ACRST-1472

ORIGINAL

UNITED STATES NUCLEAR REGULATORY COMMISSION

IN THE MATTER OF: **DOCKET NO:**

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON DECAY HEAT REMOVAL SYSTEMS

LOCATION: WASHINGTON, D. C. **PAGES:** 1 - 208

DATE: MONDAY, DECEMBER 2, 1985

TR01 0/1

ACE-FEDERAL REPORTERS, INC.

Official Reporters
444 North Capitol Street
Washington, D.C. 20001
(202) 347-3700

NATIONWIDE COVERAGE

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON DECAY HEAT REMOVAL SYSTEMS

Nuclear Regulatory Commission
Room 1046
1717 H Street, N.W.
Washington, D. C.

Monday, December 2, 1985

The subcommittee meeting convened at 1:00 p.m., Mr. David A. Ward presiding.

ACRS MEMBERS PRESENT:

MR. DAVID A. WARD

MR. JESSE EBERSOLE

MR. HAROLD ETHERINGTON

MR. CARLYLE MICHELSON

DR. CALTON, Consultant
MR. DAVIS, Consultant

PUBLIC NOTICE BY THE

UNITED STATES NUCLEAR REGULATORY COMMISSIONERS'

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

MONDAY, DECEMBER 2, 1985

The contents of this stenographic transcript of the proceedings of the United States Nuclear Regulatory Commission's Advisory Committee on Reactor Safeguards (ACRS), as reported herein, is an uncorrected record of the discussions recorded at the meeting held on the above date.

No member of the ACRS Staff and no participant at this meeting accepts any responsibility for errors or inaccuracies of statement or data contained in this transcript.

P R O C E E D I N G S

MR. WARD: The meeting will now come to order.

This is a meeting of the Advisory Committee on Reactor Safeguards Subcommittee on the Decay Heat Removal Systems.

I'm David Ward, the Subcommittee Chairman. Other ACRS members here are Mr. Ebersole and Mr. Etherington. Mr. Michelson, I believe, will join us later this afternoon, and Mr. Reed may join us tomorrow.

We also are privileged to have in attendance ACRS consultants, Mr. Catton and Mr. Davis.

The purpose of the meeting is first to discuss the issue of auxiliary feedwater system reliability. That will be the sole item on the agenda this afternoon, and then, second, tomorrow, we will review the status of the NRR's resolution position for USIA 45, entitled "Shutdown Decay Heat Removal Requirements."

Paul Boehnert, on my right, is the cognizant ACRS Staff member.

The rules for participation in today's meeting have been announced as part of the notice of the meeting previously published in the Federal Register on Tuesday, November 19, 1985.

A transcript is being kept and will be made available as stated in the Federal Register notice.

I request that each speaker each identify herself or himself and speak with sufficient clarity and volume so that she or his can be readily heard.

We have received no written comments from members of the public, nor have we received requests for time to make oral statements from members of the public.

I have no comments to make at this time, other than as events move on, and the experience in the industry seems to be telling us again and again that the subject of today's meeting is extremely important and concerns itself with one of the most important safety systems in nuclear power plants.

Unless Mr. Etherington or Mr. Ebersole have any comments, we'll go ahead with the agenda.

First is a speaker from the Office for Analysis and Evaluation of Operational Data, Mr. Rob Dennig.

MR. DENNIG: Good afternoon. My name is Bob Dennig. I'm the Section Chief of the Program Development Section in AEOD.

I thank you for the opportunity to participate in the meeting, and actually, I'm hoping to learn as much from listening to you as you learn from listening to me, perhaps more.

I have agreed, or I agreed when contacted, that we would try to provide some recent context of operational

experience as a backdrop for your discussions on auxiliary feed reliability.

I notice on the agenda there are two items listed under my bullet.

The first item, I'm afraid that I really don't have any material to address or background to address. About the only thing I can say is that the systems are used for startup and shutdown, because we do receive reports in which problems crop up during those phases of operation, but beyond that I can't really say very much.

So my time will be spent on Item No. 2, for which I chose to look at 1984. What I thought I'd try to do --

MR. WARD: Bob, could I interrupt just a minute.

I guess the point of the first item on the agenda was to help the Subcommittee develop an appreciation for what the significance of the challenge is to the aux field system.

As I understand it, in the large population of plants in the U.S., there's quite a spectrum of how aux field systems are used by design and in practice, relative to main feedwater systems. For example, apparently in some plants, any reactor trip invites a challenge to the aux feed system.

In other plants, the main feedwater system can be relied on to carry the plant cooling load for some period of

time. In order to understand the raw statistics about aux feedwater failures mean, I think we have to understand better than we do now or certainly better than I do, how these systems interrelate.

If you can help us with that, we'll be grateful.

MR. DENNIG: The primary thing that I was able to do in preparing for today, was to come up with what I would characterize as an educated guess, the actual challenges to auxiliary or emergency feedwater systems. Part of that guesswork involved looking at auto start signals for the system. And I think you'll be able to see from some of the signals that I used in coming up with this actual demand guess, some of the ways the system is used. Part of the difficulty in preparing for this presentation is that there are a wide range of system designs, and as far as I can tell from looking at published documents, there is always as wide a range of start signals.

Almost any statement you make about this particular system, trying to pull together a general picture, generalized to any great extent, you are wrong about some particular set of plants, from what you said, no matter what it is.

There seems to be an exception for just about every generalization. So maybe as I go through the early parts of what I've prepared, that will help introduce some

DAVbw

of the ways the system comes on, theoretically comes on.

MR. EBERSOLE: May I ask -- we know there are systems which ramp down on turbine trip, and thus meet the low water demand required by shutdown heat removal. We also know there are many systems that can't do that and must jump to aux feedwater but have the prerogative of some sort of modulated low flow system off the main feedwater system.

The lowest class of all plants, of course, have to be the ones that can't use the main feedwater systems, because that's one of the tracks of heat removal. I was astonished in, I think, 1968, to find out that in the presence of no exit at all, there was no qualified heat removal system for PWRs whatsoever. The AFW system had been relegated to the vendors who had little, if any, special interest in it.

Out of that has grown this chaos of design, which you say you can't track down. I don't think we can escape having to track that down, in the absence of any controls over the process.

Probably the worse example of this was, you know, Davis-Besse.

MR. DENNIG: I certainly can't disagree.

As far as I can see, the information even that I was using to make this preparation, based on post-TMI documents, as far as the prescription for the systems and

start signals, and so forth, has evolved, and there are changes. So the exact status of any one of those systems at any particular time requires a fairly large effort to keep track of it.

I apologize for the hand waving. I'm not trying to be evasive, but I'm not your best witness on this, but I can say that part of my job or most of my job involves trying to make generalizations about operating experience. In the U.S. reactor population, that's always difficult to do. We joke about it kind of being like trying to do epidemiology studies on Noah's Ark. There's two of this and two of that and two of the other thing and never much data on any particular thing.

And this system certainly has that problem.

(Slide.)

If might, one thing that I'm going to try to do --

(Slide.)

-- is pull together an operating demand estimate. The reason why we have to do that, why I wouldn't have the information tabulated somewhere or tracked somewhere, is that the way things stand now, the LER reporting requirements require reporting all the SF actuations. That's one of the major items in the Rule. The problem is that the auxiliary feedwater system is not

classified as such. So that particular reporting requirement will not capture each and every and all engineering aux feedwater system starts or em‹ rgency feedwater starts.

MR. EBERSOLE: Why isn't that matter fixed?

MR. DENNIG: I couldn't say.

MR. EBERSOLE: It's certainly the most frequently challenged ESF system, that is, other than the shutdown system, which is usually coincident with it.

MR. DENNIG: The state of things as I understand them indicates that some are and some are not. At later plants, apparently there's more uniformity, but amongst the earlier plants, that's not the case. It almost goes hand in hand with diversity of designs.

MR. WARD: What are the ground rules for making that differentiation? Have you been able to puzzle that out?

MR. DENNIG: Of what is an ESF and what is not?

MR. WARD: Yes.

DR. CATTON: Who decides?

MR. WERMIEL: My name is Jerry Wermiel with the Staff. I'm going to get into some of that in my presentation, under Item B of the agenda, where I'll try to draw the line, if you will, about approximately what point a plant would have, what would be classified as a

DAVbw

safety-related or engineering safety feature aux feedwater system, and where they wouldn't.

MR. WARD: Okay. Fine.

If we're asking you questions that can better be answered by later speakers, that's an acceptable process for us to take.

MR. DENNIG: Another problem with tracking these things, as far as the reporting tools that we have got, if someone will send in a report, say, of a reactor trip, part of the things that happen in that sequence, quite possibly, will be a start of this particular system.

We haven't seen consistent explicit reporting of system starts or sequences following such things as trips. Frequently, the reporting will just say that all systems worked as designed. So that adds a little uncertainty, as far knowing for sure in any particular case whether the system stated or not.

So what it boils down to, as far as trying to put together this actual estimate for you is that I used system start signals and reactor trip signals, which I have a fairly good record of, and where a start signal was the same or close to a reactor trip signal, I used the counts of the reactor trip signals as a way of bootstrapping into the challenges to the aux feed system.

On occasion we do get straight out reports of

actuation of the system as an engineering safety feature.

So I have those, and if you would take that, then, the combination of those two things, as a sort of lower bound on the actual operating demands in a particular year.

MR. EBERSOLE: May I ask one other detail about this.

The challenges to the system, did you differentiate between those that might be called benevolent, which were sort of an exercise, but from which you could fall back to the main feedwater system? In short, you didn't really need it. You started it as a matter of prudence.

MR. DENNIG: No, I'm afraid I did not. Not for this exercise.

MR. EBERSOLE: As far as your report would show, they were all critically necessary; right?

MR. DENNIG: Yes.

MR. EBERSOLE: And that's not really true?

MR. DENNIG: No.

MR. EBERSOLE: Isn't it important to discern the benevolent and nonbenevolent need for these things in a challenge set ?

MR. DENNIG: Yes.

MR. EBERSOLE: It's just like a square. Maybe

you don't need it. You've just got it.

MR. DENNIG: I think that would be a beneficient refinement; yes.

MR. WARD: But I guess just strictly speaking, as an indication of system reliability, if the start of the system was demanded, whether for a good cause or not --

MR. EBERSOLE: -- i. would be conservative.

MR. WARD: -- it would be pertinent, it seems to me.

(Slide.)

MR. DENNIG: For the Westinghouse PWRs, as a group, generalizing again, and again, this statement is probably not true for at least one reactor.

Lo lo steam generator level and safety injection, two start signals.

So to estimate actual demands of used reactor trips from lo lo steam generator level, the system starts reported as ESF actuations. Safety injection signals reported as ESF actuations, and then I eliminated the double counting.

What one comes up with is a figure of 130 demands. You start reporting from 34 of 37 licensed plants in 1984, which comes out to be something between 3 and 4 demands per plant per year.

Again, this is 1984, as an estimate of actual

DAVbw

challenges to the system.

Again, this is not testing, and this is not use of the system as a start up on a shutdown system under some kind of controlled circumstances.

MR. WARD: Let's see. So when you say plants, you mean units, I guess; right? Is that what you mean?

MR. DENNIG: If one understands plant as one reactor and one vessel, that's what that means.

MR. EBERSOLE: That's the three-per-year per plant, isn't it?

MR. DENNIG: A little bit more than that; yes.

MR. EBERSOLE: Then this says, since we have a higher rate of scrams than that, that quite a few plants don't start aux feedwater on stream.

MR. DENNIG: This is just Westinghouse plants. The start signals that I was able to identify generic to Westinghouse plants were safety injection, lo lo steam generator level.

There's another one. Lo lo steam generator level in one steam generator. The lo lo I'm talking about is two out of four, whatever's needed to be coincident for a trip. So there's one other signal.

There's also a differentiation on which type of pump gets started. The lo lo steam generator signal that I'm talking about, as I understand, starts the

turbine-driven pumps. That's what you've got.

The safety injection signal starts generator pumps.

MR. ETHERINGTON: I suppose some of these demands were spurious. Were they all included?

MR. DENNIG: The ones derived from the trip signals, I would say not. It's possible that some of the ones that were reported as ESF starts could be characterized as spurious or unneeded, but offhand, I can't tell you.

MR. EBERSOLE: A true ESF system ought to really never have to start, because you shouldn't have to have any accidents to start it. Here we have an ESF system that has a start every so often, maybe half a dozen times a year.

I don't know what the specter of the worst end of that is. You don't have a distribution of that, do you?

MR. DENNIG: Oh, sure. Thank you for that question.

(Slide.)

MR. EBERSOLE: 11. Which one was 11?

I hope not Davis-Besse.

MR. DENNIG: Out there at 21, this guy. Oh, no. Number of demands, I've got plants, with one demand. I've got one plant with 21.

MR. EBERSOLE: We should mark that one.

MR. DENNIG: Callaway 1.

DAVbw

MR. WARD: That was the start-up period.

MR. DENNIG: Right. The start-up. There should be other biases on this report. You know, the shakedown.

MR. WARD: Even so, that's rather many, I would say.

MR. THADANI: Ashok Thadani of the NRC Staff.

One of the things to keep in mind, it seems to me, is the specific design of some of the plants. Some Westinghouse plants, any time we have reactor trip, we also get demand feed pump trip and demand is placed on aux feed. That is not the case for a lot of other PWR designs.

So if you see 19 to 21 challenges to AFW, sometimes it's likely caused by that design feature.

DAVbur

MR. EBERSOLE: Why should Westinghouse be permitted to have that design?

MR. THADANI: I raised the same question, and we have gone through that issue in fact recently as part of our PRA review. We raised that question, and the utility -- Northeast in this case -- promised me that they were going to take a very close look to see what the downside was of making a change. We haven't heard back from them, and I don't know the answer, Mr. Ebersole.

Offhand, I would think that one ought not to trip the aux feed. On the other hand, we don't know what the downside is.

MR. EBERSOLE: You know, we have GAC-17, which on the electrical system says you must have the privilege of AC system reliability, even on the fringes of safety system reliability.

It would certainly seem prudent to have that requirement on main feed. After all, that is the endpoint of AC power.

MR. THADANI: Certainly, that is my own opinion as well.

MR. WARD: But you see, the point you raised is exactly the point brought up at the beginning of the meeting. It is hard to know what to do with these raw data unless you know how the system is used.

MR. THADANI: I agree with you. You have to pin down the cause, and as I say, the design feature that is causing all these challenges, is it really necessary?

MR. WARD: I don't know if it is the cause. Rather, it is how much dependence you are putting on that aux feed pump start, and if the overall system is not designed to depend on that aux feed pump start, there may be some subtleties in the design which make it less reliable. I don't know whether that is the case or not. That is what we would like to find out.

MR. DENNIG: Let me reiterate one more time that what you are seeing is synthesized. In a large part, it relies on the assumption that given a trip on lo-lo steam generator level, I will get a start of this system based on general statements found in Westinghouse design documents in discussions with some people in ROAB. That is where this is coming from.

So it is kind of dependent necessarily because of the way it is done, and as I say, that is the fallback because we don't have good tracking of starts in that system. We just don't have any requirement.

(Slide.)

The case for Combustion Engineering is as follows. Again, this is based on looking at updated FSARs, Combustion Engineering plants' auto start, their aux feed

DAVbur

systems on a lo steam generator level. There is also the trip on lo steam generator level.

So once again, estimating demands from reactor trips from lo steam generator levels, those efforts are reported as ESF actuations and then eliminated the overlap, resulting in 22 demands from eight of 12 plants licensed in '84, a high of six, which was Arkansas 2. That comes out to something approximating two per plant per year, which is less than my guesstimate for the Westinghouse per year.

MR. EBERSOLE: Is this the kind of number on demand frequency that they would stack up against the 10 to the minus 4 failure rate per demand?

You know, Combustion has that sort of goal. At Palo Verde they don't even have any other way to cool it.

MR. DENNIG: In the sense of throwing in actual demands and using them in the denominator?

MR. EBERSOLE: Yes.

MR. DENNIG: I would suspect that that is really standard procedure.

MR. EBERSOLE: About six per year is the nominal demand frequency?

