Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Advisory Committee on Reactor Safeguards 505th Meeting
Docket Number:	(not applicable)
Location:	Rockville, Maryland
Date:	Friday, September 12, 2003
Work Order No.:	NRC-1069 Pages 1-52

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS) 505TH MEETING

+ + + + +

FRIDAY

SEPTEMBER 12, 2003

+ + + + +

ROCKVILLE, MARYLAND

The Committee was called to order at 8:30 a.m., at the Nuclear Regulatory Commission, Two White Flint North, Room T2B3, 11545 Rockville Pike, Dr. Mario V. Bonaca, Chairman, presiding.

COMMITTEE MEMBERS PRESENT:

DR. MARIO BONACA,	ACRS Chairman
DR. GRAHAM B. WALLIS	ACRS Vice Chairman
DR. GEORGE E. APOSTOLAKIS	ACRS Member
DR. THOMAS S. KRESS	ACRS Member
DR. GRAHAM M LEITCH	ACRS Member
DR. DANA A. POWERS	ACRS Member
DR. VICTOR H. RANSON	ACRS Member
DR. STEPHEN L. ROSEN	ACRS Member-at-Large
DR. WILLIAM J. SHACK	ACRS Member
DR. JOHN SIEBER	ACRS Member

ACRS STAFF PRESENT:

SHER BAHADUR	Associate Director, ACRS
SATISH AGGARWAL	NRR
RAMIN ASSIN	RES
MARK BLUMBERG	NRR/DSSA/SPSB
SAM DURAISWAMY	Designated Federal Official
RALPH CARUSO	ACRS Staff
O.M.P. CHOPRA	NRR/DE/EEIB
CLIFF DOUTT	NRR/DSSA/SPS
MICHELLE HART	NRR/DE/EEIB
HOWARD J. LARSON	Special Assistant, ACRS
PAUL LOESER	NRR/DE/EEIB

I-N-D-E-X

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

(8:30 a.m.)

CHAIRMAN BONACA: Good morning. The meeting will now come to order. This is the third day of the 505th meeting of the Advisory Committee On Reactor Safeguards. During today's meeting the committee will consider the following.

Draft final revision-1 to Regulatory Guide 1.53, application of the single failure criteria to safety systems.

Preparation for meeting with the NRC Commissioners. The subcommittee report on fire protection issues. Future ACRS activities and a report of the planning and procedures subcommittee. Reconciliation of the ACRS comments and recommendations; and proposed ACRS reports. Seven of those.

A portion of this meeting will be closed to discuss a proposed ACRS report on safeguards and security.

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 comments or requests for time to make oral statements from members of the public regarding today's sessions. A transcript of portions of the meeting is being kept, and it is requested that the speakers use one of the microphones, identify themselves, and speak with sufficient clarity and volume so that they can be readily heard.

Now, before we start on the first item on the agenda, I would like to just make a brief announcement regarding the agenda itself, okay? Dr. Wallis has to leave by 3:00 p.m., and also Dr. Apostolakis, I believe, shortly after?

DR. APOSTOLAKIS: No, before.

CHAIRMAN BONACA: So, what I would like to do after the first presentation and discussion, and before the preparation for the meeting with the Commissioners, we will get a reading of Graham's letter so that we can give him feedback, and back to it in the early afternoon.

And also a reading of George's letter, and hopefully we can even approve it maybe.

DR. APOSTOLAKIS: As far as I am concerned, you can approve it right now.

CHAIRMAN BONACA: I don't want to prejudge it. So with that, I will turn to Dr. Shack, who is going to lead us through this presentation. Be aware of the timing issue that we have. We have a very tight schedule, and I am sure that you will be policing this hour.

DR. SHACK: You kept such tight control yesterday, right. You set such a good example yesterday.

CHAIRMAN BONACA: I am not sure about that.

MR. AGGARWAL: We will try to help you and not ask too many questions.

CHAIRMAN BONACA: Today I will make a better example.

DR. SHACK: One thing that I would like to point out to the members is that our revised draft final has been revised once more. You have a memo from Mike Snodderly, which contains some last minute changes.

These are mostly again to address the possibility that every time you revise a reg guide that there is always this concern about back fits, and again this will -- the reg guide is intended for essentially applications for all future discussions, and can be adopted voluntarily by licensees who are making changes, but it is intended as a back fit.

In addition to Satish Aggarwal, who is the author of the reg guide, we also have a distinguished visitor today, Mr. David Zaprazny, who is the Chairman of the IEEE working group. Basically the reg guide endorses an IEEE standard 379-2000, and Mr. Zaprazny is the chairman of the working group that developed the new standard, and I will turn it over to Satish then to discuss the reg guide.

MR. AGGARWAL: Good morning. Before I provide the background on the reg guide, let me at the outset state that the purpose of this briefing today is to seek your concurrence with this staff position in respect to single phase criteria to safety systems.

So we are hoping at the conclusion of our presentations that subsequently we will receive a letter to that effect. Now, let me first of all make it clear what is a single failure.

You all know power instrumentation and control portion of each safety system consists of more than one safety group, and any one of which can complete the safety function.

Thus, a safety system must perform all

safety functions required for a design basis event in the presence of any detectable failure within the safety system. And in a nutshell is the single failure criteria.

DR. APOSTOLAKIS: So the idea of a single failure then applies to a well-defined system and not a function?

