviewing the Reg Guide, it doesn't contain these pages right now, so we have to understand what we're going to do.

MS. HERMANN: The intention is that the new information, the new diagrams, tables, will go into the Reg Guide. That's on the backup slides.

MEMBER APOSTOLAKIS: Well, the Committee will have to discuss later what the course of action

is because we -- if we have to write a letter, we have to write it on what we have. Yeah. And if you revise a Guide, you plan to come back to us because of the pleasant experience?

MS. HERMANN: Whatever you would like.

CHAIR BONACA: There is Slide Number 18 that sets the stage.

MEMBER APOSTOLAKIS: We are jumping around here.

MR. STURZEBECHER: Yes, we are.

MEMBER APOSTOLAKIS: Can we go back -- well, let's look at 18 first. Yeah, that's the future -- the path forward. Let's go back to Slide whatever we were. We were on --

MEMBER BANERJEE: 8.

MEMBER APOSTOLAKIS: Huh?

MEMBER BANERJEE: You were on 8.

MEMBER APOSTOLAKIS: Yeah, and I think we've exhausted 8. Let's go to 9.

MR. STURZEBECHER: Part of -- when you develop the program for the Reg Guide is to coordinate with the safety engineering and reliability engineering. The idea is you want to integrate the cyber security into these processes when you're doing a design. You don't want to just bolt on your

security. It has to be a coordinated effort.

MEMBER RYAN: Just one comment. I don't know if you have this or not yet, but there's an awful lot of jargon in your presentation. I think what you mean by reliability engineering might not be what other folks mean. So if you could think about a glossary of terms and how you're using them, that might help with a lot of this discussion of, you know, what you mean by a threat, what you mean by reliability engineering, safety engineering, physical security.

I mean, in computers physical security doesn't necessarily mean lock it up. You know, so there's lots of terminology here that's beyond what we normally think about, you know, from a hardware management point of view and it's a lot different. So you have to, I think, take on a role of educating your readers in the Reg Guide.

MEMBER APOSTOLAKIS: Yeah, they have a glossary but these terms are not there, so it should be expanded.

MEMBER BROWN: Technical approach 3.4.1.2, is that a paragraph in the Reg Guide? I couldn't find it. It doesn't exist.

MS. HERMANN: At one point in time it was

3.4.1.1.1.

MEMBER BROWN: Oh, so you changed the numbers. That's the life cycle phase activity?

MR. STURZEBECHER: Yes, it's under life cycle phase.

MEMBER APOSTOLAKIS: Okay, let's move on. This is --

MEMBER BROWN: All right, that's fine. That's enough.

MR. STURZEBECHER: If we step back and look at where the Reg Guide sits --

MEMBER APOSTOLAKIS: By the way, we received an NEI document, what, yesterday?

MS. ANTONESCU: Yes.

MEMBER APOSTOLAKIS: Who sent it to us?

MS. ANTONESCU: Debra.

MEMBER APOSTOLAKIS: Did you do that, Debra?

MS. HERMANN: Just background information that shows up on some of the charts here.

MEMBER APOSTOLAKIS: It is a bit unusual to receive a document the day before the meeting. Maybe next time we'll have read it.

MEMBER SIEBER: Better than the day after.

MEMBER APOSTOLAKIS: Okay, okay, Karl,

let's move on.

MR. STURZEBECHER: In creating the Reg Guide and we have -- in association with the NEI 08-09 which is going to be the -- part of the plan, which is in Section 2 of the Reg Guide and that template is being worked on by NEI and we're going to be reviewing that at a later -- actually today.

MEMBER BROWN: That's the document you just sent out?

MR. STURZEBECHER: Right.

MEMBER APOSTOLAKIS: So what is this chart telling us?

MR. STURZEBECHER: This shows the touch points with other guides and how we positioned it and also shows -- right below it is the NUREG that NSER is planning on moving on some of those attributes and then expanding on the features and try to do more NUREGs to support the Reg Guide.

MS. HERMANN: Order of precedence of the documents and all the interactions.

MEMBER APOSTOLAKIS: I think we would all benefit if we had subcommittee meetings reviewing those documents in more detail. Then we'd all be up to speed when we reference them. Another thing that -- I'm really bothered by this arrow that goes from the

Regulatory Guide to NEI. It could be the other way around?

MS. HERMANN: It could be either way. Basically, what's going to happen is once we're comfortable with the NEI 08-09, we're going to endorse it in 5.71.

MEMBER APOSTOLAKIS: But the center point should be the Regulatory Guide.

MS. HERMANN: Right.

MEMBER APOSTOLAKIS: That has the force.

MEMBER POWERS: I note that the NEI uses liberally the words "adequate protection, high assurance", instead of -- I have yet to come across "graded approach", but I've haven't gone through it. But they seem to have set their objective as an adequate level of protection and not an assurance. You said insure with a graded approach and they don't seem to do that. They seem a high assurance of adequate protection.

MS. HERMANN: I think ensure is on the slides. The Reg Guide itself uses high assurance.

MEMBER POWERS: High assurance.

MEMBER APOSTOLAKIS: Well, the rule uses high assurance. So they want high assurance of adequate protection.

MS. HERMANN: Right.

MEMBER APOSTOLAKIS: And all the subsidiary -- supporting documents should strive to achieve that, correct?

MR. STURZEBECHER: Yes.

MEMBER APOSTOLAKIS: And I guess your argument is that the graded approach is a means of getting there. Ultimately, you want to have high assurance. Right? So okay, let's move on unless there is something special you want to say about this. Okay. Slide 11.

MR. STURZEBECHER: So this is how the Reg Guide if you drive deep into it, you start with a security plan, which is what we referred to before about the template that's being worked on. The cyber security program and the outlying drivers of security controls and the three listed here is management, operational and technical controls and these are items that are a part of NIST, that NIST uses in the 800-53 document.

Below each one of these controls you have a listing of attributes that we are suggesting or strongly recommending I should say that are applied for each one of these areas. From here underneath one of these particular, we're going to get into an

example. We're going to get into the authentication. You would pick features and you can see that. I have it there. It's access control.

MS. HERMANN: It's identification.

MR. STURZEBECHER: Identification, yeah, identification authentication. There it is right there. That's the example we're going to show later.

MEMBER APOSTOLAKIS: Now, one question that arose at the subcommittee meeting is that it would be nice to see an overarching model how all these things tie together, what is needed and my question now is are these slides along with the backup slide that Eric referred to earlier along with Figure 1, all this stuff, is that what we would call a model so people understand how the pieces fit together and so on? And that presumably will also be in the next version of the guide or some version thereof.

MS. HERMANN: Yes.

MEMBER APOSTOLAKIS: Okay, all right, so I understand now that -- because all we saw at the subcommittee meeting was Figure 1, which is also reproduced here on Slide 14, which the members or at least some members felt it was a little vague and high level and it didn't really give advice what to do and I believe the staff now is coming back and saying,

"Well, look, this is how the whole thing fits together".

MR. STURZEBECHER: Right.

MEMBER APOSTOLAKIS: Okay, that's good. Communication is very important, Karl.

MR. STURZEBECHER: Here we're showing the steps that you use. The first part is the attributes you're trying to -- that you select for what you're trying to protect. Using the cyber security plan, the policies, the implementing procedures is the how. You connect these different aspects of the Guide together and the rationale is below and we've kind of gone over this maybe in a different way but and it relates to the rule that this combination provides site specific when your particular site that you're dealing with for cyber security and the -- you know, the system engineering methodology and the business practices that exist at that particular site, there's a -- it helps -- the benefits are that you have -- there's a rapid evolution in any of these cyber security technologies depending on that site and so that they have to provide and the high assurance that they're meeting this by using the program we've set out, we laid out.

MEMBER APOSTOLAKIS: Well, I guess --

MR. STURZEBECHER: Flexibility.

MEMBER APOSTOLAKIS: -- I'm sorry, for the benefit of the members, it's the first bullet that the subcommittee felt there was a particular weakness in the Guide in the sense that it didn't go one or two steps beyond what they have and be a little bit more specific. The Staff said, "Well, gee, this is security. We can't be specific". So the counter-argument was, "Give some examples of what would be acceptable".

And as it turns out, the Draft Guide 5022 I believe, did have those and somehow they disappeared on the way to the Regulatory Guide 5.71. So that was something that the subcommittee felt needed some improvement. And that's why I asked the question earlier what is performance-based? I mean, just asking somebody to give you a plan, would you call that performance-based or should you have to give a little bit more advice as to what the plan should be all about and give some examples and so on?

And in fact, if you compare it with DG-5022, there are examples that are pretty good, I mean, you know, as long as they're taken as examples. So that's a point of contention. So the first bullet there is something that the subcommittee felt

uncomfortable with. Okay.

MEMBER MAYNARD: Yes, but I believe that a number of us became more comfortable with the performance-based approach if there could be some examples put in.

MEMBER APOSTOLAKIS: That's what I said.

MEMBER MAYNARD: I don't think we were pushing for --

MEMBER APOSTOLAKIS: That was my argument, that if you give some examples, you send a message, "This is the kind of thing I'm expecting you to give me", without saying, "You should really do 1, 2, 3, 4", but you can't just say, "Give me a plan". Yes, John.

MEMBER STETKAR: Well, and those examples would help to clarify what they mean by the term "performance-based approach" as compared to what many other people might interpret that term to mean.

MEMBER APOSTOLAKIS: Exactly, yes.

CHAIR BONACA: Okay.

MEMBER SIEBER: Actually, all the comments we made during the subcommittee are on your Slides 19 and 20, which I presume you will go through.

MR. STURZEBECHER: Yes.

MEMBER SIEBER: Examples is one of those.

MEMBER APOSTOLAKIS: You mean 19? Yeah. Well, I just wanted to point it out here.

MEMBER SIEBER: Yeah, so if we get there ever.

CHAIR BONACA: All right.

MEMBER APOSTOLAKIS: Okay, let's go on to the -- you have 31 minutes. We've got 31 minutes.

MR. STURZEBECHER: This shows a list of exploits.

MEMBER APOSTOLAKIS: Okay, what do we have here?

MR. STURZEBECHER: This is a list of exploits that we put together as an example and this is what the security controls would try to mitigate or, you know, prevent or mitigate the consequences of that particular cyber attack. Any one of these is a particular attack.

MEMBER BROWN: You intend to include these?

MS. HERMANN: All the charts are going into the Reg.

MEMBER BROWN: Okay, all right.

MEMBER APOSTOLAKIS: Well, let me understand. Let's pick one. Let's pick one to understand what it means. The third one -- the left

column, the third one from the top, "Browsing surveillance precursor event", would you explain what that means?

MS. HERMANN: Yes. Generally, attacks don't just happen. There's a lot of intelligence gathering ahead of time. And so you do surveillance to find out what kind of system is installed, what kind of network, what kind of operating system. You poke around, you find the vulnerabilities and then you come back later and actually launch the attack. So this is an exploit where you're just gathering information in order to prepare your attack.

MEMBER BROWN: So the --

MEMBER APOSTOLAKIS: The point of this is if you see somebody doing that?

MS. HERMANN: Yes.

MEMBER APOSTOLAKIS: Ah, good.

MEMBER BROWN: Yeah, you should be looking for people pecking away at your network. Did I get that right?

MS. HERMANN: Yes, they're snooping.

MEMBER BROWN: I wanted to put it in English.

MS. HERMANN: Sorry.

(Laughter)

MEMBER RYAN: If you want it in English, you'll have to take the last one off; virus, worm, zombie, bot net.

UNIDENTIFIED MEMBER: What's the problem, bot net or the whole line?

MEMBER RYAN: I understand what a virus is. I think I know what a worm is. I have no clue what they mean by zombie or bot net.

MS. HERMANN: Yes, the short definition is it's malware, bad software that somebody installs on your system.

MEMBER BROWN: That's the bot net?

MS. HERMANN: That's the zombie.

MEMBER APOSTOLAKIS: And the bot net?

MEMBER BROWN: Oh, malware, I love it.

(All speaking at one time.)

MEMBER RYAN: This language evolves very quickly. I understand that. Please take this stuff out because your NUREG will be beyond old two weeks after it hits the press if you keep this kind of language in.

MEMBER APOSTOLAKIS: Or have a very extensive glossary.

MEMBER RYAN: Well, you know, even that's going to age pretty quickly. So, you know, it's

better to describe what the functions of some of these bad things are rather than trying to give all the buzz words.

MR. STURZEBECHER: That's why we tried to boil it down to an attribute, because the attribute will always be the same, that type of attack or whatever, but the feature, what you're trying to protect from the exploit --

MEMBER RYAN: You didn't get it in this statement.

MR. STURZEBECHER: Right.

MEMBER RYAN: I understand your goal but you need to have somebody that doesn't understand the jargon go and highlight all the jargon and say, "Get these words out".

MEMBER APOSTOLAKIS: What's a Trojan Horse?

MS. HERMANN: A Trojan Horse, well, that's an example, you were talking about last week with eproms. You had eproms coming in being delivered. They could have installed some malicious code on the eprom that nobody knows is there and then once installed it launches an attack on its own.

CHAIR BONACA: It's actually a Greek gift.

(Laughter)

MEMBER APOSTOLAKIS: So this must be the most intelligent thing they can do.

(Laughter)

VICE-CHAIR ABDEL-KHALIK: So how do you maintain adequate vendor supply chain controls to prevent Trojan Horses?

MS. HERMANN: Well, that's why under the System and Services Acquisition the requirements of the Security Reg Guide were supposed to be passed from the vendor all the way back to the supply chain. So they have to have a security engineering license. So they have to do everything the vendors or applicants have to do.

VICE-CHAIR ABDEL-KHALIK: Where do you check? Do you do audits out at --

MS. HERMANN: That's part of the inspection procedures.

MEMBER APOSTOLAKIS: So if I were to recommend to the Regulatory Guide that a flat assessment be done, would I give these as examples of the kinds of threats we're talking about?

MS. HERMANN: These are like the top 30 today.

MEMBER BROWN: Yeah, that's a good list, George. It's a good list. You shouldn't pick on this

one.

MEMBER APOSTOLAKIS: I'm not picking on it. I'm just saying -- you didn't let me finish. If I saw that thing I would be fairly pleased. This is what was missing.

MEMBER RYAN: No, the list is fine. But again, if you're not a jargonist, you lost the meaning, if you don't understand the principles of what all these things do. I mean, for example, you mentioned that the supply chain has to be checked for the vendors. Well, what if they lie? What if they're bad guys and they lie about what's in their software?

MS. HERMANN: You still test it when --

MEMBER RYAN: See, so you'd have to test it. So those -- I mean, those are the kind of principles and concepts that are very top level you have to, I think, deliver carefully, so people understand, you know, what the totals are rather than what the details are.

MEMBER APOSTOLAKIS: In any case, I think this information of this type goes a long way towards onsetting the subcommittee's questions. Here are examples of threats. Here are -- you know, without saying, "Look at every single one of those", and without claiming completeness. So this is good. We

can praise when appropriate.

MEMBER BROWN: These are really attacks, right, as opposed to exploit? This is another piece of terminology I --

MS. HERMANN: Yeah.

MEMBER BROWN: You used attach earlier and then you shifted the language.

MEMBER SIEBER: Are they two different meanings? Is that what you're saying?

MEMBER BROWN: I don't know. That's why I asked the question. Throughout the rest of it, we talk about cyber attacks and then here all of a sudden we talk about categories of exploits as opposed to categories of attacks. And it's --

MS. HERMANN: Attack is like -- exploits are categories, highest level category and then you drop down about five levels and you have the exact attack method. So it's related. It's different levels of abstraction.

MEMBER APOSTOLAKIS: So, like browsing --

MEMBER BROWN: They're attack categories.

MS. HERMANN: Pardon me?

MEMBER BROWN: They're attack categories.

MS. HERMANN: Yes. I'm going to leave it referred to as exploits, it's just the jargon.

MEMBER APOSTOLAKIS: I think it comes back to glossary. We need -- some things you obviously, you need to be put in there. So if I'm browsing, as we discussed earlier, I'm preparing for an attack, but I'm not actually attacking at that moment. Okay. Let's move on to --

MEMBER BROWN: No, I wanted to make one point that Mike was very valid on in terms of the ultimate protection is what you can do when you actually receive the software in your hot little hands. Do you want -- does the Commission -- do we want to see, does the staff want to see some part of this program involved on site, receipt of software type testing, verification, or are we just going to be -- depend on this non-really verifiable chain that goes clear back to the guy that's entering the code and compiling it, loading it onto an eprom at some vendor in Malaysia before it vectors on over here? And there's no -- to me, that's an example of a type of protection that is very valid because it's the ultimate in terms of your ability to check that software before you actually install it.

It's like before you ever put anything in your PC at home, you've got all those virus protection that checks the disc before you actually load it in,

whatever you do. So and that's -- I'm just trying to -- I agree with the examples and yet, we still are lacking getting to some examples of you know, the types of protection you would expect to see in terms of monitoring and checking for this stuff before it can come in from the outside -- it's a different type of outside attack but that's --

MEMBER SIEBER: Yeah, the down side of examples is all this stuff is continuously changing.

MEMBER BROWN: Well, the example of checking your stuff is not continuously changing. That's --

MR. LEE: One of the comments that we have received from the, I guess, during our meeting, our last meeting was that the -- well, the comment that we have received was that the examples, you know, that there's some danger of -- because a lot of times when we write the Regulatory Guide, industry sometimes takes that as you have to do that and do only that and the --

MEMBER APOSTOLAKIS: Well, just say they're examples. We cannot baby people and okay.

MEMBER BROWN: That's mindless. I know they do that, don't get me wrong. I've watched it happen for 35 years. So I'm well-aware of that.

MEMBER APOSTOLAKIS: When you say "shall they", there's a difference between shall and --

MEMBER BROWN: Should.

MEMBER APOSTOLAKIS: -- should and here are some examples. Okay.

MR. STURZEBECHER: This is a concentric ring model that we suggested an example in the Reg Guide and it's a horizontal view. Starting from Level 4 would be where your safety system and your DCS would reside. Level 3 you could put your data monitoring equipment. Level 2 is where you get the interconnection between the plant data network and possibly to Level 1 where you're going to the outside or the corporate network and then you have the outside world from there.

MEMBER APOSTOLAKIS: So where is the control room in all this?

MR. STURZEBECHER: Well, physically, if you would -- you would say the control room is here in Level 4, if you're going to try to say that's like the vital or the owner's area, or excuse me, the protected area. The control room could be here. At the same time you may have -- if you're thinking that this is the outside world. I'm drawing this line here. And this is on the site, you could have a small cell at

the Level 4 here if it's controls running the cooling towers. So that's where the physical side of security comes in where you've got to protect the line that connects between the two. So it just adds a depth of complexity that goes on with putting these systems together.

I mean, this is just a virtual model from a higher level on just cyber security.

MEMBER ARMIJO: Does your chart schematically tell you that you're going to block outside information at the Level 2? Is that the concept, that there's some level at which you -- the outside world can't even get information?

MR. STURZEBECHER: That is correct, yeah. That's where we're talking about the different mindsets between IT versus controls and the difference in the function of the actual equipment. So Level 2 is that break point.

If we do a vertical drive-down, this would be, you know, the standards that you can use. For any one of those levels, you would perform these particular -- this level of functions for providing cyber security and we have -- we're going to use the identification as an example. That's one of the attributes for transport under 4. And here I have the

authentication as a technical control and this would be the types of features you could use in whatever combination to provide authentication. Any one of these features, which like we discussed, it does change depending on how the environment, the cyber environment, the threat, keeps moving.

MEMBER APOSTOLAKIS: Is this what you wanted, Charlie, the Slide 15, the last column, some security --

MEMBER BROWN: Is that 15 or -- well, I haven't quite figured out what peer entity authentication is yet, so --

MEMBER APOSTOLAKIS: Where are you?

MEMBER BROWN: Or -- that's on Slide 15.

MEMBER APOSTOLAKIS: Yeah, yeah.

MEMBER BROWN: So there's a bunch of buzz words in -- I mean, that applies all the way through.

MEMBER SHACK: You know, this thing really isn't written for our grandmothers. You know, this Reg Guide is for security experts.

MEMBER BROWN: No, I know.

MEMBER ARMIJO: But Charlie is kind of in that business. If he doesn't understand it --

MEMBER SHACK: But I mean, I certainly hope the guy that's in charge of cyber security at my

plant knows what IP Sec is.

MEMBER APOSTOLAKIS: Yeah, but Charlie should understand it, too.

MEMBER BROWN: Well, no, I shouldn't because I never dealt with this. Our stuff was not connected to anybody. So we didn't -- you know, we didn't do this. All right, I maintain control, the prom control, and you know, if we had to take it, you know, from a plant to the ship, we need a guy and we followed him till he got there and we handcuffed it to his wrist with his briefcase, planted a bomb inside of it in case he died. You know, dead man control.

I'm kidding, okay, but the plain thing is we had absolute control and then we verified it on site before we -- you know, before we went and installed it. So there was a very -- we didn't have to deal with this. So a lot of this terminology I agree, but I still think for those who have to under -- to put the Betty Crocker Good Housekeeping Seal of Approval on it to us and other folks management that don't necessarily understand all of this, should have some ability to understand what your, you know, English words of what you've got.

That's a personal opinion. I agree with you, Bill, that yeah, the cyber security guys are

going to know all this stuff but there still ought to be some connection --

MEMBER SHACK: Well, I mean, in some ways you begin to lose communication if you get too far from the jargon of the community, I mean.

MEMBER APOSTOLAKIS: There is a glossary at the end. It should be explained in a few lines.

MEMBER BROWN: Glossaries are good things, and that's all I'm suggesting a glossary. Cobol -- I don't know the next one is --

MEMBER SIEBER: I think most of this is pretty well-known in the computer community.

MEMBER BROWN: No, I agree. This is some stuff, examples of what you want people to do and there -- it gives an idea of what you're looking at. It doesn't -- it's not all inclusive and that's fine. I think this is what you were looking for in some circumstances.

MEMBER APOSTOLAKIS: What is peer entity authentication?

MS. HERMANN: Peer entity authentication? That could be if you have two control systems that need to talk to each other, they authenticate them to each other. In other words, I know -- I tell you I'm Debra and you tell me who you are and then we mutually

authenticate at the same level in the protocol stack.

MEMBER APOSTOLAKIS: Great, simple.

MEMBER BROWN: It's like handshaking.

MS. HERMANN: Yes, at a different level, yes.

MEMBER BROWN: Thank you. It's a different term but I do understand that one. I'm not going to take the data till I get the right handshake.

MS. HERMANN: Right.

MEMBER APOSTOLAKIS: Did you do that again, Eric?

MR. STURZEBECHER: Under authentication, the licensee or applicant can bundle any one of these sets depending on the need or how they do their cyber security assessment. And this is -- covers the --

MEMBER APOSTOLAKIS: Well, we just said -- I mean, I'm curious. These are known and everything. Who else worries about digital I&C to the extent that we worry about it?

MS. HERMANN: Air traffic control systems, aerospace applications, medical applications.

MEMBER APOSTOLAKIS: They do?

MALE PARTICIPANT: Let's hope so.

MR. SANTOS: Defense Department.

MS. HERMANN: You don't want somebody

hacking into the --

MS. HERMANN: You don't want somebody hacking into the --

MEMBER APOSTOLAKIS: Air traffic I can believe. I don't know about the others.

MR. SANTOS: Finance.

MEMBER APOSTOLAKIS: What did you say?

MR. SANTOS: The finance community.

MEMBER APOSTOLAKIS: The most unfortunate example you can give but you really had to say it.

(Laughter)

MEMBER BROWN: The truth hurts.

MEMBER APOSTOLAKIS: They're getting better. Okay.

MR. STURZEBECHER: And the guide also requires the cyber security program be tied to the physical protection program and that's a flexible line, matrix to the cyber security program and the reasoning for that is to have a check on what -- how the program is running from a physical perspective.

So in summary, the Guide provides that flexibility that we're looking at -- looking for but we also have certain -- we've outlined certain attributes that we have expectations for the licensing applicant to follow through with the plan and the

program in our path forward.

MEMBER APOSTOLAKIS: Well, was the version of the Guide we saw citing NEI 08-09?

MR. STURZEBECHER: No.

MEMBER APOSTOLAKIS: No. The new version will?

MR. STURZEBECHER: We would like to do that, yes. We're working on the template now.

MS. HERMANN: The plan is to endorse it. When we're comfortable with the NEI 08-09, we'll endorse it in the --

MEMBER APOSTOLAKIS: So the final version of 5.71 will --

MS. HERMANN: That's the plan.

MR. LEE: If and only if we get to that review and agree with the industry that the version they have is acceptable to the NRC and if that comes to --

MEMBER APOSTOLAKIS: Yeah, sure.

MEMBER BROWN: What is the purpose of NEI 08-09? Does that provide -- I mean, you talk about a template. Is that the plan that they want to endorse, that they want you to endorse that then industry would use to comply with --

MS. HERMANN: Yes and no.

MEMBER BROWN: -- the fundamentals that you have in here?

MS. HERMANN: It's a template that corresponds directly to the Reg Guide and what it does is it organizes information that they have to present in the plan which will demonstrate that they've met the requirements in the Reg Guide.

MEMBER BROWN: So it's what we want in the Reg Guide.

MEMBER APOSTOLAKIS: That's right.

MS. HERMANN: And it's specific to each company site location.

MEMBER APOSTOLAKIS: This is common practice. They do it a lot.

MEMBER BROWN: No, I have not problem with it. It's just the backdoor way of getting it, that's all.

MEMBER APOSTOLAKIS: But I guess then what I suspect we should do is have another subcommittee meeting, where we will also have the opportunity to review the NEI document.

MS. HERMANN: Exactly.

MEMBER BROWN: Well, we really need to see how it interfaces with whatever changes they make.

MEMBER APOSTOLAKIS: Sure, we have to know

what's in the document.

MEMBER BROWN: No, but this is a stand-alone document.

MS. HERMANN: Right.

MEMBER APOSTOLAKIS: For the moment, it's a stand-alone and that's my next question.

MEMBER SHACK: What's the time scale for this integration? Is this going to be issued and used for a couple of years before you get around to it?

MS. HERMANN: Oh, no, we're talking maybe early summer.

MEMBER APOSTOLAKIS: So what was the purpose then of issuing the draft we have now?

MS. HERMANN: Just background information in response to some questions we got last week.

MEMBER BROWN: From industry.

MS. HERMANN: No, from --

MEMBER APOSTOLAKIS: From us.

MEMBER BROWN: Oh, from us.

MEMBER APOSTOLAKIS: We are reviewing a document that is not intended to be the final version of the Regulatory Guide and that's where I'm a little bit confused why it was submitted to us.

MS. HERMANN: Oh, I answered the wrong question. There will be -- basically, it was going to

be one sentence added to the Reg Guide that says that this is -- where we're talking about the plan, it will be like one sentence added endorsing the NEI document.

MEMBER APOSTOLAKIS: But that's a dynamite sentence. I mean, the Committee should be aware of what's in 08-09.

MS. HERMANN: Right, right.

MEMBER APOSTOLAKIS: So I suspect, in fact, I don't suspect. I'm pretty sure we'll have to have another subcommittee meeting then.

MEMBER SIEBER: Well, you're asking for a letter, so we presume our letter, if we had one to endorse this, endorses it the way it is today.

MR. STURZEBECHER: Yes. Yes, sir.

VICE-CHAIR ABDEL-KHALIK: If we go back to the previous slide, I do not understand the logic of having the same organization responsible for both physical security and cyber security. I mean, the skill set required for the management and implementation of these two functions are totally different and I'm not sure where that sort of interface comes in.

(Simultaneous speaking)

MEMBER SIEBER: That one came from the subcommittee and it's on Slide 19, the Rule.

MEMBER BROWN: That was a comment out of the subcommittee that we --

MEMBER APOSTOLAKIS: Well, okay, so let's go onto 19.

MR. STURZEBECHER: It's the first bullet right there.

MS. HERMANN: We're kind of stuck with it because it's in the Rule.

MR. STURZEBECHER: It's in the Rule, so --

MEMBER APOSTOLAKIS: Can we have one person speak? Please, Karl, go ahead.

MR. STURZEBECHER: I was going to say it's in the Rule that you have to have this connection between the cyber security organization, the physical width, I should say the physical security organization has a connecting point with your cyber security program. And the reasoning behind it is there's different drivers for economics and so on when you're doing the plant and obviously, cyber -- the physical security has one -- oh, their mission is to hold the security line and keep the protection of the site and the plant.

So the idea was to kind of cover the cyber security program, keep it orientated with a check, someone to check who's doing the work.

VICE-CHAIR ABDEL-KHALIK: I'm sorry, I don't understand what you said. It just seems to me that, you know, the words on Slide 17 say "Thou shall do this", and presumably that's what the Rule says you should do. And yet, I don't understand what can come out of that connection given the fact that both the management and implementation of these two functions require a completely different skill set.