MR. DENNIG: No, two.

MR. EBERSOLE: I am sorry, two.

That is 22 from eight plants?

MR. DENNIG: Remember again the kind of

calculation you are talking about, this doesn't include any kind of test situations. Those usually get thrown in, too, plus the failures during tests.

Does anybody else have anything?

MR. WARD: I don't want to be picky, but when you say -- I will go ahead, anyway. When you say two per year, do you get that by dividing 8 into 22?

DR. CATTON: After you subtract 6.

MR. DENNIG: No, I wouldn't do that. Yes, that is how I should come up with it. It should be 12 into 22. I have got 12 plants out there. Theoretically, they all could have been reporting.

MR. WARD: I thought you said only eight plants; you have data from only eight plants?

MR. DENNIG: I have data from all 12 plants.

MR. WARD: I see. You have data from all 12. I was misinterpreting that. I am sorry.

MR. EBERSOLE: But again, if you generalize --

MR. WARD: Four plants had zero, in other words? Is that what you are saying?

MR. DENNIG: No, you are right. It should be 22 divided by 8.

DR. CATTON: If you take the high volume of 6 and subtract the 6 and divide by 7, you get close to two.

MR. WARD: There's all kinds of ways you could

DAVbur

get two.

(Laughter.)

MR. WARD: I think he really means three, though.

DR. CATTON: If he has got one squirrelly plant --

MR. MICHELSON: He isn't going to have one squirrelly --

DR. CATTON: He has a high volume of 6.

MR. WARD: Why don't we ask Bob? What did you mean, Bob?

MR. DENNIG: I am using LER data. I have got stuff from eight plants. Zero is from 12 plants. So as far as actual demands are concerned, I will backtrack again and I will say that 12 is the number that I would use to make an average.

MR. EBERSOLE: What sort of average do you use by picking the average versus the worst plant, since I would imagine we would get as much news out of the worst plant as we would the best?

MR. DENNIG: No particular rationale. Just trying to generalize.

MR. EBERSOLE: That is pretty terrible. When we have got both spectrums, you will want the worst end that will do us in.

MR. DENNIG: You really wouldn't, given any other choice. You would stick with plant specific information.

MR. EBERSOLE: People who don't have standard plants, the worst one is your marker plant, what do you do?

I would rather deal with one plant. I don't know how good the logic would be in getting a distribution of six.

Don't let me hold you up.

MR. THADANI: Ashok Thadani again, Mr. Ebersole.

As part of some of the recent discussions on the issue of the auxiliary feedwater system, the staff has met with a number of utilities. One of them has to be Arkansas Unit 2.

And, yes, indeed, over the last, I think, roughly five years, they have had, I think, 11 loss of feedwater events, as I recall, which was much higher than the norm, and the utility is in the process of implementing some improvements in their main feedwater system to reduce the frequency of those transients.

And that issue of challenges presented from actual loss of feedwater events is also part of the recent CRGR package that I suspect the staff is going to tell you about.

MR. EBERSOLE: I see. Thank you.

(Slide.)

DAVbur

MR. DENNIG: Last but not least, Babcock and Wilcox units.

I didn't have any good handle to use statistics from scram information to augment reports of ESF actuations. I just listed a couple of the starts that I could identify. One could, if one went through the gray books, possibly do a better job of coming up with a number similar to what I did for Westinghouse and CE. What that left me with was just using the reports of ESF actuation, which came out to be three starts at two of seven units that were licensed for 1984.

MR. EBERSOLE: Do you have any data on the boilers?

MR. DENNIG: No, sir.

MR. EBERSOLE: Those are the feedwater systems on boil. Why isn't that included in the investigation? You know, the aux feedwater system. What do they call it?

MR. DENNIG: HPSI, RCIC.

MR. EBERSOLE: Just because it is not called feedwater?

MR. DENNIG: I am not sure.

MR. EBERSOLE: It is feedwater.

MR. DENNIG: This is true.

MR. MICHELSON: Refresh my memory. The new reporting system was January of '75, is that right?

DAVbur

MR. DENNIG: January of '84.

MR. MICHELSON: Sure, '84. Was it '84 or '85?

MR. DENNIG: '84.

MR. MICHELSON: So all your information came from the new reporting system?

MR. DENNIG: Specifically from 1984. This doesn't include 1985 information.

MR. MICHELSON: I realize that.

MR. DENNIG: But, yes.

MR. MICHELSON: Why do you seem to have difficulty getting the information that you need for this statistical study?

I thought all those actuations would be adequately reported. Am I missing something?

MR. DENNIG: If it were true that this particular system was designated as an engineered safety feature, we would get that.

MR. MICHELSON: It hasn't been in all cases?

MR. WARD: I don't think you were here at the beginning, but he brought out at the start that in some plants it is not an ESF. We are going to hear more of an explanation of that from NRR in a little while.

MR. MICHELSON: Yes, that would make quite a difference.

On those that are classified as ESF, did you have

DAVbur

any difficulty with the kinds of information that the LER gave?

MR. DENNIG: I can't give a real good answer to that because that would require compiling which places it is and which places it isn't, which I did not do, to make that judgment.

But outside of that problem, we still have difficulty in getting detailed discussion of things like post-trip actuations, so that there is that problem.

MR. MICHELSON: Is this an item that has been highlighted to the utilities as in need of improvement?

MR. DENNIG: Oh, yes. I believe the revision to NUREG-1022 specifically called that out as a problem, and then we have an ongoing LER quality program that is linked up with SALP -- one of the things that gets pinned on, if necessary.

MR. MICHELSON: You are hitting at when it is an ESF, but if it isn't an ESF you don't have a leg to stand on very well, do you?

MR. EBERSOLE: Well, there is another leg.

MR. MICHELSON: Let me get the answer to my question first.

Is there a problem if it is a non-ESF? Are they even writing LERs on it then unless it is related to some other aspect?

DAVbur

MR. DENNIG: If it is an ESF, I believe we get the report.

MR. MICHELSON: If it is not an ESF, how do you happen to get it?

MR. DENNIG: The only way you get it then is if it is part of a reportable sequence and they are kind enough to call out all the steps in the sequence. Sometimes that does not happen. It doesn't happen even when the thing is an ESF. The statement will be made that all engineered safety features performed as designed.

To make use of that, either you have got to have the person looking at that know that for this particular plant that is an ESF and it does start, and therefore I have got to hit on that.

What we would certainly prefer and what they are supposed to do is call out specifically what the systems are.

MR. MICHELSON: So it hasn't been working quite as planned?

MR. DENNIG: I think that is correct.

MR. EBERSOLE: So it isn't an ESF, but is it a safety grade system?

And now I am going to go back now to service water. That is not an ESF either. It is a safety grade system which you lose all the time.

Why should we only look at the system, you know, which has an occasional demand versus those we head for all the time? Can you not get it on the grounds that it is a safety grade system? Is it a safety grade system?

MR. DENNIG: We get reports of problems with the system through the route of saying -- and I will show this a little later. This is a reporting requirement for reports of failures of systems that are required for accident mitigation, removal of decay heat, and a couple of other things.

So as one removes decay heat, we would argue that, yes, we should get reports of all problems with the system but not all actuations of the system.

MR. WERMIEL: Maybe I can help, Mr. Ebersole. The service water generally is safety related or ESF because it is a support system for post-LOCA safe shutdown.

MR. EBERSOLE: That is all? What about new LOCA shutdown?

MR. WERMIEL: That is part of the problem. In the old days, as I understand it, from what I have been able to see, most of the review of engineered safety features were safety-related -- equipment systems and problems and structures. That was geared around the large LOCA, and for that reason equipment and systems and structures required to support shutdown following such an event received that

classification.

Others, unfortunately, even though they may -- like aux feed -- be challenged, didn't receive that same treatment.

It wasn't until -- as I will get into a little bit in my presentation -- the advent of the standard review plan was it really recognized that indeed there are other events or challenges to plant systems that would warrant better classification, better quality, better attention to the availability of other systems.

MR. EBERSOLE: As a matter of fact, it doesn't have to be an event. It is an everyday affair, isn't it, that you have to have these things running?

MR. WERMIEL: In some plants, well, service water definitely.

MR. EBERSOLE: So certainly the most critical demand is the one that comes quick.

MR. WERMIEL: As I said, the service water was treated as an ESF system or a safety system.

(Slide.)

MR. DENNIG: Okay. The other half of the discussion has to do with the reported problems that we have knowledge of. Again, this is based on licensee event reports under the new reporting requirements.

We have one particular criterion that covers

basically an operating problem or unavailability of the system that is used for shutdown, removal of residual heat, control of the release of radioactive material, or mitigating the consequences of an accident.

We would argue that auxiliary feedwater fits at least the remove residual heat criterion.

In reporting from licensees, just for your information, we ask them to indicate which reporting requirement they are responding to. A lot of times, more than one will apply, but they don't indicate that more than one would apply.

So indications of aux feed problems can be found reported under ESF actuations, tech spec violations. There is a criterion that covers common cause, degraded condition, or the system fault, which is the paragraph that I alluded to at the top of the slide.

MR. EBERSOLE: What would a fire be called?

MR. DENNIG: What would a fire be called?

MR. EBERSOLE: Is it an accident?

MR. DENNIG: There is another criterion that talks about threats, external threats or internal threats to equipment and safety of personnel. Most likely a fire would come under that situation.

MR. MICHELSON: Would you consider that the auxilliary feedwater is not a safety system at a particular plant, which I gather can be the case? Then your first bullet doesn't apply at all, since it doesn't perform any safety function; even though it may remove residual heat, it doesn't perform any safety function by definition.

Main feedwater removes residual heat, too, in a way, but it has no safety function other than some isolation and tripping requirements.

(Slide.)

MR. DENNIG: This slide summarizes what we had reported for 1984 via LER's. It's not voluminous, there's not a great deal. Again, the criteria that we are reporting are set very high at system level. These are multi-train systems and a number of things have to fail before the system is unavailable.

There are no particular highlights. Let me say something about the first item under Westinghouse that refers to an advent at Trojan in September of '84, in which the plant was able to recover using a motor-driven startup pump that is apparently not part of the defined aux feedwater boundaries.

It was just there for operational purposes and that's what they used to recover.

MR. EBOERSOLE: They had a pump similar to Davis-

Besse that was ready to go, right. Is that what you say?

MR. DENNIG: I'm not that familiar with the configurations.

MR. WERMIEL: I can answer that, Mr. Ebersole. In about 1981, they added a large startup motor to the pump. It's a manual start pump. It can be loaded on a diesel generator because it is operated from an on site bus and it is also tech spec-ed. Its operability is governed by tech specs.

MR. EBOERSOLE: Was that mandated by NRC, or was it just something they volunteered?

MR. WERMIEL: This was a volunteered backfit. The utility had been having over a number of years problems with the direct diesel-driven and the turbine-driven aux feedwater pumps, both of which, incidentally, were classified as engineered safety features or safety-related.

They added this motor-driven pump to provide additional diversity and capability for startup and shutdown without having to rely on two safety pumps.

MR. EBOERSOLE: Had they performed a PRA that showed that they needed to do nothing to this?

MR. WERMIEL: I'm not aware of what had been done.

MR. MICHELSON: What is the classification of the Turkey Point auxilliary feedwater system? Is it safety-

related?

MR. WERMIEL: I don't believe it is, no. I believe that plant is so old that they did not classify it as such.

MR. MICHELSON: So that event may not even be on this listing.

MR. DENNIG: The two train level failures on test under Westinghouse, those are both Turkey Point.

MR. MICHELSON: The real one wasn't under test.

MR. WERMIEL: No, they had a demand where two out of three pumps failed to operate, as I understand, on demand.

MR. MICHELSON: There's some question about the true availability of the third one as well. Clearly, to quit.

MR. WERMIEL: As I understand, that was in '85. That was in June. It wouldn't be in this.

MR. MICHELSON: I'm sorry, this is only '84. I stand corrected.

MR. WARD: Is that right, Bob? Are these '84 events operating problems?

MR. DENNIG: Exclusively, yes. And the only other system level failure on demand is under Babcock and Wilcox. That was Oconee III. There was a nine-minute lapse due to some missed timing on some valves opening and

closing recovered from the event by opening the proper isolation valve on there, which is the feedwater system. So that was nine minutes for that one.

MR. EBOERSOLE: How many of these failures contradict the standing PRA on nominal grounds? Any of them? You know, that's the popular way of not getting things done, is to do a PRA.

MR. DENNIG: I would say that there are no situations that were described in the events that I reviewed that are not on the list of things to include in a PRA.

MR. EBOERSOLE: Oh, is that so? Because they're not a safety feature?

MR. DENNIG: One of the specific instances encompassed by a PRA, that is another question. But, as far as unusual things that aren't covered by the methodology,

MR. WARD: Okay. A similar question, I guess. If I look just simplemindedly at the aux feed requirement in the standard review plan of the reliability requirement, the standard review plan as given, a reliability of 10 to the minus 4. So you want one failure per 10,000 demands. So if I look at the experience in 1984 with the Westinghouse plants, you said there were 130 demands.

There is one system level failure. I presume that 10 to the minus 4 reliability, that's a system number.

MR. THADANI: Mr. Ward, Ashok Thadani. There are

two elements. Number one certainly is what you're suggesting, one system level failure per 130 demands. I don't know exactly what the real number of demands was because, in reality, the systems are tested as well. And that would be construed as a demand if the tests are done properly.

Number two, the probabilistic techniques also followed in recovery factors. They tried to make a determination as to whether those flaws were recoverable or not. Appropriate credit is given for recovery aspects.

MR. WARD: That's in the PRA, but I'm not sure if it's in the standard review plan.

MR. THEDANI: Oh, yes.

MR. WARD: Is that number as given in the standard review plan intended for recovery?

MR. THEDANI: Yes, and it is done that way. The calculations are done that way. There will be somewhat of a discussion later on about that.

MR. WARD: Okay.

MR. MICHELSON: When the system is tested normally, is it tested under flow conditions or is it just a bypass from the pump?

MR. WERMIEL: Generally, when the system is tested, it's a test of a single train, a single pump in recirc.

MR. MICHELSON: It's generally a very small recirculation line.

MR. WERMIEL: Some plants, yes; some plants, no. Some plants have full flow recirculation lines and can simulate closer to an actual demand on the system.

MR. MICHELSON: You're saying it's probably a pretty fair test of the pump complex, not necessarily the valving?

MR. WERMIEL: That's correct. I don't know of any plants on test pump water that's been generated.

MR. MICHELSON: I'm acquainted with some that you don't get full flow on on bypass.

MR. WERMIEL: That's correct.

MR. WARD: Let me continue with my simple-minded analysis here. Let's set aside the testing failures because I'm not sure you have testing demands up there.

MR. DENNIG: I don't have testing demands.

MR. WARD: These are both operational failures and operational demands.

MR. DENNIG: Some of these are testing failures. The demand stuff I did was just on actual demands. Some of these are testing failures. The one that you picked on Westinghouse wasn't.

MR. WARD: Okay. Let's just assume then that's again comparing with the standard review plan reliability

of 10 to the minus 4. What we're saying here, the actual failure rate was 10 to the minus 2nd. So if these systems indeed meet the requirements of the standard review plan, that means that recovery would have to be called out in 99 out of 100 failures to start.

Then, in Combustion, there weren't any system failures. In Babcock and Wilcox, there was one failure out of three demands.

MR. DENNIG: Which I tried to pitch as a lower bound on the number of demands.

MR. WARD: Now, I guess, in a PRA, if it was done right, you'd credit the fact that there are fewer demands. But I don't know that the standard review plan does that or not. We'll find out about that.

But this means that if the B&W systems meet anything like the standard review plan, that recovery has to be credited 99.9 percent of the time, or something like that.

MR. DENNIG: I wouldn't lean too heavily on the B&W stuff here. That's where things get a little shaky as far as our knowledge.

MR. WARD: We're trying to develop some kind of understanding of what the real performance of these systems is compared with what the requirements are, and compared with what the probabilistic risk assessments are claiming

DAV/bc

for them. And it's a murky picture and I agree it's difficult to see through the murk, but let's keep trying.