MR. AGGARWAL: That's right.

DR. APOSTOLAKIS: So if I consider the function of removing decayed heat, I will not necessarily think in terms of a single failure that I am losing one system, and therefore I have a redundant system, right? That is a different kind of concept?

MR. AGGARWAL: If you look at the safety functions, and you look at your more than one group that performs that safety function, and you fail one of the functions, and show to me that you will still be able to perform. I will present some more examples as we proceed.

DR. APOSTOLAKIS: So it applies to functions as well and not just systems?

MR. AGGARWAL: It applies to both.

DR. APOSTOLAKIS: So if my function is to inject water under high pressure into the core, I must have at least one way of doing this?

MR. AGGARWAL: Exactly. That is a given design, and we are saying show it to us, and this is single failure.

DR. APOSTOLAKIS: Even if the system is highly redundant and meets the criteria and not the system level?

MR. AGGARWAL: Right.

DR. APOSTOLAKIS: Wow.

MR. AGGARWAL: And the specific design is nothing new. This has been there for years. This is fundamental to a nuclear power plant design.

DR. LEITCH: But let's say, for example, in a boiling water reactor, in George's scenario, you want to inject water at high pressure. So you have the HPSI system and if that fails, there is no direct replacement for it.

What you have is an alternate means to blow the reactor down to low pressure and then inject. So --

MR. AGGARWAL: Exactly. You have to show how you can accomplish that function by a different matter.

DR. APOSTOLAKIS: So, wait, that is a good example. You are not really accomplishing the function, because you don't have another way of injecting water under high pressure.

MR. AGGARWAL: Right.

DR. APOSTOLAKIS: But you are getting around it by reducing the pressure?

MR. AGGARWAL: Reducing the pressure and then injecting the pressure.

DR. APOSTOLAKIS: So essentially you are managing the accident --

MR. AGGARWAL: Right, mitigating it.

DR. APOSTOLAKIS: In more than one way.

MR. AGGARWAL: I just wanted to clear where --

DR. APOSTOLAKIS: Well, you are doing a very good job.

MR. AGGARWAL: Thank you.

DR. APOSTOLAKIS: But would this apply to advanced reactors as well?

MR. AGGARWAL: It should apply to all.

DR. APOSTOLAKIS: Okay.

DR. LEITCH: I always thought to carry that example a little bit further that single failure was really that -- well, to continue to talk about HPSI, for example, and a piece of instrumentation on the HPSI system would not -- that is, the failure of a piece of instrumentation would not render the HPSI system inoperable, and there would be another piece of instrumentation that would trigger the HPSI system to initiate, for example.

MR. AGGARWAL: By design all safety related equipment should be able to perform its function. Single failure is saying that you take one system, one increment, fail it, and show me how you can accomplish the purpose of the function and mitigate the accident.

DR. WALLIS: This is a very difficult thing, because a system is a meaningless word. I mean, a system encompasses whatever you wait it to encompass. So I could say the ECCS system, and that is everything, and that is accumulators, and --

DR. APOSTOLAKIS: That's why I went to the function level.

DR. WALLIS: Yes, but even then you have got to say how are you going to divide the functions. I mean, keeping the core cool is a function.

DR. APOSTOLAKIS: But the reality is that the actual function -- well, I mean, what you do is you are looking for the worst single failure. So you are going sensitivities on individual trains, and not functions, until you find the one which is the most limiting one, and then you assume that one.

DR. WALLIS: That is very different though. You have got three trains and one is out of order, you can still perform the function with two.

DR. APOSTOLAKIS: Exactly.

DR. WALLIS: And that is quite different

MR. AGGARWAL: May I suggest that you hold that thought and let's proceed, and we will give you the imperfect examples to make a point, and tell you what that all means.

CHAIRMAN BONACA: Now, is this consistent with the move towards risk-informed regulations? Probably not.

MR. AGGARWAL: Not really. What we are going to talk about is the PRA in a minute. Also, I would like to point out that the single failure could occur prior to or at any time, during or the DBE for which the safety system is required to function.

It is a given, but keep these two ideas in mind as we progress. Now, I --

DR. APOSTOLAKIS: Now, if I said that the single failure criteria means a specific implementation of the concept of defense in depth, I would be right, right?

MR. AGGARWAL: Yes.

DR. APOSTOLAKIS: It just makes that concept specific and implementable in a particular case.

MR. AGGARWAL: That's correct.

DR. APOSTOLAKIS: All right.

DR. SHACK: And this only holds true, of course, during design basis events.

DR. APOSTOLAKIS: True. True.

DR. ROSEN: Well, the whole idea of risk informing the regulations is that we know serious events don't have just a single failure. There is almost never a significant event with just one thing happening.

DR. SHACK: Well, you design it with just a single failure event, period.

DR. ROSEN: All serious events, not just in the nuclear industry, but in all industries, are combinations of multiple issues.

MR. AGGARWAL: Well, if I may proceed, let me give you the feedback background under that guide. The issue that (inaudible) 11-18 for public comments.

DR. ROSEN: Well, excuse me, but I may

have missed this. Why are you doing this?

MR. AGGARWAL: Why are we doing it? This is the commission policy to look at the IEEE on a national consensus standard on single failure criteria, whether they meet our regulations or not. If they do, we would like to introduce them in a reg guide or regulation.