MS. HERMANN: Perhaps an analogy would be useful at this point. In BTP 7-14 which talks about the software development life cycle, we require independence between the person or group that designs the software and the group that verifies it. What we were trying to accomplish here was some level of independence between the people that are responsible for operating the digital I&C versus the people doing the cyber security, just as a check and balance.

MEMBER SIEBER: Mistake.

MEMBER ARMIJO: Yeah, I don't think you got your money's worth from that.

MEMBER MAYNARD: Well, I personally don't have a problem with the security organization having the overall responsibility as long as you have the expertise and we do that right now with certain other activities. You can run into the same problem if you

want to make your IT organization the cyber security deal and there's a disconnect with the security organization. At some point, it's got to come together where somebody with security in mind -- and I agree it's a totally different skill set but I think that it can work depending on how you make it fit in. Right now most organizations have -- for maintenance, for I&C type work on security systems, you have specific people make their extent to the organization so that you have the right expertise. You don't have security officers out there doing I&C work but you still have the security organization responsible for knowing what the overall security requirements and stuff are.

I think it can work either way. I think you have equally as big a problem if you say that the responsibility has to be totally in a separate organization and you have a disconnect between the two there. So I think that -- the realty is to have the right level of expertise doing the cyber security work where they report -- there's various ways you can do that type of work.

MR. STURZEBECHER: And there's connections between if you have a PLC that's doing a safety system, it has to be locked. You have a physical

element to that to keeping it protected that way. So that's why the tie also.

MEMBER RYAN: But I mean, at that level I'm with Dr. Abdel-Khalik. I don't understand that. I mean, a guy with an M-16 and a padlock is a lot different than a guy who's working at a keyboard, you know, with all the elements of cyber security. I don't see that linkage. I do understand what Mr. Maynard said, you know, managing the two programs can be done at a higher level and you know, there is an integration there of -- you know, across these issues, but at a detailed level, I don't see it.

MEMBER SIEBER: Well, we're suggesting a rule change then.

MS. HERMANN: Yes.

MEMBER MAYNARD: I don't think this is saying that the security officers have to be the one doing the computer work.

(All speaking at once.)

MEMBER RYAN: I don't understand your explanation either.

MEMBER SIEBER: I don't want security organization managing the I&C department either.

MEMBER RYAN: Right.

MEMBER APOSTOLAKIS: The staff has to

modify the dictates of the rule. If we don't like the rule, that's a separate issue.

MEMBER SIEBER: And their fix is to blur it by dashed and solid lines, and I guess that means you can find the skills in your organization, assign it to it and the other becomes the administrator which is okay, I think.

MEMBER APOSTOLAKIS: All right.

MR. STURZEBECHER: So that was the top bullet. The next bullet was one of the other suggestions that --

MEMBER SIEBER: That was mine, too.

MR. STURZEBECHER: -- that we carry security requirements through the supply chain and we were proposing to reword the second sentence so it would read, "Vendor/supplier and maintenance security and developments like life cycles", and that's part of 34.1.1.

VICE-CHAIR ABDEL-KHALIK: Shouldn't that be further modified to include audit to assure that whatever is being required throughout the supply chain is actually being done?

MR. STURZEBECHER: We have a section on audit.

MS. HERMANN: There's a separate section.

MEMBER BROWN: I'm going to give you a clue, okay? When you get down to certain levels and that supply chain, people are just not -- they're just going to say you know, they're not going to put in place anything. That's what we found with our major manufacturers. When they tried to -- when they tried to pass through requirements of this nature to other than the giant Northrop Grumman or the Lockheeds, they'll accept anything as long as they get government money to do something. The smaller guys are reluctant to start putting in place --

MALE PARTICIPANT: They can't afford it.

MEMBER BROWN: -- organizations to manage and have a -- I don't want to call it a bureaucracy but the paper trail and documentation. It's very expensive to do that.

MEMBER ARMIJO: But you can get around that with testing.

MEMBER BROWN: Yeah, we said, okay, yeah, we've got that and we do -- we just do it at a higher level to insure that security. So -- is that in the Rule, by the way? I don't remember that detail being in the Rule.

MS. HERMANN: No.

MEMBER SIEBER: That's part of the Reg

Guide. I think they've addressed it properly because different licensees do this a different way. You know, for example, a software change to your operating system in the plant, typically will come from the vendor and rather than give him a data link so he can put it right in, you have to intercept it, review it, make sure that it doesn't contain Trojan Horses, malware and other stuff and then have your own people install it and test it.

MEMBER BROWN: Yeah, but that's different than what these words say in terms of having these security --

MEMBER SIEBER: Well, you try to get the vendor to do it if you can. On the other hand, you've got to have some kind of backup check in the plant to make sure that, you know, it's your plant.

MEMBER BROWN: Yeah, my only point being, this is a Reg Guide and if that's -- if people perceive these as requirements, that they have to execute, then it becomes -- it can become very defeating relative to trying to get --

MEMBER BLEY: But it is a Reg Guide which means if they really can't carry it all the way down, they can come in and say what they're going to do and then it has to be approved on a case basis.

MEMBER RYAN: Flexibilities could be built into the Reg Guide.

MEMBER SIEBER: It's like buying known qualified equipment. If the vendor doesn't do it, you've got to do it yourself.

MS. HERMANN: That would fall into the --

MEMBER BROWN: The point is, it's rigid. The statement is rigid. I agree with you, you know, Dennis, from the standpoint, yeah, but then you've got to get approval. You've got to wait. You've got to do this. You've got to do that, as opposed to building in flexibility into this -- into the statement like this. Yeah, that's a desirable thing to have everybody down to the guy who makes the chip, you know, not allow any, you know, types of chip manufacturing, you know, allow a tag that you can get in there and pull stuff out or insert some nasty software that nobody knows about, which has happened.

There's been pieces that come in where there's been capability designed into the thing where, you know, somebody can come in that's knowledgeable of the chip design and do stuff that nobody else knows but it's not in the spec sheets.

MEMBER BLEY: Do you believe -- do you believe -- maybe you folks know but many of the

integrated I&C systems that are coming forward in the plants, the vendors claim control through the whole manufacturing process, that they're being done within their organization. So maybe this isn't as onerous a problem as it was for the --

MEMBER BROWN: On the -- when you're developing it, that's many cases you can get that. It's five, 10 years from now that may atrophy somewhat in terms of the ability to get that type of stuff.

MEMBER SIEBER: It depends on how much you're going to integrate.

MEMBER SHACK: A broader range of systems, too, that you're talking about here.

MEMBER APOSTOLAKIS: Okay.

MEMBER BROWN: My only point, it's not very flexible. We can --

MS. HERMANN: We'll work on it.

MR. STURZEBECHER: The next point was about configuration management, the importance. We've added -- well, we believe it's stated in 3.4.1.2 references to Chapter 7 of the SRP on this, the item of configuration management. And there was a comment about adding more definitions to the glossary. We need to add more diagrams and examples. Some of the tables and slides we've shown today will be considered

to be added to the document.

MEMBER APOSTOLAKIS: These examples that you gave though, are not -- maybe I'm wrong, but are not the examples that were in DG-5022, and I'm wondering why not. Those were pretty good. Is there anything bad about those that you really don't want them to be in the Guide?

MR. STURZEBECHER: No.

MS. HERMANN: They're too site specific. They're too technology specific.

MEMBER APOSTOLAKIS: You can go back and clean them up but remember, these are examples. If they specific again, they give a example of the kind of thing you have to worry about. In some other technology, maybe they don't apply. That's why they're examples.

MR. LEE: We absolutely agree with you, Dr. -- if I say your name, I know for a fact that I'm going to say it wrong. So I'm not going to say your name. One of the items that I think Scott Morris, my Division Director, I mentioned was in the process of writing a NUREG CR, clean up this and -- I guess, I'm just -- beef up the examples and we'll provide that as a separate document. So and we'll continuously, if there is something else we could easily --

MEMBER APOSTOLAKIS: You could do that, too, but there is a proliferation of documents here. I mean, I remember in one case there were about seven or eight examples. If you feel that two or three of them are way too specific, take them out but the essence of the examples that were in the Draft Guide was pretty good. So I would recommend that you go back and revisit those and keep whatever you think is a problem.

MR. STURZEBECHER: Thank you.

VICE-CHAIR ABDEL-KHALIK: Is there a group within NRC that will continually challenge the vulnerabilities within the various plants or are you totally reliant on the licensees?

MS. HERMANN: The ongoing inspections will. The ongoing inspections will.

MEMBER ARMIJO: He's talking like actual -- he's --

MALE PARTICIPANT: He's talking cyber text.

MEMBER ARMIJO: Right.

MEMBER SIEBER: Generating Trojan Horses and malware.

VICE-CHAIR ABDEL-KHALIK: Rather than this sort of formal audits.

MS. HERMANN: NSIR has done some Red Team testing already at sites.

MEMBER RYAN: What does Red Team testing mean?

MS. HERMANN: That's the testing against the vulnerabilities. We try to break into a system but they know you're --

MEMBER RYAN: They know you're trying to break in so that's not what he's asking about.

MS. HERMANN: Well, no, what I'm saying is you have their legal permission to break into their system as opposed to just somebody breaking into the system.

MEMBER BROWN: You hire hackers.

MS. HERMANN: Yes.

MEMBER BLEY: But you don't know they're coming at 10:00 o'clock on Thursday.

MS. HERMANN: Right.

CHAIR BONACA: Okay.

MEMBER APOSTOLAKIS: Okay, okay, let's go on.

MR. STURZEBECHER: The second bullet is to show some exploits and that we have them on Slide 8 and 13. That can be added, though they will be dated obviously as things change. The third bullet, add

acceptance criteria. Well, the burden is on the licensee for providing that high assurance.

MEMBER BROWN: This allows the standards to change if you don't have acceptance criteria, so somebody can come in and one licensee gets one set and they say, "Oh, yeah, that's okay". And the next guy comes in a year later and, "Oh, no, no, we want more now". I mean, that's what happens.

MS. HERMANN: It allows -- it allows them to adapt to the changing environment that they have to operate in.

MEMBER BROWN: That's not what I said.

MEMBER APOSTOLAKIS: On some level, though, you have to give them an idea as to what would be acceptable.

VICE-CHAIR ABDEL-KHALIK: Right, high level.

MEMBER APOSTOLAKIS: Huh?

VICE-CHAIR ABDEL-KHALIK: If the acceptance criteria stayed at a high level, then they should remain invariant.

MEMBER BROWN: Yeah, but that's what they think -- it says, "Security control selected is appropriate for the vulnerability it is intended to mitigate".

MEMBER SIEBER: And I think that's as good as you can get because the hackers have full time jobs. They're constantly inventing new ways to get to your system.

MS. HERMANN: Yeah, this is referred to as security assurance evidence. That's where you tie everything together, that you're control is appropriate, it's appropriately resilient and it's continually monitored. So standard criteria that DOD, NSA, et cetera, used to prove that systems are secure. And I can't say any more.

MEMBER APOSTOLAKIS: I guess we have competing requirements here. On the one hand, if you don't give acceptance criteria, it's difficult for people to know what would satisfy you. And there may be inconsistencies from applicant to applicant and decisions. On the other hand, if you do, you have these problems that you just mentioned. So maybe you ought to think about it again, how to strike the right balance here and maybe to up to a higher level or something, because it's not an easy problem. Anything else?

MR. STURZEBECHER: That is it.

MEMBER APOSTOLAKIS: Now, again, I'm curious, our letter of April last year had three

recommendations. One was to do a prep assessment, another one was to do a dependency analysis and the third one is to elaborate a little bit on the plant PRA and how it can be used. And I haven't heard anything about those. I mean, have you decided that these are not worth doing or what? Why are you silent on these?

MS. HERMANN: I think the problem is none of the three of us have seen those -- saw your letter, so we can't respond.

MEMBER APOSTOLAKIS: Okay, the letter is from this Committee April 29, 2008 and it was a comment on the Interim Staff Guidance that preceded this Regulatory Guide. I'm surprised you didn't see it. Who reads our letters, Mr. Chairman? Does anybody read them?

CHAIR BONACA: Could you repeat your question?

MEMBER APOSTOLAKIS: We commented last year on the Interim Staff Guidance that preceded this Guide and all three representatives of the staff say that they are unaware of the letter.

CHAIR BONACA: Well, the letter exists.

MEMBER APOSTOLAKIS: The letter exists. It's in the archives and I think my second comment is

that when you revise the Guide and add this sentence about NEI, I think we will need more than just a presentation to the Committee. We will need a Subcommittee meeting and we already have one in August to review the Research Plan, so maybe you can coordinate with our staff and add one day. Is one day enough?

MS. HERMANN: Uh-huh,

MEMBER APOSTOLAKIS: Add one day. I think Friday of that week --

MS. ANTONESCU: We have three days.

MEMBER APOSTOLAKIS: Huh?

MS. ANTONESCU: We have three days. We have a lot on the agenda already.

MEMBER APOSTOLAKIS: You have to speak to the microphone and say who you are and why you're speaking.

MS. ANTONESCU: I believe we have a three-day meeting for the Subcommittee in August and there are certain activities that you already outlined last time and I think --

MEMBER APOSTOLAKIS: All I said was add a day for these guys.

MS. ANTONESCU: Okay, so a fourth day?

MEMBER APOSTOLAKIS: If it was three

before, it will be four.

CHAIR BONACA: What date is that?

MEMBER APOSTOLAKIS: Tuesday, Wednesday, Thursday as I remember. So I suggest we add Friday.

CHAIR BONACA: What days are those? What are we talking about?

MEMBER APOSTOLAKIS: If we don't do it now, we'll never have the Subcommittee, so it's --

MEMBER BROWN: Is Slide 21 going to be added to the Reg Guide? There was a comment earlier about referring to the NUREG.

MR. STURZEBECHER: That is from 68.47.

MEMBER BROWN: But the suggestion was you incorporate that somehow into the -- that's not in the rest of your notes in here in terms of what you're putting in.

MEMBER BLEY: George?

MEMBER APOSTOLAKIS: Yeah.

MEMBER BLEY: The IMC meeting was August 19, 20, 21.

MEMBER APOSTOLAKIS: Okay, very good and these days are working days, Tuesday, Wednesday and Thursday, right?

MEMBER BLEY: Wednesday, Thursday, Friday.

MEMBER SIEBER: August is our month off.

MEMBER APOSTOLAKIS: Oh, 19, 20, 21, so Wednesday, Thursday, Friday. So maybe we cannot Tuesday. Mr. Stetkar wants to come here for a full week. So --

MEMBER SIEBER: Hey, stay next week.

MEMBER APOSTOLAKIS: Yeah, so we cannot on Saturday, so Tuesday the 18th. That doesn't mean that is your day. We may start with the Research Plan.

MS. ANTONESCU: Right now we set up three days, 19th, 20th and 21st of August.

MEMBER APOSTOLAKIS: Right, we know. Yeah, so we are adding Tuesday, the 18th.

CHAIR BONACA: Yeah, let's discuss the schedule later on.

MEMBER APOSTOLAKIS: Yeah, I know but finding another time will be awfully hard, so let's say tentatively, so it will be a week of I&C.

MS. ANTONESCU: Okay, so this would be a Subcommittee meeting.

MEMBER APOSTOLAKIS: Yes.

CHAIR BONACA: Anything else on this?

MEMBER APOSTOLAKIS: Are we done? Do we need anything else? Okay, very good. Thank you very much. Back to you, Mr. Chairman. Three minutes ahead of time.

MEMBER ARMIJO: Can I ask a question?

MEMBER APOSTOLAKIS: Yes.

MEMBER ARMIJO: Back on your Slide 12, you had that about defense technologies widely available to mitigate threats and you emphasized regulatory constraints being an impediment. What were you trying to get across to us with that?

MS. HERMANN: Yes, this is a quote from the DNI's presentation to the Senate Select Committee on Intelligence a couple weeks ago and the point he was making is that overly-prescript regulations hinder the implementation of current and correct security controls and the example was the regulation that required the of FIPS 140-2 Level 2 Encryption Standards which have already been compromised but in order to comply with the regulation, the industry was still having to use it when they should have moved on to elliptic curve encryption.

MEMBER ARMIJO: Okay, so --

MS. HERMANN: That's the reason why we're not being held fairly prescriptive in our regulation.

MEMBER ARMIJO: Okay, so you're responding to that point.

MS. HERMANN: Yes.

MEMBER ARMIJO: And that's in the Reg

Guide, at least the philosophy --

MS. HERMANN: Yes.

MEMBER ARMIJO: -- approaches. Okay, thank you. I thought there was a problem that we had to address here.

MS. HERMANN: We're taking care of it.

CHAIR BONACA: Thank you for your presentation. It was informative and with that, we're going to take a break for 15 minutes. We'll get together again at 10:30.

(Whereupon, a short recess was taken.)

CHAIR BONACA: Let's get back into session. The next item on the agenda is the Draft Final Revision to 10 CFR 50.61, "Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events", and Dr. Shack will take us through the presentation.

MEMBER SHACK: Okay. We had a Subcommittee meeting yesterday to discuss this alternate PTS rule, and we've had a long history of discussions within the ACRS reviewing the technical basis for the rule. The question - and, again, we've commented favorably on the technical basis for the rule. We think the Staff has done an excellent job considering all the factors that are involved, and

addressing uncertainties, and providing an excellent technical basis.

The rule, I think, will be discussed today. One of the questions is how you generalize that technical basis, which was based on a detailed analysis of three plants, and now we're proposing a rule that could be essentially adopted by any PWR. And that was the focus of yesterday's meeting.

I think the technical basis provides some grounds for understanding why it seems possible to do the generalization. The Staff has undertaken a number of studies that further support that matter of generalization, and, hopefully, they'll discuss that today.

What they are asking for on a plant-specific basis is to evaluate the toughness of the vessel, and that is a very plant-specific sort of thing, and to verify that the flaw distribution in the vessel is identical with the ones used for the three plant study. And we should point out that the three plant study, although it's prototypical in everything as far as the events, and the design of the plant, the flaw distribution in there was taken basically from a study of two vessels that were not the vessels of interest here. And so, even for those plants, you

would still have to undertake a verification that the actual flaw distribution in those plants is comparable to the one used for the technical basis study.

And with that introduction, I'll turn it over to John Lubinski, who will introduce the Staff's presentation.

MR. LUBINSKI: Thank you. Good morning. As stated, I'm John Lubinski. I'm the Deputy Director of the Division of Component Integrity in the Office of Nuclear Reactor Regulation. I appreciate the introduction this morning, and I appreciate the opportunity to have a briefing of the Subcommittee yesterday on this topic.

I'm pleased to be here today to do the introduction of the Staff's presentation on the final rule package for 10 CFR 50.55(a), the Alternate Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events. 10 CFR 50.61(a) is the culmination of approximately 10 years of work by the NRC Staff from multiple offices, including the Office of Nuclear Reactor Regulation, the Office of Nuclear Regulatory Research, the Office of General Counsel, and the Office of New Reactors. And it has been also supported by a number of contractors, as well as industry representatives. This collaborative

effort and the consideration of the diverse views that came to light during these talks is a nasty outcome in the final rule that will be presented today.

We believe that the rule being discussed today represents one of the most comprehensive treatments of a complex, multi-disciplinary issue completed by the NRC. We believe this because pressurized thermal shock involves multiple disciplines, including the consideration of fracture mechanics, radiation embrittlement, thermal hydraulics, neutron transport, probabilistic risk assessment, and in-service inspection.

Our goal today at the end of this presentation is that we hope the Committee will agree that the final rule that the Staff is proposing to publish delivers a sound regulatory structure that will one, primarily, maintain adequate protection against pressurized water reactor pressure vessel failure due to pressurized thermal shock. And, in addition, at the same time, will provide an effective, efficient, and open method for addressing unnecessary regulatory burden placed on some licensees by the current pressurized thermal shock rule, which is included in 10 CFR 61.

I would now like to turn the presentation

to Veronica Rodriguez from NRR's Division of Policy and Rulemaking. Veronica is the Project Manager for this final rule making, and Veronica will introduce the topics that we will discuss today, as well as introduce the additional presenters. Veronica.

MS. RODRIGUEZ: Thank you, John.

As John mentioned, my name is Veronica Rodriguez, and I'm the lead Project Manager for this rule making action. And I would like to start by saying that the rule making action that we're going to discussion today, as John mentioned earlier, is the result of hard work and dedication from many, many Staff members within the Agency. There have been many experts involved in this rule making action from thermal hydraulics, mechanical engineers, material engineers, PRA experts, attorneys, branch chiefs, like I said, numerous amount of employees within the Agency. So I would like to give special thanks to the active members of the Working Group, Barry Elliot, Matt Mitchell, Steve Dinsmore, Lambros Lois from NRR, Mark Erickson Kirk, Bob Hardies from Research, Nihar Ray from NRO, and Gary Mizuno from OGC.

I would also -

MEMBER APOSTOLAKIS: What did you call those, Veronica?

MS. RODRIGUEZ: I'm sorry?

MEMBER APOSTOLAKIS: What did you say they were?

MS. RODRIGUEZ: Working Group members.

MEMBER APOSTOLAKIS: Special thanks.

MS. RODRIGUEZ: These are the active members of the Working Group. We also have other members that are not actively participating in the Working Group; like, for example, the rule making staff in the Office of Administration, and the Information Collection Team in the Office of Information Services, so we also need to thank them for all the help that we have received from them.

I would also like to recognize the participation of Mr. Bill Arcieri, who's here from ISL. He's going to be helping us with questions that we get on thermal hydraulics.

So, today we're going to discuss three main topics - I'm sorry - four main topics. The first one, we are going to be talking about the technical basis of the rule making. Then we're going to move on and talk about the generalization study, which is a study that we made, that led us to the conclusion that the data and the results obtained from the technical basis can be applied to the operating fleet of PWRs.

Then we're going to be talking about the current PTS rule, and the motivation for developing the alternate PTS rule. And then we'll provide a quick overview, and highlights of the alternate PTS rule.

With that, I'm going to ask Mark Kirk to provide you an overview of the technical basis.

MR. KIRK: Okay. Thank you, Veronica.

What I'm going to do in, I suppose, about a half a dozen to a dozen slides, is review the technical basis work, and also the findings of the generalization study that led to the Office of Research, its contractors, and our colleagues in the nuclear power industry to issue a series of reports dating back to about 2004, that formed the basis that the NRR and NRO rule making teams used to craft what's now become 10 CFR 50.61(a).

The slide in front of you -- so, the first set of slides concerns the technical basis leading us up to our proposed reference temperature limits, and now appear as a table in 10 CFR 50.61(a). I believe it's Table One, if I recall. And then, after that, I'll give some insights on generalization, which is a broad overview of the basis for the Staff's conclusion that these reference temperature limits can be applied to the whole operating fleet of PWRs currently

operating in the United States.

So, to start with this figure and work it through, this shows how we, at a high level, how we performed the calculations that led us to upper temperature screen limits. If I could direct your attention to the large black box headed, "Probabilistic Estimation of Through-Wall Cracking Frequency", the analysis starts with a PRA event sequence analysis, considers both PRA and human factors. There are two main outputs from that. The definition of sequences that could lead to over-cooling events with and without pressure, and, also, the PRA analysis quantifies the frequency with which those sequences are expected to occur, and the uncertainty in those frequency estimates. Leave the second aside for a minute, we'll get back to that.

The sequence definitions then pass to a thermal hydraulic analysis, which we perform using the code RELAP. That models the primary and secondary systems of the plant to allow an estimate of the temporal variations of pressure, temperature, and heat transfer coefficient on the downcomer of the RPV. That's then passed as input to the probabilistic fracture mechanics analysis. The code is called "FAVOR". FAVOR also has a number of other inputs,

most notably, as Dr. Shack mentioned, the flaw distribution, material properties, fluence variation, design information, and a host of other things that aren't shown at this high level. But based on all of that input information, and various models of material behavior, FAVOR estimates what we call the conditional probability of through-wall cracking. It's conditional in that it's conditioned on the event occurring, so those conditional probabilities are then matrix multiplied with the sequence frequencies, which I ask you to remember for a moment, to estimate the yearly frequency of through-wall cracking. So we could run that analysis conceptually for a plant after some duration of operation.

What we did in our analysis, which I'll discuss on the next slide, is we performed that type of analysis for multiple plants after multiple times of operation to get a relationship between the through-wall cracking frequency, and the level of embrittlement in the vessel. And that's what's shown by the green upward sloping line.

Then we can compare that variation with an acceptance criteria on through-wall cracking frequency that was established consistent with Commission safety goals and policy statements at one times ten to the

minus six events per reactor year to derive an embrittlement-based screening limit.

And then, as the gray box says, the last step is to assess whether or not we felt confident that those screening limits could be applied -- that those same screening limits could be applied to all operating PWRs in the U.S., or if they needed to be somehow tuned, shall we say, say different manufacturers, or whatever. But I'll get into that in a minute.

MEMBER BLEY: Mark, before you leave this one.

MR. KIRK: Yes.

MEMBER BLEY: Could you just explain the detail for me now of the little picture there. You picked ten to the minus six.

MR. KIRK: Yes.

MEMBER BLEY: And the actual screening limit corresponds to the -- based on the curve that's the sum of all of the contributions?

MR. KIRK: Yes. The green line is the -- so, let's just talk about the green line, as if it was just one plant.

MEMBER BLEY: Okay.

MR. KIRK: So we take a plant, and we,

essentially, increase time to increase embrittlement. So we analyze the plant at 32 EFPY, 60, and so on until we get up to -- so the increase in time, a major factor that you're changing. In fact, the only factor in our analysis that we're changing is the embrittlement, so the embrittlement is going up, which means the conditional probability of through-wall cracking for each of the sequences we've analyzed is going up, but the event frequencies are remaining the same. So, for any given plant, there would be one green line. And then, as you know from our discussions yesterday, we analyzed three plants in detail, found out that the three green lines for those plants were all pretty close to each other, and then we went to the generalization step to make the leap. We feel that result will be consistent across the plants. Each green line for each plant represents the sum of all the PTS challenges that were identified by the PRA.

MEMBER APOSTOLAKIS: Why is it a single green line? I mean, is there a -

MR. KIRK: Well, we'll -- because it's a cartoon.

(Laughter.)

MEMBER BANERJEE: Well, you're going to

discuss it on the generalization, right? How you take this -

MR. KIRK: Yes. And, in practice, our results, there are three green lines. But, like I said, they're close together.

MEMBER APOSTOLAKIS: I mean, for each plant shouldn't there be some uncertainty there?

MR. KIRK: Oh, yes. Again, I think I'll get back to my statement, that because it's a cartoon. I think that's a good -

MEMBER APOSTOLAKIS: Now, I know that ten to the minus six is something that has been used a lot. Is that part of the regulations, the ten to the minus six for the -- this is the vessel. Right?

MR. KIRK: This is the vessel. The ten to the minus six does not appear in 10 CFR 50.61(a). The reference temperatures that were derived, what's called the screening limit there, the yellow box. The reference temperature screening limits that were derived from our technical basis results do appear in the regulation, and so they correspond to ten to the minus six, but there's no actual mention in 50.61(a) of a ten to the minus six value. You have to -- but it's there. It's in the technical -

MEMBER APOSTOLAKIS: You can infer it.

MR. KIRK: Yes, you can infer it.

MEMBER SHACK: It's in the Statement of Considerations.

MR. KIRK: Yes. That's correct.

MEMBER APOSTOLAKIS: And this is only for the vessel.

MR. KIRK: This is only for the vessel. That's right.

MEMBER SIEBER: And this applies only to existing plants.

MR. KIRK: And this applies only to existing plants. That's correct.

MEMBER SIEBER: Ten to the minus six per reactor year becomes one times ten to the minus four through the fleet, two times ten to the minus three for the fleet through their lifetime.

MR. KIRK: Yes. If all the plants in the fleet through their entire lifetime were operating at the reference temperature limit, which is -

MEMBER SIEBER: With the flaw distribution.

MR. KIRK: With that flaw, yes.

MEMBER SIEBER: Okay.

MR. KIRK: Assuming everything is correct.

MEMBER BLEY: And the last question along

that line for me is, for a particular plant now, you could draw another line on here that would tell me where that plant is on the embrittlement scale at 60 years lifetime.

MR. KIRK: Yes.

MEMBER BLEY: And can you say anything about where that falls for any one of the plants we looked at?

MR. KIRK: Yes. Sure.

MEMBER BLEY: And how far below the red line that is?

MR. KIRK: And since with plasma screens, I can no longer use my laser pointer. I know how to go back to using a stick. I mean, they're all down here. They're in the ten to the minus seventh range.