MR. EBOERSOLE: Dave, may I ask a question?

There's another aspect of this. When you said Babcock and Wilcox is murky.

MR. WARD: No, I was misquoted.

MR. EBOERSOLE: Well, he said it was murky.

MR. WARD: I said the whole picture seems to be murky.

MR. EBOERSOLE: Babcock and Wilcox' system operate with virtually dry boilers. They need water in a hurry at the other end of the spectrum. Combustion Engineering uses great big boilers with all sorts of water standing. I think Westinghouse is somewhere inbetween.

How do you fold in the degree of urgency of beginning feedwater?

MR. WARD: Somehow, that seems to be discounted, Jessie. We look at the Westinghouse and C.E. numbers he showed us and there's two or three demands per reactor year. In the B&W plants, there's only half the demand.

MR. EBOERSOLE: The reason for that of course is B&W better damned well be good because they can't afford an outage. If they have one for the long haul, they're in trouble.

MR. WARD: But I'm just saying that they are. If

we take these data at face value.

MR. EBOERSOLE: I guess Combustion Engineering, like Palo Verde, with all the unused boilers they have, they can stand a substantial time of outage before they're in trouble; whereas, B&W can't stand anything at all.

MR. DENNIG: Mr. Ebersole, at least in the world of reliability studies, people pay attention to time, to dryout. B&W plants typically, that's in the range of five minutes or less depending on what transient we're talking about. The credit for recovery is much less numerically than that for Westinghouse and Combustion Plants.

MR. EBOERSOLE: So that is credited then?

MR. Thadani: That is folded in the analysis.

MR. DENNIG: For whatever it's worth, the B&W plants do not trip very much either.

MR. EBOERSOLE: They'd better not.

MR. DENNIG: That concludes what I have.

MR. EBOERSOLE: Maybe that aspect of th8e B&W design could be profitability used by Westinghouse.

MR. MICHELSON: Can the staff explain to us later if they have any plans to improve the level of information that's going to become available in the future on auxilliary feedwater reliability?

MR. WERMIEL: We're going to be addressing that, yes.

MR. MICHELSON: Thank you.

MR. DAVIS: Dave, I have a question. I understand, at the Institute for Nuclear Power Operations, they have or are about to complete a rather exhaustive study on auxilliary feedwater reliability.

Their data was not constrained by whether they were LER reportable events or not. Are you aware of the results of that? Can you say anything about what that study has indicated?

MR. DENNIG: Yes, we are aware of that study. I think its publication date was in October. It covers 1981 through 1984, or 1980 through 1984.

As far as sources of information, the one thing that they claim that they did do was, after compiling information from the available sources provided by the licensees for validation and glancing through one of the appendices very quickly, I did not see anything in there that wasn't picked up in an LER or very much beyond what comes out of LER.

So I'm not sure how much to weigh the value of going back to the licensees as opposed to what we know from that mechanism. We probably ought to look at it closer, but I'm not sure we're that bad off.

But, yes, that study has just been issued. It might be beneficial for me to talk with them.

MR. WARD: Is that a public document?

MR. DENNIG: No, it's in limited distribution.

MR. WARD: But you've seen it?

MR. DENNIG: Yes.

MR. WARD: Have you come to any...I mean, there are some sorts of tentative, vague, general conclusions one could reach from what you just told us. From studying the INPO document, would you come to markedly different conclusions?

MR. DENNIG: To be honest, I didn't read it with this discussion in mind. I hate to mislead you by just trying to recall what I saw.

MR. WARD: If you don't know, that's all right.

MR. HERNON: Mr. Ward, Ron Hernon with the Staff. Mr. Michelson, would you please repeat your last question? I'm not sure we understood it.

MR. MICHELSON: You mean the question of the future availability of information?

MR. HERNON: Are you talking about the quality of the LER's that are coming out?

MR. MICHELSON: No, I was merely interested in the quality of the reliability data.

MR. WERMIEL: I understood the question.

MR. WARD: I think his point is here is an extremely important question about the reliability of

plants. One of the most important systems in the plant. And our system of quantifying operating experience doesn't seem to be giving us anything.

MR. HERNON: My perspective is, you know, that the reporting requirements are probably less stringent than they were before the new LER rule as far as the information we're getting. It's certainly important to have the operating history, but I think by the end of the afternoon, it will be apparent to you that our main thrust has been reliability of the system itself as a result of PRA studies, and making sure that gets folded back into what's really happening.

I think I hear that as one of the concerns.

MR. WARD: We're trying to find out what's really happening. I don't care what a PRA tells me or what are the requirements if we don't have something to make sure of what's really happening in the plants. Neither of those two things mean anything.

MR. DENNIG: One thing, auxilliary feedwater, emergency feedwater, is a system within the scope of NPRDS, so all the component problems, component failures, are reportable. NPRDS doesn't have any mechanism for demand information other than guestimates. There is no real time or actual tracking of usage of the system.

But the failure information that used to come in in LER's is covered by NPRDS, which was the way it was supposed to work.

MR. MICHELSON: Have you actually gone into NPRDS during this study to see what kind and quality of information is actually being deposited in the system?

MR. DENNIG: We do that, as you know, but not in connection with this.

MR. MICHELSON: Did you as a part of this work?

MR. DENNIG: No.

MR. MICHELSON: You didn't use NPRDS?

MR. DENNIG: No, I did not.

MR. WARD: That sure seems to be going a long way around in trying to construct. I mean, here, you've got a

nicely defined system, the aux feed system, and trying to construct the performance and reliability of that system from NPRDS component reliability data.

MR. DENNIG: It seems that way, but let me put my last slide up. Somebody else brought up INPO. This gets into something that they're doing, the approach that they're taking.

(Slide.)

System level failures are practically non-existent. They don't go that high. So if you want to come up with some kind of an estimate of the performance of that system, the fallback is, you know, the original reason for doing fault trees, if I don't have any observations high up here, I go down to the lower level. That's the fallback.

And, in fact, I believe the auxilliary feedwater system is one of the systems that INPO has been pitching as part of their performance tracking system, getting each licensee to calculate based on component unavailabilities an estimate of his system unavailability.

But they're taking that tack again because of the lack of system level failure information. You have most of the people sending in nothing and saying, well, we've never failed the system. So they must have a 100 percent system.

MR. WARD: I accept that. That's a good point. One is a small number.

Jessie, excuse me.

MR. EBOERSOLE: I was just going to say I was thinking on this matter of things being engineered safeguards or not. There's a related set of pieces of equipment that make the steam generator work. Of course, that's the PORV's. They're not safety grade either. Neither are their block valves.

One can imagine a situation where there's plenty of secondary water. But you can't maintain pressurization unless in a delta T to take the primary heat out to the secondary. So the system is stalled from a heat pull standpoint.

In this condition, do they report the PORV sticking open and the counterpart block valve failings, since they're not safety grade? There's no tech specs on them.

MR. DENNIG: This is in the primary side?

MR. EBOERSOLE: Primary side. They're not on the secondary side either.

MR. DENNIG: The PORV is covered by NPRDS for what that's worth. In a trip sequence, the PORV opens and hangs up, or opens at all, we would expect that we would be told about that.

That's a significant event as part of that sequence. That's what the requirements require. The

performance in that area detailing the sequence of events post-trip, our experience has not been good.

MR. WARD: Okay. Jerry.

(Slide.)

MR. WERMIEL: My name is Jerry Wemiel. I'm Section Leader in the Plant Electrical Instrumentation and Control Systems Branch of the new PWA Division B of the NRR. That's the B&W and CE division.

MR. WARD: You remembered that one without even writing it down.

(Laughter.)

MR. WERMIEL: I got the e and the i confused. We call it "pieces" incidentally, "the pieces branch".

I've been asked to speak I guess about how the staff reviewed the aux feed system criteria governing the design of an aux feed system has evolved.

It has been an evolutionary thing and where we are today basically with that, as you can see from the first bullet, the criteria initially governing aux feed systems was at best nebulous before the advent of the standard review plan.

MR. EBOERSOLE: What does "good engineering practice" mean?

MR. WERMIEL: What it generally specified, as I understand it, was B-31-1 piping, quality to some extent but

not necessarily Appendix B. An engineered pump rather than something that you would necessarily buy off the shelf.

In other words, something that would do the job it was intended to do but without the intent behind an ESF or a SECY-related system essentially.

When the standard review plan came out in 1975 and the plants were reviewed against that, they had been providing what could be called engineering safety features, ESF, or what I like to call a safety-related system. That is where we reviewed it, specifically identified the need for the system to be seismically qualified, the need for redundancy, the need for tech specs, the need to assure its design capability, things like that. The need for quality, incidentally.

Again, that did not occur until 1975.

MR. WARD: Jerry, safety-related and ESF are not the same thing, I don't believe. Or does that distinction make any difference to you?

MR. WERMIEL: Not in the context of my discussion, no. Safety-related, to me, as defined by NRR, in my recollection, is granded in 10 CFR Part 100. Part 100 again, at least initially, was geared around the large LOCA. Since that time, I think we have expanded our thinking on what is safety-related and, for that reason, have expanded its definition to include things like aux

DAV/bc

feed.

MR. WARD: So you're really going with the definition of aux feed systems as being safety-related.

MR. WERMIEL: I'm trying to make it comparable to what we would classify, say, as a safety injection system or service water, anything required to safely shut the plant down following an accident, or mitigate the consequences of that accident.

MR. EBOERSOLE: How do you distinguish between safety-related and safety grade in a physical context?

MR. WERMIEL: I don't think there's any difference. Safety-related, safety grade are interchangeable words. I don't happen to like the word "safety grade". I like the word "safety-related" more because it's more easily definable in the documentation I've seen.

Safety grade is not as easy to define.

After the TMI-II accident, it became apparent to the staff, and that was in 1979, that additional focus needed to be made on the aux feed system, and what we actually had, what was out there, what it was doing. In other words, what was really existing in the industry at that time.

That task was undertaken by the Bulletins and Orders Task Force. What was done was this task force in a

very short time period, as a matter of fact, put together a deterministic and a probabilistic review of the aux feed systems in those plants that had operating licenses at the time of the TMI-II accident.

The deterministic review was essentially a quick comparison of the systems as defined by those utilities against the standard review plan.

The probabilistic evaluation was a stylized, rather quick fault tree to try to determine what the availability of the aux feed system would be on demand, without a particularly detailed look into support systems, common cause, or things like that.

MR. EBOERSOLE: As I recall, there were 10 of them that had to be nonseismically competent. Is that correct?

MR. WERMIEL: I think there were more than that. I'm going to get to the seismic aspect; that's on the last page. But I believe there were more than that. Certainly, seismic was a problem.

The main focus, incidentally, of the probabilistic review was not to come up with an industrywide, numerical unavailability or goal, say, for the system. It was primarily to identify the major contributors to unavailability and to develop a range of availability of systems for comparison purposes -- how does this

DAV/bc

Westinghouse plant compare to this one? Why is there a difference? What are the major vulnerabilities? What can we do about something like that?

The results of those efforts were published in NUREG's 06-11 and 06-35 for the Westinghouse and Combustion Engineering plants respectively.

At this time, the B&W plants were being treated differently. They were under shutdown orders. A different set of people had reviewed the aux feed systems of those plants prior to the shutdown orders being lifted. And, subsequent to that, the staff asked for reliability studies, numerical studies of those systems, and received it in the form of a topical report from B&W, No. B&W 15-84. That study was reviewed by the staff.

MR. WARD: Jerry, it was reviewed. Was there an SER issued?

MR. WERMIEL: There was a document developed for internal use. It was never published for external use like the NUREG's were on the Westinghouse and C.E. plants. It was used in the course of subsequent reviews under II.E.1.1. and II.E.1.2.

MR. WARD: But is there an implication that the staff accepted the B&W study?

MR. WERMIEL: We argued, as a matter of fact, with the utilities during the II.E.1.1 reviews about the

numbers, and the results of those studies as they were presented. So, no, there was not a tacit acceptance.

MR. EBOERSOLE: The last bullet says there was.

MR. WERMIEL: Let me get to what that bullet is saying. All plants were reviewed against II.E.1.1 and II.E.1.2 and trying to be acceptable. The II.E.1.1 and II.E.1.2 specified a deterministic criteria only; there was never any review done under those TMI items. The need to comply with an unavailability goal.

MR. EBOERSOLE: May I ask a question at this time about the standard review plan? Would it be available to the decay heat removal system, like Salem's and aux feedwater like Davis-Besse?

MR. WERMIEL: Yes.

MR. EBOERSOLE: There seems to be a reluctance on the part of the staff, I would presume, on the grounds of its being too proscriptive to mandate diversity. Is this true?

MR. WERMIEL: Diversity of aux feed.

MR. EBOERSOLE: Or reactor shutdown.

MR. WERMIEL: As in the standard review plan.

MR. EBOERSOLE: How did Davis-Besse escape having it?

MR. WERMIEL: Davis-Besse was not reviewed against the standard review plan. They received their

license prior to that review.

MR. EBOERSOLE: I'm talking about in the backview, which you took here.

MR. WERMIEL: There was internal staff concern about diversity at Davis-Besse and, as a matter of fact, prior to their event, there was a license condition on them to backfit a motor-driven pump.

MR. EBOERSOLE: When?

MR. WERMIEL: I believe it was in January of that year the license condition went in. So the staff had already recognized a deficiency, shall we say, in Davis-Besse.

MR. EBOERSOLE: Is there a comparable one at Turkey Point today?

MR. WERMIEL: Turkey Point has a motor-driven pump in each of its two units. In addition, Turkey Point has committed to tech spec that motor-driven pump. So the staff is very pleased with the upgrades Turkey Point has made and their volunteering that tech spec.

MR. RUBINSTEIN: Les Rubinstein of the Staff.

You're touching on a subtlety in the staff's review which NUREG 07-37 recommended guidelines. And when Jerry said in response to your question on B&W plants did the staff accept them, yes, they did but with the full knowledge that we would have in preparation in future time

DAV/bc

additional requirements which dealt with some of those kinds of points, and would go through the process. And, for example, in terms of power diversity, there were a number of CRGR packages.

MR. EBOERSOLE: This is apart from any PRA requirements? It's just deterministic?

MR. WERMIEL: That's correct, Jessie. Let me point out that we indicated to a number of plants after completion of the review on the II.E.1.1 and II.E.1.2 that we may be coming back to them because we held additional concerns in various areas. And although, at that point, the ball so to speak was dropped, staff continued its effort to get to that point.

And I'm getting to that on the next slide.

MR. EBOERSOLE: Are you going to pay particular attention to the aux feed system at Paloverde in particular? You know, it's the one real issue.

MR. WERMIEL: We paid attention to the aux feed system at Paloverde.

(Slide.)

To answer the question about seismic qualification, it was recognized that many plants, many of the older plants did not have seismically qualified aux feedwater systems, as the standard review plan would define them.

Generic letter 81-14 was issued to ask those plants to upgrade their system to withstand, functionally withstand an SSE, and all those plants had been reviewed, with the single exception that we still have Oconee under consideration.

Getting to your point about Paloverde, Paloverde and plants of that vintage are what we would call the latest standard review plan plants. They're required, or they must have satisfied the criteria of Section 10.4.9 for AFW unavailability. That's 10 to the minus 4, 10 to the minus 5 criteria.

We asked that those plants perform a reliability study. They have all done that. We asked that they utilize an approach comparable to that in 0611 and 0635 so we could again make the comparison that we were anxious to make, and understand where they ranked.

There were 12 of these plants total. By "plants", I'm speaking in some cases of multiple units. And I provided a listing of those in the back which, based on our review of their reliability studies, have shown or have demonstrated compliance with the reliability goal. And that list is this one here.

(Slide.)

MR. EBERSOLE: I gather then that all other plants have not satisfied the SEW?

MR. WERMIEL: That is the logical question, but that is not the case. If you go to 611 and 635, despite their old date, you will note a number of plants in there that satisfy the goal.

It is also our judgment that based on the upgrades in many of these plants, additional operating plants have satisfied the reliability goals.

However, there is a list of 11 plants that the staff had under consideration for additional upgrade.

MR. EBERSOLE: Do you have that list?