DR. ROSEN: This is a national standard on single failure criteria

MR. AGGARWAL: Yes, sir. What you have is a national consensus standard.

DR. ROSEN: But who issued it?

MR. AGGARWAL: IEEE.

DR. APOSTOLAKIS: It applies only to nuclear facilities?

MR. AGGARWAL: That's right.

DR. APOSTOLAKIS: So why should IEEE care?

MR. AGGARWAL: Well, if you would like to circulate that standard among the members.

DR. APOSTOLAKIS: Why would IEEE care about nuclear facilities?

MR. AGGARWAL: Sir, George, IEEE assigns the maximum number of standards for operations in nuclear power plants.

DR. APOSTOLAKIS: Well, I can see them publishing standards for instrumentation and control, and things --

DR. SHACK: This is single failure for instrumentation control systems.

MR. AGGARWAL: Power, and electrical, and --

DR. APOSTOLAKIS: Oh, it is not general?

MR. AGGARWAL: No, this is what my first opening line was, that the (inaudible) control systems.

DR. APOSTOLAKIS: I think though the --

CHAIRMAN BONACA: The question I think is that this kind of concept somewhat, which I think is very appropriate for a component or system, et cetera, is really a casualty analysis to determine how it is capable of performing its function with a failure in it, was really translated later on in the accident analysis it seems to me.

When instead you have a much more complex grouping of systems, et cetera, and you should consider possible multiple offenders, I think.

DR. APOSTOLAKIS: Well, this was actually a very good when it was proposed.

CHAIRMAN BONACA: Well, sure.

DR. APOSTOLAKIS: But it really makes sure that you don't have single element minimal concepts. That is really what it does.

MR. AGGARWAL: Exactly.

MR. LOESER: And in this case the original document that was endorsed was dated 1972. A lot has happened since then, and --

DR. APOSTOLAKIS: The reactor safety study, for example.

MR. LOESER: And in this case there have been several other versions that have not been endorsed. I am not sure why. But we decided that it was time to endorse the latest one, the 2000, and that is what this draft guide is for, is to help update Reg. Guide 153 to a remedial standard.

DR. POWERS: Let me ask, and I may be asking this question out of turn here, but I will ask it anyway. When you think about modern electrical systems, and you say the failure is when there is a termination of the ability to perform its intended function.

And I think about software controlled digital systems with design requirements embedded in them that may in fact be flawed. So the system does not perform the function that one group of people intended it to do, but the other group of people definitely didn't address that because they didn't put the requirements on the software to address that particular set of circumstances. Have we had a single failure?

MR. LOESER: Yes, and that's why the branch technical position 19 requires a diverse method not subject to the same single failure to accomplish the same basic function.

That's why if you have all of the software and all four channels using identical software, they is supposed to be some alternative way in case that software fails to perform its function, whether by specification error, or coding error, or just something else.

If there is a common failure of all the systems using that software the plant still has to be able to survive.

DR. POWERS: That is what we have done on safety. What I am really asking is that with regard to the standard have we had a single failure?

MR. ZAPRAZNY: Yes. Design error can be a single failure.

DR. POWERS: And so the fact that these

guys developed a piece of electrical equipment, and it meets all of their requirements, but it just does not happen to meet what the systems requirements are. There has been a failure, and their failure.

DR. APOSTOLAKIS: A design error can be a single failure as long as it affects one component. I don't think you are dealing with common cause failure.

MR. ZAPRAZNY: It is dealing with common cause failure, yes, and that is addressed in the standard.

MR. AGGARWAL: And then I also might point out that that there is this IEEE 7.432, which addresses the basic issues raised.

DR. POWERS: I know it is, and --

MR. AGGARWAL: And which we have endorsed.

DR. POWERS: And you brought that before us, and we spent hours trying to understand everything there.

MR. AGGARWAL: Right.

DR. POWERS: I was just looking at the definition of your standard and trying to think about what was missing, and what you brought up, I think I understood. But it is a question with respect to this standard itself, and whether that was recognized as a failure, because I would not have.

They did, but I would not have if I were kind, but that's okay. That's okay.

DR. APOSTOLAKIS: You will talk about common cause failures later?

MR. AGGARWAL: Yes.

DR. APOSTOLAKIS: Okay.

MR. AGGARWAL: I did say earlier that we received four comments letters, and as a result of those comments letters, we made a few minor changes in the (inaudible) section.

I might point out that comment letters may be found to be long, several pages, but what is contained on those comment letters is noting new. One of the lawyer firms sent this letter every time he devised an electrical regulation or reg guide, bringing up fundamental issues which the Commission had addressed before, in terms of the rule making when their endorsement of IEEE Standard 603, and more specifically 10 CFR 50 (a) (h) subparagraphs.

So we met with CRGR to discuss this reg guide and seek their endorsement, and it might also be noted that when we issued the draft reg guide, in the implementation section, we are given the option that you can use the old one and be subject to review by the staff on a case-by-case basis, or you can use the civilian.

This language we have used at the insistence of CRGR, and brought it (inaudible) in the industry, because the project changed, and the change was not acceptable to the public.

This (inaudible) something be done in this language, and they didn't like it, okay? In other to resolve this, if you will turn over to the next page, the final reg guide.

This is the language that we have been using in all reg guides over the last 10 years, and so all we did was bring it to the same language which is accepted by the industry and in our opinion and OGC's opinion it not clear.