MEMBER BLEY: So, at least an order of magnitude below the -

MR. KIRK: Yes. And, unfortunately, I don't have it on this plot. I have it on another -

MEMBER APOSTOLAKIS: You can use the cursor, though.

MR. KIRK: Yes. I have it on another plot. Well, there's no scale on that. I'm pointing to a cartoon. The highest -- the plants that were closest to the screening limit clocked in at 60 years,

if memory serves, at like two times ten to the minus seventh.

MEMBER SHACK: In 1806 there's only one plant that's above one times ten to the minus eight at 60 years.

MR. KIRK: At 60?

MEMBER SHACK: Yes.

MR. KIRK: I can have the figure here in a second.

MEMBER SHACK: Okay.

MEMBER BANERJEE: This flaw distribution doesn't change with lifetime of the plant.

MR. KIRK: You're right. The flaw distribution -- no, there are no active sub-critical damage mechanisms that would cause the flaws to get bigger.

MEMBER BANERJEE: Or new flaws to form.

MEMBER SIEBER: Characteristics do change.

MR. KIRK: Or new flaws to form, yes.

MEMBER SIEBER: But characteristics do change.

MR. KIRK: What's that? The material characteristics change.

MEMBER SIEBER: Yes, like embrittlement

changes with -

MR. KIRK: Yes. But the embrittlement, it's -- irradiation embrittlement is irradiation strengthening. You're increasing the strength of the material, so you're pushing it farther out on the transition temperature scale. You're not spawning new defects.

MEMBER SIEBER: Right.

MR. KIRK: Yes.

VICE CHAIR ABDEL-KHALIK: If the applicant were to use a different thermal hydraulic analysis tool than RELAP, with different downcomer mixing model, for example, could the outcome of this screening process be affected?

MR. KIRK: We don't believe so. And I think that gets to the generalization, that the transients that matter most are invariably the larger break transients, where the detailed differences of the thermal hydraulics don't really have a very large impact on the structural integrity analysis. But I should also point out, and I don't know if you meant to imply this or not, but if an applicant comes in and wants to apply 10 CFR 50.61(a), our colleagues in NRR are not requesting that they do a thermal hydraulics analysis. They don't have to do a thermal hydraulics

analysis, and I'll get to that. Maybe we can go to my next slide. Well, the next slide. Never mind.

All we're asking them to do is to calculate to be informed about the embrittlement state of their vessel, to calculate how embrittled their vessel is that gives them what we call reference temperatures that are then compared to reference temperature limits. If the calculated reference temperature for a plant falls below the reference temperature limit stated in Table One of 10 CFR 50.61(a), they're good to go. They don't have to do a thermal hydraulic analysis, or a PRA. That's not a requirement. Of course, they can. There's nothing that precludes them from doing so, but they're not required to.

MEMBER SIEBER: But they do have to know what their defect -

MR. KIRK: They have to know what their defect population is, and they have to know about the embrittlement state of their material.

MEMBER SIEBER: Right.

MEMBER SHACK: And, we should point, they did try to assess the model uncertainties, as well as the parametric uncertainties associated with that thermal hydraulic analysis.

MEMBER APOSTOLAKIS: Are you going to talk about that, Mark?

MR. KIRK: The what?

MEMBER APOSTOLAKIS: Model uncertainty.

MR. KIRK: I was hoping not to, but -

MEMBER SIEBER: Yes.

MR. KIRK: We can try.

MEMBER SIEBER: For what, the thermal hydraulic?

MEMBER SHACK: There's only an hour and a half, George.

CHAIR BONACA: Yes, let's stay -

(Off the record comments.)

MEMBER APOSTOLAKIS: For some reason, these have been reviewed before. I don't know why, I know there have been presentations in the past. Maybe Mark can outline the approach.

MR. KIRK: Let me see if I can do that as I go through.

MEMBER APOSTOLAKIS: Yes.

MR. KIRK: Okay. So I've lost track of where I was. Okay. So that's our overall approach. Detailed analysis of three plants, compared with, essentially, a policy limit on through-wall cracking frequency gives us some provisional reference

temperature screening values that we then do some further analysis on to convince ourselves are generally applicable to all plants.

VICE CHAIR ABDEL-KHALIK: I think, I find it very difficult to understand how you can come up with a general rule without calculating specific temperature limits using a thermal hydraulics model for a plant. After all, whatever rule you come up with is based on calculated temperature histories, and whatever material properties exist pertain to specific material performance at, presumably, a measured temperature.

MR. KIRK: I'm sorry. I'm not quite sure what question you're asking.

VICE CHAIR ABDEL-KHALIK: I guess that just relates to the issue of model uncertainty.

MR. KIRK: If I can get through the generalization, I think what we'll find out is that, again, the -- we analyzed a wide variety of challenges that were identified by the PRA analysis. And what we found out in each and every case is, you need to have a very severe challenge to even calculate a probability of crack initiation or failure. And those severe challenges, like, say, a large break LOCA, the degree of challenge is very, very similar from plant,

to plant, to plant across the USA, because once you punch, say, an eight inch hole in the side of the vessel, the depressurization is very rapid. The thickness of the vessel wall is all about the same. The vessel can't cool as fast as the primary water inventory, anyway, so the level of thermal stresses from a large break LOCA are, I think, defensibly stated as being similar across all the plants. And the nuances I think that - and, I'm sorry, I might be going on and not even touching your question, because I'm guessing it is one of two questions - the nuance differences in the thermal hydraulic analysis just simply don't matter at that point.

Once you get -- what we found out is, once you get beyond a break diameter of about five inches, the cooling rate of the water inventory in the primary system is so fast that the vessel wall can't keep up. The vessel has a much slower --

MEMBER SIEBER: Thermal inertia.

MR. KIRK: Has much more thermal inertia. The vessel can't cool as fast, and so now the stress state in the vessel, which is what's going to drive the flaws to failure or not, depends on only two things. It depends on the coefficient of thermal expansion of the steel, which is a physical property

of the steel; and, therefore, has exceedingly little uncertainty, and the diameter and thickness of the vessel, which if you look across the whole PWR fleet is very, very similar. So the differences that yourself and our other colleagues in thermal hydraulics are used to seeing cause havoc on thermal hydraulic traces of differences of injection water temperatures, and when operators act or don't act, or a whole host of other things, and I apologize. I'm not a thermal hydraulic specialist. The vessel doesn't know about them. It can't know about them.

MEMBER SIEBER: And the interesting thing is, in a large break LOCA, you can't repressurize very much.

MR. KIRK: That's right.

MEMBER SIEBER: In a small break LOCA, you can't cool it down fast enough, even though you can repressurize.

MR. KIRK: Yes.

MEMBER BANERJEE: So, I guess, high embrittlement, what you're saying makes sense. And maybe, Said, it doesn't really matter because things go so fast.

MEMBER SIEBER: That's right.

MEMBER BANERJEE: It's all -- the heat

transfers into the vessel is controlled on the vessel side. You just change the boundary condition.

MEMBER SIEBER: That's right.

MEMBER BANERJEE: Virtually instantaneously.

MEMBER ARMIJO: Well, it's really independent, really. They only can cool, whether you have flaws or radiation damage, or whatever. It's the stress that you can build up by the event.

MEMBER BANERJEE: I think it's more subtle than that.

MEMBER ARMIJO: And the variable is, if you have different degrees of embrittlement, you'll have different responses.

MEMBER BANERJEE: Yes. It wasn't the fact that it was deep down in the vessel, where things are mixed, well mixed. It would matter, so what -- if you look at the fine structure of this, what I understood yesterday, which he's going over lightly, is because this is deep into the downcomer, where this high embrittlement occurs, that, therefore, the mixing is pretty good, if you look at new PTF and all these things. So the fine structure of the plumes coming down and all that stuff gets washed out. And as far as I can tell, there is a significant database that

supports that.

Now, that's because of the criteria they're taking, which is through-wall cracking. So if you take a different criteria, you're going to get a different answer on this. But assuming that this criteria is okay and stuff, it's going to be fairly well mixed, and there's not going to be these plumes and things, so this all gets washed out, and the problem gets shifted to large break LOCA, than small break LOCA. It's sort of a sleight of hand in some ways, but that's what happens.

MEMBER ARMIJO: I wouldn't call it sleight of hand. It's just that's the way it worked out.

(Simultaneous speech.)

MEMBER BANERJEE: Well, the criteria, really. I mean, if you take a different criteria, you're going to get a different answer.

CHAIR BONACA: So let's move on.

MR. KIRK: Okay. And I hope -- well, we'll see, I'm sure the Committee will ask questions. I hope some of these questions are addressed in the generalization.

So, our approach involved, first off, a very detailed study of three different pressurized water reactors. Our sample set included Palisades,

Beaver Valley Unit One, and Oconee Unit One. Here, we have representation from all of the PWR manufacturers. We have one plant, namely, Oconee, from the original 1980s PTS study that formed the technical basis for the current rule. And we have the other two plants, Palisades and Beaver Valley, who are very close to the current PTS screening limit at the end of their 40-year licenses.

And then in terms of generalization, we'll get on to that later. But we then expand -- first off, we drew insights based on the three detailed plants' analyses of what transient classes were important, versus were not important. And then we looked at what the important factors were that were driving the bulk of the risk in five more high-embrittlement plants to see if there were any major differences from the three that we looked at in detail. I'm sorry. We go on to the next one just to summarize, and then we'll get into some of the details. I think I've said the first bullet point before.

What we find out, is that only the most severe transients contribute to risk. The characteristics of those transients are very similar across the operating PWR fleet. And, also, operator

actions, while we did account for them in our analysis, are not very important to the scenarios that dominate the risk; and, therefore, that dominate the -- how we set the reference temperature screening limits.

CHAIR BONACA: I seem to remember the Oconee regional analysis were dominated by steam line breaks with no operator action intervention.

MR. KIRK: Right.

CHAIR BONACA: So you have extended cool-downs, and so, now, it seems to me that in this case, operator action makes a big difference.

MR. KIRK: I would have in the original analysis, it wouldn't in our's, and we'll -- I think I'll just go ahead so that I'm not talking to a blank screen.

What we find out in our analysis is the main steam line breaks contribute between nothing and about 10 percent of the total through-wall cracking frequency, which you're correct to point out is a very big change in our perception of what transients dominate risk from the understanding of the 1980s. And the major reason for that difference is that the 1980s main steam line breaks were very conservatively modeled. Of course, since the main steam line is one

of the largest pipes in the plant, once you severe that, you get a screening fast cool-down rate, but the major difference between the old analysis and our analysis is in the old analysis, that very fast cool-down rate was taken all the way to ambient temperature, all the way to like 75 degrees Fahrenheit. Whereas, in our analysis, we recognize that the physics of the plant prevent the temperature in the primary from falling below the boiling point of water. And, so, in our main steam line break analyses, the temperature in the primary didn't fall below 212 degrees Fahrenheit. And that makes a big difference on the embrittlement side to the point that the effect of the transients is relegated to something that's, indeed, very minor.

The other thing, since you brought up operator actions, in our analyses, operator actions were credited. And, again, this is not my area, so I might be a little bit vague here. My understanding is that operator actions were credited conservatively, operators were assumed to act at 30 and 60 minutes. But our structural analysis tells us that if a failure occurs due to this type of transient, it occurs within the first five to ten minutes. So even though operator actions were credited, and this is not to say

that operators are a bad thing, or the actions that they take are bad things. They're very critical to the plant integrity, but in terms of this event sequence, whether or not we credited operator actions has absolutely no impact on the through-wall cracking frequencies from these type of transients.

CHAIR BONACA: I'm totally in agreement on the use operator action, particularly for a BNW plant, where you have a very clear understanding of the cool-down, we have feedwater was assumed to be there in our condition. There was no isolation, so you drove down the temperature as low as you could, and then you repressurized. And I agree that that's reasonable, but I'm saying that operator action in a particular case makes a big difference, it seems to me.

MR. KIRK: For a particular case, that's right. And I think we'll get back.

CHAIR BONACA: Okay.

VICE CHAIR ABDEL-KHALIK: Excuse me. Before you leave this slide, you indicate that the temperature in the primary cannot fall below boiling point. If safety injection was initiated on low pressure on the primary, would that statement still be true?

MR. KIRK: I'm sorry. I might have to

defer to one of my colleagues at the side table for that.

MR. ARCIERI: Generally, what we saw is that if you do start your safety injection because of primary size shrinkage of the coolant, it will repressurize, and basically cut it off, so you just won't get that much water into the system.

VICE CHAIR ABDEL-KHALIK: For steam line break?

MR. ARCIERI: For steam line break.

MEMBER ARMIJO: Well, I mean, when -

MEMBER STETKAR: I'm sorry. What high pressure injections will be repressurized and shut off, if I have a viable high pressure injection -

MR. ARCIERI: The system is going to shrink. Okay?

MEMBER STETKAR: I know. If I have a high pressure injection system that can pump water into the code safety valve pressure, that system will not shut off until I get to the code safety valve pressure. And several plants have those.

MR. ARCIERI: Yes. Okay. I stand corrected. I'm sorry.

MEMBER STETKAR: So I wanted to get that second thought in there.

MR. ARCIERI: Okay. No, I stand corrected.

MEMBER MAYNARD: Those systems are also a very low volume system, the pressures are fairly low.

MEMBER STETKAR: It depends on the plant. That's just before -

(Simultaneous speech.)

CHAIR BONACA: The point I want to make is that the -

MR. ARCIERI: My point is, though, I don't think you're going to be injecting so much water into the primary from the HPI that you'll have significant cool-down below 212 degrees or so.

MEMBER SIEBER: There is still a rate of -- a change in the rate of decline of heat once boiling starts.

MR. KIRK: Yes. Absolutely.

MEMBER SIEBER: Because of heat vaporization. One of the plants that they modeled in detail was one that you're talking about, where they have high head injection that will go up and look at safety. So, from that standpoint, what they modeled is conservative.

MEMBER BROWN: 212 - I guess I've still got the same questions. I don't know why the bottom

is - I didn't understand why the bottom is 212. The previous analyses took you clear, much colder.

MR. KIRK: I think, and, again, I might have to be -

MEMBER BROWN: I didn't understand it.

MR. KIRK: Yes. I might have to be deferring to Mr. Arcieri from ISL. But the -- I think, Bill, what you're saying is there is some direct injection into the primary during a main steam line break, but the volume is very small. The volume of the injection is very small relative to the overall volume of the primary.

MEMBER BROWN: Yes, but you've still got your blown-down system, your coolant. What stops the cool-down?

CHAIR BONACA: One of the things that could add to that is those transients in the BNW plant, was the steam generator having very little inventory, and you're flushing through, and cooling down very fast on the primary side. I mean, that was the reason why you have those steam line breaks being pretty limiting for those plants. They have disappeared from the table in the new analysis, and the reason is that operator action is credited, it seems to me. I mean, at least when we got the

presentation from the Professor from Maryland, the early -

MR. KIRK: Dr. Maderas.

CHAIR BONACA: Right.

MR. KIRK: Yes.

CHAIR BONACA: Those disappear from the table, and the LOCAs have become dominant now. And I agree with your results of that, because operator action is totally acceptable to me for the steam line break of that type. I just was arguing about the statement that operator action really was not important.

MR. KIRK: Well, all I can say, that I'm absolutely sure that I remember from our analysis is the earliest that operator actions were credited, and you can certainly debate, and it has been debated as to whether this is an appropriate time or not; the earliest the PRA analysis said that operators were allowed to act in response to a main steam line break in our analysis was 30 minutes. So that's included, that insight, that model is included in what Bill Arcieri and his colleagues at ISL modeled through RELAP. So that's part of the pressure temperature and heat transfer coefficient traces that went to FAVOR. When we feed those pressure temperature and heat

transfer coefficient time variations into FAVOR, what FAVOR, the structural mechanics code, tells us is that if the vessel is going to fail, it fails within five to ten minutes or never. So the fact that the operator - and that's the basis of my statement - is that, the fact that the operator is doing something out at 30 minutes doesn't matter, because by then, the severe thermal stresses that were generated in the first five to ten minutes, which have resulted in some very small proportion of vessel failures, has started to die away, and from a structural viewpoint, the operator action isn't influencing our outcome. Again, it doesn't mean operator action is a bad thing to do, it just hasn't influenced our numbers.

CHAIR BONACA: Okay.

MEMBER BANERJEE: Mark, perhaps you repeat - I think I get it, but why the temperature cannot fall below 212. Charlie asked the question.

MR. KIRK: Yes, I didn't.

MEMBER BANERJEE: So can you give us the -

MR. KIRK: I didn't get to the end of that. And, again, I might be deferring to Bill here, if I get tripped up.

First off, there is a small amount of

direct injection into the primary in response to a main stream line break. However, the amount of that injected water is very small relative to the overall primary volume. So it's, in some ways, fighting a losing battle. Secondly, the main steam line breaks, so you're getting loss of coolant out of the secondary side. The steam generator is ultimately going to boil dry, but while it's in the process of boiling dry, the temperature in the generator is 212. The primary is thermally coupled to the secondary through the steam generator tubes, so there's no driving force to take the primary below 212. Did I get that?

MR. ARCIERI: This is all true, and we also have to remember that you have a second steam generator that's basically full of water.

MR. KIRK: That's true, which is keeping the temperature even higher.

MR. ARCIERI: And it's just going to sit there hot, and just gradually cool down.

MEMBER BANERJEE: So, does that answer your question, Charlie?

MEMBER BROWN: Yes, I think so. I get the point now. Yes.

MEMBER MAYNARD: I believe the 212 -- my question, any localized effects. I haven't had direct

vessel injection, so I'm not sure exactly where that goes into some of these, because there would be a localized effect for the cold water that would be injected at that point.

MR. KIRK: Perhaps -- well, where is the water injected when it's injected, Bill?

MR. ARCIERI: The water is injected into the lines. We didn't look at direct -

MR. KIRK: Yes.

MEMBER SIEBER: You have a choice between hot leg and cold leg injection. I think it goes into the hot leg first.

MEMBER MAYNARD: Well, I understand it's going to the leg. Some of these plants do have a direct vessel injection.

MEMBER SIEBER: Yes, none that was specifically examined.

MEMBER MAYNARD: That would have -- if a plant had direct vessel injection, that the localized effects would have to be taken into account. I understand. Most plants, you have hot leg, cold leg. And it's certainly going to be mixed by the time it gets to the vessel. But if you have direct vessel injection, you could have the potential for a localized effect that would have to be accounted for.

CHAIR BONACA: All right. We need to move on.

MS. RODRIGUEZ: Yes. If I may, I would suggest to go back to the technical basis, and then progressively walk our ways towards the generalization studies. We will go back to the main steam line breaks and the LOCAs.

MR. KIRK: Yes. You'll get another shot at that. I'm trying to remember where I got off this. Okay.

So the most severe transients model contribute virtually all the risk, and we'll talk more about that in a minute. The axial flaws and their associated material properties dominate the risk, and there's a preference here to axial versus circumferential flaws, because of the cylindrical geometry of the vessel. The probability for crack initiation, if crack initiation occurs, for an axial in a circumferentially-orient flaw, because the flaws are very small, and the vessel is very thick, is essentially the same. However, as the vessel initiates and starts to grow, if it's circumferentially-oriented, there's a natural crack mechanism that's borne of the geometry of the vessel, basically, the driving force just dies off when the

flaw is about a third of the way through, and it stops. So it doesn't meet our through-wall cracking failure criteria. Whereas, the axial flaws, as they get bigger and bigger, the driving force just keeps going up, and up, and up, and they would, under some circumstances, punch all the way through the vessel.

MEMBER BANERJEE: These flaws are mainly in the welds. Right?

MR. KIRK: Yes. Well, yes. We have two flaw populations. We have actually -- I'm sorry, this is getting more complicated.

The largest flaws and the most populous flaws are associated with the fabrication, be they circumferential or axial. There's then a smaller density population of flaws that's in the plates, well, small in number density, but bigger in absolute numbers, because you've got a lot more plate real estate. But they're about a factor of five smaller in physical size than the axial flaws. And then you also have the potential for surface breaking flaws oriented circumferentially due to lack of fusion defects between the adjacent passes of the austenitic stainless steel welds, and in some rare cases you could have subclide cracks.

CHAIR BONACA: All right.

MR. KIRK: And our screening limits treat the peculiarities of all of those flaw distributions, which we'll get to in a second. So maybe we can just go to the screening limits.

These are -- first off, I should say, I've got one of these graphs for -- I'm sorry. I have one of these graphs for PWR vessels that are constructed from welded plates, and then the next one is for ring-forged vessels. So for welded plates, what we have is the requirement for the licensee to calculate two embrittlement parameters, the maximum embrittlement of their axial welds, which is shown on the horizontal axis. The symbol is RT MAX-AW, and the maximum embrittlement of their plates, that's on the vertical axis. And then the red curve is, essentially, our criteria, our one times ten to the minus six limit, and this curve doesn't appear in the rule. It's been expressed in tabular form.

But, anyway, what the graph gives you is, if a particular plant is inside the curve, that means their estimated through-wall cracking frequency in this case at the end of 48 EFPY, or almost 60 operating years, is projected to be below one times ten to the minus six. Whereas, if somebody was outside of the curve, which you see nobody is, then

they would be projected to be above the screening limit, and would have to take some action. So the curves on here, and the blue lines represent what we're proposing as being the regulatory reference temperature limits. As you can see, there are two different graphs. Those limits depend on the thickness of the vessel wall, and that's because thicker vessels are stiffer, so they generate more thermal stress. And then the individual dots here are an analysis of all the plants now operating at 48 EFPY, so almost 60 full operating years, using the information that's currently been docketed with the NRC in terms of the vessel material characteristics, meaning their initial toughness, their chemical composition, and their fluence. And, as you see, everybody -- what we find out is everybody is safely inside the limits pretty much to the end of first license extension.

We have a similar graphic depiction of the tabular limits that are in the rule for forged plants. Now, in forged plants, of course, you don't have axial welds, so you don't have the embrittlement associated with -- you don't have a limit associated with axial welds. So, in that case, the licensee is asked to calculate, or estimate, I should say, the

embrittlement associated with their circumferential weld, which is depicted on the horizontal axis, and the embrittlement that's associated with their forging, which is depicted on the vertical axis.

There's a little bit more complexity here than in the last graph. The blue lines are the outcome of our technical basis calculations, and our graphical depiction of the table that's in the rule. The individual points show our assessment similar to those on the last graph of where the ring-forged plants are at 48 EFPY.

The reason why there are two different limits on the maximum allowed embrittlement for a forging is there are different limits here depending upon the flaw population. The upper limit would be appropriate for a plant that can demonstrate that it's in compliance with Regulatory Guide 1.43, which essentially says that we don't have reason to believe that that vessel is susceptible to sub-clide cracking. The lower limit would be if they couldn't demonstrate compliance. But, again, as you see, none of the plants have a problem, even out to one license extension, even if they were to have sub-clide cracks, and that's based on a very conservative model. Yes, sir?

MEMBER SIEBER: I have two easy questions, I think.

MR. KIRK: Good.

MEMBER SIEBER: One is, in the fabrication of the forged vessels, is there a circumferential weld in the vicinity of the core, or is it at the top and bottom of the core?

MR. KIRK: I think that's a vessel-specific feature that I wouldn't want to make a general comment on. I think the aim is to certainly keep them away from the core.

MEMBER SIEBER: Yes. That's why they -

MR. KIRK: Yes, but in any event, our screening limits would take account of that. You would be monitoring the embrittlement at the location of the weld.

MEMBER SIEBER: My second question is, does underclad cracking affect your analysis in any way?

MR. KIRK: Yes, indeed it did, because underclad cracks are a different flaw population entirely. And, so, we did specific analyses of vessels with underclad cracks, and that was the basis for the - and I'm just trying to pull a number off the graph - roughly, 250 degree Fahrenheit screening

limit on underclad cracks. Yes.

Also, one thing I should point out just as a brief, and I'm sure not complete response to Dr. Apostolakis' question on uncertainty. Just as a practical matter, this limit that we're drawn here on one times ten to the minus six per reactor year is based on the 95th percentile of the through-wall cracking frequency distribution.

MEMBER APOSTOLAKIS: Which frequency?

MR. KIRK: The 95th percentile of the through-wall cracking frequency distribution. So we've used an upper bound value, not a mean value.

VICE CHAIR ABDEL-KHALIK: Physically on this graph, why would there be a limit on the sum of the two RT values?

MR. KIRK: All that's saying is, if this curve wasn't a curve, but if it was a pure box, then there would no interaction between the two. But, clearly, I mean, if you draw a box and you project up here, you can come to a situation where you meet the limit on the axial welds, you meet the limit on the plates, but you could be out here; and, therefore, in the space where you're above one times ten to the minus six.

VICE CHAIR ABDEL-KHALIK: I guess my

question is, why is it a curve? I mean, after all, you're analyzing an individual crack.

MR. KIRK: But it's just saying that if you're getting a probability for through-wall cracking arising from flaws in your plates, and flaws in your axial welds, and if you use it all up in one place, you can't use it in another.

MEMBER BANERJEE: In that region, you've got both types of cracks being important, I take it. That's why it's -

MR. KIRK: Yes.

MEMBER BANERJEE: -- sort of curving around. Okay.

MEMBER RAY: You said the 95th percentile was an upper bound. Why is that?

MR. KIRK: Why is it an upper bound?

MEMBER RAY: Yes.

MR. KIRK: You mean like why not the 99th?

MEMBER RAY: Why is the 95th percentile an upper bound in this case, yes, for analysis purposes?

MR. KIRK: I'm tempted to make a flip comment, so I'm going to suppress that.

MR. KIRK: Is your question, why is 95 high enough?

MEMBER RAY: Yes.

MR. KIRK: Okay. Well, one is because it's a screening limit. This is not an absolute limit after - and I think this may be the best answer I can come up with on short noticed - it's a screening limit. It's not a limit above which failure occurs. And, moreover, if any -- if the plant that's represented by any of these dots projects themselves to be on the blue line, they're required by law to send a letter to my colleague, Mr. Mitchell, three years in advance of that happening. So I think, to me, the notion that this is a screening limit says that we don't have to be sure that absolutely everything is under the curve. But that's a -- I guess I'd have to say then, that's a policy decision, which you should express your opinions to our Commissioners on.

MEMBER RAY: Well, that's why I asked the question.

MR. KIRK: Yes.

MEMBER RAY: It's a choice that's made.

MR. KIRK: It's a choice, yes.

MEMBER SIEBER: I have a follow-up question to that.

MR. KIRK: And if I could just interject, it's a choice that's inconsistent, and more

conservative than our standard approach in PRA analysis of using means.

MEMBER RAY: Well, that's a whole other discussion I don't think we want to get into.

MR. KIRK: Yes.

MEMBER RAY: But for this purpose, anyway, 95 percent was selected.

MR. KIRK: Yes.

MEMBER RAY: Some other value could have been used.

MR. KIRK: Absolutely. Yes.

MEMBER RAY: Okay.

MEMBER BANERJEE: Ninety-nine could have been.

MEMBER RAY: I always use the -- excuse me, Jack. I always use the fact that in our economy today we're observing how things sometimes fall outside the 95 percent confidence level.

MEMBER SIEBER: Economics is not engineering. My question revolves around Harold's question, and that is that if you have 95 percent confidence of the screening level, you get margin out of the three-year notification. On the other hand, you must have margin beyond what you expect that absolute value to be. Have you evaluated that

additional margin, or do you feel confident -

MR. KIRK: Not quantitatively, but qualitatively. And some of our previous discussions with members of this Committee, I tried to emphasize that while we've taken a very comprehensive look at the detailed models that went into all the PRA, GH, and PFM -

MEMBER SIEBER: They're all conservative.

MR. KIRK: Well, where we suffered from lack of knowledge, which was in many areas, we've adopted conservative models. So I think it would be appropriate to characterize this as we're approaching the 95^{th} percentile of a distribution of calculated values that's based on models that where we had inadequate information, we made inherently conservative judgments.

MEMBER SIEBER: Now, my memory of the embrittlement curves to fluence is that they have a sort of an exponential shape, so in the later years where this becomes important, the rate of change of embrittlement, continuing fluence becomes less and less.

MR. KIRK: That's right. There is something of a saturation effect.

MEMBER SIEBER: That's right.

MR. KIRK: Yes.

MEMBER SIEBER: Thank you.

MR. KIRK: Okay. So the next graph -

MEMBER SHACK: I'm going to try to preserve a half an hour for Matt, so you've got about 15 more minutes. So how many more -- so members should keep that in mind, 15 minutes.

MR. KIRK: Okay. So I have 15 minutes, and I have five slides, so that's three per slide.