MR. WERMIEL: Yes, I do. I didn't make a slide of it, but I can give you that list.

MR. MICHELSON: Before you leave the present list, as I recall, Bob Dennig cited Callaway as the one with 21 failures on his slide. Admittedly, it was the startup period.

MR. DENNIG: Those were challenges.

MR. WARD: That doesn't have anything to do with this.

MR. WERMIEL: Those were challenges to the system, and also remember that Callaway in 1984, which the data represented, was in startup.

MR. MICHELSON: Okay, those were just the challenges to the system. I stand corrected.

Thank you.

MR. WERMIEL: The 11 plants at the time we finished the II.E.1.1 and II.E.1.2 reviews where we had additional concerns are the following:

Arkansas Nuclear One Units 1 and 2; Crystal River; Rancho Seco; Fort Calhoun; Prairie Island 1 and 2; Maine Yankee; San Onofre 1; Davis-Besse; Haddam Neck; and Turkey Point 3 and 4.

The first six plants -- let's start with the latter five. Maine Yankee, San Onofre 1, Davis-Besse, Haddam Neck, Turkey Point 3 and 4 have fairly recently committed to upgrades or are going to be asked through arm waving or actual arm twisting to make the necessary upgrades to, we believe, satisfy us that they would meet the goal of 10 to the minus 3.

The first six, Arkansas Nuclear One Units 1 and 2, Crystal River, Rancho Seco, and Fort Calhoun and Prairie Island 1 and 2, we still have concerns about. We recently met with all these utilities and asked them to address aux feed reliability, asked them to address feedwater challenges and generally bring us up to date on what the conditions were in those plants.

We got a good understanding of where we stand

with them, and as was already alluded to, we have under consideration the need for additional action through the CRGR.

MR. EBERSOLE: Does that mean they will get the PRA treatment, or will it just be deterministic?

MR. WERMIEL: We don't know. At least I don't know.

(Slide.)

MR. EBERSOLE: Does the CRGR operate without PRAs to a great extent -- or to what extent?

MR. WERMIEL: My only experience with CRGR has been fairly limited, and every time I have dealt with them they have relied on cost/benefit, which to a large extent relies on probabilistic risk assessment.

MR. WARD: Jerry, could I ask you a couple before you go on?

In the first item up there, does your view of the three standard review plants against the seismic criteria -- were those plants, with the exception of Oconee, I guess, which is still under review -- they were all found acceptable? Was this before any backfits or were just the systems as there found acceptable?

MR. WERMIEL: No. In quite a number of cases backfits were necessary. In other cases, additional analyses were needed to confirm seismic resistance of

certain structures and components. But backfits did go into place in a number of plants, with additional constraints in some cases.

As a matter of fact, some plants have committed to additional tanks, seismically qualified kinds of storage tanks, some additional valves in a number of plants or replacement of valves, valves that were not qualified with valves that were.

So there were backfits.

MR. WARD: Okay.

Then a related question, I think. If something is safety grade that has to be seismically resistant, then also the other big requirement is that the system should be single failure resistant. You haven't said anything specific about that.

Were all these older plants found already to be single failure resistant, or what is the story on those?

MR. WERMIEL: What 81-14 specified -- I guess I should have gone into that. I didn't realize there would be so much interest in that -- 81-14 asked that the plants demonstrate capability to safely shut the plant down with the aux feed system following an SSE or with some other qualified, acceptable alternative decay heat removal system.

In so doing, it asked that they would meet the

DAVbur

requirements of GDC-2 and GDC-34.

GDC-34 specifies that you be able to withstand a single failure.

So the review under 81-14 confirmed the capability to shut down with aux feed following an SSE and a concurrent single act of failure.

MR. EBERSOLE: Since these older plants were built, with even a minimum of records for the safety grade systems in the context of construction, weld records, et cetera, what did you do with the difficult problem of finding the history of fabrication and assembly and installation of all these nonsafety grade systems? What recipe did you use, and why is it not applicable to other plants that don't have records?

MR. WERMIEL: We asked where the recipe, as you call it, or whether the qualification documentation wasn't suitable, we asked for additional analysis, new analysis, seismic analysis of the system.

MR. EBERSOLE: What did you do, for instance, about the quality of welds, the records of the welders, et cetera, et cetera, since they were presumably nonexistent?

MR. WERMIEL: I don't recall the specifics of things like welder qualification.

MR. EBERSOLE: Why don't we find out what recipe you did you to qualify these -- I should presume -- poor

DAVbur

systems with poor records of fabrication and installation and find out what the difference in rationale was in qualifying those plants versus qualifying some new plants that don't have records today?

You know, that is one of the flaps we always have.

MR. WERMIEL: You are talking about the QA flap?

MR. EBERSOLE: How do you escape the QA flap? What is the cookbook you used?

Because it might be useful if it is good.

MR. WERMIEL: Again speaking from what I know, I recall in a number of cases where reanalysis of the piping configuration was necessary, but I don't know how that relates to the welds within the system.

MR. EBERSOLE: Or the metallurgy?

MR. WARD: Are those systems now on operational Q lists? Are they all treated as Q list items as far as tech specs?

MR. WERMIEL: All the systems are tech spec now. All aux feed systems have tech specs that are fairly consistent now.

One of the major items of II.E.1.1 was to get comparable tech specs from plant to plant.

As far as Q listing for the system, I am just not familiar with that.

DAVbur

MR. MICHELSON: Does your reply then mean that they now control the quality during modification, maintenance, et cetera? Are these auxiliary feedwater systems controlled just like systems that are classified as engineered safety features?

MR. WERMIEL: I would assume so, but I honestly don't know. I am not that familiar with the modification.

MR. MICHELSON: Covering by tech specs doesn't necessarily control, prolong the quality or make sure the quality is protected as the quality might be.

MR. WERMIEL: No, but there is a disadvantage to the operation of the plant if you are not controlling quality, in that if the system happens to be unavailable too frequently you may enter the action statement and force yourself to shut down.

So there is an inherent need, I would think, from the operational staff of the plant to want to do quality work and control that.

MR. WARD: But I am not sure --

MR. WERMIEL: To make that analogy, though, because it is a tech spec system it is on the Q list, which is what I think you are trying to drive at, Mr. Ward, I don't believe you can make that direct comparison.

DR. CATTON: But you could set the tech spec so loosely that it really doesn't matter.

MR. WERMIEL: The tech specs are not loose on aux feed in that respect. The operability of the system is governed pretty stringently.

DR. CATTON: Is there a criterion for the tech specs?

MR. WERMIEL: Yes. Generic No. 83-7 went out which provided generic guidance on what we want in the way of tech specs on these plants. My recollection is that that review has been completed on all the plants. We have very comparable tech specs now, even in the oldest plants.

MR. WARD: Okay. See, what we are trying to find out -- you said these older plants have been reviewed, you have sort of tried to backfit the safety grade requirements of the older plants, and let's say there is three main parts, and let's say you require seismic resistance -- you told us about that -- and single failure resistance -- you told us about that.

The third part is the QA. Mr. Ebersole pointed out that it is hard to backfit the original QA construction requirements. There is some question about that. But there are ongoing in-service inspection requirements --

MR. WERMIEL: Yes.

MR. WARD: -- for Q'd systems.

MR. WERMIEL: You raised a point. Section 11 does govern, I guess, ISI and IST for the aux feed system.

It is included.

The staff has -- although I am not specifically familiar with the details of it, the staff has under review the Section 11 ISI, IST programs, for all these programs. What is specifically included in those programs I don't know, but the aux feed system is covered by those programs.

MR. WARD: Could we find out? I can understand why you might not have the answer right off the top of your head, but could we get an answer to the question of whether these aux feed systems in the older plants are now treated as safety grade systems from the standpoint of operation and QA?

MR. WERMIEL: There are probably people within the staff who could answer that question. I am just not equipped to.

MR. WARD: Maybe we can get that answer in the future.

MR. HERNON: We will get that answer for you.

MR. WARD: Thank you.

MR. MICHELSON: Did you look into the environmental qualification of the equipment associated with auxiliary feedwater, and what did you conclude?

MR. WERMIEL: Aux feed systems were covered under 50-49. It was not part of this review. That was done by a different group of people. But in those cases where the

DAVbur

aux feed system was exposed to a harsh environment, the system was either qualified --

MR. MICHELSON: I am trying to struggle for a moment with this concept of being so-called nonsafety grade or non-ESF, or whatever you call it. I am struggling now how the environmental qualification people dealt with this issue. If it is non-ESF, it probably doesn't have to be environmentally qualified. So they could kind of ignore it.

But did somebody tell them you can't ignore auxliary feedwater even if it may not be called safety grade or safety related or something?

MR. WERMIEL: They were told that, yes.

MR. MICHELSON: And they reviewed it as though it did have to perform an important safety function, and they somehow fortuitously, even though these systems weren't ever designed to be safety grade, they turned out to be environmentally qualified.

Is that the case?

MR. WERMIEL: I don't know the answer. It only needs to be qualified to a harsh environment if it is exposed to it.

MR. MICHELSON: It is a pretty good opportunity for that harsh environment if the auxiliary feedwater steam line breaks, for instance, and gets both the electrical,

which is often located in the same room with the steam.

MR. WERMIEL: You have to remember the criteria governing breaks in that steam line. It is not normally pressurized.

MR. MICHELSON: It depends on the utility whether it is normally pressurized or not.

MR. WERMIEL: That is correct, and if it is and it breaks and it exposes all the system to a harsh environment, my understanding is that it is qualified.

MR. MICHELSON: I am not so much worried about that as of course also exposing other equipment. But it was found that it was qualified, and I am not sure what you meant by -- now by this harsh environment part.

You mean it was found to be qualified for harsh environments?

MR. WERMIEL: It may have been, or it may have been that they had to make a modification to qualify it.

MR. MICHELSON: But they are all now qualified for harsh environments; is that what you are saying?

MR. WERMIEL: No, I am not saying that. I am saying my understanding of the 50-49 rule would have said if the aux feed system is exposed to a harsh environment it is necessary to shut the plant down to mitigate that harsh environment, and then it is either qualified or shown not to be necessary.

DAVbur

MR. MICHELSON: So they have either shown that they don't need it anyway in the situation or it has been qualified, whether or not it was considered safety related to begin with?

MR. WERMIEL: That is correct.

MR. MICHELSON: Thank you.

MR. EBERSOLE: There is a subtlety in this business. Qualification of some of this electrical apparatus has been claimed on the basis of saturating it in a steam environment but having it initially warm so that surface condensation does not take place on electrical contact. Thus, short-circuiting to ground doesn't occur. There are some neat escape routes if you get that warmed up first.

Do you happen to know how rigorous and how thoroughly this was done if you were to bathe all this equipment in a Turkish bath?

MR. WERMIEL: I am not, no. I assume our equipment qualification people could address something like that. I am not equipped to answer that.

MR. EBERSOLE: I am dismayed to find a lot of completely open equipment like you have in any factory subjected to this hypothetical Turkish bath.

MR. DAVIS: I have a quick question. Do you get in on the changes if a utility makes a modification

DAVbur

to its aux feed system which was a voluntary change, which may or may not be related to safety?

MR. WERMIEL: Not necessarily. You can make changes to anything in the plant by 50-59, and not have to notify NRR. 50-59 allows modifications at any time, provided certain criteria are satisfied. And then I believe those are collected and notification to the region is made.

MR. DAVIS: That concerns me a little bit. I know of a case where a plant increased its trip level to improve its reliability but made it operate outside its design basis.

I wonder if this kind of thing gets picked up.

MR. WERMIEL: If that trip level is something incorporated into the technical specifications, the change cannot be made. Then NRR would be involved in the review of it.

One of the criteria for 50-59 indicates that the change could not affect the license or tech specs.

MR. DAVIS: In this particular case it was an overspeed trip on the diesel driven pump, which I don't think would be in the tech spec.

MR. WERMIEL: I think you are probably right. I think a change like that can be made under 50-59.

MR. WARD: Thanks, Jerry.

Why don't we take a short break. Let's take a 10-minute break at this time.

(Recess.)

MR. WARD: Our next speaker is Mr. Frahm.

(Slide.)

MR. FRAHM: I'm Ron Frahm, from the Division of Safety. I'm Section Leader in the Reliability and Risk Assessment Branch, which is now changed in a new organization into a Section Leader in Safety Program and Evaluation Branch, the Division of Safety and Review Oversight.

MR. WARD: That's your old title.

MR. FRAHM: That's my old title. I was handed this assignment before we reorganized.

(Slide.)

Then what is on the agenda. To quantify these trees we used the data as specified in 0611 and 0636, and the Staff, assisted by Brookhaven National Laboratories and Sandia National Laboratories reviewed about 17 plants and provided our results to Jerry Wermeil and his group. The auxiliary feedwater system, as analyzed in this document, includes the hardware from the water source to the nozzle on the steam generator, and the analysis did not include high energy line break or external events.

The review by the Staff generally identified the dominant contributors for each initiator. Basically, these were maintenance, hardward failures of pumps, valves, involvements with the actuation logic. We pointed out the single and/or common mode failures.

I might point out that the 611 results are point estimates and have very large uncertainty bounds and that the staff review discussed improvements that could be made to increase the availability and relilability of the auxiliary feedwater system.

(Slide.)

The Staff reviewed, I think, around 17 LWRs. There were two train systems, such as ANO 1, Crystal River, Davis-Besse and also three train auxiliary feedwater systems, such as Catawba, Seabrook, Midland, Waterford. The two-train unavailability was generally in the range for loss of main feedwater of about 10 to the 3, 10 to the minus 4. Similar for the loss of offsite power. The loss of AC was about 10 to the minus 1 to 10 to the minus 2. We found in the three-train system, loss of main feedwater availability was 10 to the minus 4 to 10 to the minus 5. The loss of offsite power was 10 to the minus 4 to 10 to the minus 5 again.

The loss of AC was about 10 to the minus 1, 10 to the minus 2.

MR. MICHELSON: Is there some historical reason why the B&W reactors had the two-train auxiliary feedwater? Is there some rationale, something unique about them?

MR. WERMIEL: This is Jerry Wermiel again, with the Staff.

We were not able to identify anything, historically or otherwise that would indicate that. Westinghouse, we were able to identify, had an interface among its utility users to specify, generally, that they provide three pumps, but again, that's just an interface, and just a general criteria in there, because you will find, prior to the TMI accidents, there were Westinghouse plants with just two pumps. Even today, there is still a Westinghouse plant with two pumps. So that plant does satisfy the reliability criteria.

MR. MICHELSON: It says it's two-train. Is it necessarily one electric, one steam, or sometimes two electrics, or a mixed bag of two steams, or what? It could be anything.

MR. WERMIEL: It's always diversity. The only plants that just have steam-driven plants until recently were Turkey Point and Davis-Besse. All plants have diversity now. Electric and steam. In some case, they're electric and direct diesel.

MR. MICHELSON: On the slide, the two-train

system included Davis-Besse. They were older vintage, I assume. So this was a mixed bag of electric and steam, without any clear rationale.

MR. THADANI: That is correct. Davis-Besse was one of the plants looked at that did not have diverstiy.

MR. MICHELSON: Are these all being fixed now? Are there still two-train systems that haven't been agreed to?

MR. WERMIEL: Yes, there are. That list that I read off during my presentation were basically two-train plants.

MR. RUBINSTEIN: However, all have in place power diversity, all plants.

MR. MICHELSON: What does that mean -- one steam, one electric?

MR. RUBINSTEIN: Yes.

MR. MICHELSON: Crystal River, was it two electric?

MR. WERMIEL: No. Crystal River has a turbine and a motor.

MR. MICHELSON: It was always that way?

MR. WERMIEL: Yes. You can go back far enough in any of these plants and find cases where they may have had a different configuration than the subsequent years added pumps.

MR. DAVIS: Just to help me a little bit, Ron, when you say three train, does that, by definition mean any single train can provide sufficient capacity for decay heat removal?

MR. FRAHM: Yes.

MR. DAVIS: Some of these three-train systems are called 50 percent capacity on the motor-driven pumps, but actually, they have enough --

MR. FRAHM: Right. The first thing you said. 100 percent.