The bottom line is that backfitting is not intended. Now in doing so, and the industry raises the issue of safety systems, protection system, and what not, CRGR asked us in the Section A, and this is a reg guide, dated August 25th, 2003, and copies of which have been provided to the committee.

And this is under Section A, which we

expanded to clarify what a safety function means, and what a protection system means, and all this information is nothing new. It was already there when we were doing the rule making.

So it is simply that we are reproducing it here, and in the instrumentation section, we made it clear that no backfitting is intended, and this will be used for the operating plants on a voluntary basis if there are any modifications proposed by the licensee,

DR. LEITCH: What does the word evaluate mean? In other words, if a license voluntarily proposes modifications to a safety system that do not comply, then that is a cause for a rejection of that modification?

MR. AGGARWAL: Technically, this is one matter that the staff will accept without question. The licensee is always free to come up with an orderly matter of accomplishing it.

And naturally that will be evaluated by this staff and that is all that it means.

MR. LOESER: In this particular case, if they had previously committed, for example, to the 1972 version --

MR. AGGARWAL: Right.

DR. LEITCH: -- and their new modification met the 1972 version, but did not meet the 2002 version that's okay?

DR. LEITCH: That's okay. Okay.

MR. LOESER: There is not a requirement for them to meet this new one, because there is no backfit required as long as they meet the commitments that they made at the time of their license.

DR. LEITCH: Okay. And obviously an encouragement to do so, but not a requirement to do so.

MR. LOESER: That's exactly correct.

DR. LEITCH: I understand. Thank you.

MR. AGGARWAL: At this time I would like to raise or discuss the issues of the significant technical changes between 1972 and what we are endorsing now.

The first item is that in the current version which you have before you, we have included a requirement for a single failure analysis in design using digital computers.

And that brings you to the IEEE Standard 603, and 7-4.3.2. Incidentally, I might point out to the committee that if the standard had been revised and approved by the IEEE standard vote yesterday, and we wold have Standard 7-4.3.2, which is still a much m ore improved standard for guidance in the digital computers.

And it is the staff's intention to endorse that standard in the near future, and so we will be back to you again explaining to you how we are going to meet all these requirements in terms of digital computers.

DR. LEITCH: Let me ask another question and perhaps that I should have asked earlier. Those definitions that you referred to right at the beginning of your talk, are they different in the new standard versus the 1973 standard, or are they still the same old definition?

MR. AGGARWAL: They are different. They are much more improved based on our experience, and clarity. If you would like to hear, we can tell you exactly what changed, but it includes improved language just for clarity.

And even in the reg guide, I had made this point very clear what that really means, because I know often that the term single failure is misunderstood, and so I thought that this is the time that we put that to bed, and this is exactly --

yes, sir?

DR. APOSTOLAKIS: I guess I am still struggling to understand what the single failure is. The safety systems you say here will be capable of performing the required safety functions. Is a single failure an actual failure, or could it be a cause for failure of 3 or 4 different systems?

MR. AGGARWAL: It could be either.

DR. APOSTOLAKIS: It could be a cause.

MR. AGGARWAL: Right.

MR. LOESER: Well, in this case, when you consider a single failure, you have to consider not only the failure itself, but all the subsequent failures that that causes.

For example, a software failure could cause more than one component to fail, because there is more than one component using that software.

DR. APOSTOLAKIS: Right.

MR. LOESER: So you have to use sort of a trickle down effect. If you have a power spike of some sort and that equipment that is not fused, everything that power spike will blow out is part of that single failure.

DR. APOSTOLAKIS: So you are moving now towards PRA, and that is really what you are doing.

MR. LOESER: Well --

DR. APOSTOLAKIS: You are considering the consequences of a failure.

MR. LOESER: We are not doing this on a -- well, it is a cause and effect, and not only the failure itself, but all subsequent failures that that failure causes are all part of the same single failure.

DR. ROSEN: I would say it is more like failure modes and effects.

MR. LOESER: That is actually correct.

MR. AGGARWAL: You're right.

DR. APOSTOLAKIS: Yes, but the initiator here must be a failure itself, and not a cause. In other words, it can not be human error of omission or commission.

It has to be an actual failure. As you said, you know, power fails, and then it proprogates. But it cannot be a cause that is not a failure by itself. That is the way that I understand it.

MR. ZAPRAZNY: If you have a circuit breaker fail on a load center --

DR. APOSTOLAKIS: Well, that is a failure.

MR. ZAPRAZNY: But your failure results in loss of all the --

DR. APOSTOLAKIS: Fine, fine, I understand that.

DR. ROSEN: And then later on the sequence, if there is an operator action required, and the operator failures to do it, that is not one failure. That is two failures.

DR. APOSTOLAKIS: Right. And the other question is how about passive failures? I mean, does that make sense in this context?

MR. AGGARWAL: It does, and I intend to touch on that area.

DR. APOSTOLAKIS: So if I have a fire that just deteriorates and all of a sudden I have a hot short, that is a failure?

MR. AGGARWAL: Yes.

MR. LOESER: A failure to do something is not considered any differently than a failure to not do something. So a failure to trip or a failure for a component to react because it is burned out, or because a wire worked its way lose or something, a failure to act in some manner is still a failure.

But I think that there is an important difference between electrical and mechanical systems. In the mechanical systems, you don't consider a pipe failure as a single failure. I think there is a fundamental difference here.