Okay. So this is -- and this gets back to many of the questions that were being asked before, and is the transition slide into generalization. This slide shows the relative importance of different broad classes of transients to the total through-wall crack frequency numbers that you've seen on some of the previous slides. So what we have is that, at lower levels of embrittlement, down around 200 degrees Fahrenheit, valves that are stuck open on the primary side, they might later reclose and cause a late stage repressurization, are responsible for about 70 percent of the through-wall cracking frequency. The medium to large diameter pipe breaks, or what's often called LOCAs, are responsible for the other 30 percent, and pretty much nothing else counts at that stage.

MEMBER BANERJEE: But you don't know what

TWC is, or what is -

MR. KIRK: The total is whatever the total was, which at 200 is about one times ten to the minus twelve. As you get up -

MEMBER BANERJEE: Like the age of the universe.

MR. KIRK: Something like that, yes. So at 200, it's something like one times ten to the minus twelve. As you get out in the 270-300 regime, it's one times ten to the minus sixth. Yes.

MEMBER BANERJEE: Do these numbers have any real significance in absolute terms, or are they important only in relative terms?

MEMBER SIEBER: Regulatory terms.

MEMBER BANERJEE: In regulatory terms.

MR. KIRK: I think that's above my pay grade.

(Laughter.)

MR. KIRK: Again, I get back to my previous comment, that our belief is that we've created as accurate a model as the current state of knowledge allows, but that state of knowledge is inherently limited, and so where we bump up against limited state of knowledge, we embed conservatisms into the model.

MEMBER BANERJEE: Well, what are the sort of uncertainties? Of course, you can't compare these directly, because the totals are very different on the left-hand side, ten to the minus twelve; whereas, to the right-hand side you've got ten to the minus six. So, in a way, it's only showing you the relative contribution. But what are sort of uncertainty bands on those?

MR. KIRK: The uncertainty, if we went to a graph where there are numbers and not percentages here, the range of through-wall cracking frequencies from which the 95^{th} percentiles were taken, generally span two orders of magnitude or more. And that's the amalgamated effect of the uncertainties in the PRA judgments, and the HRA, and the embrittlement, and the flaws, in everything, sums up to say two to three orders of magnitude. So if we're at a screening limit, if we're at a 95^{th} percentile screening limit of one times ten to the minus six, the distributions going down to probably one times ten to the minus ninth. And, in fact -- well, I don't know whether it's anecdotal or useful, these distributions are highly skewed to the low end, because we've -- I often say that my business over the last 10 years has been calculating zero, because most of the transients that

we've analyzed don't produce a very big challenge, and so you get a very small driving force compared with a relatively much larger fracture resistance, and so, all of these distributions are heavily skewed towards zero. So they're stacking up towards the low end.

VICE CHAIR ABDEL-KHALIK: So, if I -- just one question. I'm sorry. For steam generator tube ruptures in which the operator has failed to terminate safety injection, would contribute absolutely nothing to the risk in this picture. Is that your conclusion?

MEMBER SIEBER: Yes.

MR. KIRK: Yes.

VICE CHAIR ABDEL-KHALIK: And what is the basis for that?

MR. KIRK: Our calculations.

MEMBER SIEBER: Doesn't cool down.

MR. KIRK: We have -- we analyze that transient through RELAP, put it into the structural code, FAVOR, and it didn't calculate a high failure frequency. Again, because even with unmitigated safety injection, the amount of injected water isn't that large. The affected steam generator is boiling dry at 212, and there is another steam generator out there that's still cooking along at a high temperature that -

VICE CHAIR ABDEL-KHALIK: The amount of injected water can't be very small. After all, the RCS pressure drops to almost the secondary pressure, which is way below the shutoff head of the safety injection pumps.

MR. KIRK: Bill, would you -

MR. ARCIERI: Okay. I'm Bill Arcieri. In the case of the steam generator tube rupture, in terms of the results of the results of FAVOR, I think what you would find is that the cool-down rate just wasn't sufficiently fast enough to produce any significant failures, compared to LOCAs and the other transients that we looked at.

MEMBER STETKAR: If the operators successfully cool down at 100 degrees Fahrenheit, an hour? That's not -

MR. ARCIERI: That's not a problem.

MEMBER BLEY: Is it fair to say that the major difference that we're seeing from the old calculations where we saw lots of other things contributing, is that in the older calculations we were looking at crack initiation, and here we're including the rest, as well?

MR. KIRK: No, that would not be correct.

MEMBER SHACK: The big difference is, as I

read from the thing, no breaks larger than 2.5 inches were considered in the original analyses. That's one of the big differences.

MR. KIRK: Well, that's one of the big differences, is the major contributors were -

MEMBER SHACK: Well, I'm quoting from 1806. I'm old, and I've been on the ACRS for a long time, but I wasn't around in 1980.

MEMBER BLEY: Well, that would tell us why these might be higher, but the things that were showing up in the old one are not showing up now at all.

MR. KIRK: Well, there are two -- the reason on the main steam line breaks is, again, I think a very conservative model was adopted before for the secondary side faults that assumed that they could -- the temperature in the primary could go down to very low temperatures, which all of our calculations and understanding tell us isn't the case. And then the other -

MEMBER RAY: You should call it an unrealistic model, rather than very conservative, because, basically, we try to be very conservative, but unrealistic, we don't try and be. Physics won't allow you to get there.

MR. KIRK: Yes, yes. The previous analysis was unconstrained by physics. The other factor that I think is making a substantial difference, and I reflected on this yesterday, is that in the circa 1980s analysis, and I shouldn't be overly critical of the thermal hydraulics or the PRA, in all areas there was -- as I said before, where we bumped up against our knowledge limits we have adopted conservative or may even sometimes say unrealistic models. The investigators in the 1980s hit those limits far sooner than we did in the materials area, as well, and so they adopted very conservative, unrealistic models of the material behavior, such that the model of the material in the 1980s said that the vessel was much more brittle than it really was. And so, if you've got a much more brittle material, more things can break, more benign classes of transients can break it. And that's why when you look at the 1980s studies, you see the much greater variety of challenging transient classes, is because the model of the vessels said they were more brittle. Whereas, now, when we adopt a more realistic view, we find out that it's only the most challenging things that count.

MEMBER BANERJEE: Can you sort of also expand a little bit about the relative focus of the

through-wall cracks being the criteria compared to -- you said something about this yesterday.

MR. KIRK: Yes.

MEMBER BANERJEE: I think it might be of interest to hear it again, even if it's -

MR. KIRK: Okay. The difference between through-wall cracking and crack initiation won't make any difference at all to the contribution of the stuck open valves at the late stage repressurization, because when you get the repressurization, crack initiation is followed almost invariably by failure. It will make a difference to the medium and large diameter pipe breaks, and the main steam line breaks. Those would -- the contributions would go up there if the criteria were crack initiation, because without -- well, actually, I'm sorry. Let me back up.

It would probably not have a big effect on the main steam line breaks, because they're operating at full pressure anyway. So once they initiate, they also -

(Cough.)

MR. KIRK: The big change would be the medium to large diameter pipe breaks would become even more significant. No, no. I'm sorry. I'm sorry. I did it wrong. I did it wrong.

MEMBER STETKAR: You're going to get the small cool-down high pressure -

MR. KIRK: Yes, they would become less significant. I apologize. Yes, because they arrest a lot.

MEMBER STETKAR: Mark, let me ask you one really naive thing, and I wasn't sitting in the meeting yesterday. What I'm hearing is that we call this phenomenon pressurized thermal shock, but I'm learning that it's more thermal shock. Is that -

MR. KIRK: Yes.

MEMBER STETKAR: Okay. If that's -- if I've got that settled, then why are we concerned only with pressurized water reactor vessels, and not boiling water reactors?

MR. KIRK: That's a question I can answer, I hope conclusively; is that in the boiling water reactors, which could, arguably, be subjected to thermal shock, the water gap is much bigger between the core and the vessel, which grossly reduces the fluence that the ID sees, end of -- for example, end of license even 60 year, ID fluences in BWRs don't get much up above one times ten to the nineteenth at the worst. Probably below that, they're in the ten to the eighteenth regime; whereas, PWRs can get out to five,

six times to the -

MEMBER STETKAR: That's just literally the embrittlement.

MR. KIRK: Yes. Much tougher.

MEMBER STETKAR: Thank you.

MR. KIRK: Yes. Okay. Veronica is trying to make me go further than I went.

MEMBER SHACK: I think you better go. I'd get off that chart.

MR. KIRK: Yes, I think I'll go to the chart. Where did it go? Okay. Okay.

MEMBER SHACK: It's the generalization study in one slide.

MR. KIRK: Okay. We'll talk about the three transient classes, and I hope, but I'm not very confident, we'll convince you that they should be reasonably similar across the PWR fleet. So for medium and large LOCAs, the factors that are driving the failures are similar across the fleet; namely, that the rate of cooling in the primary system, once you get a five inch and larger break in it, exceeds that achievable by the reactor pressure vessel, so the transient severity now depends only on the steel thermal conductivity and the vessel diameter and thickness, and those factors are very uniform across

the fleet. So what we find out is that for this transient class, the details of the thermal hydraulic analyses really don't matter, because it's the vessel that's controlling. And, also, that operator actions don't really play a role in these transients, so there are, again, differences across the fleet.

MEMBER BROWN: There is still a flaw size implicit in that study.

MR. KIRK: There is still a flaw size, which is -

MEMBER BROWN: That's one of the inputs.

MR. KIRK: Which is checked, yes.

MEMBER BROWN: Okay.

MR. KIRK: Which is required to be checked by the rule. Yes, here I'm just talking about PRA and TH factors.

For the stuck open primary valves, as we said, they dominate the risk at low embrittlement. Once we get up to the reference temperature screening limits, they're probably responsible for about 20 to 25 percent of the through-wall cracking frequency. Again, the failures are driven by factors that are fairly similar across the fleet; namely, that in order for these transients to play a role, they have to get to relatively low temperatures in the primary at the

time of repressurization. The water that's being injected is coming from the outside, outside temperatures, again, are controlled by nature, not by plant-specific things. And we've analyzed worse cases of injection temperatures down to 35, so I think we'd be safe to say that bounds what's happening outside in Texas in the summer. Also, the thing that kills you, or kills the vessel in these scenarios is repressurization of the safety valve set point, which is another factor that's very similar across the PWR fleet.

We found out that on a specific transient basis, rapid operator action, in this case throttling of high pressure injection, can influence the progress of the scenario. In fact, it can prevent repressurization from occurring. However, we believe even if we were to remove that operator action credit, the screening criteria would not change significantly. And then, finally, and I guess we've spent more than the anticipated amount of time talking about main steam line breaks. They're not as important as they were believed to be before, because in our analysis we've adopted both more realistic models of both the vessel resistance to fracture, and the driving force generated by main

steam line breaks. Those two factors relegate them to a small contributor. And, also, they're a small contributor relative to the primary side breaks, because the temperature in the primary in response to a secondary break just simply can't drop as low as when you're getting direct injection of large amounts of water into the primary.

VICE CHAIR ABDEL-KHALIK: How will you address the issue of localized cooling for some plant designs?

MR. KIRK: I think we've addressed that in the technical basis, essentially to say that we don't need to. And the short answer to that is that the studies done by our thermal hydraulics colleagues on things like plume cooling show that at the -- in the belt line location, the delta T across the plume is at most I think 10 to 20 degrees Centigrade. And when we plugged even much larger plume strengths into some scoping fracture mechanics calculations, it didn't affect the through-wall cracking frequency.

VICE CHAIR ABDEL-KHALIK: My question pertains to direct vessel injection.

MR. KIRK: That issue has not arisen before, so I would have to look around to my colleagues to find out if direct vessel injection is

important to any of the plants that we would see using this. But I don't recall that being brought up before.

MR. ARCIERI: We haven't looked at direct vessel injection plants directly. Something else that I'm working on, we are looking at DDI plants. The injection lines are about the same elevation as the hot and cold legs. So if you're bringing in the cold water, and it's going into the downcomer, I would still expect to see the same plume dissipation that Mark was just talking about at the vessel belt line.

VICE CHAIR ABDEL-KHALIK: Without doing the analysis, it's just intuition.

MR. ARCIERI: That's my judgment.

MEMBER SIEBER: Well, that's out of the theory of effective fluence on the vessels. You're not going to have that embrittlement when you -

MR. KIRK: At the injection point, yes, that's right. Yes.

MR. MITCHELL: Okay. Thanks, Mark. I am Matthew Mitchell, Chief of NRR's Vessels and Internals Integrity Branch. I think my job is now in about 100 words or less to explain how we have taken the comprehensive technical basis that the Office of Research has developed, and translated it into the 10

CFR 50.61 Alpha Rule that you've received for consideration.

By way of background, let me say a few words about the current PTS rule, and how it relates to our motivation for promulgating 10 CFR 50.61(a). I want to make it clear up front that the current PTS rule in 10 CFR 50.61 has provided a sound and conservative methodology for insuring adequate protection from PTS events since the rule was put into place in 1985. The Staff in no way questions the soundness of the rule for still continuing to fulfill its intended purpose. However, the current PTS rule is fundamentally based upon 1980s technology, our state of understanding, our state of knowledge from that point in time, the computational methods that were available at that point in time, et cetera, and is not based on the best currently available information and analyses regarding potential RPV failure due to pressurized thermal shock. This has led to a level of conservatism in the current rule that imparts a degree of unnecessary regulatory burden on particular licensees, when compared to our best current understanding, as documented in the technical basis for 10 CFR 50.61(a).

By our current best available information,

the existing PTS rule would have approximately eight to twelve operating PWRs not meet the screening criteria in the rule through 60 years of operation. As was pointed out in the Subcommittee meeting yesterday, that number is subject to change if, for example, certain plants undergo power uprates, if plants choose to remove flux reduction that may be implementing flux reduction currently, other operational changes could result in other plants wanting to make use of 10 CFR 50.61(a). So that leads to why we were motivated in roughly the 1999 time frame to start the work on developing the technical basis for 50.61 Alpha.

Now, the objectives of our rule making are three-fold. The first, foremost, and primary objective, which should go almost unstated, I suppose, is that we will continue to provide adequate protection of public health and safety. 50.61(a), based upon the technical basis that Mark and his colleagues have developed, will continue to insure that the reactors that choose to use the rule will continue to have probabilities of vessel failure below acceptable limits. That's been our entire basis for setting the existing screening criteria, as well as the additional features of the rule, which I'll get

into in a little bit, that help give us confidence that the reactors that choose to use the rule fall within the technical basis.

Secondly, we have chosen the path of rule making to resolve this issue on a basis of regulatory efficiency, effectiveness, and openness. We believe that it's important for all of our stakeholders that we address this significant issue in a comprehensive fashion, rather than to use or to rely on complex plant-specific analyses that would otherwise be developed for plants that eventually would exceed, or be projected to exceed the screening criteria in the current rule. This is a comprehensive approach that we believe will serve the needs of the fleet, but it also serves the needs of interested members of the public to allow them to understand clearly what the NRC's basis will be for judging the acceptability of continued operation of the existing reactors. And then, finally, as I addressed earlier, the third objective is, of course, to address the unnecessary burden imposed by the existing PTS rule.

By way of overview, I'll point out what I suspect all the members of the Committee have recognized since you've received our rule making package, is that 10 CFR 50.61(a) is structured

similarly to the existing PTS rule. The Staff has emphasized the similarity, at least in structure, to facilitate the understanding and implementation of the new rule by both the industry and the NRC Staff. Many of the same topics, many of the same concepts are addressed in both rules; the idea of calculation of a material reference temperature, comparing it to screening criteria, looking at plant-specific surveillance data. Many of these same topics hold, therefore, we chose to try to make the rules as similar as possible, at least in structure, so that familiarity with those would help in terms of their implementation.

Now, there are notable differences between the two rules, and those notable differences reflect critical features that differ between the existing rule, and 10 CFR 50.61 Alpha. Now, what I'd like to do is to focus specifically on those notable differences, and then address any other Committee questions about any other aspects of the rule that you may find interesting. But I would point out that the key features in 10 CFR 50.61(a) that, in particular, differ from the existing PTS rule include the limitations that we have placed on the applicability of the alternative rule, the less restrictive

screening criteria that are, indeed, based upon the vast amount of technical work that's been performed to supplement this rule, a requirement to evaluate plant-specific flaw distributions so that facilities demonstrate that they are within the technical basis for the proposed rule, and the implementation of embrittlement models and reactor pressure vessel surveillance data evaluations, again, to support licensees' determinations that they meet the screening criteria in 10 CFR 50.61(a).

With regard to limitations on applicability of the alternative rule, we will point out that the technical basis for the alternative rule is based strictly on the evaluation of currently operating PWR designs. As Mark indicated, three principal study plants were investigated, five additional plants were investigated as part of the generalization study. What was not investigated specifically were advanced reactor designs, new reactor designs like, for example, AP 1000, which may be subject to different PTS event frequencies and severities. Hence, we found it to be prudent to a priori exclude those reactor designs from utilizing 10 CFR 50.61(a).

However, we also believe that improvements

in PRV manufacturing, in particular, the elimination of axial welds from the belt line region, as well as the expected use of very low copper materials, which are going to be much less subject to radiation embrittlement, will obviate the need for new reactors, reactors licensed after the effective date of the rule, in particular, to need to even use 10 CFR 50.61(a). We will expect them to continue to meet the requirements of the more restrictive existing PTS rule.

Now, this doesn't go to say that it could not be at some point in the future demonstrated that this rule is also applicable to new reactor designs. It's just that that work was not undertaken, that demonstration was not performed. But that option would be open if a licensee of a new reactor wished to pursue an exemption under 50.12, and provide a demonstration that the rule is, in fact, applicable to their design, as well.

With regard to the less restrictive screening criteria, the alternative rule is modeled similarly, again, to the existing PTS rule, except that we are now using a different material property parameter that we're calling RT MAX, as Mark alluded to in his presentation, instead of the more common, or

more recognized RT PTS value. These values are calculated differently, so comparing RT MAX to RT PTS is not an apples-to-apples comparison. And comparing the screening criteria between the two rules is also not an apples-to-apples comparison. In particular, RT MAX is based upon -- is a mean value property, as opposed to RT PTS, which, as I'm sure you all well know, includes what we call a margin term in the existing current PTS rule. It's calculating upper bound property, so they're not directly comparable, and that also makes the screening criteria not directly comparable.

MEMBER BROWN: I thought Mark said it was not a mean value earlier to 95 percentile. Am I mixing terms?

MR. MITCHELL: What Mark was referring to was how we established the screening criteria. What I'm talking about here is, how the licensee calculates their actual material property value, the material property value that's calculated for comparison to the limits.

MEMBER BROWN: Their methods for calculating RT for their vessel. Is that what you're talking about?

MR. MITCHELL: Yes. And that is directly

and completely laid out, also, in the rule, itself. We've identified exactly how you go about calculating RT MAX.

Therefore, we believe that the technical basis taken as a whole does demonstrate that PWR facilities can safely operate to higher levels of reactor vessel embrittlement. Hence, we've implemented the less restrictive screening criteria in the alternative version of the rule.

MEMBER BANERJEE: So just following on Charlie's question, since you've put uncertainty in the screening criteria, you're using some form of mean sort of -- you're not putting uncertainties then in calculating the RT MAX for the applicant. Is that correct?

MR. MITCHELL: I think that's a fair way of summarizing.

MEMBER BANERJEE: Okay.

MR. MITCHELL: Yes, there are nuances and subtleties, but that, as a whole, that's a fair way of summarizing.

MEMBER RAY: What would happen -- well, we don't have time. Never mind.

MEMBER BROWN: We have another 15 minutes, 20 minutes.

MEMBER RAY: The Subcommittee has -

CHAIR BONACA: We have time, Harold.

MEMBER RAY: Pardon?

CHAIR BONACA: We have time, if you need to ask a question.

MEMBER RAY: Well, I think, Mario, my question would take more time than I want to impose on everybody, but it went to the decision to use average -- it builds on Sanjoy's question. I'll let it go.

MR. MITCHELL: Another new and distinct feature of the alternative rule is the requirement to evaluate plant-specific flaw distributions for those plants wishing to take advantage of 50.61 Alpha. I think as Mark has laid out, and we've talked about with the Committee in the past, one of the main features of the new technical basis that's allowed us to establish these less restrictive limits is the use of a more realistic flaw distribution in the calculations. That has led to much of the benefit, and the improvement that we've seen in the current technical basis.

MEMBER BROWN: What's the basis for choosing -- I'm only vaguely - not vaguely, but flaw distributions were determined before there was a flaw distribution that was supposed to be used for the

analysis. Is that a correct statement?

MR. MITCHELL: Now, are you talking about -

MEMBER BROWN: And now you want to use a more realistic, what does that mean? You can screen materials better?

MR. MITCHELL: Let me -- I'll explain what I mean. In the original -- in the basis for the current PTS rule, which dates back to the 1980s, there was, I will call it, a very aggressive flaw distribution used. In particular, in that work, all of the flaws in the distribution were assumed to be surface breaking. They were assumed to be open to the inside surface, which is a much more challenging configuration than an embedded flaw. In fact, in reality, essentially all flaws that you will find in these reactor vessels are embedded. That one recognition, that one move toward a more realistic representation makes a huge impact on the bottom line result.

Now, there's also been some changes in the exact population of the distribution. The original population was based upon work that was done by Marshall. It's called the Marshall Flaw Distribution. It tends to have a smaller flaw density, but bigger

flaws in it, than what we have seen based upon the work that's been done to look at samples of actual nuclear reactor vessels that have been evaluated for the purposes of developing the flaw distribution that we've used in this study.

MEMBER BROWN: Are you now defining that there is some minimum depth within the -- away from the surface that you will first see any flaws develop, so that -

MR. MITCHELL: It's not a matter of seeing - the flaws are present due to the manufacturing process.

MEMBER BROWN: I understand that, but before you said they were assumed to be at the surface.

MR. MITCHELL: And that was for -

MEMBER BROWN: And now you're saying based on some reason, I guess based on methodologies for testing materials and everything else, that flaws really are embedded. I understand that point, but that doesn't, necessarily, mean that all the flaws will always be inside, so I'm just saying are you assuming that they're all inside now, or is there some distribution that you've thrown into this that still exists at the surface, or break the surface, but just

not the same volume of flaws that break the surface?

MR. MITCHELL: Well, I will say that the original assumption that was made in the 1980s work, I think was for calculational ease, and that was why -- and conservatism, the flaws were all put on the surface. There's actual physical evidence to indicate that very, very few flaws would ever be expected to be surface breaking, but those have been included within the scope. Some small population of surface breaking flaws were considered.

MEMBER BROWN: You made a judgment as to the population that would be assumed to be at the surface now.

MR. MITCHELL: Yes. Actual physical evidence was coupled with expert elicitation to develop the flaw distributions that were used in this technical basis.

VICE CHAIR ABDEL-KHALIK: So would enhancement of in-service inspection techniques that reduce the uncertainty in the flaw distribution affect the outcome of the analysis that an applicant may have?

MR. MITCHELL: Well, the short answer is yes. I mean, certainly, the closer that you're NDE results can get to reality. Keep in mind, what is

shown in the rule as the acceptance criteria, the flaw distributions that the licensees would be judged against, are considered to be actual flaw sizes. Those are the flaw sizes that went into the fracture mechanics calculation that led to failure, so we're now going to ask them to compare NDE results to what is, essentially, a real flaw size table.

Now, our expectation is, and our experience is for the very small flaw sizes that are of interest, NDE, of course, has a tendency to over-estimate the sizes of those flaws. It's hard to under-estimate something that's already very, very small, so there's a bias towards over-estimating, as a result of the NDE, anyway. So, when licensees take their NDE results that are required by the rule to be evaluated against the tables in the rule, they're taking this presumably biased and conservative NDE result, and comparing it to what's actually been shown to fail by virtue of the probabilistic fracture mechanics work that was done to support the basis for the rule.

We did include a clarification in the final rule which said licensees could make a judgment, an argument that they would have to present to the Staff, for the Staff's review, as to how they could

account for NDE uncertainty in making that demonstration. So that flexibility is already provided in the rule, so we've acknowledged that such exists. But if they were to develop better techniques in the future, that would simply mean that they're getting results that are more directly comparable to what's actually in the rule as the acceptance criteria. Okay?

VICE CHAIR ABDEL-KHALIK: Thank you.

MR. MITCHELL: So I think I've given a sense of why we already believe that having facilities go and verify this consistency with the technical basis is important. This is consistent with how we, as an Agency, make risk-informed decisions. We insist that important parameters continue to be monitored and verified going forward, and that is exactly what we have attempted to do in the alternate PTS rule.

And the last bullet just points out that we believe we are effectively able to use already required ASME code inspections consistent with performance, demonstration, initiative, practices to get the data necessary to make this comparison to the flaw distributions specified by the rule. So we're not requiring augmented examinations, per se. We're requiring, if you will, augmented evaluation of the

data that licensees are already accumulating as part of their ASME code inspection program.

And the final, I think, key point that I'll mention is the fact that we have implemented new, updated, and we believe substantially improved embrittlement models, and an evaluation of surveillance data in the alternative PTS rule. The embrittlement models that I think we're all more familiar with from the existing PTS rule, and from Regulatory Guide 1.99 Revision 2, were also developed in roughly the mid-1980s time frame. They were based on, at that time, having roughly 200 data points of shift information from which the models could be developed.

The models that you see in the alternate PTS rule are based upon roughly 1,000 data points, so we've expanded the database by a factor of five, as well as combining the statistical analysis of that data with a updated mechanistic understanding of radiation embrittlement. So we believe that sort of across the board we've enhanced, or improved the embrittlement models versus what you see in the existing PTS rule.

Along with that, we have updated, and we believe also improved how we evaluate RPV surveillance

data to make sure that the models that are in the alternate PTS rule are not performing non-conservatively. We have developed now three statistical tests that licensees will be expected to perform to show that their plant-specific surveillance data does not deviate in a statistically significant way from the models. In particular, we're interested in making sure that at high fluence ranges, at high fluence levels, that the models are not under-predicting the amount of shift that plant-specific materials are actually demonstrating.

MEMBER BANERJEE: Is this trying to make reality fit a model? I'm just sort of -

MR. MITCHELL: I'm pretty sure the answer to that is no.

(Laughter.)

MEMBER BANERJEE: To me, I mean, you're measuring these things.

MR. MITCHELL: Well, I think -- I'd put it this way. I'd say we are monitoring and confirming that our model is, in fact, predicting reality as it's being measured.

MEMBER BANERJEE: Okay. But, now, you've got these measurements. Suppose it doesn't fit your model?

MEMBER SIEBER: Then you go back to the first rule.

MR. MITCHELL: Well, then the rule will require that the licensee evaluate the data, and provide a methodology to the Staff for how they intend to account for that additional information.

MEMBER BANERJEE: Fair enough.

MR. MITCHELL: Yes. We do not try to prescribe how that would be done, but we note that it must be done, and accepted by the Staff.

MEMBER SIEBER: The analysis that used to derive the rule is based on what was considered to be the worst case plant, so that makes the rule conservative with respect to the fleet, and adequate with respect to those plants. I see you're shaking your head no.

MR. MITCHELL: That's not -

MR. KIRK: The -- it's correct to say that two of the plants that we analyzed are among the most embrittled in the fleet.

MEMBER SIEBER: The three.

MR. KIRK: Yes.

MEMBER SIEBER: Okay.

MR. KIRK: But in deriving the reference temperature limits, we analyzed those plants across -

each of those across a range of embrittlement, ranging from very unembrittled to very much more embrittled than anybody would ever permit. So I think the notion that even though at any given time those plants lead the pack, that the rule is conservative on that basis is not correct.

MEMBER BANERJEE: Now, what I understand from what you've said is, basically, that you've got models for these flaw distributions and things like that. And if you find very different results from these, then you have to explain what the -

MR. MITCHELL: Absolutely. And I didn't elaborate on that point, but yes, in that section of the rule that talks about the flaw distribution evaluation, if a licensee inspects and finds a flaw distribution that's substantially different, or not consistent with the criteria, the tables in the rule, they are required to perform an evaluation to demonstrate that their vessel will still be below one times ten to the minus six in through-wall cracking frequency, yes.

VICE CHAIR ABDEL-KHALIK: Would the changes in the methodology, and/or the limits change the order of the plants in terms of how close they are to the limits?

MR. MITCHELL: Yes. The short answer is yes, that you would see some reordering of the plants based upon if you evaluated them all under 50.61 Alpha, or under 50.61.

VICE CHAIR ABDEL-KHALIK: Right.

MR. MITCHELL: But what we take away from all of the work that's been done is that in terms of 50.61 Alpha, all the plants, even though they've been reordered, could be demonstrated to be below the screening criteria in this alternate rule out to at least 60 years of operation.

VICE CHAIR ABDEL-KHALIK: But what does that imply in terms of the level of conservatism of 50.61 versus 50.61(a)?

MR. MITCHELL: I think it implies what we have long understood, is that 50.61 is inherently a more conservative rule.