MR. WARD: Ron, would you go back to the previous slide. I need a little more explanation of what the numbers are. That's the unavailability of the aux feed system. Given each of those initiating events?

MR. FRAHM: Right. The probability of failure on demand, given that event.

MR. WARD: How do you explain why it's different for different events?

MR. FRAHM: Well, okay. You can have a loss of main feedwater, for instance. You still have your on-site AC. So generally, you would have your electric-driven pumps and your steam-driven pumps. You have a loss of off-site power. Now you're going to have your failures in your system, plus you're going to be relying on a diesel generator.

MR. WARD: Or the steam.

MR. FRAHM: Or the steam-driven. In a loss of all AC, you have failures above, plus you have your hardware failures inm your turbine-driven system.

MR. WARD: Do assumptions about recovering come into these numbers?

MR. FRAHM: Yes. These have recovery factors; yes.

MR. WARD: Those are dependent on the details of the scenario, supposedly.

MR. FRAHM: They're dependent on the details of the scenario; they're dependent on how much time is available to recover before dry out.

MR. WARD: Are they dependent on any information for the specific plan about the operator training and procedures in place at that plant or the design of the control rooms at those plants?

MR. FRAHM: In the PRA, would be on the 611 review. I would say they didn't go in and look at all the procedures. It's more generic. I would say that the recovery factors, if you will, were more under oriented, not specific plant oriented.

MR. DAVIS: Ron, one issue that's come up in the past is whether or not these systems can be controlled on loss of DC power as well as loss of AC.

Is that considered in this evaluation, or that it considers what to do of all electrical power systems failed?

We've heard some utilities claim they could control the system on loss of DC. I don't think some agree with that.

MR. FRAHM: Only the turbine-driven should be controlled with DC and have no AC dependency.

MR. DAVIS: I understand that, but your battery life is maybe two to four hours, maybe six hours. When do you assume the system fails?

MR. FRAHM: I would think you'd lose control; yes.

MR. DAVIS: There've been some claims that they can be controlled manually.

MR. THADANI: Peter, generally most of the studies assume the system fails, although, as you point out, there is some potential for recovery through manual actions. That typically is not considered in the PRAs. A lot of the plants recently have indicated that the available time is way beyond the two to four hours that you mentioned.

MR. MICHELSON: What available time?

MR. THADANI: Time before batteries are depleted sufficiently that you cannot perform certain key functions.

MR. MICHELSON: There may be other parameters

catching up with you long before the batteries, though.

MR. THADANI: I agree. The room temperature, for example, could be critical.

MR. EBERSOLE: I believe Beaver Valley claimed no DC need, although I don't know what they did for instrumentaiton to determine what they were doing, flying blind.

MR. THADANI: These analyses do not include consideration of loss of DC. There are a lot of limitations to these analyses, and they will be discussed later on.

MR. EBERSOLE: These numbers here. Is it possible to crudely translate them into the lower probability core melt accident, due to this cause?

MR. FRAHM: Yes, you could. If losing feedwater leads to the core melt, then you could take initiator frequency and multiple it.

MR. EBERSOLE: I know, but it doesn't always.

MR. FRAHM: You have recovery. You have feed and bleed. You have low pressure systems.

MR. EBERSOLE: So there's much more probability that these will result in core melt, not much lower. I don't know where it is. Is it a factor of 10 or 100?

MR. THADANI: Mr. Ebersole, recently we looked at, I think it was 10 plants. They ranged, in terms of their core melt frequency, from somewhere around 10 to the

minus 3 to well below 10 to the minus 4, and I think 10 to the minus 5.

Typically, plants in the range of 10 to the minus 3 or 10 to the minus 4 core melt frequency, were those where the aux feed availability was in the low range, which is around 10 to the minus 3 or even somewhat worse, in that they have no feed and bleed capability, or they have questionable feed and bleed capability.

The analyses they would assume, no feed and bleed capability.

If I recall, 10 plants were looked at. Davis-Besse turned out to be the worst one in the analyses.

MR. EBERSOLE: Is this considered to be one of the major contributors to core melt in a PWR?

MR. THADANI: Typically, if you look at plant-specific PRAs, this sequence was, I think, about a 10 percent contributor. It is lower than most of the PRAs, because certainly no credit was given for feed and bleed. Whereas most of the recent PRAs assumed feed and bleed, because of the training, and so on.

MR. EBERSOLE: Right. When they give credit for feed and bleed, do they acknowledge the fact that the bleed mechanism is degenerative and that the PORVs are not environmentally qualified for the environment they create in the containment. That is, they die in a closed position.

MR. THADANI: PORVs -- environmental effects resulting in closure of the PORV, I don't think is treated. I'm not really quite sure right now that that is the situation. That may be the case. Typically, the fault trees that people have done indicate about 1 percent chance that the PORV will not open on demand.

MR. EBERSOLE: If it does open, it creates that environment that hypothetically kills it later and then closes it.

MR. THADANI: I guess I'm not aware of the conditions that would cause that.

MR. EBERSOLE: Oh, well. The surge tank is blown. Discharge takes place in the containment, and the open secondaries and nonqualified character of the PORV causes it to die.

MR. THADANI: That's the part I'm not sure about.

MR. FRAHM: The surge tank decides to take a certain amount of openings and closings. I think what you're saying is, the structures, then, I would tend to agree with you, about what you're saying.

MR. WARD: The surge tank is not capable of removing decay heat.

MR. FRAHM: No, but it keeps it contained.

MR. WARD: Not if you're in a real feed and

bleed mode.

MR. EBERSOLE: It has to go. It just blows. The diaphram blows.

MR. THADANI: That's designed for only 100 pounds. I'll blow pretty fast.

MR. WARD: You're saying that you don't know whether you agree with Jesse, but that at any rate, apparently the PRAs that are done assume what Jesse says will happen or won't happen.

MR. THADANI: That is correct. At least that's my understanding. And whether that's based on looking at specific information or not, I don't know.

MR. EBERSOLE: Mr. Thadani, how can they legitimately do that? TMI used secondaries to get the heat out.

MR. THADANI: I think, Jesse, there is a fair amount of experience. I can't give you the definitive response to that, but I think, unfortunately, we've had a number of instances where the environment in containment has certainly been pretty -- the temperature is hot and people have been able to keep the PORV alive.

MR. EBERSOLE: It's got some margin, I guess. The question is, how much.

MR. THADANI: A PRA is nothing more than trying to make judgments. Solid information is not necessarily

available on every piece. There's a lot of subjectivity that goes into these analyses. One has to be careful. Look at results. If you have questions, push, that you can see the common cause failures.

It's like any other analysis. It has its limitations.

MR. DAVIS: Jesse, it's my impression in the couple of plants I have looked at that the quench tank is located a long way from the PORV.

MR. EBERSOLE: It's at the bottom of the building; isn' tit?

MR. DAVIS: Yes, and it's a tortuous path for the steam to get back to the PORV.

MR. EBERSOLE: But it's in the nature path and going up to where it is.

MR. DAVIS: All I'm saying is, it's going to take a while before the PORV sees any adverse environment.

DR. CATTON: Sometimes it's a closed room too. If you haven't got any open doorways.

MR. EBERSOLE: It could be; yes.

(Slide.)

MR. FRAHM: The next item is to compare studies with the precursor study. And what the precursor study did was to review LERs to identify and categorize the precursors to potential core damage accidents. The process was, they

DAVbw

looked at the LERs. They reviewed the accident sequence. They reviewed the system design and the plant accident analysis to determine which systems are required to function for this precursor.

And I believe in the study they reviewed about 8000 LERs in going through this screening criteria. They looked at about 400. They looked at the system design, and then they decided about 60 of them were actual precursors to core melt.

The way the process ensued was, you estimated the average frequency and the failure probability for initiating events and function failures. Then the initiating frequency and function failure estimates were used in conjunction with standard event trees to estimate the conditional core damage probability.

This conditional probability gave you a benchmark, so you could rank the precursor. You could identify the number of it at the dominant sequences. You could rank the safety functions, and you could estimate the industry average core melt frequency.

(Slide.)

The results of the study showed that coupling failures are still being observed after the first. There were two studies, one from '69 to '79 and one from '80 to '81. And these coupling failures were primarily caused by

electrical faults.

In the 1980 to '81 time frame, the number of PWR initiating events and function failures was less than in the '69 to '79 precursor study.

This was probably due to a multitude of reasons, one of them that they considered recovery such as feed and bleed. They removed the strainers from the suctions. They found you could manually operate the system even though you didn't auto-initiate.

From the study, it was found that the PWR's would give additional risk reduction from feed and bleed. And on BWR's, it was for long-term cooling. The dominant --

MR. WARD: I don't understand what you mean by that, "additional risk reduction for BWR's in long-term cooling".

MR. FRAHN: What's a good way to say it? The events on BWR's are basically transients. For core belt scenarios, they are transients with the long-term cooling function failed. On PWR's associated with auxilliary feedwater failures that contribute to risk, you can take credit for feed and bleed. You reduce that risk. That's basically it.

The dominant sequences on the PWR's that the study showed were the small LOCA with the recirculation failure. DC bus failure with no restoration. And auxilliary feedwater failure and a loss of feedwater and no feed and bleed capability.

On a BWR, you had transients. Most transients on BWR's end up loss of feedwater and you fail long-term core

DAV/bc

cooling such as suppression pool cooling, loss of feedwater with the high pressure core injection and RC/IC, which is what you were trying to say in the presentation before, was the auxilliary feedwater on the boil and loss of feedwater with the scram and standby liquid control system.

The study showed that the unavailability was approximately 10 to the minus 3. And that if you look at the events for the auxilliary feedwater, you find that most of them are recoverable.

MR. WARD: What does the 10 to the minus 3 mean?

MR. FRAHN: That's the unavailability.

MR. WARD: Is that crediting recovery or before recovery?

MR. THADANI: That is before recovery. If you look at the data, there were X-number of failures and Y-challenges. That's where 10 to the minus 3 comes from. And when you look at the data further, you realize that a number of those failures corrective action could have been taken and was taken in fact in some cases.

That would be the recovery factor one would fold in. INPO qualified that, qualified that in that their average came out 2 times 10 to the minus 4. There would have been individual failures that have occurred and concluded, I think, that with the exceptions of one or two failures that there was a likelihood of successful recovery.

DAV/bc

I estimate that if we had done it the way INPO did, we probably would have been on the safe borders. What we did instead was we looked at individual values separately.

MR. EBOERSOLE: So you pick up about a factor of 10.

MR. THADANI: I think it varies. If you look at historical data, you probably get a factor of about 5 to 10, but if you look at PRA's, they'll tell you a factor of 2 to 10, in some cases, more. But, generally, a factor of 2 to 10.

Typically, you find for B&W designs, you get less of a recovery factor than you do for other designs. But it's in that range, I think.

MR. EBOERSOLE: Now, consistent with the demand frequency, what does that come out in the way of --

MR. FRAHN: Core melts?

MR. EBOERSOLE: Yes.

MR. FRAHN: I would estimate the '80 to '81 timeframe. It would have been 2 times 10 to the minus 4; for the '69 to '79, it would have been about 2 times 10 to the minus 3.

MR. THADANI: Those estimates, I think, let's be very careful. What Ron is telling you is the '69 to '79 overall core melt frequency in the precurser study, that

does not relate to this scenario only. In the precurser study, a number of other events occurred, as you know, in the '69-'79 period.

If you look at this issue with the recovery, I would expect it would be certainly substantially below 10 to the minus 4, and may in fact be below 10 to the minus 5.

MR. WARD: Now, if I go back and take it face value, the data that Mr. Dennig presented earlier this afternoon, those numbers from 1984 are substantially different. That would indicate unavailabilities much higher than 10 to the minus 4. How do you explain that?

MR. FRAHN: I don't think so. I think the number of demands that we had in the time period, I would say about 6,000, is probably about the same thing that Mr. Dennig had for his year, his 1984 year. I think it's the same.

MR. WARD: No, he showed one failure in about 130 demands.

MR. FRAHN: And we're showing maybe six failures in 5,000 demands.

MR. MICHELSON: Where do you get your numbers for demand, as 5,000 or 6,000 or whatever?

MR. THADANI: I think that, typically, in these reliability studies, an assumption is made in terms of monthly testing. There's another assumption made that the tests are perfect, that if you have a fault, that's

identified, that fault.

Another assumption in these studies, if that were in fact the case, certainly these symptoms are tested on a mnothly basis -- I think they are. And you have real challenges and you have tests. And if you pool that data and look at the experience.

And we haven't done that for '84. This is the first I've heard of '84 experience. We're sort of behind time, I guess. I'm not convinced that you come up with significantly different estimates.

MR. WARD: We just saw some numbers. We saw 130 demands and one failure.

MR. THADANI: But, as I pointed out, the real demands, the number may be much larger than 130.

MR. WARD: If you include testing. But let's say I want to throw out testing, I don't really care.

MR. THADANI: Let's make another assumption. Sure, if you tell me, then, obviously, I could say my tests do nothing for me. That's possible. Then you would be correct. One failure, 130 demands would be absolutely correct.

What I'm saying, what's done in these calculations, credit is given for testing. It is assumed the tests will detect faults.

MR. WARD: Once you get a body of operating

experience that's sufficiently large, it seems to me that that's what you ought to use in the PRA rather than testing. It's certainly preferable. It's certainly more applicable.

MR. THADANI: If the precurser experience, '69 through '79, had been significantly different from what it was, I would completely agree with what you say. It would have certainly raised our consciousness, I would say, if they would come in with 10 to the minus 1 to 10 to the minus 2. We would have known there must be something seriously wrong with what we were doing.

MR. WARD: I guess what I'm saying is that maybe we ought to be alarmed by the 1984 data.

MR. DAVIS: It's hard to draw any statistical significance with one failure out of 130. I wouldn't be alarmed with that data just by itself. You know, if you had 1,000 tests and 10 failures, then you start to get statistically significant numbers.

Is the only failure we're talking about the Trojan one? Which wasn't really a failure because they had the third train to operate it. And, in fact, that train is now in operation and has been for some years.

So you really can't call that a failure. And, in fact, I wouldn't.

MR. EDISON: Dave, I'm told in the Trojan case

DAV/bc

that even the trains that were not immediately available were made available before steam generator dryout. So the operator action was there.

In fact, I'm not aware -- I can't really think -- of all the events I've ever looked at in the PRA data so far, I can't think of a case where an entire aux feed system failed and the operators couldn't get it back in time.

MR. WARD: It's a good thing because you ought to have it at least once in 10,000 years.

MR. EDISON: In every case I can think of where the whole system went down, the operators were able to get it back. And I kind of think that the credit taken for operator actions is probably understated. I think the operators, there's a much higher probability that they will recover an auxilliary feedwater system.

MR. WARD: They sure did at Davis-Besse.

MR. EDISON: That's right, and they had a very difficult situation to work with.

MR. THADANI: I think, while Gordon may well be correct on that point, I think we ought to point out that this 1 in 10,000, it really can't be a hard estimate. Just keep in mind the number of things that are not considered in the analyses from the point of the large uncertainties just in the data base. External events, fires, floods are not included in the analysis.

We have not been able to do a good job of qualifying common cause failures. We may be underestimating the unreliability of the system.

Gordon is correct that the recovery factors in fact may be larger. But it was for that purpose that we're always talking in terms of ranges. We think we're somewhere near, but not necessarily 1 in 10,000. It's important to me that we do keep that in mind. We're not really convinced that a system comes through with an analysis done for these techniques with the data base we suggest. But, in fact, that is where that system is.

The real issue was to identify vulnerabilities through this approach. If you recall the review process, there's two elements in it -- the so-called deterministic review process, and then there's the reliability assessment.

The two together, I think, ought to give people some confidence on this experience.

MR. MICHELSON: A little earlier, you talked about 6,000 demands. How did you arrive at 6,00 demands? I assume, per year on auxilliary feedwater. You included all the tests, admittedly. How do you arrive at 6,000? Or, did I misunderstand what you said?

MR. WARD: That was in 10 years.

MR. MICHELSON: Oh, that was over 10 years.