DR. ROSEN: Well, that is an initiating event, and we consider the pipe failure the initiating event, and then we test the responses for the single failure criteria.

MR. AGGARWAL: Right.

DR. APOSTOLAKIS: So that is a design basis failure?

MR. ZAPRAZNY: Once again, a pipe failure is a passive failure which is a single failure.

DR. APOSTOLAKIS: No, that is --

DR. ROSEN: That is the initiating event.

DR. APOSTOLAKIS: -- the initiating. It is a DBE, but it is not -- because here you said even with a DBE, I don't want a single failure to disable the system.

MR. LOESER: I think you would have to differentiate which pipe. If you are talking about a pipe that causes the event, but if there is some other valve that is now supposed to open, or a pipe that is supposed to transmit water to alleviate this situation to mitigate the accident, then that failure would be the single failure.

DR. APOSTOLAKIS: But that is the system.

CHAIRMAN BONACA: It is the system, and so you are not supposed to assume two pipe failures.

MR. LOESER: That's correct.

DR. APOSTOLAKIS: In other words, if I have an initiating event that comes from a pipe failure, a single failure cannot be another pipe failure.

CHAIRMAN BONACA: Or any other component that --

DR. APOSTOLAKIS: Is that consistent with -- would a system failure be another passive failure?

CHAIRMAN BONACA: No.

MR. LOESER: Wait a second. It could. I think there is a difference. If you had an initiating event -- for example, a computer in the feedwater system failing to do whatever it is supposed to do in cutting off feedwater; another electrical failure in a digital system, or in a valve, or anything else, would be a single failure even if the failure is similar to a software failure.

It is not like the -- I mean, the single failure could be very similar to the one that initiated the event.

DR. APOSTOLAKIS: Yes, in that sense they are different from mechanical systems.

MR. AGGARWAL: I might bring to the attention of the committee that this particular slide is addressing the issue of shared system, and what I intend to bring to your attention that IEEE standards describe the manner in which single failure criteria should be applied to shared systems.

The intent is neither to endorse or (inaudible) the hearing between the system, the standard for minimum requirements to ensure that shared systems are analyzed as adversely as possible to ensure that the fact of component failures as there was no sharing.

That is a very simple thing, that you can share systems, but you still have to have (inaudible). So this is a new addition to the IEEE standard 379.

DR. APOSTOLAKIS: Is it shared systems or shared components?

MR. AGGARWAL: Shared systems. But shared components are a part of the system.

DR. APOSTOLAKIS: Give me an example of a shared system.

MR. AGGARWAL: You might have the same diesel which you might be sharing between the two units.

DR. ROSEN: A start-up boiler at a plant that has two units, and that would share the piping and the boiler.

MR. AGGARWAL: In some old plants the D.C. power is shared, and I am in 372 in terms of control So essentially as I was speaking to you about the shared system, and these are the two basic criteria which are in this standard, that the safety system of each unit shall be capable of performing their required safety function, and with a single failure initiative concurrently in each unit within the system that are not shared.

Number 2, for reasons that will be included in the design to ensure that a single failure within one unit will not adversely affect the other unit, thereby preventing the shared system from performing the required safety function.

DR. APOSTOLAKIS: So if I have two

units, what you are saying is that I should be able to survive a single failure in one and a single failure in the other; is that what this says?

MR. AGGARWAL: Yes.

DR. APOSTOLAKIS: It says that in each unit you should be able to handle a single failure. So I an have one here and one there, and I would still be okay?

MR. AGGARWAL: Right.

DR. APOSTOLAKIS: Well, why did you have to do this? I mean, I don't understand why. Wasn't that embedded in the previous definition?

MR. AGGARWAL: Well, there were concerns over how we deal with the shared system, and the IEEE made it clear that some guidance would be provided in the failure.

DR. APOSTOLAKIS: Now the second bullet really -- and in the first -- are redundant aren't they?

MR. AGGARWAL: In a way.

DR. APOSTOLAKIS: So there is an implementation of a single failure criterion on this transparency.

MR. AGGARWAL: That's correct.

DR. APOSTOLAKIS: You don't understand

the first, but they give you the second?

MR. LOESER: There is a number of cases where things were understood to be in the original document. Everybody knew this is what was going on, but it was not spelled out. So this standard tried to spell out a number of the items, and this is one of them.

Like you said, everybody understood this, but it didn't say it very specifically. So that is one of the items that we tried to take care of.

DR. APOSTOLAKIS: Probably the second bullet is more appropriate actually.

MR. AGGARWAL: And also you should know, and I am sure that you are aware of, that in the nuclear industry it is a very aging group, and newer people are coming in, and they have no idea how the systems work.

So this is an other training tool to them to make it explicitly clear what the standards were meant. Now I will turn my attention to the analysis.

DR. APOSTOLAKIS: I think the first bullet in fact is vulnerable to criticism because of that word concurrently. I think the second bullet is more appropriately worthy. It says that if you have a single failure in one unit, it should not prorogate to the other, and that's fine.

But to say to consider two single failures concurrently is against the philosophy of single failure criteria isn't it?

DR. ROSEN: No, that is two different units.

DR. APOSTOLAKIS: Yes.

MR. AGGARWAL: All right. We are going to turn over to the analysis which is needed to be done, and there are several stats, and that might answer some of the questions which have been raised recently.