VICE CHAIR ABDEL-KHALIK: Not if the order is changed.

MR. MITCHELL: Well, it's not -- I think it's not the order that explains the conservatism, it's how close do the plants come to the screening limits in each rule. That gives you an -- because the screening limits tell you effectively the risk associated of through-wall cracking frequency for each

plant. The order may change, but the picture -- the understanding of the probability of through-wall cracking frequency for any given plant, when you look in 50.61(a) it will tell you that the probability is perceived to be less, because we now have a better understanding, and more thorough understanding of the phenomenon of PTS.

MEMBER BROWN: Well, no. It's based on one times ten to the minus six, so it's not -- that's the risk probability that you assigned in developing the rule. So if they meet the limits of your rule, they will be one times ten to the minus six.

MR. MITCHELL: No, sir. That's actually the through-wall cracking frequency if you are at -- if you're exactly at the limit. As long as you're below the limit, you'll have actually, in reality, a progressively smaller through-wall cracking frequency.

MEMBER BROWN: No, I understand that.

MR. MITCHELL: Yes.

MEMBER BROWN: And I didn't mean to interrupt somebody. I have another calibration question, the old rule. What would you -- is there an assigned number if you hit the old rule at 270?

MR. MITCHELL: Yes.

MEMBER BROWN: Would that be one times ten

to the minus twelfth?

MR. MITCHELL: No. Well, based upon the original technical basis work that was done in the `80s, the numbers -- the screening criteria in the current rule were assigned to a vessel failure frequency at that time of five times ten to the minus sixth. That was the implied failure frequency associated with the 270 and 300 limits that are in the existing rule.

Now, in reality, I don't have it off the top of my head. Mark tells me it's ten to the minus eight if you're at the screening limits in the current rule, is based -

MEMBER BROWN: Okay. So there's -- I was just trying to get a calibration as opposed to the qualitative conservatism, the margin, we've got a rule that has a factor of 100 less. Is that right? Okay.

MR. MITCHELL: That seems to be what's implied here, yes.

MEMBER SHACK: Matt, just coming back to your answer -

MEMBER BROWN: I'm not saying that's bad, by the way. I'm just -

MEMBER SHACK: To Said's question, I think because the rule itself only contains the

embrittlement now, the only reason you'd get any reordering is a slightly different understanding of the mechanisms of embrittlement.

MR. MITCHELL: That's correct.

MEMBER SHACK: So it would be the chemistry of the copper, and the chemistry of the nickel might shift them around a little bit, so that you -

MR. MITCHELL: The embrittlement modeling, in particular, and the specific methodology prescribed for how you calculate RT MAX, the subtle differences between that and RT PTS cause a subtle reordering of the plant. I think it's -

MEMBER ARMIJO: They're all found at a lower -- they're all moving further away from the screening criteria.

MR. MITCHELL: They are all moving further away, because the screening criteria are moving out so much.

MEMBER SHACK: I mean, that's independent of thermal hydraulics, flaw distributions, PRA. I mean, that's really just a materials question there.

MR. KIRK: But the other thing that influences the reordering is the different way that margin is treated in the two rules. In the existing

rule, some plants get smaller margins because they have so-called credible surveillance data. Those credits don't appear in the new rule, and so that's caused some plants to move around what I suspect they might consider to be dramatically.

MR. MITCHELL: But, fundamentally, it comes back to the question of how you calculate RT MAX versus how do you calculate RT PTS. That's really what it boils down to.

MEMBER MAYNARD: I've got a question on -- I didn't see anything in the rule that talks about flux reduction as an entry point into using this. If I'm wrong, that's fine, but if I'm not, why not? Why not have a reasonable flux reduction as part of your right to be able to use 50.61(a)?

MEMBER SIEBER: You don't need it.

MR. MITCHELL: I generally would say it's because it's unnecessary. I think it's unnecessary to use that as an entry criteria, or a condition. In fact, I mean, I think one observation we would make is that, in part, that the new insights that are in 50.61 Alpha may allow plants to move away from such management schemes, because they don't come at zero cost. Even from a safety perspective, if you'll consider that the unit is going to generate X amount

of power, if you use elaborate flux reduction in your core design, you're going to push the power somewhere else, so you're going to have higher peaking factors. So I think expecting plants to continue with certain management techniques as an entry condition to using a rule which says that they don't even have a problem, anyway, might not be the appropriate way to connect the dots.

MEMBER MAYNARD: I understand that, and that there is cost associated with it. And I understand that there is margin with regard to the old rule, but the bottom line, we are reducing margin in one of the most important pressure vessels that we've got. I would have thought it would have been worth consideration.

MEMBER RAY: On that point, I think you're better served -- the train has left the station here, but for what it's worth, to call this an alternate criteria, rather than a less restrictive criteria. It seems to me like there's way too much emphasis put on this being less burdensome, less restrictive, as opposed to merely being a better and alternate method.

MEMBER BANERJEE: But isn't it more risk-informed?

MEMBER ARMIJO: But I think you raised it,

it's more realistic criteria. That's what's really going on here.

MEMBER BANERJEE: This is -- to me, at least, it sounds like the first risk-informed rule I've seen in some -- I could be wrong.

MEMBER RAY: Yes. But, Sanjoy, if we were in the mode in which a risk-informed rule may turn out to be more restrictive, as we should be, I think, fine. But I'm just saying the label put on this makes it sound as if it was developed -

MEMBER BANERJEE: It's a little bit too much of a sales job.

MEMBER RAY: What?

MEMBER BANERJEE: It's a little bit too much of a sales job to do it this way.

MEMBER RAY: Yes. I spent years in the industry side on trying to sell risk information, and you've got to take the bad with the good. And if it turns out that this alternate, you were more restricted, well, so be it. We didn't develop it in order to reduce the restrictions; and, yet, that's the label that appears here.

MEMBER ARMIJO: I heard it -- I hear what's in the chart. I think it's an unfortunate choice of words, because I think what you've done is

you've developed a more realistic rule that just happens to be less restrictive. But it wasn't developed to be less restrictive, it was developed to be more realistic. And I think that's the -

MEMBER SHACK: You can't get away from Otto's point. You're going to allow the vessel to operate with a higher degree of embrittlement. The question is whether that's acceptable or not.

MEMBER SIEBER: From the standpoint of total risk, reduction of peaking factors, to me, is -

MEMBER BANERJEE: Very important.

MEMBER SIEBER: -- important, just as important as the approach to a brittle fracture. And so, from a public risk standpoint, this is a good approach.

MEMBER RAY: No doubt, I agree. But to Bill's point, Bill, maybe the use of RT MAX instead of RT PTS would, for some plants, wind up with a more limiting case. Now, that doesn't appear to be the case here. All the data indicate that's not so, but, nevertheless, that's a possible outcome. I just picked that parameter, but my point simply is, it will be perceived as Bill and Otto have said, that there's simply a reduction in margin taking place, when I think that's an unfortunate way for it to be seen.

And, instead, it ought to be viewed in some more positive way, if it deserves that treatment.

MR. MITCHELL: I only would go back to, I think, one of the points that I started this presentation with, which is to point out that, certainly, the Staff is committed, and has always been committed in the development of this rule to insuring adequate protection is maintained. That would never have been compromised. If we had determined that as a result of the technical basis work the current rule did not provide adequate protection, we wouldn't be talking here today about an alternate PTS rule. We'd be talking about backfitting an enhanced version of 50.61 that would require all licensees to continue to maintain an adequate level of protection, if we felt that the current rule was inadequate. So I think the way I would tend to phrase it is both rules provide an adequate level of protection, each in their own way. And that we're convinced of that.

MEMBER RAY: That's fine.

MR. MIZUNO: This is Geary Mizuno from the General Counsel's office. And just to expand upon what Matt was speaking, you have to understand that because of the backfit rule, unless we found that there was a need for adequate protection, or a

substantial increase of protection, we wouldn't impose this rule. That's why it's written as an alternative. And the fact of the matter is, is that as much as you hate it, is that we would never have expended the resources unless there was some kind of positive benefit, given that this becoming more realistic did not result in any particular benefit. The existing requirements provide for adequate protection. The primary objective, or purpose, and benefit is to allow these few licensees, or a handful of licensees who are approaching the limit, to be able to do -- basically, be able to operate without having to do additional complex calculations and demonstrations under the existing PTS rule. And, instead, have the ability to do -- to justify additional operation with a different approach. That is the primary purpose of this rule, because the existing rule provides for adequate protection.

MEMBER BROWN: But does this one.

MR. MIZUNO: There's no question that this new rule also provides for it, too, because we would never issue a rule that wouldn't provide for that. But the point is, is that we never would have expended the regulatory resources simply to develop a rule that provides for adequate protection that is more

realistic. There has to be some kind of benefit there, and here, the primary benefit, the primary driver was the 12 licensees, I believe. And, in fact, there were, I think, two or three licensees that are very closely approaching the existing PTS limits, and would require additional action. And that has always been the motivating factor behind this rule making.

VICE CHAIR ABDEL-KHALIK: From a philosophical point, I have a really difficult time with this argument, because, I mean, after all, this is why the promotional side of the AEC was separated from the regulatory side. And your argument goes towards the promotional side of the business.

MR. MIZUNO: We're not promoting the operation, but what we are doing is saying, is that if we know that our existing regulatory structure is unduly conservative, requires a licensee, or any entity, to do something more than what is strictly required for safety, then as a good regulator, and it doesn't matter whether we're regulating nuclear power, or consumer products, or anything, we have to approach things to insure that society's resources are used in the most effective manner. And that is what we're doing here, is that -- I mean, if you want to put it in that kind of words, I'll say we are doing rule

making to insure that resources are expended in the most effective manner, and they are not unduly utilized in that we force licensees to abandon assets, societal assets in a way that is not justified given our current technical knowledge.

MEMBER ARMIJO: I would like to add, what we had before in the current rule provided more than adequate protection to health and safety because of many unrealistic assumptions and analyses that were done, and the state of knowledge at the time. The current rule provides adequate health and safety, which is the goal. And it just happens to be less restrictive. That's good, so I don't see a big philosophical issue here. As long as that ten to the minus six criteria is being met, I don't see why we're dragging this horse around.

MEMBER MAYNARD: I think, overall, this is a much better approach than processing individual waivers or exemptions to the regulation.

MR. MITCHELL: I mean, we recognize that it's open, it's scrutable by everyone and the public to understand what we're going to do. And there is benefit that we gain from that, as well, in terms of being a good regulator, rather than dealing with each individual plant-specific submittal. That's the other

major driver of why this is the right way to deal with this issue.

MEMBER SIEBER: Okay.

MEMBER SHACK: Any further comments or questions?

MEMBER SIEBER: No.

MEMBER SHACK: Back to you, Mr. Chairman.

(Laughter.)

CHAIR BONACA: Very good. With that, first of all, I want to thank you for an excellent presentation, and, of course, for an excellent piece of work. I mean, we have seen it a number of times. It has moved from technical work into a rule, and that's success in many ways.

With that, I think we'll break for lunch, and get back at 1:20.

(Whereupon, the proceedings went off the record at 12:24 p.m., and went back on the record at 1:20 p.m.)

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

1:20 p.m.

CHAIR BONACA: On the record. Okay. We're getting back into session and the next item on the agenda is Draft Final Regulatory Guide 1.200 (formerly DG-1200) and I believe Dennis will take us through this presentation.

MEMBER BLEY: I think that's so. Well, I'll introduce it anyway. Reg Guide 1.200 and I think most of us have been tracking it for some time, but for those who haven't it really, and I'm quoting from the report itself, "describes one acceptable approach for determining the technical adequacy of PRA whether it's sufficient such that the PRA can be used in regulatory decision making for light water reactors." It borrows from the PRA standards that have been created by the professional societies and from the NEI document on peer review and then expands and qualifies those documents to some extent and provides the basis for certifying essentially showing that the PRAs are adequate.

We began our interaction with this back in 2003 with some early drafts followed up with another letter in 2006 after the trial applications were completed and now the version that's before us includes the public comments and is just about ready to go out the door.

I think Mary will walk us through the details. I just want to remind everybody that there are lots of places in here we could wander off forever and we've only got an hour and a half. So I'll try to pull us back whenever that starts to happen. We have some key things to hear.

Mary Drouin will take us through.

MS. DROUIN: Okay. John, do you want to?

MR. MONNINGER: Sure.

MEMBER BLEY: I'm sorry, John.

MR. MONNINGER: Good afternoon. I'm John Monninger. I'm the Deputy Director for the Division of Risk Analysis in the NRC's Office of Nuclear Regulatory Research. Thank you very much for this opportunity for us to come and brief the staff on where we are on Reg Guide 1.200. This is our second proposed revision to this document.

As Dennis mentioned this project has been going on for several years, four or five, six, or seven years or so and I think though that is a long time period I think there have been significant accomplishments along the way. You know initially with the endorsement of the Internal Events Standards and where we are today to the endorsements of standards for fire and external events and some other

areas.

This document and the document that it endorses, the combined ANS and ASME standard is a significant accomplishment and much thanks from the staff goes out to ASME and ANS and the nuclear industry for all their participation in pulling the standards together. In addition to that, there was significant support and cooperation from industry, the National Labs and staff within NRR, NRO and Research. With that, I would just like to turn it back over to Mary and Gareth and we look forward to the interactions and comments from the ACRS.

MS. DROUIN: Glad to be here. My name is Mary Drouin with the Office of Research and at the table with me is Gareth Parry from NRR. We're here today to discuss Revision 2 of Regulatory Guide 1.200. Right now, Revision 2 does not exist. It's Draft Guide 1.200 which is the proposed Revision 2, but for purpose of this meeting I'm just going to always refer to it as Revision 2 and we're here to request a letter for publication of Rev 2.

We have a lot of new members who haven't been through this history. So I'm going to try and spend not a whole lot of time, but a little bit of time going through what was their original purpose of

this reg guide, the history, the reg guide itself, the history of the standards and industry related guidance because those are the reports that we have endorsed and we'll go through the staff endorsement.

We just completed a public review and comment period and we'll go through the comments that we received from the stakeholders and how they've been dispositioned and then ultimately what is our schedule and what is the future work because there will be a Rev 3 and maybe a Rev 4 and a Rev 5. But right now we're just on Rev 2.

Dennis did quote right from the purpose of this reg guide and the main purpose is to provide one acceptable approach. It's really clear. This is one acceptable approach. This is a regulatory guide. It's not a regulation for determining what is needed technical acceptability you need in that base PRA to support risk informed decisions. You're using results and insights from the PRA and you want to have confidence in those results whether from the whole PRA or just if you use partial. So this document is providing the staff position there.

And the whole point of this as another major purpose of the regulatory guide is that when it is used in support of an application the hope is that

it will obviate the need for an in-depth, and I emphasize the word "in-depth," in-depth staff review.

The staff always, of course, reserves the right to do audits and spot reviews.

MEMBER BLEY: Mary, the document itself says, "obviates a need for in-depth review of the base case PRA."

MS. DROUIN: Of the base case.

MEMBER BLEY: So for any complications you would have to do a --

MS. DROUIN: That's right. This just focuses in on the base PRA. This document is not an application specific document and we'll try and illustrate that later on.

CHAIRMAN BINGAMAN: You're going to tell us what it means.

MS. DROUIN: Yes.

MR. PARRY: If I can just add to what Dennis asked though. Yes, what the staff would from the applications to see how that base case PRA was manipulated and changed to address the particular issue and that we would always --

MEMBER BLEY: You would look hard at any changes.

MR. PARRY: We would look hard at the

changes and that's what we do, for example, in Reg Guide 1.174.

MS. DROUIN: But you're wanting to go in to that with that. The base is okay so that you don't have to spend time looking at the base.

And this Reg Guide 1.200 is a major player in achieving the Phase 3 and the phase approach to PRA quality. Back in 2004, I think I have the right date and I think it was SECY 04118 which was the plan that was put forward to the Commission on how do you achieve PRA quality in this phase manner and still allow risk-informed applications to occur because not all the standards were in place, not all the industry guidance and NRC guidance was in place. So Phase 3 was to get us to the point where hopefully we have all the standards and related guidance in place for those applications that we envisioned. So this is a major player in getting those to Phase 3.

Just to show you some of the history here, where we've been with this regulatory guide, we first published it in November 2002 for public comment and at that point in time we were endorsing standards that had only gone out to Level 1, at-power and LERF. It did not include, for example, fire, did not include the external hazards, low power shutdown and this was

their first draft and it was also endorsing NEI0002 which was the peer review criteria.

Then we addressed the public comments. We issued it for trial use. We did some pilots with the trial use reg guides. Industry also was testing it. And so as a consequence of both our pilot and industry testing both the standard was changed. We learned a lot also from the reg guide. So we did a revision to the reg guide. The scope was still the same. We had not expanded yet to internal fire and others. It was still Level 1, LERF and at-power.

Then we issued Rev 1 for use. The trial use has gone away. In the meantime, ANS had been working on an external -- standard. They issued that. We reviewed it and issued a draft guide and this was on Rev 0 of that standard. Since then ANS has issued a revision to that standard and it's all come together now in this joint standard that you've heard about. And this joint standard, ASME and ANS, from what I understand, this is a very monumental, historical thing that's happened for these two societies to not only just work together but to jointly publish a single standard with both SDO logos.

In April of last year, the ASME/ANS PRA standard was published that now had Level 1, LERF, at-

power, internal flood, internal fire, external hazards. So the standard went from being this big to like that big (Indicating).

MEMBER CORRADINI: Just one background point that I guess I don't remember. For LERF, that is what? A simplified event tree and then some estimates on release fractions? Can you help me there?

MS. DROUIN: It's the simplified approach that was supporting what was done to support originally Reg Guide 1.174. If you go back in history, there was NUREG --

MR. PARRY: 6959.

MEMBER CORRADINI: Okay, but from a how-you-do-it standpoint, it's a simplified event tree.

MS. DROUIN: Yes.

MEMBER CORRADINI: For the post degraded core state and trying to estimate damage states and their four releases.

MS. DROUIN: Yes.

MR. PARRY: That's one way of doing it, but the standard doesn't force you into that.

MEMBER CORRADINI: Okay.

MR. PARRY: But it specifically addresses only LERF.

MEMBER CORRADINI: Okay.

MR. PARRY: So it's Large Early Release.

MEMBER CORRADINI: Right.

MS. DROUIN: It supports a simplified approach through the different capabilities categories. You can always do a very detailed LERF under the standard.

MR. PARRY: Yes.

MEMBER APOSTOLAKIS: Why is the standard defined LRF?

MS. DROUIN: Okay. I'm going to get to that if you will -- That's on a slide.

MEMBER APOSTOLAKIS: Good.

MEMBER BLEY: Something just came up. If you're going to get to it later, great. I kind of think of this reg guide as part of a suite of guidance and part of that suite is the what which is the standard and this kind of says how you adapt that standard to regulatory applications if you need to adapt it and you do in fact adapt it a little bit.

But the other part that was talked about when the standard was developed was the how and since Mike just mentioned how, the guidance on how to do parts of the PRA. You've got a handbook on parameter estimation that's pretty recent. We've got a handbook

on fault tree analysis that's really old. And we have a procedures guide for PRA that's really, really old and archaic I would say now. Is there work going on to add that third leg to this thing?

MS. DROUIN: A lot of discussion on that, yes.

MEMBER BLEY: Okay. But you're not talking about that anyway here.

MS. DROUIN: No, not at this point. This is just where we've gotten so far.

MEMBER CORRADINI: So if Dennis characterized it right then, the what is very broad parameters of what must be done, but in the how part one would have to go somewhere else to see what's been historically done or what are acceptable possibilities or the individual would just come up with something different. Is that fair? Is that a fair characterization?

MS. DROUIN: This is basically a fair statement.

MEMBER CORRADINI: Okay. Fine.

MS. DROUIN: And which is why the peer review is a critical part of the standard and a critical part of our reg guide.

MEMBER CORRADINI: Okay. That helps me a

lot. Thank you very much.

MS. DROUIN: Okay. So we did issue in June of this year DG-1200 which is the proposed revision to Reg Guide 1.200 and it has looked at this ASME/ANS standard which goes all the way out to external hazards. It's still at full power. And we have also looked at the NEI documents on the peer reviews, how to do your peer review because the peer review is a critical part. The standard and our reg guide just tells you what to do. This is what you need to have in this standard for a PRA to be technically acceptable. There's a lot of interpretation of how to do that.

That may not be acceptable. It may not meet the intent of what's in there. So the decision was made because we wanted to meet that purpose of obviating the need for us to do in-depth review to put that onus on the industry for them to do a detailed peer review of looking at the how-to and that the how-to did meet all these requirements in the standard.

So from that perspective from a regulatory perspective, then we've taken a big, in some places, a very hard line on what is an acceptable peer review because we're trying to obviate our need for doing it and we need to have the faith that the industry has

really, truly done a detailed peer review to support the ultimate purpose of the reg guide.

MEMBER STETKAR: Mary, just since we're talking about history and history is forward-looking simply, we're getting to a point where I think it seems like we're approaching the threshold of completeness, if I can use that term, in Level 1, full power risk assessment contributors. Do you have any estimates of when we're going to get the low power shutdown companion to this history?

(Laughter.)

MS. DROUIN: My last slide is going to go over the schedule and what's coming down the road.

MEMBER STETKAR: Okay. Fine. Thank you.

(Off the record comments.)

MEMBER BLEY: We're running out of time.

MS. DROUIN: Okay. So this regulatory guide is structured with two parts, what I call parts. There's the main body and then there would be appendices. The main body states the staff position on a lot of stuff and I'll go through that and the appendices give our position on the standards and the industry documents.

The one thing I want to point out is that we're up to Rev 2 on this document and there's a lot

of language that at this point because we've gone through so many revisions, we've some pilots, that we've gotten to a point where we, when I say we both the NRC and industry, are comfortable with the language. We've come to a common understanding of that language. There are still places, but for the most part we've worked out all of the disagreements of a lot of the language in the main body.

What is this main body? It does describe the relationship of this document to other regulatory guides and other activities. Of course, it provides the staff position on what constitutes a technically acceptable PRA. And given that, it then provides our position, the NRC position, of how to use a national consensus standard to meet what we define as an acceptable PRA and also the PRA review guidance. It provides the staff position on how you demonstrate that the PRA has done this and then ultimately what you need to document and we approach the documentation from both what you need to be archiving and what you need to have in your submittal.

I don't want to spend a lot of time on this, but I think that this is a good visual of how Reg Guide 1.200 works and what it is and what it isn't. And if you go across the top there is where

you have all your different applications. For example, you know licensing, using Reg Guide 1.174 which is the regulatory guide that is supporting that.

What you see here are applications and the application specific regulatory guides on things that are using risk results and insights. So this is where Reg Guide 1.200 is common across all of these. So it's a regulatory guide that doesn't support a specific regulation. It supports risk informed activities. So it's always invoked via another reg guide.

You will be seeing, for example, Reg Guide 1.174 will now reference. In the past, it didn't reference it because it didn't exist at the time. But it will reference 1.200. That's where you go for the base PRA.

MEMBER APOSTOLAKIS: Is 1.174 under revision now?

MS. DROUIN: Yes, it is.

MEMBER APOSTOLAKIS: Are we going to have a chance to look at it?

MS. DROUIN: I'm sure you will because that's part of the process that you all get an opportunity.

So the point I want to make is that this

is a reg guide that's invoked by other regulatory guides. It's not a reg guide that's invoked by regulation. So it's very unique in that regard because most reg guides are invoked by regulation. This one is not.

MEMBER CORRADINI: So just to take an example case. So if one was going to do a certification, one would look at 1.206 about how the PRA gets into a certification.

MS. DROUIN: Right.

MEMBER CORRADINI: And 1.206 would then say, "Go look at 1.200 for some general overarching principles."

MS. DROUIN: Yes. I don't know if that's exactly how it says it.

MEMBER CORRADINI: But I'm sure it will eventually.

MS. DROUIN: Yes, and it does without going -- I think it already does 1.200.

MEMBER CORRADINI: Okay. Thank you.

MS. DROUIN: Okay. The scope of 1.200 right now, it primarily addresses light water reactors and new LWRs for design certification and combined operating licenses.

MEMBER BLEY: Does this imply that staff

thinks the reg guide and the consensus standard are appropriate as is for the highly passive designs?

MS. DROUIN: No.

MEMBER BLEY: Okay, but some may be coming through this process.

MS. DROUIN: And we added in this particular version of 1.200 there's a lot of caveats there now sprinkled all the way through about what you need to maybe do in addition for design certs, well, for these new LWRs. Now we don't have any caveats in this version of the reg guide for like non-LWRs.

MEMBER CORRADINI: So just so I understand your answer to Dennis. So if you look at 1.200 it will be careful to state that certain things relative to passive safety and reliability are not there yet but the user must consider it in some manner. Is that the way you're -- I'm trying to understand.

MS. DROUIN: No.

MEMBER CORRADINI: So how would it be identified that it's not generic enough for the passive systems? I'm trying to understand.

MS. DROUIN: Because right now it's not addressing reactors or passive systems as a player, a major player. Let me rephrase that.

MEMBER APOSTOLAKIS: ESBWR.

MEMBER CORRADINI: Well, AP1000.

MS. DROUIN: Well, you did catch me on that. I don't have a good answer for you to be honest.

MEMBER CORRADINI: It's not so much that I'm trying to catch as much as I'm trying to understand how generic it is relative to the advanced LWRs and then even further --

MS. DROUIN: Let me try and answer it this way.

MEMBER CORRADINI: That's fine.

MS. DROUIN: No. It doesn't address it directly in that manner.

MEMBER CORRADINI: Okay.

MS. DROUIN: The way we handled it is that at one point in time -- let me pull it out because I'll give you the exact words because we went round and round with ASME and ANS on this because at one time the standard just was open-ended and when you read the objective and the scope of the standard it sounded like the standard could be applied to every kind of reactor and every kind of plant stage and we objected to that and we had been carrying an objection on Reg Guide 1.200 on that.

In this version of the standard, we have

removed our objection because they did add these words to the standard and they said without reading you the whole paragraph, "This standard may be used for plants under design or construction for advanced reactors or for other reactor designs. Thus revised or additional requirements may be needed." So it doesn't explicitly --

MEMBER CORRADINI: That's code for everything that's new and improved. That might be passive. There might be a different system.

MS. DROUIN: That's right.

MEMBER CORRADINI: Okay.

MEMBER APOSTOLAKIS: Everything that is new.

MS. DROUIN: so there is an acknowledgment in the standard now that you can't just go and blindly use this and say you've done all of this and so you're using it for the AP1000 that you're now okay because the AP1000 is a new -- It's not an operating LWR that this was originally written for.

MR. DUBE: Mary, can I just add? This is Don Dube, Office of New Reactors. Under the Committee on Nuclear Risk Management of ASME, there is a working group to develop additional requirements for advanced light water reactors.

MS. DROUIN: Right.

MR. DUBE: But that hasn't been accepted and endorsed yet.

MEMBER APOSTOLAKIS: So passive cooling systems will be part of that.

MR. DUBE: It may be.

MEMBER APOSTOLAKIS: If it isn't, what else is there?

MR. DUBE: I'm just saying we're still in the process of developing requirements.

MEMBER CORRADINI: Not that -- I guess I want to understand. So in some sense the standard, wherever stage it is, is always following never leading how one would attack any one particular new thing.

MR. DUBE: Correct.

MEMBER CORRADINI: Whether it would be a passive safety system, a different plant with different fuel or potential different containments that aren't really containments, more confinement. Is that a fair statement?

MS. DROUIN: On the standards that's a yes and a no and I think it depends on the particular standard and the particular committee. There's a lot of views in the standard community whether a standard

should lead or whether it should wait until every thing is tested and everybody is in agreement. Then you write the standard. So there's not a consensus at least in my view of when you should start writing a standard.

MEMBER CORRADINI: Okay.

MEMBER BLEY: Just to clarify one last thing. Are there places in the reg guide that I missed other than Table A-1 where you compare with the standards where the caveat for the new designs would be there. What I'm saying is maybe Don could address this. If somebody in NRO is reviewing a PRA that's coming in, would they know that the standard and the reg guide are not applicable under they look hard at this?

MS. DROUIN: There are caveats sprinkled in footnotes and in places through the main body of the reg guide.

MEMBER BLEY: There is enough in there to give them warning.

MS. DROUIN: I think there is.

MEMBER BLEY: We'll learn where they are so we can point to them later.

MEMBER APOSTOLAKIS: Are you -- my question.

MS. DROUIN: Sorry.

MEMBER APOSTOLAKIS: Did you talk about --

MS. DROUIN: No, I think I'm going forward.

MEMBER APOSTOLAKIS: You had the LRF there.

MEMBER BLEY: Yes.

MEMBER APOSTOLAKIS: Where was it?