MR. FRAHN: It was a 10-year period.

MR. MICHELSON: It's still a rather large number, but a little more imaginable. Okay, that was for the 10 years. Is that correct?

MR. FRAHN: Actually, it was '69 to '81 and includes tests --

MR. MICHELSON: Over that entire period of time there were 6,000 demands. Okay.

That's a little more realistic.

MR. THADANI: If you just look at the '84 experience, 130 plus I would say about another 500 or so to test. It can't be much above a thousand. That probably would be the maximum.

MR. MICHELSON: Yes, for that year.

MR. WARD: Okay, let's see. You explained away the system failure at Trojan in 1984. What was the one in the B&W plant? That was allegedly one system failure? Was that Oconee? Is Mr. Dennig still here?

MR. WARMIEL: He knew we were coming after him.

(Laughter.)

MR. WARD: Does anybody remember what that was?

MR. FRAHN: I have one listed on the precurser study in 1977 on Davis-Besse.

MR. WARD: No, this was his report on '84 operating problems.

MR. FRAHN: I don't have it.

MR. WARD: He showed one system failure on demand in the B&W design.

MR. FRAHN: Jerry, do you know that?

MR. WARMIEL: All I can remember, Mr. Ward, was that Bob said something about some valves not working and the operators have to recover the system. I don't remember the specifics of what the scenario was.

MR. WARD: Okay, thank you very much.

MR. FRAHN: Let me make a comment. In the agenda for Karl Fleming, there's a staff presentation. That's from the NRR staff. If you want to make that correction -- not PL&G. On the staff comment on Fleming's paper, it's not me.

MR. WARD: All right. Mr. Fleming.

(Slide.)

MR. FLEMING: Good afternoon. My name is Karl Fleming, Senior Consultant with Pickard, Lowe and Garrick. As I understand it, at some previous ACRS meetings there was some interest and possibly some controversy associated with the paper that I presented in Brussells last August. I've been asked to come and kind of give this presentation again with the objective of trying to promote the greater understanding of the influence of common cause events as they affect aux feedwater system reliability, possibly to

DAV/bc

try and clarify what I think are some misconceptions about that subject, which I've heard a lot of comments made today.

(Slide.)

Briefly, what I chose to talk about here to follow on with the paper is to first go over some common cause analysis procedures that are being developed in a project sponsored by the Electric Power Research Institute. This project is aimed at trying to eliminate some of the confusion and inconsistency that you will find if you examine some of the recently published PRA's, which range in treatment of common cause to no inclusion of those events whatsoever to some kind of comprehensive coverage.

And to the extent that this subject has a great influence on the results of PRA, I think it also has a big influence on the decision-making regarding the use of redundancy and diversity as a means of achieving high reliability.

So I'd like to go over some of the procedures we've come up with for how we recommend PRA's should be included in these events. And that, in the Brussells paper, we happened to pick a very typical three-train auxilliary feedwater system, very typical of some of the Westinghouse plants, and we performed a rather comprehensive but generic analysis of that three-train system.

Since it included a complete examination of the data base to the extent that we are capable of doing that, we were able to draw some conclusions and add some insights about the roll of common cause events and the impact they have on the numerical values of system reliability.

We also thought it would be appropriate to take a new look at some of the old issues, like the role of redundancy and diversity in system design.

And I think the conclusions we reached in that paper along those lines may require a little bit of clarification.

Following that, I've been asked to comment on what's happening over in the European area in this particular area. I'm not an expert on European design of auxilliary feedwater systems, but I have been associated with a benchmark exercise that 10 teams from Europe and the U.S. are analyzing a German four-train auxilliary feedwater system. I have some preliminary results to discuss with you which may have some bearing on some of these points.

That's kind of the outline of my talk. If that's acceptable, I'll just proceed.

(Slide.)

I have been working on dependent events for about 10 years. A lot of people ask me how I can stay interested in such an esoteric subject for such a long time.

I think the thing that kind of motivates me to continue working in this area is it seems to me that the industry has been asking me to accept -- and I am talking about the industry, the regulators, everybody -- the whole ball of wax has been asking me to accept two mutually exclusive propositions.

The first is they seem to be saying, well, we don't know how to define it, to model it, to quantify it, or to know what causes it. I am talking about common cause failures here.

But despite that lack of consensus on those points on how to do those things, there seems to be a warm feeling that we know how to defend against it. I think we are making a lot of progress in taking care of Proposition A, but I don't think we have reached the situation with Proposition B. That was the purpose of our paper, to try to promote that kind of understanding.

MR. EBERSOLE: May I ask a question at this time? I know a gentleman who says that unless you know A you don't possibly know B.

MR. FLEMING: That is right. That is the point

DAVbur

I am trying to make.

MR. EBERSOLE: The next thing is: what is this thing called diversity unless you know what unity you have diverged from?

MR. FLEMING: I hope to provide a workable definition of that in my talk.

The point I am trying to make is that I want to try to negate Proposition A here so we can get on with Proposition B because obviously they are mutually exclusive.

(Slide.)

In our current efforts we are looking at a dependent events analysis in the broad sense, and we are looking at two different levels, the plant level, where we concern ourselves with earthquakes, fires, floods, intersystem dependencies and things like that, and the system level, where we are looking at what had been variously referred to as common cause events, common mode faults.

In coming up with system level procedures, we went back and basically listed the procedures of the PRA systems analysis and tried to identify the key points in that analysis that are very important for a common cause analysis.

What you will see here is a fairly well-known

DAVbur

approach, a very systematic approach to a systems analysis. You have to start off by knowing something about the system you are analyzing, and while that may seem somewhat obvious, the failure to address that point has been the basis for some unsuccessful reliability evaluations.

Then there is the logic model development. Then there's certain logic model techniques -- fault trees seem to be very popular -- reliability analysis, goal, methods.

After the logic model has been developed, most of the procedures required some kind of Boolean analysis to be done, followed by the development of an algebraic model to get the probability number, then some effort to estimate the parameters, look at the data base, get the parameters estimated, propagate those parameters through the system model, and come up with a system quantification, and then try to interpret the results.

One of the somewhat surprising things we found out in our work on dependent events procedures was that every single one of these steps has critical facets that are very important for competent common cause analysis. This is in contrast with a lot of the common cause analyses that have been published thus far, which tend to go in at Step 4, no earlier Step 4, to introduce some different algebraic formulas to calculate the reliability in light of common cause failures.

What we found is that there are some pitfalls in doing this. Those pitfalls have resulted in some under and over accounting of system failure modes.

I would like to illustrate some of those points in the next sequence of slides.

(Slide.)

The system that we decide to use as an example is a very typical three-train system. It has two motor driven pumps, a turbine driven pump, and to make this problem challenging for the system reliability analyst we used a rather conservative set of success criteria, in that we required flow to at least two out of the four steam generators. So the success criteria we chose for our analysis was flow from any one of the three pumps and into at least two of the four steam generators from any of those configurations.

Of course, success also required adequate supply of water from the supply tank and a common suction valve.

That was the basic example system that we looked at.

Because we are looking at system level procedures, we are going to concern ourselves with what was described in the last presentation as a loss of main feedwater event or, stated another way, an event where all the boundary conditions, all the support systems are assumed

to be available

MR. DA IS: Excuse me a second. This is a minor point.

In your p per you assumed those four discharge valves were normally 'osed, is that right?

MR. FLEMING: That is right.

MR. DAVIS: The normal valve convention could be blacked in on these?

MR. FLEMING: That is right. These are normally closed valves on the analysis. That also coincides with the design of some of the plants.

MR. DAVIS: Some but not all?

MR. FLEMING: That is right. And of course some of the plants also use different types of valves.

So the next step is to construct your reliability model.

(Slide.)

One can use fault trees, reliability block diagrams. I chose reliability block diagrams here because you can visualize the system logic more conveniently than you could in a fault tree. But they are basically equivalent.

MR. EBERSOLE: May I ask a question here?

I notice you use the models there that had a single source, the tank and a pipe?

MR. FLEMING: Right.

MR. EBERSOLE: I know in the seismic challenge case you can always argue that if you do it well with one pipe it is probably better off with two.

What is your rationale?

MR. FLEMING: I just selected this particular example system. In some of the permutations on this that I am going to get into later on, I am going to investigate the effect of having separate water supplies.

MR. EBERSOLE: See, that is the subject of the old overall syndrome. You know, it was dropped into the water tank.

MR. FLEMING: Right. Well, the analysis I am going to do first is going to assume that we require a condensation tank. I am going to discuss the implications of having separate water supplies, which is a very important point.

In a common cause analysis, what is important to this stuff is that we have to make some decisions about what kinds of groups of components we are going to admit to a common cause model. This is a very critical assumption that can't be avoided because there is simply no general way to even write down all the combinations of components that could be involved in the common cause event. There's too many components. We have to use insights from the

operational data and physical arguments to decide which groups of components we are going to group together.

In looking at that for the pumps, we noted that in most of these designs, while we have diverse drives, the pumps are nominally very similar. So in this analysis we are treating all three pumps, the mechanical part of the pump, as identical and subject to common cause events of all combinations. We are separating the motor drives so we can give credit to the diversity only at the driver level of the pump.

DR. CATTON: But the mechanical part of the pump is usually reliable?

MR. FLEMING: And we are going to reflect that by assigning appropriate failure rates which reflect that reliability.

The issue here is really component diversity. We felt it would be inappropriate to give full credit for diversity across the entire pump.

DR. CATTON: I just wonder how I would have diversity of power.

MR. FLEMING: Maybe you can't achieve that, but the subject here is to try to the model the system the way it really is. So we modeled the drives and pumps separately.

DR. CATTON: So when you model the pumps, what do

you include as failures?

MR. FLEMING: Failures of the mechanical pumps. The packing is put in too tightly around the pump. The bolts are loose on the pump. Things like that.

DR. CATTON: Loose bolts wouldn't be loose bolts on another.

MR. FLEMING: We will let the data tell that for us that we find -- and we have in fact found motor operated valves -- we have found loose bolts on multiple valves at the same time.

The whole philosophy, by the way, of this particular approach is that we are going to do the best job we can of pulling in all the data that we are seeing into the PRA model.

The problem of past PRAs is that the common cause events didn't fit the models. The models didn't allow for common cause events, and therefore there was no way to fit them in, no real logical way.

What we are going to talk about here is how to extend the model a little bit so all the common cause events fit.

MR. EBERSOLE: What do you do about the mechanic who thinks he is told to tighten all the seals at one point in time and he goes and tightens them all too tight? Do you invoke a time spread of maintenance in this system?

You remember the whole thing on the airplane that took off to Nassau.

MR. FLEMING: We would classify that as a common cause event.

MR. EBERSOLE: Do you put up a protective mechanism against it to preclude his touching but one pump at a time per week?

MR. FLEMING: I definitely will get into that, but I would like to first start out by trying to get a handle on what is out there. Then we will talk about defenses.

MR. EBERSOLE: All right.

MR. FLEMING: To summarize, the grouping assumptions were made here. The two -- four valves are identical and subject to common cause modeling, the two motor drives and the three pkumps. We will not consider common cause events, looking at, let's say, a valve and a pump. We are just not going to admit those into our movel, and we have fairly good insights from the data base to justify that assumption.

(Slide.)

Now, if you are going to address things like how effective is redundancy as a defense against common cause failures -- in other words, can you put enough redundancy in just to overcome the problem -- the model has to be able to

DAVbur

distinguish between different kinds of common cause events, of different severities.

There was a very simple model invented about 10 years ago called the beta factor model, which basically said that you either had a common cause event or you didn't and if you did have one, you modeled it as affecting all the components in that group. That model doesn't allow you to investigate this question: what is the impact of redundancy?

We found that in order to address questions like that one has to go back into the fault trees. This happens to be a fault tree for one of the valves, one of the four valves in the group, and considered not only the independent failure, which is normally considered in a standard noncommon cause analysis, but basically identified all the different combinations of events that involve the common cause failure of either two, three, or all four valves.

Now, because of the fact that each of these common cause events shows up in other portions of the tree, these common cause events actually complicate the Boolean analysis, and this is the point that has not been emphasized very much in previous work.

(Slide.)

To give you an idea of what the impact of that is, if you are just doing an independent events analysis on

the system it will have 29 cutsets.

As indicated on this slide, you have a single order cutset, your common suction path, your tank, and you have a whole bunch of third order cutsets reflecting the high degree of reliability of the systems, one out of the three systems. It is not surprising that you end up with primarily third order cutsets. You have all the combinations of motors, motor and turbine drivers, and two pumps and valve combinations, and so on.

When you go back in and put your common cause events in the model --

(Slide.)

-- you find there is a proliferation of cutsets.

On the left side of this column I have organized the 29 cutsets that come out of the independent events analysis, and I have this whole proliferation of cutsets involved in all the dependent events introduced in the model.

If one doesn't go back and put these events into the fault trees -- and just about all fault tree analyses have not done this -- then this kind of analysis has to be done in your head when you are writing down the formulas, and we found from our practical experiences it is very difficult for the most clever, well-trained applied probability people to be able to avoid missing cutsets and

DAVbur

double counting cutsets unless they go through this kind of approach.

MR. WARD: Karl, even this 100, I guess -- the way you set the problem up, you have eliminated, I guess, a lot of possible cutsets?

MR. FLEMING: These are the minimal cutsets. These are the ones you would look to if you wanted to estimate the system unavailability by summing the cutset unavailabilities, which is, you know, the usual or proximate approach that is used.

MR. WARD: I mean, you have got an example here going from 29 to 100, but the way you set this problem up you didn't admit certain common cause interactions.

MR. FLEMING: And that would have driven the number of cutsets up even higher if I had admitted those. Now, we have done some notation here to keep them straight because in independent events analyses all the cutsets involve combinations of components.

Now, we are talking about combinations of common cause events, any of which can fail, combinations of components in and of itself. So we introduced this superscript-subscript approach.

The subscript indicates you are talking about a single cause here, 4V-sub-3, four cutsets involving a single cause affecting three valves.

DAVbur

Then the experiments just are a shorthand notation for a second order cutset, 15V-2, to the second power, 15 cutsets, each involving two causes, each affecting two valves themselves.

This is the kind of complexity you get into when you want to address these problems, but since operating experience -- and the results I am going to show you -- indicate that these kind of events dominate the results, there is no excuse now to introduce this complexity into the model. It doesn't make sense to do a rigorous analysis of independent events and slap on a 10 percent beta factor and call that a final result.

MR. EBERSOLE: Would you go through what you said about the 4V3.

MR. FLEMING: Four cut sets, each involving a common cause event that takes up three valves. Okay?

It's a companion to this guy over here. Here's three of the cut sets, each wiping out a single valve. Each cause affecting a single valve, and you have to combine three of them to get the end result.

Here's a common cause. One of its common cause companions. You can have a common cause event and wipe out all three. These are four single order cut sets. There are also combinations where a common cause can take out two valves,.and an independent cause can combine with the two, affect another valve. So 12V2, V1, for example, means 12 cut sets, each involving two causes. One cause takes up two valves, the other cause takes out one valve.

So this is sort of an unavoidable complexity you have to get into when you're talking about this quasi-general common cause model.

The reason I've bringing this point out is, if this step isn't at least conceptually performed in an analysis, then the reviewer should be suspicious that the Boolean bookkeeping didn't add up properly.

I would venture to say that if you haven't gone through this kind of a process, chances are very high for

DAVbw

problems.

MR. DAVIS: Pardon me. I have a question on that. I heard what you're saying, and I think I agree with you; however, when I look at the results, and maybe I'm getting ahead, over 90 percent of the unreliability of the system is dominated by the first two common cause failures, which you would, just by looking at the system, by inspection, you would be suspicious those would be the problems.

In other words, these cause terms don't really contribute to the failure of the system.

MR. FLEMING: I'm going to let that be a result rather than an a priori assumption. My problem is that in previous models, that kind of thinking was built in as an a priori assumption. I'm going to let the results tell me that.

Also, I'd like to be able to have a model general enough, so that when I get into defenses and try to whittle these problems down, that the model can tell me what my benefits are.