The first criteria is that a safety function for which the analysis is to be performed shall be determined, and let me give you the examples. Like reduced power, and isolate containment, and cool the core.

The second criteria is that protective action at the system level that are available for safety functions shall be determined. Let me again give you a few examples. For example, the rapid (inaudible) and not the control rods, and building of the containment isolation was safety injections, and poor spray.

These are the types of examples of that protection. The next criteria is that safety group that will sufficiently satisfy the required safety functions shall be determined. Again, let me take a few examples.

One example that comes to mind is that either a two (inaudible) system, or one (inaudible) spray and two LPSI, lower pressure coolant injection subsystem, would we advocate to cool the core.

The next criteria is the independence of the safety group that will be established shall be verified. And again just to expand on that, this independence should be verified.

And how would you verify that? By observing that there are at least two safety groups that have no shared equipment. For example, relays, switch gear, buses, power sources, and even the locations.

The next item here is for systems or parts, where independence cannot be established, a systematic investigation of potential failures shall be conducted to assure that single failure criteria is not valid.

Again, let me give you a few examples.

Failures include short-circuits, open voltage, grounds, low AC and DC voltage, and these are all examples that fall into this category.

DR. LEITCH: But it seems to me that it depends greatly on how one defines the safety function in your previous slide.

MR. AGGARWAL: That is correct.

DR. LEITCH: And, for example, to go back again to this example, if the safety function is to inject water at high pressure, the BWR would fail if you define the function as to cool the core and it passes.

MR. LOESER: In this particular case, you are defining the function and then saying that function fails. That is not really a -- you are saying the function is to inject water at high pressure, and then you are saying the system injects water at high pressure and fails, this is -- you can do that to any degree.

With any single component failure the system that injects high water or high pressure at water -- water at high pressure -- I am getting a little tongue-tied -- will not fail.

That is, you can lose any particular valve, and you can lose any particular pipe, and you can lose any particular sensor that tells it to inject the water, and it will still do that.

However, then if you want to failure the entire system -- that is, HPSI, you have to now take your function to the next higher level, and that is to say to adequately cool the core.

You can't define your function and then define the failure as that function at the same time and have a valid analysis.

DR. LEITCH: Well, if you had redundant HPSI systems, you could, right?

DR. LEITCH: Well, it would define the function of injecting water, you would have two of them, and you would say, okay, I define my failure as not being able to inject water, regardless of how many.

CHAIRMAN BONACA: That would restrict really your designing ability. I mean, you can either provide the function by having a redundant high pressure planes, or you may have provided the function of cooling a high pressure at the lowest level still. So one train of high pressure and one train of --

DR. APOSTOLAKIS: But Graham's point is very well taken. It depends on what you call function.

MR. LOESER: Yes.

CHAIRMAN BONACA: Oh, yes.

MR. LOESER: And that defines the function, because no matter what you are defining, you could always say, okay, I lose that, and what is next.

DR. APOSTOLAKIS: I have a question for Dr. Powers. In your infamous memo, or taped report, or whatever it was regarding the (inaudible) you had in big boldface letters, this design phase, and the defense in depth I think you said, or single failure criteria of the agency, isn't this really what you had in mind there?

You said if the primary way of removing heat failed, there would have no alternate way of doing it as I recall.

DR. POWERS: I think in fact I had them failing on a couple of bases, and one of them is that they lost their final heat sync and they had no way to get to the heat sync.

DR. APOSTOLAKIS: All right.

DR. POWERS: And the second one is if they SCRAMed the reactor, they had to use the safety systems to shut it down, because just using the control rods to cool it down, because the temperature coefficient and reactivity it came back alive, and so you had to put in the SCRAM rods in order to shut it down.

So if your SCRAM rods failed, you can't shut the reactor down. In other words, if you have a single failure and your SCRAM is (inaudible), you can't shut the reactor down and that is a violation of the single failure criterion.

DR. APOSTOLAKIS: Well, it is a violation of the system level, the fire level, because you are assuming that you are losing the whole SCRAM system, independently of whether you are losing it due to a single failure or some other failure, it is the function level that we are talking about.

DR. POWERS: Well, clearly in my memorandum, I was thinking of the function level, but in fact that particular SCRAM system can be lost by failure of a single digit component.

DR. APOSTOLAKIS: I see. So the heat sync is what? You don't need an alternate heat sync. There is one heat sync, but getting there --

DR. POWERS: You have to be able to get there.

CHAIRMAN BONACA: The point that I was making before was that in the function of the accident analysis, I don't think the regulation is prescripted that you must have two trains of high pressure, two trains of low pressure, and especially for boilers.

The old boilers used to have many isometric means of providing redundant functions. So you could use high pressure injection and in compliance with only one train.

But then you have other means through the installation condenser, and to provide a function of cooling during a LOCA, and what you have to demonstrate is that either way we will take you to shutdown, and there were different ways to get there.

So I don't think in defining the function of the regulation that it is prescriptive of high pressure injection, and you have to have two trains or whatever. That is one vital design, but it was left free to perform the function, which is the one of cooling, at high pressure, mid-pressure, and low -pressure until you get to shutdown.

DR. LEITCH: But if we are starting with a blank piece of paper to design an advanced reactor wouldn't that redundancy be required at the system level?

I mean, what I am trying to say is that say we design, and you are starting with a clean piece of paper to design a BWR today, would these regulations require that you have two HPSI systems?