MS. DROUIN: Okay. Sorry. Right now, when I say addresses it was meant to cover CDF, LERF and Large Early Release. Now when we issued DG-1200 we did have a definition of a Large Release Frequency in there and during the stakeholder comments we got a minor comment on the definition but it wasn't a big deal.

However, on the application of this, there's been a lot of discussion going on and because of that and since the standard yet for the new reactors isn't out, what we have elected to do -- Where did Don go? Did he abandon me in my time?

MEMBER BLEY: No, he's here.

MS. DROUIN: Just in case you want to add to what I'm going to say. In the last couple of days what has been decided is to remove the definition from 1.200 and just put a footnote in referring to a

particular SRM.

MR. DUBE: Yes, SRM on SECY 90016.

MEMBER APOSTOLAKIS: But the version we have still has it.

MS. DROUIN: Because as I said, this just happened in the last couple of days.

MEMBER APOSTOLAKIS: I just wanted to raise the issue of the utility of LERF and LRF and as you know what we found in the power uprates is that LERF is not the best metric to use because it's just the frequency of the -- It doesn't tell you what is released and how much. And I'm wondering for how long we're going to tolerate that.

Now I admit that for most risk informed applications CDF and LERF and probably CDF and LRF would be good enough. But for those special cases where they are not good enough especially LERF should there be some effort to give some additional either guidance or metric or something that will allow us to truly be risk informed when we consider for example power uprates?

All I'm saying is I'm not saying drop LERF and LRF. But at some point we have to acknowledge that there was an application where this was not a very good metric and we recommend this. Do a little

bit more to make sure that your decision is really based on everything that is relevant.

MS. DROUIN: That belongs -- That discussion and that concern would not be addressed in 1.200. That concern would be addressed in that application-specific regulatory guide. All this guide says is that given that you have to do a PRA for LERF or a PRA for a Large Release Frequency here's what that PRA needs to address.

MEMBER APOSTOLAKIS: That may be. But it seems it was presented earlier that this is really a foundational guide that feeds into the other. I can see your point. I mean it could mean something somewhere else, but I'm afraid it's going to be lost again.

MR. PARRY: I don't think it's this foundational, George. I think this is a support document.

MEMBER APOSTOLAKIS: A support document.

MR. PARRY: The Reg Guide 1.200 is a support. It's not fundamental.

MEMBER APOSTOLAKIS: I understand. As I say, maybe Mary is right. Maybe it should be somewhere else.

MR. PARRY: Right.

MEMBER APOSTOLAKIS: But I'm wondering where that somewhere else.

MS. DROUIN: Well, in my mind, it goes into the application-specific regulatory guide.

MR. PARRY: Yes, I think that's right.

MS. DROUIN: Now it may be that it applies to more than one guide.

MEMBER APOSTOLAKIS: It could.

MS. DROUIN: But it goes to the application-specific guides.

MEMBER APOSTOLAKIS: But the problem is we don't have a risk-informed regulatory guide addressing power uprates. We do not. So, in fact, power uprates are not risk-informed, right?

MR. PARRY: Right.

MEMBER APOSTOLAKIS: And it's an integrated decision making process, right, Gareth?

MR. PARRY: Right.

MEMBER APOSTOLAKIS: It ought be somewhere it seems to me. I mean if we find a deficiency somewhere we should point it out and make sure that it's addressed.

MEMBER BLEY: I think that's one we can follow up on. You know, the standard itself under applications tells you have to look for things like

that. But I think you're right, George. But maybe we can go ahead.

MEMBER APOSTOLAKIS: And maybe -- You said that you removed it. When you put it back in, maybe you want to add a few words about what one should do in certain applications where the LRF and LERF might not be the best method to use. That's all I'm saying. Give some guidance on that.

MS. DROUIN: Is that something we could take under advisement? Yes.

MEMBER APOSTOLAKIS: That's all I want from you, Mary.

MS. DROUIN: Okay. The scope does address all operating statements and you will see that in the main body of the reg guide we don't just list the attributes and characteristics for the PRA for at-power conditions. We go all the way through for low power and shutdown also. We address both internal and external hazards. So it does cover internal bands, internal flood, internal fires, seismic, high winds, floods, external floods, etc.

Does not provide a staff position and other risk analysis. Okay. The reason I put this slide here because this is an area where we and industry are not in agreement.

MR. PARRY: We and some of industry.

MS. DROUIN: Some of industry, you're correct. He's absolutely correct because industry is kind of split down the middle. This guide is addressing what we say is probabilistic risk assessment where we are diverging with some of industry is what is meant by a PRA and these are the exact words that show up in this reg guide. Over the versions going from Rev 0 now to Rev 2 we've added more words because when you start getting into other risk analyses, not a probabilistic risk analyses, but other risk analyses you can't come in and say they are equivalent or can be used as a substitute for a probabilistic risk analysis.

MEMBER APOSTOLAKIS: Are you referring to the qualitative risk assessment that we see every now and then?

MS. DROUIN: I'm referring to, for example, seismic margin is not an alternative to a seismic PRA, doing configuration control and it's not that we don't say that these things don't have value and don't have their place. But they aren't a substitute for a probabilistic risk assessment.

MEMBER APOSTOLAKIS: I'm with you.

MS. DROUIN: So configuration control, low

power ship-down is not a low power ship-down PRA. Okay.

(Off the record discussion.)

MS. DROUIN: So we haven't backed off on this position and we keep thinking that it's gotten resolved, but it keeps coming back to the standards and there are people there who still want to call these things or making them as an acceptable alternate.

MR. GRANTOM: Can I add something please? This is Rick Grantom. I'm also the Chair of the ASME Committee on Nuclear Risk Management that produced the standard that's being endorsed here in Reg Guide 1.200.

Mary is absolutely correct. We wouldn't use seismic margins or I personally wouldn't use seismic margins as being a substitute for a seismic PRA. However, the point of me standing here right now is to inform you that when we talk about risk management we are talking about a discipline where PRA supports that and in the context of risk management there is a need for qualitative type standards out there, shutdown risk being one of them, and there may very well be other qualitative type standards that are necessary to support applications and decision making

out there. So in the risk management we view both the need for qualitative and quantitative standards recognizing the distinction that Mary Drouin just brought up that is kind of split down the middle from the industry in the sense of those who view that it's really to be probabilistic and those that there may be other qualitative standards that are risk management standards but may not be necessarily probabilistic.

MS. DROUIN: And the only thing I would want to add because we agree that there is a place for these and they should be developed and there is a place for them to be used under certain applications. But we don't believe that when you write a standard for example on low power shutdown for a PRA that you have in there as an acceptable PRA for low power shutdown configuration control. It should be in its own separate standard supporting risk management activities.

MEMBER APOSTOLAKIS: By the way, your first bullet is not quite accurate. You're really providing the minimum requirements that are technically acceptable a PRA should meet.

MR. PARRY: I think that's probably right.

MEMBER APOSTOLAKIS: Because you don't go into the details of how to do it.

MR. PARRY: That's correct.

MEMBER APOSTOLAKIS: Something that they do to meet one of your requirements may not be acceptable to this.

MS. DROUIN: That is correct.

MEMBER APOSTOLAKIS: So you are really providing the minimum. I understand that this.

MS. DROUIN: This is what I was trying to get into.

MEMBER APOSTOLAKIS: No, I understand.

MS. DROUIN: That our technical acceptability is defined in terms of these elements and we don't get into the how-to.

MEMBER BLEY: Mary, before you leave this one. It will come up on some of your others. I guess our last two letters with respect to the reg guide both recommended that there would be a separate reg guide on sensitivities and uncertainties and now there's a NUREG on that. But I don't see anything in the definition of the PRA and when I search I don't see anything that even says uncertainty in here until I get into the internal fire technical elements. I'm a little surprised at that and I wonder why it's that way.

MS. DROUIN: Uncertainty is addressed

several places in the regulatory guide.

MEMBER BLEY: It certainly shows up in the --

(Off the record discussion.)

MS. DROUIN: No, it's --

MR. PARRY: Actually, probably if you look at -- of results I think it will be in that.

MS. DROUIN: That's where I think that's where we put it.

MEMBER BLEY: It is in there.

MR. PARRY: Yes, and that's where I think we address it.

MEMBER BLEY: It seems such a central thing to me.

MS. DROUIN: That's why we -- At one point in time, the interpretation of results was buried under the various technical elements. We just happened to call it interpreting instead of having uncertainties sprinkled through the various technical elements and that was one of the comments that we got from the stakeholders. They didn't feel that that was a technical element and we thought, "No, that is a technical element." In the standard, it doesn't show up as a technical element. It's part of the quantification element. But in our regulatory guide

we brought the interpretation.

MEMBER BLEY: I don't want to stay on this too long because you have a lot to cover. But do you suspect in later revisions of this guide once that NUREG is completely out, the reg guide will refer to that.

MS. DROUIN: We do refer to NUREG 1855 in here.

MR. PARRY: I think we do refer to it in here.

MS. DROUIN: It is referred to in here.

MEMBER BLEY: All right. Go ahead.

MS. DROUIN: It is in here.

MEMBER BLEY: -- in the definition, but that's fine.

MS. DROUIN: Okay. So the other part of the scope it does allow when you walk through the main body it goes through and it identifies the different technical elements you need in a PRA, what are the attributes and characteristics and we go through pages and pages of that and then the next position in the regulatory guide is you can use a standard to demonstrate that you've met our position, i.e,, that you've met all these attributes and characteristics that we've defined that you need for a technically

acceptable PRA.

And part of that is the peer review. Our reg guide also states our position of what is a technically acceptable peer review and again that's really important so that we go back to obviate our need.

Now in using of the consensus standards when you read the main body of the reg guide you look at the standard that's written to these different capabilities categories. I won't go through the long history of it, but at this point in time we feel that those capabilities categories has cause more confusion than help and we're highly recommending that the standards, that the SDOs, I see people shaking their heads, "Yes, I love that," get rid of these capability categories and do one category.

MEMBER APOSTOLAKIS: Yes.

MS. DROUIN: It just causes a lot of problems.

MEMBER APOSTOLAKIS: How many licensees have come to NRR and request for some change and they say we're going to do Category 1?

MR. PARRY: Actually, I think nobody would say that because I mean the categories are on a supporting requirement by supporting requirement

basis.

MS. DROUIN: Yes.

MR. PARRY: They may say that "Okay, my PRA is being peer reviewed and I only have capability category 1 for the supporting requirement, but it doesn't affect my application." But I think that a general philosophy and the philosophy of the peer review groups that are out there is they aim for capability category 2.

MS. DROUIN: That's correct.

MR. PARRY: That is generally the goal that we hear that they're working towards which is why we put in that third bullet.

MEMBER STETKAR: George, the only place that I've seen it lately was in the design certification stuff.

MEMBER BLEY: It's in the SECY.

MEMBER STETKAR: Is it in the SECY?

MEMBER BLEY: I think it was in the SECY.

MEMBER STETKAR: It says capability category 1 treatment is adequate for PRAs.

MEMBER APOSTOLAKIS: I don't know that.

MEMBER STETKAR: I can't quote the prose and poetry, but I remember we had some discussions over that for design certs.

MR. PARRY: No, but I think that's because --

MEMBER STETKAR: Nobody's come in with that. That's right.

MR. PARRY: They don't have the plant specific information. If you look at the definitions of the capability categories, you get more plant specific information 2 and 3. Don wants to add something.

MR. DUBE: Yes, just quickly. Don Dube. It's an interim staff guidance and it says capability category 1 and that's because they don't have plant specific operating experience. They don't even have in most cases concrete and steel to do walkdowns. So it's hard to expect to do anything more than capability category 1.

MEMBER APOSTOLAKIS: But even for the design certifications I don't need the category 1 officially someplace to tell me what I can do. I thought from the beginning that was a useless thing to do and it's good to see that practice confirms that.

MR. PARRY: No arguments here.

MEMBER APOSTOLAKIS: Thank you very much.

MEMBER BLEY: There were some political reasons.

MEMBER APOSTOLAKIS: I know.

MEMBER BLEY: It's not been used.

MS. DROUIN: So we do have that in the regulatory guide now that doesn't quite say it this way because of how you write a regulatory guide, but our recommendation is as we move forward let's not keep carrying all those categories.

The last thing is the peer review and again this is -- I know I've said it several times, but because it is a very important part, as important as it is to all the requirements written again since they're written to the what levels it's equally important to have a peer review that you can have the confidence in. So Regulatory Guide 1.200 addresses the peer review process that you need to have and we'll come back to this one because this is where we're not sure we're in agreement with industry because the peer review process has to be current with both the PRA and the standard and the peer review guidance documents that are written so far are keeping it current with the PRA, but the standard has also changed. So as the standard changes new requirements are added. Requirements may be revised. The peer review has to be addressing that also.

MEMBER POWERS: Mary, what level of review

of the staff have for a PRA once it's gone through this peer review process?

MS. DROUIN: I'm sorry. I couldn't hear what you said.

MEMBER POWERS: -- the staff relies on the peer review to be sure that you have an adequate PRA. But do they indeed give the PRA some review when it's used in a licensing application? It's been so long since I've had a risk informed application in front of this Committee that I don't know what the staff actually does.

MS. DROUIN: They do ask for the results of the peer review, the findings, and that's why on some of the places we've taken objections because we don't think that what the standard had was documenting everything that we would need when we look at what their peer review did.

MR. PARRY: But can I answer that in terms of there is an SRP section 190.1 which is a companion for this and what that does, it states that the staff can audit the PRA if they think that there's a need to do so and typically that would be triggered by results that didn't smell right for example or they might look at specific assumptions which the peer review had identified that looked suspicious.

So I mean the idea behind this whole process is that we do not do an in-depth review of the base PRA because they replied in Dennis though. Any time the PRA is used and the way it's used and the changes that are made to the model certainly are reviewed.

MEMBER BLEY: But that lacking the in-depth review, you do some kind of spot-checking or at least rationality check.

MR. PARRY: Yes.

MEMBER BLEY: It will send you into the PRA if you --

MR. PARRY: It could do, yes.

MEMBER POWERS: So you're saying that odor is the motivator for the staff to review the PRA.

MR. PARRY: Using the term loosely.

MEMBER POWERS: Why would you not want to at least look at some of the elements that are crucial, for instances, if one has looked at, I don't know, manual actions and fire protection? Why would you not look at the human reliability parts of it?

MR. PARRY: You might in that case because that's one area where there isn't good agreement to do things. It has to be a --

MEMBER POWERS: -- two people to agree on

how to do things.

MR. PARRY: I think it has to be a judgment based on why we think that there would be potential weaknesses. I mean the Commission told us that we should use the standards to the extent possible to determine the PRA quality and it's a matter of I think using our resources wisely.

MS. DROUIN: I think it's going to depend on the application.

MEMBER POWERS: No, I don't think you're saying it wisely. I think you want to be parsimonious with your resources.

MEMBER CORRADINI: Cheap.

MS. DROUIN: I don't know that I would agree with that. I think if you've made the decision that you want to put the burden on the licensee and the licensee has done this peer review, it's our obligation to make sure that they're doing will meet our needs and there's different ways to do that. We have --

MEMBER POWERS: All I'm asking you is what are the different -- Which of all the infinite number of ways are you going to do because the optics to the rest of the world is peculiar. Industry does a PRA and the industry reviews it and the staff accepts that

product. I would not want to be in a position of trying to defend that.

MS. DROUIN: Personally I think it can be defended because we have laid down what we will find an acceptable peer review and this is why on some of the requirements on the peer review we have not backed off on. There are requirements on the process that we have not backed off on. They have got to do this if they want their peer review to be acceptable. We had not backed off on some of the qualifications we want that team to have and we have not backed off on what we want that peer review team to document and I think that those things are crucial if we're going to rely on, not rely on, will rely and use a peer review that's been done by industry.

MR. PARRY: We've also participated as observers in some of these peer reviews and so we do have a feel for what they do and the depth to which they go to and, believe me. They go to quite considerable depth to look through the models, probably better than we could do.

MEMBER CORRADINI: So can I just go back to Dana's original point since I haven't seen? So what's an example of this process on a practical level recently so that I can understand what you're talking

about? Where has it been done that you can go and look and say "Okay, this is what the applicant did. This is the peer review process. This is what the staff did in light of that"?

MS. DROUIN: I can't speak to that because I'm not in NRR looking at applications.

MEMBER CORRADINI: Okay.

MR. PARRY: I don't look at applications either even though I'm in NRR. Sorry about that.

MEMBER POWERS: There have been some -- risk informed applications coming through. I don't know. Maybe this is just all a waste of time.

MEMBER APOSTOLAKIS: Actually, the process is being used internationally right now. Has been used internationally.

MEMBER POWERS: Believe it or not, we don't review international.

MEMBER APOSTOLAKIS: I understand that. But there must be some value to it.

MR. PARRY: We have a comment from one of the NRR's reviewers of licensing applications.

MR. DINSMORE: My name is Steven Dinsmore. I work within NRR. Last week we were doing --

MEMBER APOSTOLAKIS: Speak to the microphone, Steve. I can't hear you.

CHAIR BONACA: A little louder please.

MR. DINSMORE: Okay. Steve Dinsmore NRR. Last week we were down at Oconee reviewing a fire PRA and, for example, we noticed that there seemed to be a common factor between the CDF and the LERF. So we went and reviewed their LERF models and actually we discovered that they hadn't included -- steam generators.

(Off the record discussion.)

MEMBER BLEY: Can you start up in the middle again?

MEMBER APOSTOLAKIS: Tell us again what we lost.

MR. DINSMORE: Okay. We went to Oconee last week to audit their PRA which they're using to support their transition NFPA 805. Can you hear that? He's looking around the corner.

MEMBER APOSTOLAKIS: No. You have to speak straight.

MR. DINSMORE: Okay. My name is Steve Dinsmore. I work at NRR PRA branch.

(Off the record comments.)

Last we to review or to audit the PRA they're using to support transition to NFPA 805. When we were there, we noticed that the CDF and the LERF

were almost always the same difference and so we wanted to see to make sure that that was appropriate for this submittal. So we went and reviewed the LERF calculations that they're doing. That's kind of the way we do it all the time.

You said earlier odor. Well, it's not so much odor. It's just something caught your attention and you look at the things that are important for the application you're looking at and if something catches your attention you would go check that.

MEMBER APOSTOLAKIS: But was that PRA reviewed by the industry?

MR. DINSMORE: Yes. There was a peer review.

MEMBER APOSTOLAKIS: And they did catch the same thing and they commented on it.

MR. DINSMORE: The peer review said that they needed to better document their LERF evaluations.

MEMBER APOSTOLAKIS: I see.

MR. DINSMORE: So they didn't really say that what they were doing was incorrect. They don't usually say incorrect. They usually say it could use more work or could have been done better.

MS. DROUIN: That's why I would go on to say we don't take the industry peer review blindly and

why we have been very careful on what we want them to document, you know, what we want the peer review to document and that's part of their application. If we need to go look at something, we've got their findings from the peer review and we don't consider their findings "Oh, this was a good job." What we have required them to document gets into a lot more than that and it gets into that we want to know where did they consider this PRA to be strong and where did they find it weak. We want them to document the results of the assumption. We have a whole list of things that we accept to see out of this peer review.

MEMBER CORRADINI: But if I can just -- I'm sorry. I think you're helping me at least. So back to what you've just said. So is there kind of -- Independent of the peer review is there a checklist through which the staff goes through to look at things and then as a separate guidepost if the peer review says something has to be improved there, you modify your checklist? In other where is there a protocol for looking at the PRA regardless of what the peer review says?

MR. DINSMORE: There is no checklist. If we're looking at an AOT extension that has to do with diesels we might look at, pay particular attention to,

how the peer review discussed any offsite or if the peer review identified any problems with the or any questions about modeling of the offsite power and recovery of power and then we're doing an AOT extension. We would go look at that. If the peer review didn't say anything about that we probably wouldn't. But if they said anything about it we would go look at it or we would ask questions. So there is no checklist. It's more what exactly are they requesting.

MEMBER CORRADINI: So let me tell you my analogy where I'm coming from which is when we were looking, I hate to connect you to this, but when we were looking at ITACs and the statistical method in which when the plant is supposedly done you would look at ITACs and what we heard was there was a procedure or methodology. You also used very experienced people from the past time and memoriam that actually looked at construction. But the combination of experienced people and some sort of checklist is the wrong word, but some sort of methodology to look at it you kind of looked at the ITACs and make sure things were settled. I'm kind of trying to figure out is there some sort of methodology or protocol here that might be modified by the peer review, but is always there independent of

the peer review.

MS. DROUIN: I'm going to try and answer that for you because I think we're not going to totally get to your answer.

MEMBER CORRADINI: That's fine. I just want to understand.

MS. DROUIN: But Regulatory Guide 1.200 is very specific on what we expect out of this peer review.

MEMBER CORRADINI: Okay.

MS. DROUIN: In terms of how they approach it, the team that needs to be used and what we want them to look at and what we want them to document.

MEMBER CORRADINI: And therefore by that in some sense you think you've covered a lot of this.

MS. DROUIN: I think we've covered the vast majority. Now when you're on a specific application the results of that peer review is part of that application.

MEMBER CORRADINI: Okay.

MS. DROUIN: So I can't put in Regulatory Guide 1.200 to go look at X because X may not be important for that application.

MEMBER CORRADINI: I understand.

MR. PARRY: That's the point. I think

what the reviewers do is they look at the results that drive the decision and by looking at that you can see if there are any concerns with the, that's what Steve was saying I think, parts of the PRA that drive those results.

And if you do have concerns with them then you go and look at them. But typically a lot of these things are relatively straightforward and done according to a consensus approach, right. I mean there are a couple of consensus approaches to do recovery of offsite power for example, accepted approaches I should say.

MR. DINSMORE: Yes. And there are the recovery curves.

MR. PARRY: Right.

MR. DINSMORE: Essentially it's especially a number of these things you know when the results are somewhat reasonable for AOT extensions and if they get to be unreasonable and even if there were no comments or FNOs, we would go -- we would usually ask some questions. We don't go look that often.

With brand new things, you get a lot of attention like the new fire stuff. So then everybody -- You've got quite a number of people involved and they all try to decide which ones, what's important.

But once the system is kind of up and running for past applications that you've had a lot of experience again there's no checklist, but it's kind of stated.

MEMBER BLEY: I think we've got this picture. I would like us to move ahead.

MEMBER ARMIJO: I just want to ask a real quick question. If someone has completed a PRA right now and has done their peer review but it's not consistent with the requirements in this new reg guide, what happens then? How do you accept an application or how do you --

MS. DROUIN: Now you're getting over into applications space.

MEMBER ARMIJO: No, I'm just saying the PRA isn't good enough because the peer review wasn't good enough.

MS. DROUIN: But that's --

MEMBER ARMIJO: That's the assumption I'm getting. I'm confused.

MS. DROUIN: All I'm -- My whole scope is just to define this is what an acceptable peer review is. If they don't meet that, then --

MEMBER ARMIJO: Then you question the PRA.

MR. PARRY: Well, you don't have a basis for accepting the PRA.

MEMBER ARMIJO: But people have it. So how do the applications people use it?

MS. DROUIN: I'm just saying that's not part of Reg Guide 1.200. You're talking to the wrong people.

MEMBER ARMIJO: I would just like to see if the whole organization knows what he's doing.

MEMBER APOSTOLAKIS: It is important though it seems to me to bear in mind that all the information we have received over the years about this peer review is that it is a rigorous and good process. Let's not forget that. We sent one of our own engineers there, in fact, a guy who was a former inspector and not easy to please and he came back and he said, "This is great."

Now admittedly he had attended only one, but this is not the only input we have seen. So it's not just -- I mean it's a process that's working well and now in the final analysis it is the staff's responsibility to make sure that the supporting evidence in a decision is sound and whether a peer review has occurred or not really is irrelevant here. I mean they can make mistakes without the peer review.

MS. DROUIN: The reason I can't answer it

is because for example for a particular application let's just say that the peer review was not a good review. But it could turn out that how they're using the PRA in this particular doesn't matter anyway. So I can't tell you what they're going to do because it's all application specific driven. You know, my job is just to make sure that I have provided this is what is going to be an acceptable peer review for this base PRA.

CHAIR BONACA: All right.

MS. DROUIN: Okay. I know you can't read this. You're not meant to read it. It's just meant to give you a headache. No, just joking.

(Off the record comments.)

All I'm trying to demonstrate is that there's been a lot of the standards work has been going on. There has been addenda, revisions. NEI has been producing the peer review guidance documents. You know, they're on their second and third revision. So there's just a lot of history here and not even finished yet. So as I said Rev 2 is just one along the way.

CHAIR BONACA: All right.

MS. DROUIN: Okay. So now we went through the main body. Now we're going to try and quickly

take you through the endorsement of where the standards are now and the ones that we're endorsing.

When you go through the appendices what you will see the staff will either say for that particular requirement we have no objection. We're fine with it. Or we have what we call an objection with a clarification where we don't have a technical disagreement, but we think that the language is still vague enough. It's sufficiently vague. We think there's a good likelihood someone is going to misinterpret it. So we provide language to clarify what we think they were trying to say. Then the last objection we take is what we call a qualification and that's where we have a disagreement with what they've said. We don't agree with them.

In both the clarification and the qualification, we provide them with language that if you wrote it this way it would remove our objection. So we're not just trying to tell them, "Bring me another rock." We're trying to be very clear with them on what would make it acceptable.

MEMBER BLEY: How does the licensee deal with this reg guide? Do they just report that they have carried all of the steps that are in the reg guide and then we certify that they've met your

clarification?

MS. DROUIN: When you read the main body of the reg guide and we talk about how you use the standard, we say that you have to meet our objections. You can't just meet the standard. You have to meet it in light of our objections.

MEMBER BLEY: So they essentially just certify that they've done that.

MS. DROUIN: Yes. It's an important part though --

MEMBER BLEY: No. I understand.

MS. DROUIN: -- because they are under oath and affirmation.

MEMBER APOSTOLAKIS: Is this slide referring to what ASME or somebody is proposing? Is that what this is doing?

MS. DROUIN: The appendices in Regulatory Guide 1.200 go through literally like, for example, Appendix A goes through the standard. The standard right now is divided into ten parts. We have ten tables. It goes line by line and tells you whether or not we have an objection.

MEMBER APOSTOLAKIS: The standard? Which standard?

MS. DROUIN: Appendix A to Regulatory

Guide 1.200 is a 50-page --

MEMBER BLEY: The joint ASME/ANS standard.

MEMBER APOSTOLAKIS: Okay. That standard.

MR. PARRY: That standard, right.

MS. DROUIN: So our endorsement of that standard shows up and the way we endorse it, we either say for each requirement we say we have no objection, we have an objection with a clarification or a qualification.

MEMBER APOSTOLAKIS: Right.

MEMBER BLEY: And for those who didn't notice it, Appendix B is exactly the same with respect to the NEI peer review process.

MR. RYAN: Right. Appendix B is the NEI which is the peer review process for your Level 1 LERF. Appendix C, that looks at NEI 05-04 which is the peer review for your updated PRA. And then Appendix D is the peer review guidance of internal fires.

MEMBER APOSTOLAKIS: Very good.

MS. DROUIN: Okay. So I'm going to let you all now take a pop shot at Gareth.

MR. PARRY: Okay. One thing that's different from this revision to Rev 1 is that now Appendix A as Mary said is now split into ten parts.

That's because in fact what we're endorsing in Appendix A is an Addendum A of the combined standard. The combined standard was originally issued back in February I guess.

MS. DROUIN: April.

MR. PARRY: April. Okay, April but the addendum was written to try and rationalize it and break up the different what we now call hazard groups. So it's structured in terms of general requirements which are across the board for all the hazard groups. A-2 is just for just internal events. You'll notice that we split out in the standard internal -- has been split out as a separate group. So it goes through all the separate parts of the standard. So we'll go to the next one then.

As far as the general requirements go, we had a lot of, not a lot, we had some clarifications on the general requirements in DG-1200. Most of those have been addressed during this addendum. There are still some issues on peer review which we objected to the language that was used. Specifically we wanted to be made clear that we expect the peer reviewers to be assessing the appropriateness of the assumptions that are made by the analysts. We also require that they review all the applicable requirements and applicable

there means applicable to however the PRA is being used.

We feel there should be a minimum list of the topics to be reviewed. The language in the standard says typically the peer review would address these and it also says this is neither a complete list nor a minimum list. So we weren't really sure what it meant. But we feel there should be at least a minimum list and that there is a requirement to document what was reviewed because at least that gets to some of the concern about the quality of the peer review. The next one.

In terms of the internal hazards for which I mean internal events, internal floods and internal fires, again the majority of the concerns we had were addressed. I'm not sure it's worthwhile going through these individual qualifications that we still have. They're very technical and I don't think they reflect on the general use of the standards. In the interest of time, I think we'll just move on.