So I agree with what you're saying, but I just want to keep --

MR. DAVIS: Your case would have been better made, if you'd picked a system where the top two weren't over 90 percent of the contribution, it seems to me.

MR. FLEMING: I think that happens to be the results of one particular systems analysis, and I hate to try to generalize that to all cases.

MR. DAVIS: Thank you.

MR. FLEMING: This is a procedure we apply to all the system, not just to aux feed.

(Slide.)

The other thing that we're trying to get rid of, and I've heard a lot of comments made this morning, there's a lot of suspicion that PRAs aren't accounting for what's been happening in the experience base. I think there's an element of truth to that. The procedures that we're recommending ask for as thorough a job as possible to be done to evaluate each event in the data base, common cause or independent on an event-by-event basis, especially if it happens to be common cause events. And carefully think about the impact of each event on his model.

When we do that, for example, this happens to be an event at point B. This was one of those strainer problems that affected one pump, and when they went in, checked the situation with the other strainers. According to the report, there were similar strainers in three other pumps.

In fact, these were not even on the same unit. There were two units involved here. We made use of a

DAVbw

classification system which was developed by another contractor for EPRI, very similar to a system that's been developed from NRC programs, although not identical, trying to map out the relationships between the causes and the impacts of those causes on components.

DR. CATTON: So you can consider the strainer part of the pump.

MR. FLEMING: That's right. It just reflects the level of detail at which I decided to develop my reliability model. One could opt to identify that as a separate component, and that would be fine, but based on the way we modeled the system, the key is to make the data analysis compatible with the assumptions being modeled.

DR. CATTON: I thin I would have made the strainer separate.

MR. FLEMING: It's common in most of the PRAs, I think, to include that as pumps, but that's an arbitrary decision.

MR. DAVIS: The problem with including the strainer is that some systems don't have strainers as part of the pump.

MR. FLEMING: That's not my problem, because this procedure requires the analyst to think about the applicability of each event to a system. That's what this example was intended to show.

First of all, there was another point here I was trying to show. Data is not black and white, you know. The classifical statistical people will tell you, well, we'll wait until we have enough data, and it's all going to be done by statistics.

Well, I think, as you know, it's very difficult to interpret what happened at the event, from an event report. It was not clear in this case whether all four pumps had, in fact, failed. It wasn't clear that they had not all failed. We have to treat this fuzziness in our data. The way we do this is rather than force this fuzzy event into a black and white categorization scheme, we assign, you know, we incorporate the fuzziness into our analysis, by basically identifying an impact vector associated with that event and estimating subjectively based on all the information we have, the probability that that event affect how many different components.

So that for the Point Beach plant in this kind of a situation, we would say there's a 90 percent chance, based on our judgment that this event affected one and only one pump. The other ones are just in a potential state. There is a 10 percent chance that it affected all four. One interpretation is that if such an event happened ten times, on the average, we might expect on one of these events, it to affect all four. This event is telling us something.

DAVbw

We don't want to pretend like we only affected one.

That's one aspect of this procedure. The other aspect is, that if you know that your plant doesn't have strainers or it took out its strainers, and you have confirmed that in your analysis, then you can throw the event out as not being applicable.

That's, I think, a legitimate judgment of screening for data that must be taken into account.

We've also classified this data to be compatible with this binomial failure rate by Bill Masley and Corey Atwood. That's one of the things I address in the paper in a few seconds.

We've done that for each of these sets of components in our analysis.

(Slide.)

This just happens to be the first page of the data we found for auxiliary feedwater pumps. What we do here is that we, first, after summarizing the event, we apply our impact vector, based on our understanding of what happened at that plant. Then we come up with a different impact vector for the plant we're doing the analysis of.

This happens to be -- this is not the same analysis that was done for the Brussels paper, but the Brussels paper has its own data in there. I didn't happen

DAVbw

to have a slide for that.

This happens to be for the four-train European system that we're going to tell you about later on.

MR. WARD: Carl, these impact vectors are judgment numbers?

MR. FLEMING: In many cases, it's just a question of mapping, you know, the event into the model. For example, at Zion, it was known that this event affected two pumps, and if we were doing an analysis of Zion, the impact vector would reflect that.

MR. WARD: So if it's 0 or 1, it's pretty clear, but when it's .9 --

MR. FLEMING: That basically reflects uncertainty or the knowledge of the analyst. It just reflects the fact that a deterministic resolution of what happened could not be made. There's three sort of conditions that give rise to this. One is, the report wasn't clear on what happened. That's pretty common. The second one was, the components, we modeled them in PRA as being successful or fail. We observe some intermediate states.

One is called degraded, one means incipient. Degraded means there's a noticeable reduction in the performance.

MR. WARD: For that type of thing, you could refine the model, theoretically, I guess.,

DAVbw

MR. FLEMING: Right. So in each of those three situations, these numbers are non0, 1, nonbinary. They reflect the judgment of the analysis team which, by the way, is a judgment that has to be made anyway.

It's just that we're going with numbers. If we didn't do it with numbers, it would be varied by either its inclusion or exclusion of the analysis in some innocuous way, a seemingly innocuous way.

The upshot here -- I don't want to get bogged down in the details, but as far as the common cause events are concerned, there's few enough events that the analyst should be able to devote a few percent of his resources to do a careful event-by-event evaluation and interpret that event on how it impacts his model.

This is the way we have chosen to do it.

There are questions that have to be addressed anyway.

(Slide.)

This happens to be the second page of the data. We were able to find 10 events in a data search that roughly included 10 years of data in the 1970s, ending at about 1981. We found, looking through, basically, LERs, an LER-based system called nuclear power experience.

We found 10 events involving multiple problems in the emergency feedwater system. This was just for the

DAVbw

emergency feedwater pumps.

We also looked at data for valves, diesel generators, and so on, and all the data that is relevant to this analysis has been followed.

(Slide.)

At some point in time, this all has to be fed into parameter estimation. This is a little work sheet that shows -- this happens to be again for this German problem I'll tell you about later. This is an analysis for a diesel-drived pump or a system of diesel-driven pumps. It reflects the totals of all those impact vectors, basically, the expected value on the frequency distribution of all that data, in terms of what kind of impact the event has on a number of components. And the reason, again, we have these fractions, these .1s, and so on, these events are then folded into estimators for parameters.

This happens to be parameters for an extension of the beta factor. It shows for a diesel-driven pump, we have a beta factor of .08, a gamma factor, which is, you know, given a common cause event has occurred, what's the initial probability that three or more components are involved.

That was .82, and for a four-train system, we also need a delta factor. The probability, given a common cause event, it affected more than three, and given the further probability, it could affect all four. These

DAVbw

numbers tend to be quite high. That's just to illustrate how the event-by-event screening should get traced into the calculation of the parameters.

(Slide.)

We do our best to quantify uncertainties. This happens to be out of the Brussels paper. It shows an uncertainty distribution for the beta factor and the gamma factor for emergency feedwater pumps. And as you can see, relative to the two factors, the beta factor distributions are rather well defined. The entire distribution is within a range of 0 to about 30 percent for the beta factor.

One of the reasons why this is rather well-defined here is sort of the confidence levels on parameters, you know, are affected by the number of each kind of event that's fed into the model. In the case of beta factors, it's a function of not only the number of common cause events. It's also the number of independent events. Since number of independent events is rather large, we have relatively good confidence in what the beta factor is.

On the other factor, for this gamma factor which is, you know, given that two pumps have failed, what's the condition like, when all three pumps have failed in the model? There's very little data for that, because you're basically only relying on common cause events for that

parameter. And as you can see, it's all over the map from 0 to 1 with a mean value of .62.

The point I'm trying to make here is that all these parameters have uncertainty, and to be able to make numerical statements of confidence have no effect whatsoever on the contemplated results.

We recommend very strongly, you should try to quantify as many uncertainties as possible.

(Slide.)

This shows the way in which we organize our results for determining dominant contributors. We look at the breakdown in two dimensions.

First of all, across the bottom, we look at the contributions in terms of what the initial alignments were at the time of the event. The three alignments we happened to pick for this example problem wre the normal alignment, the alignment with the motor-driven pump train in maintenance and the one with the turbine driven pump train in maintenance.

In this particular example, we assumed the design characteristics of a test override function, which enable us to neglect the testing alignment as a conservative assumption in this case, but one would normally also have testing alignments, as well as in a complete PRA, alignments for degraded support systems, like loss off off-site power,

DAVbw

loss of all AC power, and so on.

This happens to be the focus for just this one set of battery conditions.

Then for each one of the alignments, you can see the normal alignment in this case dominated. It was a couple orders of magnitude greater. 8 times 10 to the minus 4 was the point estimate system unavailability we had for this three-train system. This shows the contributors, in terms of the cut set groups. Common cause events involved in all three pumps is the first-ranking contributor. Common cause events involving all four valves was next, and you had to go pretty far down the list before you would come in to the area where cut sets involved purely independent events coming into play.

As you can see here, we could have neglected common cause events, independent events, entirely in this analysis, and we wouldn't have been offered very much. A fraction of the common cause events is very high.

As you can see, the breakdown is a little bit different in each category, but these results are very typical and bring out what Pete was saying earlier. After all that trouble we've gone through to model all these various event combinations, these, what we call global common cause events, seem to dominate this typical generic analysis that we're into right now.

DAVbw

(Slide.)

We also looked at those several different parametric models out there, you know. After you've gone down to the point of needing an algebraic formula to calculate the unavailability, there's different models that have been proposed, and we looked at three in the Brussels paper.

One is called just the basic parameter model. This is very similar to some work down by Marshall and Wolfe back in the '60s. As I said, that would probably be the reference for that model.

The multiple Greek letter model, which is a recent extension of the beta factor technique and the binomial failure rate model, the one that's been improved, there's two different binomial failure rate models that have been talked about. One of them has what's called lethal shocks, included for common cause events that effect all four valves in a nonbinomial way.

That's the one that's used here. We took our best shot to come up with a consistent interpretation of the data base, to feed each one of the models, and we found that just by using the different models, there wasn't a very, very large amount of variation in our final results.

That's one of the conclusions of our study, that some of these more fundamental things, like incorporating

DAVbw

the common cause events into your cut sets and making sure that the bookkeeping is done correctly, and the judgments you make on interpreting the data and the judgments you make on improving your components are far more critical than whether you pick one model or the other, as far as those three different models.

DAV/bc

(Slide.)

I think of maybe a little more interest to this particular meeting is that we went back and played some games with the system. We assumed the system was designed differently. We did these three cases. I repeated the case we did on our base case. This was the two motor-driven and one turbine-driven pump train system.

We looked at one where all three trains of the plant or of the system were motor-driven. And one where we only had a two-train motor-driven system.

For each one of these, we went back to the data base and reexamined the data in light of the new system and corrected for things like the size of the system and the number of components to be affected.

So we fixed the interpretation of the data in the most consistent way. We found that there wasn't a whole lot of variation across these three particular configurations. The two-train system was 1.1 X 10 to the minus 3 on the high side, and the slightly diverse system was 8.2 X 10 to the minus 4.

So that, by looking at these two, we can see the benefits of diversity. Four of these events where all boundary conditions were available. That's a very important qualification. As long as you're looking at systems that don't take out electric power, then there's a very, very

small benefit here because of the diversity.

The main reason for this is very clear when you go back to look at the data base that all three of these pumps were headed for the common suction path. Had one gone back and assumed that three separate water supplies for each one of these pump trains and more physically separated loops, you would have seen a much bigger difference between these two. In fact, across all three of these, that there were a fair number of these events. The fact that they were tied together to a common water source was the key to why the common cause event had occurred.

MR. EBOERSOLE: What were the internal components of that failure? The suction piping failing? Or was it stoppage of the intake due to the overall syndrome?

MR. FLEMING: The events that we had in there that I showed on the previous slide were things like steam-binding of the pumps. There were common points where air or steam could find its way back into the multiple pumps.

There were tight-packing events; each one of these events, when you look at it by itself, looks like a nonrepetitive off-the-wall kind of thing. But, collectively, they represent as a class of events that seems to happen with a regular pattern as far as their frequency.

That's one of the motivations behind the parametric model.

MR. EBOERSOLE: Just as an outgrowth of this, does this suggest that a conservatism should be commonly bounded, multiple sections as well as multiple discharges?

MR. FLEMING: I think that's to be considered, yes. Another point to bring out, I heard a lot of comments this morning and I know this has been a standard approach. The key parameter that came around from this morning's discussion -- I'm sorry, earlier this afternoon -- was how many pumps the plant has.

When you look at these results, it's not clear that that's the key to achieving high reliability, because what you find here is that these global common cause events are the ones that are killing you.

And just by going from two to three pumps or from three to four, for all that matter, when you look at these individual events, they don't seem to respect redundancy very much.

A very small proportion of these common cause events that we've looked at and the work that I've done on the PRA's, I've looked at about 400-500 of these common cause events and examined each one of them. It's very difficult to see how all but a small fraction of these can be influenced to any great event just by stacking on more redundancy, because a lot of them have to do with human-related problems.

DAV/bc

The design function is sort of a common point. The writing of the maintenance procedures is a single act that gets repeated on all fronts. All the functions that we ascribe in the industry are given to people and they say, You take this system, you take that system. If you have some misunderstanding or problem with the computer model, or whatever, it's going to find its way into all four event trains.

So I think that's one of the important -- it sort of blends into some of the conclusions.

(Slide.)

There's two types of conclusions we reached in our paper. One is about methodology, and I think we have demonstrated that there is a more systematic way than has been done in the past to treating these problems. A lot of it is just based on a natural extension of the basic principles of fault tree analysis. The choice of parametric models is not really that critical.

There's many papers being written at PRA and reliability conferences doing all these comparisons about using this model or that model. We're finding the choice of the parametric model is not as critical as some of the other uncertainties listed below here.

There is a lot of data available. It has taken quite a lot of resources to convert the data into useful

information for reliability engineers. Atwood has classified a lot of data for common cause models. And, in our EPRI-sponsored work, we have taken another crack at classifying this information.

I think some of the ongoing NRC programs are going to provide even more volume of event data to tap into. But it needs to be analyzed. It needs to be pooled into the PRA analysis process. There shouldn't just be a list of parameter values that are lifted from some table and some report and stuck into the analysis; there's still some very important judgments and uncertainties that I think drive the results.

One is how you define these component groups. We're involving some criteria for how you define these. But they're not all that completely defined here.

The assessment of impact vectors we're trying to develop some rules so we can evaluate events consistently because this does require a lot of judgment, and this is something we're working on right now.

And there's still a sparsity of data for these higher order parameters that we've been interested in in the model. But I think we've reached a point where realistic reliability predictions no longer hinge on unproven assumptions about independent events.

And I hope that we can see a rapid end to

analyses that simply assume that all the events in the model have been independent.

MR. EBOERSOLE: Could you venture an opinion about the accuracy, therefore, and reliability of the current PRA's?

MR. FLEMING: Oh, yes, I think there's a wide spectrum. Even if you take the PRA's that have been published in the last two years, you have a couple of examples there where essentially no common cause analysis was done at the system level.

MR. EBOERSOLE: What about Indian Point?

MR. FLEMING: I think that's probably somewhere in the transition. I think the IREP and Oconee PRA's, for example, did not do any common cause analysis as I defined it.

I think the most recent PRA's, for example, the one on Seabrook -- I'm biased on that one. I was the project manager. But, you know, in the Midland PRA, I think they had a very thorough common cause analysis there. I think Indian Point was in the transition. There was a concerted effort to treat common cause in there, but I think it was not as complete as we would do it today with the benefit of what we've learned.

MR. EBOERSOLE: Can you make a general observation about the degree of error by not incorporating

common cause?

MR. FLEMING: I think, without a doubt, depending on what system you're talking about, you're going to consistently underestimate system reliability of redundant systems. It has to be redundant systems. A single failure system is a different matter, but redundant systems could be underestimated by one to three orders of magnitude easily.

There's probably examples. There have been auxilliary feedwater analyses done at or below 10 to the minus 6. I think the three systems, the chief reason for that has been the omission of common cause events.

MR. DAVIS: Excuse me, Karl. It's my recollection that, for Seabrook, the auxilliary feedwater system reliability was 7 times 10 to the minus 6. I thought you used that as an example of one that was well done.