MR. LOESER: I don't think so. I would think that it would define the function and what the licensing comes in, but once again we are probably not prescriptive enough.

We would want to know that if you lost that system that there would be no consequent to the health of the public or the safety. That is, you have some other way of cooling off the core before there is any problem.

And if that way was to depressurize and then use low, I would suspect that that would be acceptable. However, I might point out that I am ont in the accident analysis branch, or the reactor systems branch.

DR. LEITCH: I understand that.

MR. LOESER: So I may be making a bad supposition.

CHAIRMAN BONACA: That is a good question. There were old boilers at the Vermont

Yankee, for example, that had in fact -- they were isometric in that sense, and had redundant systems.

But they had multiple systems, and Vermont Yankee, for example, had only one high pressure injection train. Then you have the isolation condenser, and you have other means of system safety failure, and so you have in an isometric plant, but still it was not licensed. But today I don't know if you would --

DR. ROSEN: I don't think there is anything that would mitigate against it, and in fact those older plants having different means of getting the same function or more armor against a common mode failure.

CHAIRMAN BONACA: They are very, very -- in fact, the core damage frequency for those plants is very low.

DR. APOSTOLAKIS: Even if you have redundant ways, that is where the mechanical systems differ from electrical systems. And in a lot of what the old plants, there is a single suction line for both trains from the RWST, and so you have the design basis event somewhere else, and it is a LOCA.

Now you have to cool the core, but that single failure doesn't count as a single failure.

CHAIRMAN BONACA: But you would not design it today that way.

DR. APOSTOLAKIS: You would not.

CHAIRMAN BONACA: And typically the (inaudible) because some of the earlier plants had it that way.

DR. ROSEN: You would not do it not because it is not strictly allowed by the regulation. You would just do it because it is a better practice.

CHAIRMAN BONACA: A good practice.

DR. APOSTOLAKIS: Yes.

MR. AGGARWAL: Let me conclude with regard to the analysis and further observations. Electrical, mechanical, and system logic failures shall be considered in a single failure analysis.

A given component can have different failure modes, and all analyses will be made for all or each mode the failures. The location of safety equipment shall be also analyzed to determine the effect of common cause failures.

I am going to turn to the PRA now. The IEEE or the industry has concluded that PRA analysis is no substitute for a single failure analysis.

DR. ROSEN: Nor is a single failure

analysis a substitute for a PRA.

MR. AGGARWAL: So conversely that is very well said. However, I would like to add something. A failure can be excluded for a single failure analysis based on PRA operating experience.

DR. APOSTOLAKIS: In other words, I can argue that -- well, first, I have a single failure someplace, and I fail the criteria. But then I can come back and say, look, based on this, and this, and this, and that, and that, and that analysis, the reliability of this particular piece of equipment is so high that you should exclude it. I mean, the failure cannot happen, and that is what you say.

MR. AGGARWAL: And that would apply here.

DR. APOSTOLAKIS: Is that a new thing, a new idea?

MR. LOESER: No, no. What about the reactor vessel?

MR. LOESER: It is not a new idea, but one that has been spelled out clearly.

MR. AGGARWAL: Clearly and explicitly.

MR. LOESER: It is one of those things that we always knew this.

DR. ROSEN: We never took the failure of

a reactor vessel.

DR. APOSTOLAKIS: Well, it allows you to have a common --

DR. ROSEN: We argued that the reactor vessel is not going to fail.

DR. APOSTOLAKIS: Well, the reactor vessel is a different beast, but the suction lines, that is a basis on whether you allow it.

MR. AGGARWAL: Another example that comes to my mind is that we essentially are considering the passive failure, and you take a motor controlled sample (inaudible), and you take it granted that it will not fail, and that is based on your analysis, judgement, PRA, or whatever it is.

And you don't have to conclude in your analysis that let's fail the whole thing.

DR. APOSTOLAKIS: Wouldn't the more accurate expression be passive component failure. The failure itself cannot be passive.

MR. AGGARWAL: Okay. You are right.

DR. APOSTOLAKIS: It is like expert elicitation.

MR. AGGARWAL: You're right.

DR. APOSTOLAKIS: It is an expert opinion elicitation, right?

MR. AGGARWAL: The last significant change involves the sensing lines, and now the standard explicitly states that the lines connecting sensors to the proper system shall be included, and let me again give an example.

Equalizing walls, chambers, and isolation walls. In conclusion --

DR. LEITCH: All the way back to the penetrations to the vessel, right?

MR. AGGARWAL: What about it?

DR. LEITCH: I mean, you have to have redundant penetrations to the vessel.

MR. AGGARWAL: Correct.

DR. LEITCH: And not just coming out of the vessel and then (inaudible) redundant valves.

MR. LOESER: And this is another one of those cases where everybody knew this was meant all the while, but it was never spelled out. So it was just spelled out.

MR. AGGARWAL: In conclusion, it is my submission to the committee that IEEE standards in question is a much improved standard over the number of years, and the staff is working with the IEEE hand-in-hand.

In the last reg guide with the many

exceptions to the IEEE standard, and looking over a number of years, although those sections have been incorporated or resolved, it is the opinion of the staff that this standard, if it satisfies so that the requirements are met, it will meet the commission requirements on the part of single failure.