Similarly, with the external hazards which are addressed in Tables A-5 though A-9. Again, as Mary said, we originally reviewed the ANS standard which was the origin of these requirements several years ago and they have been revised and most of our

concerns have been addressed. The only issue that we feel that we wanted to make a stand on was the issue of the tornado wind hazard where they had included in the standard in a note useful things to think about and we thought they were essential to think about when modeling tornados.

The seismic margins section which is A-10 in the standard we haven't endorsed it because we think it's outside the scope of Reg Guide 1.200.

MEMBER BLEY: Because it's not PRA.

MR. PARRY: Because it's not PRA, right. Yes, not because it's not a useful method.

Okay. Now Appendices B-D get our comments on three sets of three NEI documents. It's NEI0002, NEI05-04 and 07-12. NEI 0002 is the original industry peer review process. In the main body it has a process. It also has what they call sub-tier criteria for judging various grades of PRA and the most important part to us was a self-assessment process.

The history was that this document was produced before the standard. Therefore they had a set of criteria which don't match one-for-one to the ASME standard. The self-assessment process was designed to do the gap between what the old peer reviewers using the NEI0002 had done and what they

should do against the standard. And this has been, this self-assessment process is measured against an earlier version of the standard, the 2005 addendum B of the original ASME standard.

Since that time, of course, we've got now a whole new standard which is the combined standard. So our position is and we've made this clear in the discussion both on NEI0002 and 05-04 that if the results of the self-assessment are going to be used to support statements about PRA quality then there has to be a delta between the standard and the PRA as was done historically in that self assessment and what it would be now. Because basically some of the -- Although I don't think really many of the requirements have changed, there has been some rationalization of them. But I don't think many of them have really changed significantly. Certainly, the PRA has changed.

Our statement is that, yes, you can still use the results of the self-assessment process, but you'd better do a delta against the current state of the standards in the PRA.

The NEI 07-12 is I believe the fire PRA review standard and the way it's written it says that it should be performed against Rev 1 of the ASME/ANS

standard. I think our statement is that it needs to be done against the Addendum A of the standard because there are differences between Addendum A and Rev 1. And again, I think that we want every applicable requirement needs to be reviewed. So NEI 07-12 and NEI 05-04 really are more current I think as processes in that they really use the ASME/ANS standard as the basis for the analysis.

And I think that's all I needed to say about that. Did you want to talk about the stakeholder comments made?

MS. DROUIN: Well, we got stakeholder comments from eight or nine different organizations and really the vast majority was one organization and another seven saying, "I agree with that one." But we had when we broke them down in excess of 100 comments. Most of them were really technical edit and I was impressed that they read it that clearly that they could find places where we needed a period or a comma.

The ones that were, if you want to call them, technical --

MEMBER APOSTOLAKIS: They should have come here. We're pretty good at that.

(Laughter.)

MEMBER BLEY: We're good on periods, not

so good on commas.

MS. DROUIN: They did find some things that were accepted we thought and we made -- places where the reg guide wasn't as clear as it could have been they found a lot of those and we accepted those. A lot of comments that just weren't applicable to the reg guide, not that we disagreed with the comment. There was nothing we could do about it in the reg guide. You always get tons of those.

There were places where we didn't agree with them. Probably the most significant comment we got was they don't feel at this point that we should endorse either the fire standard or the external hazard standard and their position for that is those standards haven't been piloted. Our view is these are official standards. They're out there.

The standard is a living document as our reg guide is a living document. When we first endorsed the Level 1 standard, it hadn't been piloted. The standards will change and as they change we will update our endorsement. But we don't agree at this point not endorsing these standards because they haven't been piloted. How much and when they're going to get piloted, who knows how long that's going to take.

But I also feel that having our endorsement out there is good for the pilots because they have that information of where our issues are also. So that was one we didn't agree with. The acceptability of the seismic margin as a seismic PRA and again we kept saying, "Good method. It has its uses, but it's not a seismic PRA."

The self assessment is historical. Gareth talked about that one a little bit. It's not historical because when you read, for example, NEI 05-04 it talks about using the self assessment. So again if you're going to use that self assessment, it needs to be current to what the current requirements are and to the current PRA.

Assessment of non-routine activities, that was one of the thing. Someplace we have in the Level 1 part and it's an objection we carried for a while is that we think that they should look at non-routine activities. They shouldn't just be limited to routine and so this one is that they wanted us to remove that non-routine.

MEMBER STETKAR: Mary, just real quickly, what is a non-routine activity in this context? An example?

MR. PARRY: Emergent maintenance maybe.

MS. DROUIN: Something is happening and you've gone out and you haven't particularly -- It's something that you haven't done as a formal part of going out and doing your maintenance. Something has happened and you've gone and had to do some maintenance. So that's a non-routine.

MEMBER BLEY: Go on.

MS. DROUIN: Level of expertise for tornado hazard analysis, I think that one is self evident. Use of bounding for fire scenarios for capability category two, we think that ought to be -- If you're going to use the bounding that's more of a Category 1. But again we're hoping to get rid of these capability categories.

And the last one is the independence of peer reviewers. What that issue is is industry coming back and saying, "Well, we don't have enough peer reviewers. So we got to use the people who have been doing these PRAs" and our position is "No." If they worked on that PRA, they can't peer review it. So either start training people or whatever, but if you've reviewed that PRA you cannot be part of that peer review team.

Now their rebuttal to that was "Well, they won't peer review the part that they did." Our

rebuttal is "Wait a second. One of the big parts of your process is exactly. It's a consensus process." So he is not even though he may have worked over and he's peer reviewing. The results of the peer review is a consensus of the peer review team. So he's not independent.

Now we're not even forcing them to be independent from their organization. We're just saying you have to be independent from who did the work. You can still be a peer reviewer from that utility. But you cannot have worked on that peer and do this independent peer review.

MR. PARRY: Yes, and I think particularly the issue of coming from the same utility is magnified by the fact that so many of the utilities now own a large proportion of the plants which reduces the number of options you have.

MS. DROUIN: Okay. Schedule and future work. I know you're all familiar with the term WITTS item. This is a Commission due date that has been established by the Commission for many years and I want to reiterate what John said earlier. A lot of people within the NRC, utilities, labs, industry, all over have been working really, really hard to produce this latest 400-page standard over the years.

This is an incredible accomplishment that we've gotten to this point and I know I feel very proud. I don't think everybody knows that we have met to this date that the Commission set for us and the Commission has never backed down. I mean even though we've come in and said, "Well, it's taking longer here." They have never allowed this date to slip with us.

There are still issues remaining to be resolved. When all of these standards, these different pieces, were pulled together into this joint standard, even though originally it was supposed to be written like it was one standard, you know, it springs eternal. There were things that were noted. The more significant ones were addressed, but there are some technical concerns that ASME/ANS are working on for the next revision.

PRA standards, that was me involving PRA because I'm just talking about the PRA parts that are under development.

Low power shutdown, I know someone brought that up. I don't remember who. Dennis brought that up.

MEMBER BLEY: No. John.

MS. DROUIN: John. They have developed a

standard. It went out for ballot. Lots of issues with it and I'm just now talking from a personal perspective. I think they have a lot of work still to do before it will pass ballot.

MEMBER STETKAR: Do you have any guess? I mean, are we talking about another year or eighteen months?

MS. DROUIN: At least. Just because of the way the consensus process works. You're at least a good year.

MEMBER BLEY: A year ago or two they tried to merge a qualitative standard in with the quantitative standard.

MS. DROUIN: They did and that is part of the stuff.

Level 2 and Level 3 are standards being developed where ANS has the lead for that. My understanding is that they do have some drafts written within the working group. They're having some financial problems and what I mean by that is that in these two particular areas most of the experts working on the working groups are retired. So they don't have organizations behind them who can pay for their travel. They're donating all their time for free.

New reactors. A draft of that came out

and it went to ballot. It did not pass ballot. So they're making revisions. I don't think that one's probably too far off in going through the consensus process. I think that one and again I'm just speculating from watching this for the last 12 years how quickly things happen. But I think you're probably at least a year before that one will be out ready for endorsement.

Advanced non-LWRs. That one has not gone for ballot, but it has gone out for a review and I can just say at least from the NRC perspective we had a lot of issues with it. So I think that one's a couple of years at least.

And this is just the PRA standards under development. There's other stuff that's under development that has to deal with risk management. As Rick noted, we are involved in that. When and how those will get endorsed to be decided. But for this particular regulatory guide as the standards are revised, as the scope brings in for example low power shutdown, brings in the new reactors, we will continue to revise this reg guide to stay current with the standard.

MEMBER BLEY: Mary, I had two brief questions.

MS. DROUIN: Okay.

MEMBER BLEY: That you didn't address and in one of the tables, the table on success criteria, it requires the use of best estimate engineering analyses. I doesn't say anything about uncertainty. Is it a given now among the staff that best estimate includes uncertainty or is it done intentional?

MS. DROUIN: The standard also requires you and we note that also in Regulatory Guide 1.200 that you've got to go through and identify your sources of uncertainty. So as part of that process --

MEMBER BLEY: That requirement would cover this even though it isn't explicitly stated.

MS. DROUIN: Yes.

MEMBER BLEY: The other one was between the Rev 1 and Rev 2 it looks like you did a fair amount of expanding the requirements tables on the thing that you call "Hazard Groups, Internal and External" and one thing that just jumped off the page to me as I read them for the fire one you required post fire human reliability analysis, but you don't recall post flood, post seismic or any of those others. I wonder why that is. It seems to me they ought to be there.

MR. PARRY: Yes. Okay. I think the

reason they're that way is that these are written to match the requirements in the standard so a large extent at the high level. If you look at the standard though when it gets to things like seismic, they will have supporting requirements that actually ask you to look at a human reliability under the seismic conditions. They're buried a little deeper. That's all.

MEMBER BLEY: It's kind of a shame they are not parallel.

MR. PARRY: Yes. You're probably right.

MEMBER BLEY: I would like to see it.

MS. DROUIN: when we looked at the original if you go back to Web 1, we wrote our regulatory guide first and we identified the technical elements and when it came down to internal flood, internal fire, the external events, the technical elements were rather terse is how I would capture it.

MEMBER BLEY: But you're reflecting that and you don't see a need to change that.

MS. DROUIN: So when the standard was done, we agreed we did not have a problem with their definition of "Here are the technical elements of a fire. Here are the technical elements." So we then said, "We agree with the technical elements." So we

went and changed our table to have the same technical elements and then identified what we thought were the attributes and characteristics necessary for those technical elements.

MEMBER BLEY: Okay. That just seems like a little gap to me. Any other members have any other follow-up?

(No verbal responses.)

Mary, thank you, Gareth, everyone else.

MS. DROUIN: Thank you.

MEMBER BLEY: Mr. Chairman, two minutes short of an hour and a half, but three minutes past the --

CHAIR BONACA: You're right. You did a good job.

Mary and Gareth, thank you very much for an informed presentation and we're going to take a break now for 15 minutes and be back at 3:05 and we will start to work on the reports. Off the record.

(Whereupon, the portion of the meeting to be transcribed was concluded at 2:24 p.m.)

Regulatory Guide 1.200 Revision 2

Presented to:

Advisory Committee on Reactor Safeguards

Mary Drouin (301-251-7574, mary.drouin@nrc.gov)
Gareth Parry (301-415-1464, gareth.parry@nrc.gov)
US Nuclear Regulatory Commission

March 5, 2009

Purpose of Meeting

- Discuss Revision 2 to Regulatory Guide (RG) 1.200
  - Currently documented as DG-1200 (referred to in presentation as RG 1.200, Revision 2)
- Request letter approving issuance for use

Agenda

- Purpose of RG 1.200
- History of RG 1.200
- RG 1.200
- History of Standards and Industry Guidance
- Staff Endorsement
- Stakeholder Comments
- Schedule and Future Work

Purpose of Regulatory Guide 1.200

- Provides one acceptable approach for determining that the technical adequacy of the PRA is sufficient to support the risk-informed decision-making
- When used in support of an application, should obviate the need for an in-depth review of the PRA by NRC staff
  - Provide for a more focused and consistent review process
- A major technical guidance document in achieving Phase 3 of the staff's phased approach to PRA quality to support risk-informed regulatory activities

History of RG 1.200

- **November 2002**, DG-1122 (draft Revision 0 to RG 1.200) issued for public comment
- **February 2004**, Revision 0 to RG 1.200 issued for trial use
- **September 2006**, DG-1161 (draft Revision 1 to RG 1.200) issued for public comment
- **January 2007**, Revision 1 to RG 1.200 issued for use
- **August 2004**, DG-1138 (draft on staff position on external events) issued for public comment
- **June 2008**, DG-1200 (draft Revision 2 to RG 1.200) issued for public comment
- **March 2009**, Revision 2 to RG 1.200 to be issued for use

Regulatory Guide 1.200 Structure

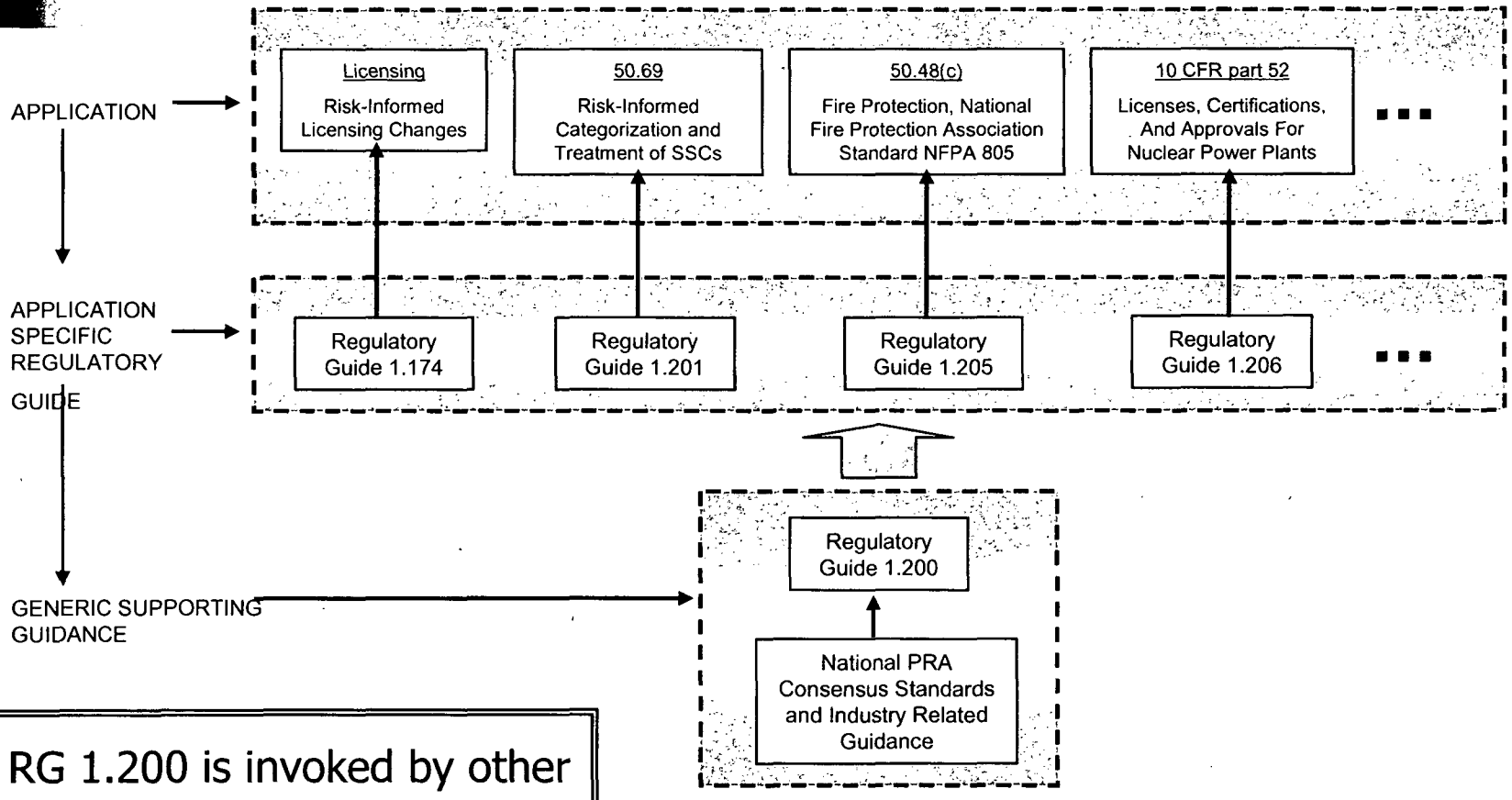
- Main Body
  - Provides staff position on one acceptable approach for what constitutes a technically acceptable PRA
- Appendices
  - Provides staff position (endorsement) on national consensus PRA standards and industry PRA peer review guidance

⇒ ***Majority of staff positions in the main body have not changed since Revision 0 – both NRC and stakeholders, in general, have understanding and are comfortable with the language***

Regulatory Guide 1.200 Content (main body)

- Describes the relationship of RG 1.200 to other guidance documents
- Provides staff position on what constitutes a technically acceptable PRA
- Provides staff position on how to use a national consensus standard and industry peer review in meeting staff position on a technically acceptable PRA
- Provides staff position on demonstrating that the PRA used in regulatory applications is of sufficient technical adequacy
- Provides staff position on the documentation to support a regulatory application

Relationship of RG 1.200 to Other Guidance Documents



⇒ RG 1.200 is invoked by other regulatory guides

Scope of RG 1.200

- Primarily addresses currently operating light water reactors (LWRs), and new LWRs applying for DC and COL
- Addresses CDF, LERF and LRF
- Addresses all plants operating states
- Addresses both internal and external hazard groups

Scope of RG 1.200 (cont'd)

- Provides approach for a technically acceptable PRA, does not provide a staff position on other risk analysis approaches
- Defines PRA

  For a method or approach to be considered a PRA, the method or approach (1) provides a quantitative assessment of the identified risk in terms of scenarios that result in undesired consequences (e.g., core damage or a large early release) and their frequencies, and (2) is comprised of specific technical elements in performing the quantification. A method that does not provide a quantified assessment of the defined risk or does not include the technical elements specified in Regulatory Position 1.2 is not considered to be a PRA.
- Technical acceptability defined in terms of technical elements and their associated attributes and characteristics

RG 1.200: Use of National Consensus Standards and Industry Peer Review

- RG 1.200 allows the use of national consensus PRA standard to demonstrate conformance with the staff's position on what constitutes a technically acceptable PRA
- Standard provides requirements on what a technically acceptable PRA needs to include
  - A peer review is needed to determine if the intent of the requirements in the standard have been met
  - RG 1.200 provides staff's position on what constitutes an acceptable peer review
- Use of a standard has to address the staff's concerns (as addressed in Appendix A to RG 1.200)

RG 1.200: Use of Consensus Standard

- Technical requirements written to different "capability categories"
- Use of the capability categories has caused confusion
- While technical requirements in a PRA may vary, current good practice (Category II) is adequate for majority of applications
- Staff recommends that next revision of the standard address a single category, current good practice

RG 1.200: Peer Review

- NRC has to have confidence in industry peer reviews to achieve a primary purpose of RG 1.200:
  - obviate the need for an in-depth review of the PRA by NRC staff
- Staff position for a technically acceptable peer review addresses:
  - Peer review process
    - Has to be current with both the PRA and the standard
  - Team Qualifications
    - Has to have credibility (e.g., expertise, independence)
  - Documentation
    - Has to document the strengths and weaknesses of the PRA
- Use of a industry peer review process has to address the staff's concerns (as addressed in Appendices B-D to RG 1.200, Revision 2)

History of Standards and Industry Guidance

Standard/Industry Guidance			NRC Endorsement	
Document	**Scope**	**Date**	**Document**	**Date**
ASME RA-S-2002	• At-power • Internal events • Internal flood • CDF and LERF	April 2002	DG 1122	Nov 2002
Addendum A	Same	Dec 2003	RG 1.200, Rev 0	Feb 2004
Addendum B	Same	Dec 2005	DG-1161/RG 1.200 Rev 1	Sep 2006/Jan 2007
Addendum C	Same	July 2007	---	---
ANS 53.21	External hazards	2004	DG-1138	Aug 2004
Revision 1	Same	March 2007	---	----
ASME/ANS RA-S-2008	• Internal hazards • External hazards • CDF and LERF • At-power	April 2008	DG-1200	June 2008
Addendum A	• **Internal hazards** • **External hazards** • **CDF and LERF** • **At-power**	**Feb 2009**	**RG 1.200, Rev 2**	**March 2009**
NEI 00-02	• At-power • Internal events • Internal flood • CDF and LERF	March 2000	RG 1.200, Rev 0	Feb 2004
Revision 1, Self Assessment	same	Nov 2006	RG 1.200, Rev 1	Jan 2007
NEI 05-04, Peer Review Update	• At-power • Internal events • Internal flood • CDF and LERF	Aug 2006	RG 1.200, Rev 1	Jan 2007
Revision 2	**Same**	**Nov 2008**	**DG-1200, RG 1.200, Rev 2**	**March 2009**
NEI 07-12, Int Fire Peer Review	Internal Fire	Dec 2007	DG-1200	June 2008
Draft H	**same**	**Nov 2008**	**RG 1.200, Rev 2**	**March 2009**

RG 1.200: Staff Endorsement of Standards and Industry Guidance

- Staff position categorized as "no objection," "no objection with clarification," or "no objection subject to the following qualification," and defined as follows:
  - **No objection**. The staff has no objection to the requirement.
  - **No objection with clarification**. The staff has no objection to the requirement. However, certain requirements, as written, are either unclear or ambiguous, and therefore the staff has provided its understanding of these requirements.
  - **No objection subject to the following qualification**. The staff has a technical concern with the requirement and has provided a qualification to resolve the concern.
- The staff clarification or qualification to the requirement is indicated in either bolded text (i.e., **bold**) or strikeout text (i.e., ~~strikeout~~); that is, the necessary additions or deletions to the requirement for the staff to have no objection are provided.

RG 1.200: Appendix A Contents

- A-1: General Requirements
- A-2: Internal Events
- A-3: Internal Flood
- A-4: Internal Fire
- A-5: Seismic Events
- A-6: Screening
- A-7: High Winds
- A-8: External Flood
- A-9: Other Hazards
- A-10: Seismic Margins

RG 1.200: Appendix A Table A-1, General Requirements

- Majority of staff concerns addressed
- Remaining issue on peer review
  - Need to assess the appropriateness of the assumptions
  - Need to review all the applicable requirements
  - Need a minimum list of topics to be reviewed
  - Need to document what was reviewed

RG 1.200: Appendix A
Table A-2 thru A-4, Internal Hazards

- Internal Hazards: Internal events, internal flood, internal fire
- Majority of staff concerns addressed

Remaining issues:

- Internal Events: Failure to repair
  - Data collection and estimation should use both plant-specific and industry data where appropriate
- Internal Flood: Flood-induced failure mechanisms
  - Some level of assessment needs to be included in the analysis
- Internal Fire: equipment selection
  - Supporting requirement needs to state what to do

RG 1.200: Appendix A
Tables A-5 thru A-9, External Hazards

- External Hazards: Seismic, screening and conservative analyses, high winds, external floods, other external hazards, seismic margins
- Majority of staff concerns addressed
- No major "qualifications" remain
- Remaining issue on tornado wind hazard
  - Basic elements of the analysis need to be provided as requirements and not as a "note"
- Seismic margins – staff has not endorsed, outside of scope of RG 1.200

RG 1.200: Appendices B-D
NEI Peer Review Guidelines

- Majority of staff concerns addressed
- NEI 00-02 and NEI 05-04
  - Self-assessment performed against ASME RA-Sb-2005
  - Standard has changed since 2005 (e.g., revised requirements, new requirements)
  - PRA may have changed
  - Self-assessment needs to be against both the current PRA and the current standard
- NEI 07-12
  - Peer review needs to be performed using Addendum A to the standard
  - Every applicable requirement needs to be reviewed

Stakeholder Comments on DG-1200

- Majority of comments were of a "technical edit" nature
- Majority of comments were accepted by the staff
- Numerous comments not applicable to the RG

Major outstanding industry issues:

- Do not finalize until fire and external hazard parts of the standard have been fully piloted
- Acceptability of seismic margin as a seismic PRA
- Self-assessment is historical
- Assessment of non-routine activities
- Level of expertise for tornado hazard analysis
- Use of bounding for fire scenarios for Capability Category II
- Independence of peer reviewers

Schedule and Future Work

- Commission due date of March 31, 2009, for Revision 2 of RG 1.200
- Other technical concerns are being addressed by ASME and ANS
  - Addressed in either future addendum or revision to ASME/ANS RA-Sa-2009
- **PRA** Standards under development
  - Low power shutdown
  - Level 2
  - Level 3
  - New Reactors
  - Advanced non-LWRs
- RG will continue to be revised/updated to stay current with published standard

Alternate Fracture Toughness Requirements for Protection against Pressurized Thermal Shock (PTS) Events Rule (10 CFR 50.61a)

NUCLEAR REGULATORY COMMISSION

10 CFR Part 50

RIN 3150–AI01

[NRC–2007–0008]

Alternate Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events

AGENCY: Nuclear Regulatory Commission.