And it is my submission to you that the committee concur with our findings, and permit us to publish this guide as a final guide. Thank you. I would also like to thank Dave, who took the time to come from Susquehanna River to join us today, and on behalf of the NRC, I would like to thank him.

MR. CARUSO: Excuse me, Satish.

MR. AGGARWAL: Yes.

MR. CARUSO: I was wondering if you could please -- in my review of the reg guide, I saw that there is additional guidance with regard to single failure analysis in the designs that used digital computers.

And that this guidance is provided in the common cause failure section and refers the reader to the IEEE standard 7-4.3.2-1993.

MR. AGGARWAL: Right.

MR. CARUSO: And it discusses common

cause failures, but yet design deficiencies are specifically exempted from the standard. Could you please elaborate on why those were exempted from the standard?

MR. AGGARWAL: I really don't understand the question. Do you, Dave?

MR. ZAPRAZNY: Could you repeat that again?

MR. CARUSO: When I looked at the standard --

MR. AGGARWAL: This is the standard that we are talking about now, 379, or 7-4.3.2?

MR. CARUSO: Well, 379, and it refers or it says that additional guidance was added to address single failure analysis in designs that used digital computers, and that this guidance is provided in the common cause failure section and refers the reader to IEEE Standard 7-4.3.2-1993.

And it identifies some important common cause failure mechanisms for digital computers, and that it would be a software flaw, which can be considered a design deficiency. Yet, design deficiencies were specifically exempted from the standard.

MR. AGGARWAL: Ralph, could you tell us

the section number also? Are we on 5.5?

MR. CARUSO: This was based on 1.53 in the reg guide, I guess.

MR. AGGARWAL: Okay. And where are you reading it from?

MR. CARUSO: This was --

DR. ROSEN: Excuse me. Cliff Doutt, do you remember the design deficiency section?

MR. DOUTT: I think --

MR. AGGARWAL: Cliff, could you please move to the mike, please?

DR. ROSEN: Thank you.

MR. DOUTT: Are you talking about the next to last paragraph on page 5?

MR. CARUSO: Yes.

MR. DOUTT: I think what he is asking is on your single failure criteria, and you go to common cause, common cause has some exceptions for the single failure criteria, based on -- you know, you have design issues which are exempted because you are saying that surveillance, or quality control programs, or whatever, will take care of that.

But in digital systems, it references you back to 7.4.3.2, because that common cause there is a design.

The standard itself exempts some common cause based on I think one's design, and the reasoning being that if you go back over and say you are going to take credit for either surveillance or quality control programs, but in software the design flaw is common cause. I know the standard references you back to 7.4.3.2.

MR. LOESER: Let me see if I understand what you are saying. You are objecting because this particular paragraph has on the third line, it says things that are exempted are design deficiencies.

But in fact if you take into account 7.4.3.2, which talks about V&V, for example, on the design and on the specifications and all of this, where you ensure that there are no design deficiencies, or at least to the probability of a design deficiency, is sufficiently small that you are not capable of finding it anymore, despite your best efforts.

MR. DOUTT: Yes, I think the standard actually draws you off, because common cause failure in software is unique, and so it takes you to 7.4.3.2 to resolve that.

MR. AGGARWAL: Exactly, and that is the subject matter of the IEEE Standard 7.4.3.2.

MR. DOUTT: Right.

MR. AGGARWAL: And as I submitted to the committee before, that the latest (inaudible) IEEE standard yesterday, and the staff plans to endorse that, and we will be back to you, and provide information on how single failure will apply to digital computers.

MR. LOESER: In this particular case the last paragraph of Section 5.5 happens to be on page 6, and it says guidance on using diversity to address common cause failures in digital computer systems as provided by IEEE Standard 7.4.3.2-1993.

And that in fact does address design errors. So if you think about it, that last sentence is sort of an exception to the fact that it talks about design deficiencies being exempted from common cause failure. Does that answer your question?

MR. CARUSO: Yes, and it seems like there was -- and maybe I am missing something, but it appears that it is going to be addressed --

MR. LOESER: Well, design deficiencies are addressed in the existing version of 7.4.3.2.

MR. CARUSO: Yes, that's correct.

MR. LOESER: Design deficiencies are addressed in the existing version of 7.4.3.2.

MR. CARUSO: Yes.

MR. LOESER: And the fact that there is a new one coming out doesn't really change that.

MR. AGGARWAL: But he is talking about the reg guide, and what we are saying is that the reg guide will endorse the standard will be forthcoming, yes.

MR. LOESER: But, Satish, that has nothing to do with what we are talking about. The fact that we are planning to endorse a new version of 7.4.3.2 doesn't matter if the existing version takes care of this version.

MR. CARUSO: I think the reference for 7.4.3.2 was intended to cover common cause software failure in 7.4.3.2 right now, and the new standard will just be whatever enhancements there are.

MR. AGGARWAL: That's right.

MR. LOESER: So what is the question?

MR. CARUSO: That the design deficiencies are considered as a common cause failure.

MR. LOESER: In digital software, yes. That's why we review the design.

MR. CARUSO: Very good.

MR. AGGARWAL: This will conclude our

presentation.

DR. SHACK: Any further questions from the committee? If not, thank you for a detailed presentation, Satish.

MR. AGGARWAL: Thank you.

CHAIRMAN BONACA: I think we can go off the record now. We do not have to record the meeting anymore.

(Whereupon, at 9:31 a.m., the meeting was concluded.)