ACRS Full Committee Meeting
March 5, 2009

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

Rulemaking Working Group
Alternate PTS Rule

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

• Barry Elliot	NRR/DCI
• Matthew Mitchell	NRR/DCI
• Stephen Dinsmore	NRR/DRA
• Lambros Lois	NRR/DSS
• Veronica Rodriguez	NRR/DPR
• Mark EricksonKirk	RES/DE
• Robert Hardies	RES/DE
• Nihar Ray	NRO/DE
• Geary Mizuno	OGC

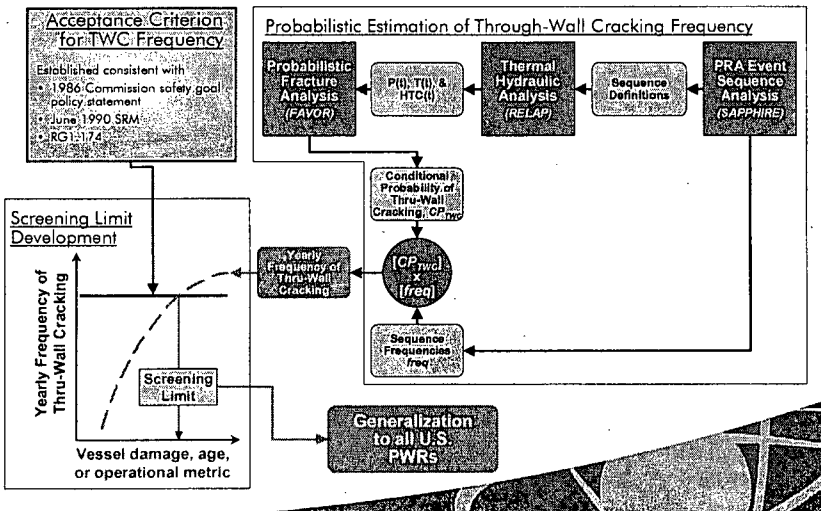
Agenda
Alternate PTS Rule

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

- Main Topics:
  - Technical Basis for the Rule
  - Generalization Study
  - Current PTS Rule and motivation for developing the Alternate PTS Rule
  - Alternate PTS Rule

Technical Basis
Overall Model

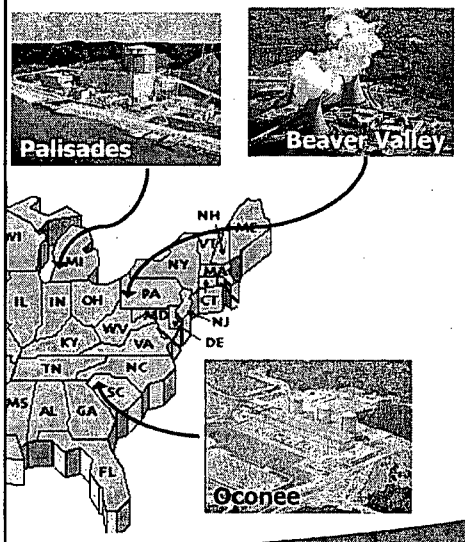
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment



Technical Basis

Detailed Study Plants (Baseline)

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



- Detailed analysis of 3 pressurized water reactors (PWRs)
  - All PWR manufacturers
    - 1 Westinghouse (W)
    - 1 Combustion Engineering (CE)
    - 1 Babcock & Wilcox (B&W)
  - 1 plant from original (1980s) PTS study
  - 2 plants very close to the current PTS screening criteria
- Generalization to all PWRs
  - Characteristics of materials and transients that dominate failure frequencies
  - Examination of 5 more high embrittlement PWRs

Technical Basis

Summary of Findings – 3 Study Plants

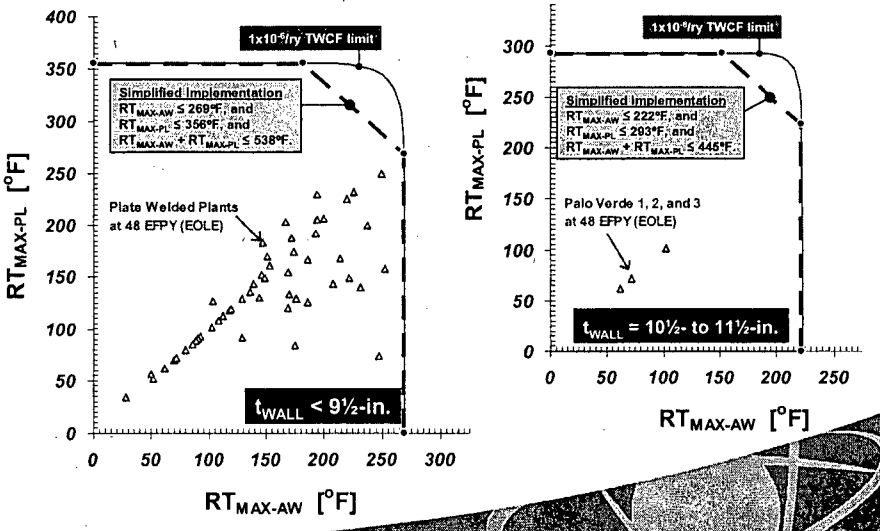
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Only the most severe transients modeled contribute to risk
  - The characteristics of these transients are similar across the operating PWR fleet
  - Operator actions, while accounted for in our analysis, are not important for the scenarios that dominate RT_{MAX} limits
- Axial flaws, and their associated material properties, dominate risk
- Study plant results support development of embrittlement-based through-wall cracking frequency (TWCF) estimation formulae useful for all plants

Technical Basis

RT Limits – Implementation for Plate Plants

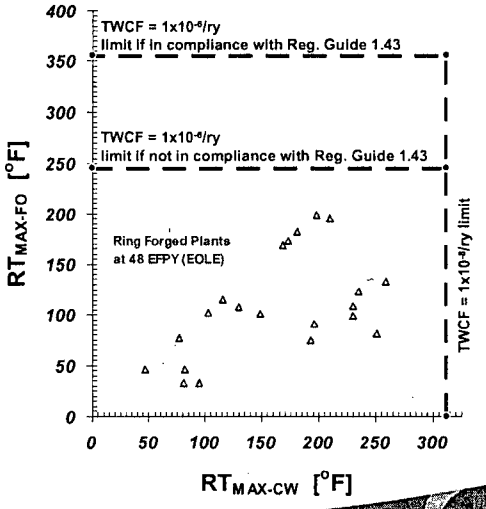
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment



Technical Basis

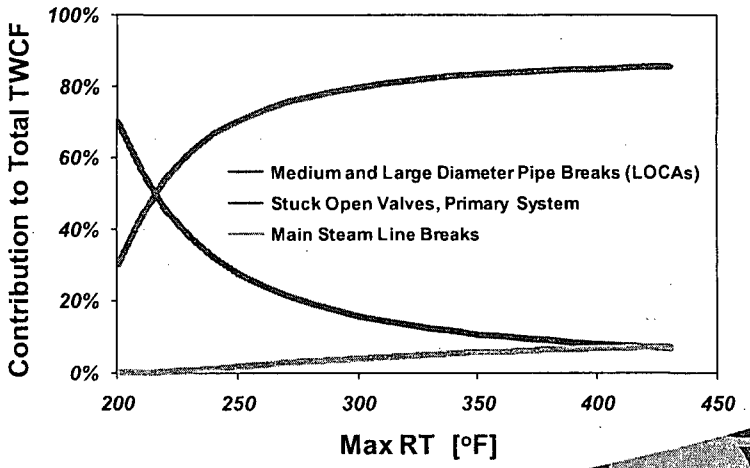
RT Limits – Implementation for Forgings

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



Technical Basis
Important Transient Classes

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



Generalization Study
Methodology

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

- Original detailed study - 3 plants
  - Beaver Valley (W – 3 Loop)
  - Oconee (B&W)
  - Palisades (CE)
- Chose 5 more high embrittlement plants
  - Salem, Unit 1 (W – 4 Loop)
  - Three Mile Island, Unit 1 (B&W)
  - Fort Calhoun (CE)
  - Diablo Canyon, Unit 1 (W – 4 Loop)
  - Sequoyah, Unit 1 (W – 4 Loop)
- Questionnaire used to collect information on the 5 additional plants

Generalization Study

Medium and Large LOCAs

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

- Dominate risk at higher embrittlement
  (75% contributor at new RT-limits)
- Failures driven by factors that are similar across fleet
  - Rate of cooling of the primary system water exceeds that achievable by the reactor pressure vessel (RPV) wall, so the transient severity depends on:
    - Steel thermal conductivity
    - Vessel diameter and thickness

    Not by the thermal hydraulic (TH) characteristics of the transient (i.e., is vessel-limited)
  - Emergency core cooling systems operate automatically. Therefore operator actions do not play a role in these transients
- These factors suggest generalization is possible

Generalization Study

Stuck-Open Primary Valves

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

- Dominate risk at low embrittlement
- Failures driven by factors that are similar across the fleet
  - Low reactor coolant temperatures at time of re-pressurization
  - Re-pressurization to the safety valve setpoint
- Rapid operator action (i.e., high pressure injection (HPI) throttling) can influence this scenario; however, even if credit for operation action was removed, the screening criteria will not change
- These factors suggest generalization is possible

Generalization Study

Main Steam Line Breaks

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

- Slight effect at very high embrittlement
- Failures driven by factors that are similar across the fleet
  - Rate of cooling of the primary system water exceeds that achievable by the RPV wall
  - Temperature in primary cannot fall below 212°F because of secondary side interaction.
- Failures, if they occur, happen before operator action is probable
- These factors suggest generalization is possible

Background

Current PTS Rule – Technical Summary

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

- The current PTS rule, 10 CFR 50.61, has provided a sound, conservative methodology for ensuring adequate protection from PTS events since its promulgation in 1985

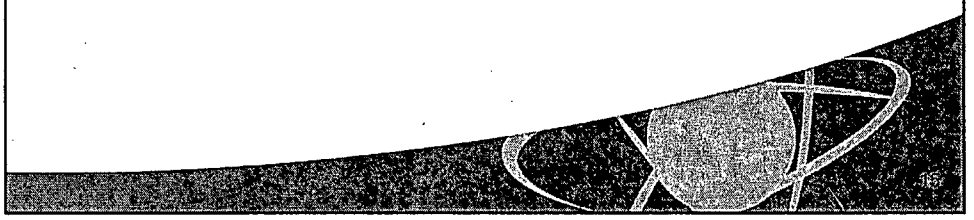
- However,10 CFR 50.61 is fundamentally based on 1980s technology and is not based on the best available information and analyses regarding potential RPV failure due to PTS

Background

Current PTS Rule – Regulatory Summary

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

- The level of conservatism in 10 CFR 50.61 imparts a degree of unnecessary regulatory burden on licensees when compared to our best current understanding of PTS events and the risks they pose
- Under 10 CFR 50.61, approximately 8 to 12 operating PWRs would not meet the screening criteria of the rule through 60 years of operation

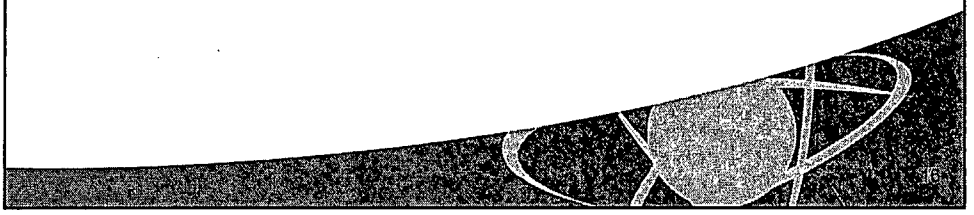


Background

Alternate PTS Rule – Objectives

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

- The objectives of the alternate PTS Rule, 10 CFR 50.61a, include:
  - Adequate protection of public health and safety
  - Regulatory efficiency, effectiveness, and openness
  - Remove unnecessary regulatory burden



Alternate PTS Rule
Overview

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

- 10 CFR 50.61a structured similarly to 10 CFR 50.61
- Similarity emphasized to facilitate implementation by both the industry and the NRC staff
- Differences between the two rules reflect critical features

Alternate PTS Rule
Key Features

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

- Key features of 10 CFR 50.61a include:
  - Limitations on applicability
  - Less restrictive screening criteria
  - Evaluation of plant-specific flaw distributions
  - Implementation of new embrittlement models and RPV surveillance data evaluations

Alternate PTS Rule

Limitations on Applicability

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

- Technical basis for 10 CFR 50.61a based on evaluation of currently operating PWR designs
- New reactor designs may by subject to different PTS event frequencies or severities – hence, 10 CFR 50.61a not explicitly applicable
- Improvements in RPV manufacturing expected to obviate need for application of 10 CFR 50.61a to new reactors

Alternate PTS Rule

Less Restrictive Screening Criteria

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

- Modified material property parameter (RT_{MAX}) used instead of RT_{PTS}
- Technical basis for 10 CFR 50.61a demonstrates that PWR facilities can safely operate to higher levels of RPV embrittlement
- Hence, less restrictive screening criteria implemented in 10 CFR 50.61a

Alternate PTS Rule

Plant-Specific Flaw Distributions

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

- Less restrictive screening criteria in 10 CFR 50.61a due, in large part, to use of a more realistic flaw distribution in technical basis development
- Important to verify facilities implementing 10 CFR 50.61a are consistent with this assumption
- Requirements established to evaluate data acquired via ASME Code-required inservice inspections to verify plant-specific flaw distribution

Alternate PTS Rule

Embrittlement Models and Surveillance Data

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

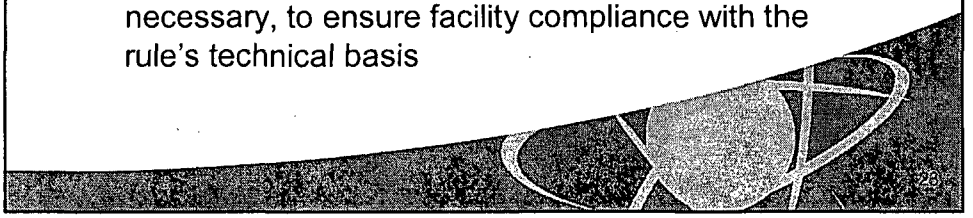
- 10 CFR 50.61a embrittlement models based on:
  - a significantly enhanced RPV surveillance database
  - a combined statistical analysis of data and a mechanistic understanding of radiation embrittlement
- Enhanced RPV surveillance data evaluations:
  - are more statistically rigorous
  - ensure embrittlement models are not behaving non-conservatively

Alternate PTS Rule

Conclusion

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

- 10 CFR 50.61a provides:
  - an effective option for those facilities projected to exceed the screening criteria of 10 CFR 50.61, while
  - ensuring that adequate protection of public health and safety is maintained based on the rule's thorough, state-of-the-art technical basis and specific requirements incorporated in the rule, where necessary, to ensure facility compliance with the rule's technical basis



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

RG-5.71
Cyber Security Programs for Nuclear Facilities
(DG-5022)

Karl Sturzebecher
Digital Instrumentation and Controls Branch
Division of Engineering
Office of Nuclear Regulatory Research

1

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

Agenda

- RG-5.71 Development
- Technical Approach
- Path Forward
- Backup Slides
  - Comment Response
  - NUREG/CR 6847

2

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

RG-5.71 Development

New Rule 10 CFR 73.54

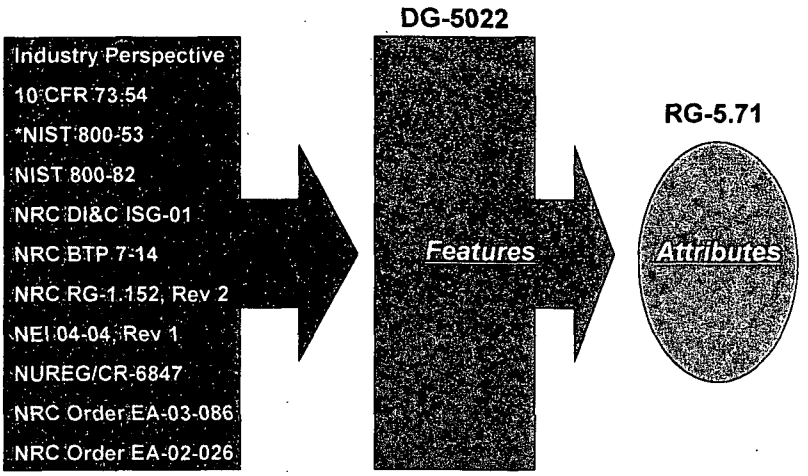
- Protection of digital computer and communication systems and networks from cyber attacks
  - Safety-related and important to safety functions
  - Security functions
  - Emergency preparedness functions
  - Support systems, which if compromised, impact above
- Approved by Commission 1/09
- Anticipate OMB approval April/May

3

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

RG-5.71 Development

Conceptual Development



*Merger of IEC 15408 (Parts 1-3) and IEC 17799

4

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

RG-5.71 Development

Stakeholder Comments

- Participation by NERC, FERC, DHS, NIST, Joe Weiss, vendors, licensees, NEI
- 7/11/08 Stakeholder Meeting (208 comments)
  - High number of questions, assumptions, move and delete comments
- 12/4/08 Stakeholder Meeting (14 comments)
  - Cyber security plan needs to be clearer
  - Should leverage existing NRC/industry regulations, programs, and processes
  - Should use a graded approach
  - Physical and logical security boundaries do not have a one-to-one correspondence
- 1/12/09 Stakeholder Meeting (6 comments)
  - Reorganize document to discuss plan first, next program, then security controls
  - Emphasize performance-based attributes
- 2/11/09 Stakeholder Meeting (final closure)

5

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

Technical Approach

Time Frame	Security Engineering Paradigm	Technical Environment
1960s – 1970s	COMPUSEC – computer security COMSEC – communications security	Digital mainframes Analog communications
1980s – mid 1990s	INFOSEC – information security	Distributed computing LANs Digital communications
Mid 1990s – today	Cyber security -Management controls -Operational controls -Technical controls	Convergence of computing and telecommunications Advances in digital technology, ASICS, PLDs, FPGAs, etc.

Cyber security: combination of : (1) inherent technical features and functions that collectively contribute to a system, system of systems, and enterprise achieving and sustaining confidentiality, integrity, and availability, and (2) implementation of standardized operational and management controls that define the nature and frequency of interaction between users, systems, and system resources, the purpose of which is to achieve and sustain and known secure state at all times, and prevent accidental and intentional theft, destruction, alteration or sabotage of system resources.

6

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

Technical Approach

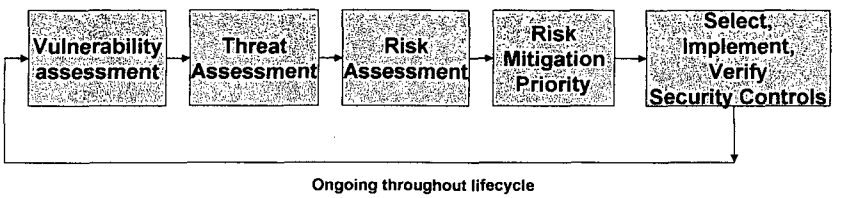
Purpose of RG-5.71

- Per 10 CFR 73.54 establish performance based requirements to ensure that the functions of critical systems and critical digital assets are protected from cyber attack throughout the system engineering lifecycle, using a graded approach

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

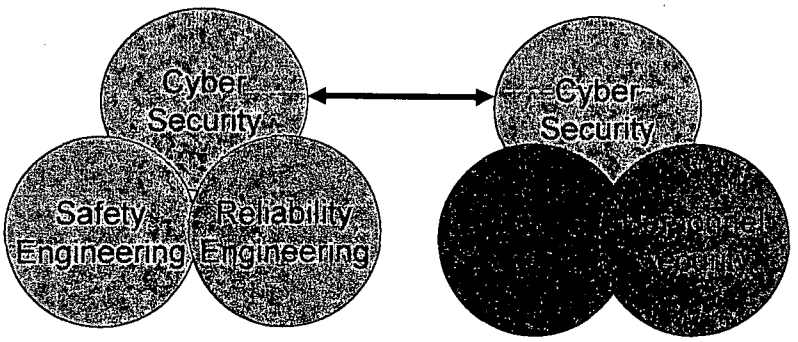
Technical Approach (3.1, 3.9)

- **Vulnerability**
  - Inherent weakness in a system, system of systems, or enterprise, its design, implementation, operation, or operational environment
- **Threat**
  - Potential for a vulnerability to be exploited, accidentally or intentionally, a function of the opportunity, motive, expertise, and resources (OMER) needed and available to effect the exploitation
- **Risk**
  - Likelihood of a vulnerability being exploited and a threat instantiated, plus the worst-case severity consequences



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

Technical Approach (3.4.1.2)

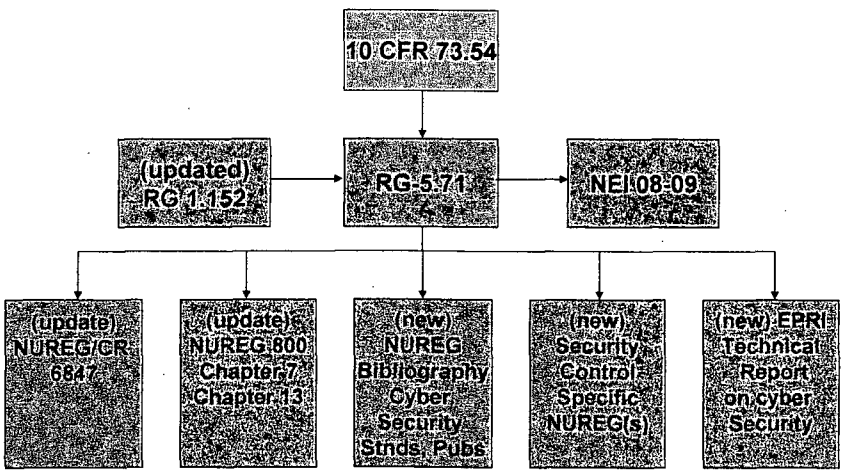


3.4.1.2 The licensee should perform concurrent security engineering lifecycle activities, to achieve high assurance that safety, reliability, and security engineering activities are coordinated.

9

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

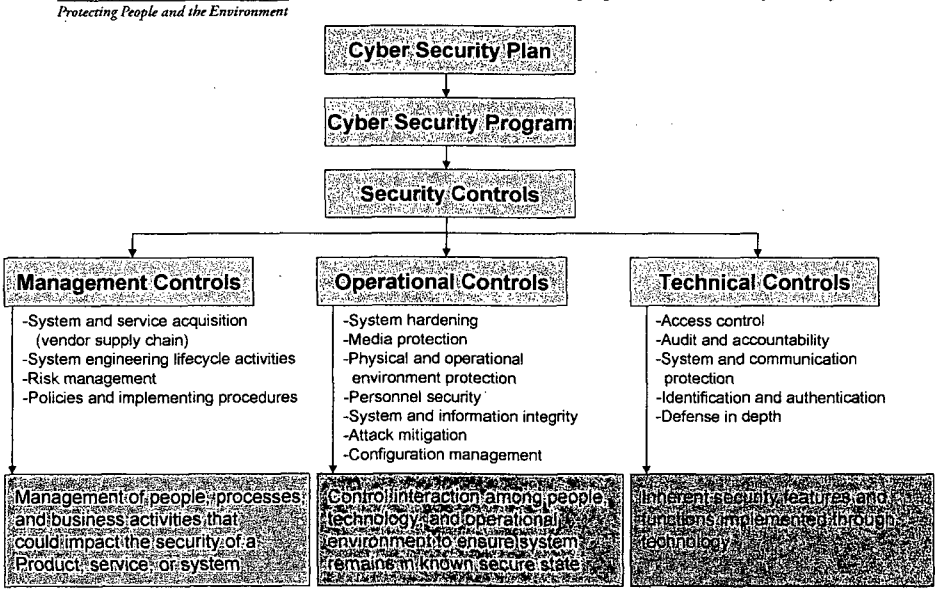
Technical Approach



10

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

Technical Approach (3.4)



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

Technical Approach

Performance based

- RG-5.71 specifies attributes ("what") for which applicant must demonstrate high assurance
- Cyber security plan, policies, and implementing procedures specify details ("how"), along with applicable NUREGs
- Rationale:
  - Security architecture is site specific, tied to each system, its design, implementation, operation, and operational environment
  - Security engineering is a concurrent engineering activity, ties into existing system engineering methodology and business practices
  - Rapid evolution of cyber security technology
  - Constantly changing attack methods and threat environment
  - Security sensitive information doesn't belong in a public document
  - Approach is similar to other federal security rules and NERC cyber security standards
- " ...defense technologies are widely available to mitigate threats but have not been uniformly adopted due to associated costs, perceived need, operational requirements, and regulatory constraints."
  - Director of National Intelligence Annual Threat Assessment, provided to U.S. Senate Select Committee on Intelligence, 2/12/09, p. 39.

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

Technical Approach (3.6)

Most Common Categories of Exploits (accidental or intentional)

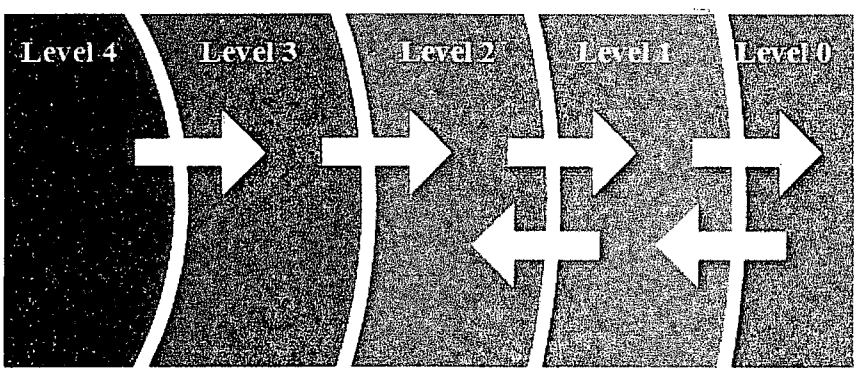
-Action, command, response triggering	-Masquerading, IP spoofing
-Blocking access to system resources	-Modification of information or commands
-Browsing, surveillance (pre-cursor event)	-Lack of fault tolerance, error detection or correction
-Corruption of resource management information	-Overwriting information or commands
-Deletion of information	-Password guessing, spoofing, compromise
-Denial of service, network flooding, system saturation, lack of capacity planning	-Replay, reroute, misroute messages
-EMI/RFI	-Site or system specific vulnerabilities
-Environmental, facility, power faults or tampering	-Theft of information or service
-Illegal operations, transactions, modes/states	-Trojan horse
-Inference, aggregation	-Unauthorized access or use of system resources
-Insertion of bogus data or commands	-Uncontrolled, unprotected portable systems, media, archives, hardcopies
-Lack of contingency planning, back-ups	-Unpredictable COTS behavior
	-Virus, worm, zombie, bot net

13

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

Technical Approach (3.5)

An example of such a defensive architecture is one that includes a series of concentric defensive levels of increasing security



Security Architecture: Concentric Ring Model

14

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

Technical Approach (3.5)

ISO/OSI Reference Model	Sample Protocols	Sample Security Controls
7: Application Layer	FTP, HTTP, SMTP, SNMP, Telnet, APIs	Prohibit use of Telnet, require HTTPS, Digital certificates, system hardening
6: Presentation	Context and syntax management	**Information hiding**
5: Session	Session management and Synchronization	Digital certificates
4: Transport	TCP, UDP	**Peer entity authentication**
3: Network	IP, X.25, ATM	IPSec, **partitioning, wrappers**
2: Data Link	IEEE 802.3, Frame relay	Asymmetric block encryption
1: Physical	V.90, OC-3, SONET, RS-422	Electrically isolate signals, channels, etc.

Defense in depth strategy: apply multiple different technical and operational security controls to all layers of the protocol stack.

15

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

Technical Approach

Sample Implementation of Technical Controls

Access Control 3.4.3.1	Authentication 3.4.3.4
• Domain and type enforcement	• Biometrics
• Least privilege	• Data origin
• Wrappers	• Digital certificate
• Role based	• Kerberos
• Time based	• Unilateral
• Origin based	• Mutual
• Encryption	• Peer entity
• Information hiding	• Smart cards
• Partitioning	• Non-repudiation of origin, receipt

Arbitrate initiator request (person, or process) to perform an operation on a target resource

Establish the claimed identity of a user, process, device, or other entity

16

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

Technical Approach (3.3)

Incorporating the Cyber Security Program into the Physical Protection Program

10 CFR 73.54(b)(3) security program a component of the physical protection program

- Security organization is responsible for protecting the facility from physical and cyber attacks up to and including the design-basis threat
- Align key personnel who are responsible for the management and oversight of the licensee's cyber security program
- Flexibility in regard to solid line/dotted line reporting chain

17

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

Path Forward

RG-5.71 Next Steps

- Respond to ACRS comments
- Complete development of generic cyber security plan template NEI-08-09
- Conduct licensing reviews
- Develop and implement oversight process

Requesting ACRS letter endorsing issuance for use

18

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

Backup: Comment Response

- **Cyber security should not be located in the physical security organization.**
  - Response: The rule, specifically 10 CFR 73.54(b)(3) requires this. However, we understand this concern and have allowed flexibility in regard to the dotted line/solid line reporting structure between cyber and physical security.
- **Need to ensure that cyber security requirements are carried forward all through the supply chain.**
  - Response: We will add "..including all suppliers, vendors, and maintenance contractors." to the end of the first bullet under 3.4.1.1. We will reword the second bullet under 3.4.1.1 to read "...vendor, supplier, and maintenance security and development lifecycles."
- **Need to emphasize the importance of configuration management, especially during hardware/software upgrades.**
  - Response: We believe the configuration management requirements stated in 3.4.1.2, which references Chapter 7 of the SRP and BTP-14, 10 CFR 54, 10 CFR 59, and section 3.10 of this document, address this concern.
- **Need to add more definitions in the glossary.**
  - Response: The additional definitions provided in this slide set will be added to the glossary.

19

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

Backup: Comment Response

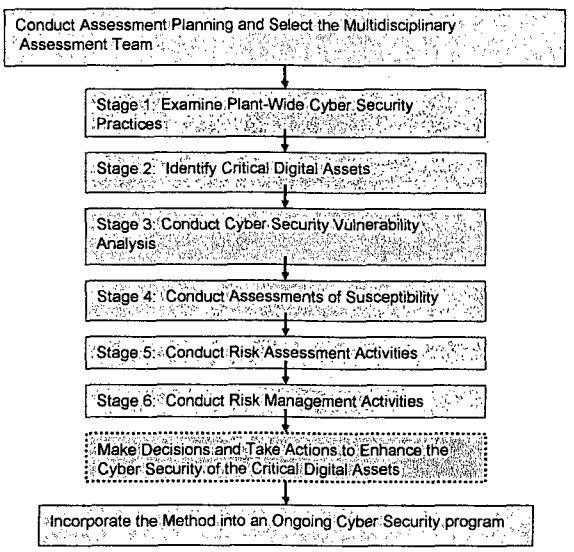
- **Need to include more examples and diagrams**
  - Response: The new diagrams and tables provided on slides 8-11 and 13-16 will be added to the document.
- **Need to emphasize the deliberate exploitation of vulnerabilities.**
  - Response: This point has been added to slides 8 and 13, which will be added to the document.
- **Need to add acceptance criteria**
  - Response: The burden of proof that a security control or set of controls is acceptable and meets the high assurance test lies with the applicant. That said, a security control would be considered acceptable if:
    - The security control selected is appropriate for the vulnerability it is intended to mitigate.
    - The implementation, configuration, operation, and execution of the security control are sufficiently robust and resilient to mitigate the threat of the vulnerability being exploited.
    - The implementation, configuration, operation, and execution of the security control are consistent with industry best practices, national and international consensus standards, applicable NUREGs, site specific policies and procedures, and the due diligence criteria.
    - The security control is consistent and compatible with the overall site security architecture
  - [This statement will be added as the third paragraph in Section 3.4.]

Due diligence: (Black's Law Dictionary) such a measure of prudence, activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent person under the particular circumstances, not measured by any absolute standard, but depending on the relative facts of the special case.

20

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

Backup: NUREG/CR 6847



21