MR. FLEMING: I'll address that. That was not the result of the auxilliary feedwater system. What I call the auxilliary feedwater system. And Seabrook only has two trains. The numbers we got for that were in the vicinity of three times 10 to the minus 4 for the two-train system; and the lower number is the number you get when you throw in the startup shutdown pumps, which is sort of like the third train, which I think there were a lot of arguments to support the independent assumption because it's a totally separate system.

If you look at that number and you're kind of getting in to my first conclusion, based on the analysis we've done in the paper, I would say that a typical order of magnitude estimate for auxilliary feedwater system reliability based on everything we know about common cause is on the order of 10 to the minus 3 per demand.

And based on plant to plant variations that are out there, before I gave this talk, I talked with some of our most experienced systems analysts and people who actually do this sort of work back in their shop. And I asked each of them, you know, we've done probably 15 auxilliary feedwater system studies using techniques comparable to the ones I've shown to you here today.

And based on those evaluations plus what we think we would get if we would analyze Davis-Besse, which we haven't, and all the other plants out there, we think that the very, very widest you could stretch the range of results for plant to plant variability would be 10 to the minus 4 to 10 to the minus 2.

Ten to the minus 4 would represent probably an ultra lower bound that 100 percent of the plants would fall above. And you could see numbers as high as 10 to the minus 2 per demand based on the kind of analyses we've been through here.

In the case of Seabrook with the two-train

system, the numbers were in the vicinity of 3 times 10 to the minus 4. The main reasons why those numbers depart from this number stems from the specific event by event screening that was done at that particular plant.

And you would have to go back and do an event by event comparison to figure out just exactly why it was lower.

MR. EBOERSOLE: What would your method of analysis have done to the two-train circuit breaker systems for reactor scram such as we had at Salem?

MR. FLEMING: I'm glad you asked that. In November of 1982, we had done our preliminary reactor scram analysis using these techniques in the Salem reactor trip system, which was pretty similar to the one at Salem.

MR. WARD: You said "of Salem".

MR. FLEMING: We were analyzing Seabrook. I'm sorry. We were analyzing the Seabrook plant in the Seabrook PRA about three or four months before the Salem events occurred. We were discussing our results with the Seabrook folks to see whether those results were reasonable based on--I can't remember what the exact number was, but it was between 10 to the minus 4 and 10 to the minus 3 per demand. Close to 10 to the minus 3 per demand was the number we got for that system without recovery, without having the scram included.

When you multiplied that times the number of Westinghouse reactor years experience -- in fact, our clients did that and said, well, gee, Karl, if your analysis is correct, we should have seen one of these.

MR. EBOERSOLE: So it was just about on time.

MR. FLEMING: As a matter of fact, the dominant cause of system unavailability identified in our analysis was common cause failure of the reactor trip breakers, because we had seen some events in the data base. We found something like 50 or 60 LER events involving reactor trip breaker problems. And we found a couple that we classified as common cause problems. And that gave us a beta factor which, when multiplied by the failure rate, indicated a very high likelihood.

MR. EBOERSOLE: What about the boiler with its common dump boiling?

MR. FLEMING: I can't speak to that because, for some reason, they won't let me touch those boilers.

MR. EBOERSOLE: Oh, they don't?

MR. FLEMING: Well, that was a joke.

(Laughter.)

MR. FLEMING: Just by circumstances, I've only had the opportunity to look at the pressurized water reactors. But, in principle, we try to apply these same techniques to each system, mechanical, electrical or

otherwise.

MR. WARD: Karl, a question. Your first item up there, you talk about a two-train system. You mean two diverse trains?

MR. FLEMING: No. The example I showed in the previous slide was two motor-driven pumps only. That got a number just a little bit greater than 10 to the minus 3. Okay? So, without diversity, two motor-driven pump trains, you know, you ought to be able to get pretty close to 10 to the minus 3. I think two steam-driven would be an underestimate.

But the ones that we studied in the paper seemed to indicate that 10 to the minus 3 was a typical range. I hope in the paper I have adequately qualified this. But I certainly wouldn't want to overstate, you know, that all plants are 10 to the minus 3. I think there might have been some misunderstanding that was caused by that.

Like I said, I think there's probably a 2 order of magnitude spread to take into account plant variability, but 10 to the minus 3 is probably a good sort of medium central value for most of the plants we've looked at.

MR. DAVIS: Karl, excuse me. It wasn't clear to me in your paper whether you considered recovery. I guess I have concluded that you have not considered it.

MR. FLEMING: I'm sorry. There's no recovery in

these numbers whatsoever.

MR. DAVIS: So they wouldn't be expected to be lower?

MR. FLEMING: Absolutely. I think, for that reason, I think the numbers coming out of here seem to be pretty consistent with the numbers that I heard in the previous presentations.

(Slide.)

With recovery, it included substantial reductions. But I have a comment about that, too. I would be very careful about setting reliability targets for systems and including recovery factors in those because I don't regard recovery as a system characteristic. I think it's more of a plant characteristic.

Whether you can justify a factor of 10 versus a factor of 2 recovery for an auxilliary feedwater system may have a lot to do with a lot of things beyond just steam generator level inventory.

So you're really assessing the entire plant. I think there are pitfalls. It also invites the systems analysts to vary recovery in the systems analysis without looking at the plantwide implications.

Now, in looking at these results or sensitivities, the main benefit of having the steam-driven pump in the plant is --

DAV/bc

MR. THADANI: Mr. Ward, may I make a comment?

MR. WARD: Yes.

MR. THADANI: At least to clarify in terms of reliability studies, we agree with you that recovery should not be folded in, in an analysis done that way. But the reliability studies do it both ways. It's done without recovery and then with recovery.

MR. FLEMING: That's good.

DAVbur

In looking at this question of the steam driven pump, it seems that the primary benefit of having a steam driven pump is that it provides the capability of operating without electricity, at least in principle, at least without AC power.

That is a definite plus, and that would come out of a full-scale PRA study.

As far as looking at system level common cause failures, if you would convert from steam to all electric and not have that diversity, you would get about the same answer if you assume that electric power was available.

So you know, the reason why that might seem obvious, just because we have something diverse in there doesn't provide you some kind of mystic benefits against common cause failures. It only provides you from that very specific defense against the situation where we don't have electric power.

MR. EBERSOLE: What happens when you include steam?

You develop a dedicated diesel generator carrying its own pump. It is electric, but it is not connected to the grid.

MR. FLEMING: That is in fact the system we analyzed in this benchmark which I am about to tell you about.

DAVbur

I think after going through the sensitivity studies and having the benefit of not having to apologize about the analysis, not including common cause failures, and looking at the nature of the results, there is a cause to sort of rethink the use of diversity and even redundancy as a defense against common cause failures.

The results are showing us that the redundancy in and of itself doesn't seem to be very effective, and diversity also has to be thought out very carefully because I think just because you have -- like I said in the steam driven example -- just because you have some differences in your redundant trains, unless you have thought your way through to how the specific common cause events you saw in the data base would have acted differently in light of that kind of diversity, it just doesn't follow to me that making things different is going to make it actually better. I think there is a need to rethink this.

In the case of the auxiliary feedwater system, the idea of having diverse drive in there, maybe it would have been more effective if the trains had been more independent. But, see, that is the key. What we are really trying to achieve here through the use of redundancy is independence.

Diversity is not an end in itself. Diversity is a technique or a theory about how to achieve independence.

I think it is very important to keep those concepts in that kind of perspective because I think that a lot of people -- they say, well, I have got diversity in my system, I throw in some steam instead of electric or diesel, and I have met some kind of diversity requirement, and therefore it is going to be better.

I don't think it necessarily follows from that. You ought to think about how to achieve independence. While I think there is something to be said for diversity, I don't think that it has had the kind of impact on performance as many would have expected.

I just think we need to rethink that a little bit. I am not saying it is not a bad idea.

That is pretty much the conclusions of this Brussels paper.

If you would like, I can go on and talk about this European exercise.

MR. WARD: Go ahead.

(Slide.)

MR. FLEMING: The Common Market countries in Europe have been in a sort of evolutionary way developing a sort of consensus of procedures to do PRAs. They have not gone aggressively into performing big full-scope level PRAs, as is frequently done in the U.S. The approach they are taking is they are getting all the countries together and

trying to work on small problems and develop a consensus approach on pieces of the pie and gradually build up to some kind of a consensus approach.

Earlier they had done a reliability study. They had picked a system, and they asked each of the teams who participated -- I am not sure exactly how many participated in that exercise -- to perform an independent events reliability study on the system, and they had a sequence of meetings to try to figure out why they were getting different results. And they tried to keep normalizing to evolve a more consensus approach.

This project had been completed sometime last year, and recently, this year, 1985, they started an extension of that to address common cause events. PL&G became involved in that through the sponsorship of EPRI and NRC to provide another team to also have a chance to test our procedures that we have been developing, and talked about in the Brussels paper, and also try to work with them to try to develop some kind of consensus approach.

So what was done is there was basically a six-train auxiliary feedwater system that was selected for the example. What this is in actuality is a four-train dedicated diesel driven pump type auxiliary feedwater system that has been combined with a separate two-train startup/shutdown motor driven pump system in a fault tree

analysis, where all six pumps are postulated to fail.

These ten teams went to this plant. It is a brand new KWU plant at Grohnde in Germany, on the Grohnde River. It had just started commercial operation earlier this year. It is a typical four-train German design that meets all of their current safety requirements with respect to aircraft crash, seismic events, fourfold level redundancy, and so on.

Each of us visited the plant and has performed a preliminary analysis of the system -- of this collection of systems, if you will, and we have had one meeting to discuss results, and we are in the process right now of doing some adjustments and trying to normalize our differences, and there will be a finalization of this in March next year.

Basically, what has happened is that the joint research center at Ispra is coordinating all this. There is ten teams, one from the U.S. There's parallel efforts at EPRI and NRC to develop procedures, and we are going to test these out.

As I mentioned, it is a KWU plant, six-train system. The independent failure analysis was fixed. Each team was given a fault tree, a set of independent component failure rates, a statement of the boundaries of the problem, and a lot of information about how the system was designed, operated and maintained.

DAVbur

There's two phases to the analysis and, as I mentioned, will be finished in March 1986.

(Slide.)

Based on the first phase of the analysis, each of the ten teams submitted a report. The analysis of those reporcs is still in development right now. But you can see by the different approaches -- each of the teams are identified here on the left -- took to the qualitative and quantitative phases of the analysis.

In the U.S. contribution we basically went through the process I showed to you in the previous slide. Each other team used whatever process they felt was appropriate.

They basically seemed to distinguish themselves by whatever factors they used to approach the qualitative factors. That is everything leading up to parameter estimation, and the different models they used -- algebraic models and parametric models -- they used to quantitate common cause events where there is a little bit more similarity.

In the quantitative analysis, some teams used the simple beta factor model, its extension the multiple Greek letter model, the Marshall-Olkin technique, which is very similar to that basic parameter model we mentioned in Russell's paper, as well as the binomial failure rate

method.

So those are the various techniques that are used for one out of six needed for success, to calibrate your thinking.

(Slide.)

It is not the same kind of numbers I showed you before. This shows the kind of spread we got on point estimates that were made by each of the teams. In each case, people did at least two separate analyses, which should be regarded more as a limited sensitivity study as opposed to a formal uncertainty propagation.

This dotted line indicates the results of the independent analysis that everybody was given to start with for somewhere in the vicinity of 10 to the minus 8th to 10 to the minus 7th for any of these six pump trains to be unavailable -- all of those to be unavailable.

As you can see, this is the kind of spread that the teams were getting, a three orders of magnitude spread on those. But based on the results that were presented at the meeting and the amount of interchange that was taking place, I would just offer my own personal judgment that when the second round of analyses are completed, I think we will find a much tighter spread in the results, between 10 to the minus 5 and 10 to the minus 4.

When you break this down and break off the piece

DAVbur

that looks like the auxiliary feedwater system, the four-train auxiliary feedwater system, our U.S. analysis analyzed that system at between 10 to the minus 3 and 10 to the minus 2. It was actually higher, or more unfavorable, than the three-train system that we had found in Russell's paper.

So the four-train system actually was worse than the three-train U.S. system. The reason for that was that while we were able to identify these benefits of the train separation -- and there were lots of events that were not classified as being very important, physically separated events, such as the common section path, and so on, their component selection of choosing diesel generators to drive the pumps -- we applied electric power-diesel generator data to that problem, which is the only data we had.

That data indicated the failure rates of diesel generators are like an order of magnitude higher than the motors, or more. Since the failure rate went up by a very large factor, the reduction in the common cause factors was swamped out by the component structure.

I think we would have seen a much different kind of number had we looked at four motor driven pump trains that were physically separated. I would have expected to see numbers significantly less than 10 to the minus 3.

DR. CATTON: On that diagram that you have,

France and the U.S. both used the same technique, yet there is about the biggest spread between the two.

MR. FLEMING: Right. The reason for that is that only the U.S. team actually analyzed event data to go in the analysis. All the other teams that used the parametric model either assumed parameters for that model or were quoted a parameter from some other study that was probably not even appropriate for that system.

As a matter of fact, for that reason one of the assignments to the ten teams in Phase 2 is to have all ten teams go back to the same U.S. data base and go through that evaluation process so we can focus on what kind of consistency we can get among the teams, and we want to see if that will affect the process.

But that is the major reason. The model in and of itself is not that important, as much as all the thought that goes into feeding the information into the model. That is where the differences came into play.

DR. CATTON: So the fact that Denmark and Italy are the same is not surprising. They used exactly the same information.

MR. FLEMING: That is right.

DR. CATTON: The others are model differences?

MR. FLEMING: Model differences and other kinds of judgments that went into the analysis, like the selection

DAVbur

of common cause groups.

For example, the Swedish team used the mutliple Greek letter model. They modeled the whole train of auxiliary feedwater as a single component. They had one set of beta, gamma, and delta factors for the whole train of equipment items that needed to take place; whereas, in the U.S. design we followed the approach in the paper. We had a separate model for the diesels, the pumps, the demineralizer pumps, the valves, and so on. Each one had a separate model.

And then depending upon how you feed your parameters on that model, it might have some bearing on the final results.

A comment on the design of the German plants is that while this particular analysis was confined to system level considerations, the thing that impressed me about the German design was the emergency feedwater system was almost self-contained as far as support systems were concerned. It had its own component cooling water pump, which sucked off the water supply that was dedicated to that train. There was a generator on the diesel to provide electric power in the event that the station diesels did not provide power.

So there was not a lot of dependence on the service water pump on cooling water type of support systems like you will find in some U.S. designs, and I think that

whenever a full scope PRA is done on plants like this, these kinds of benefits will be quantified better than we have been able to do in this study.

That concludes everything I had to present.

Any further questions?

MR. WARD: Let's see, Karl, do these numbers credit recovery actions?

MR. FLEMING: No, there is no recovery actions. It is just a Boolean analysis to keep the scope of the analysis fixed.

MR. WARD: Let's go back to the other topic. Your conclusions about a two- or three-train system as a typical system might have an unavailability of 10 to the minus 3, and you agree if recovery was credited that could become 10 to the minus 4 perhaps.

MR. FLEMING: I don't think that is unreasonable to expect, a recovery factor like that. Again, I want to make sure that that is tied to some kind of plant level analysis.

MR. WARD: I got sort of a disconnect there because the staff is claiming that most of the plants they have looked at can just about meet this standard review plan number on unavailability with recovery included, 10 to the minus 4, but their methods of analysis didn't really treat -- I don't think they did -- didn't treat common cause

to the extent yours did.

MR. FLEMING: There was some analysis of common cause, but I don't think it was the same approach that was indicated here. I think we will hear about that in the next talk.

But you know, the possible things that could give rise to differences are the data that was used -- for example, I know the failure rates assigned to these valves in the common suction path are administratively monitored. I think the failure rates that we have in our data base for those contributors are much lower than the failure rates assumed in the NRC analysis.

So the failure rates could give rise to the differences. Whatever differences there are in common cause treatment can cause differences, and how you interface everything in the logic model could cause differences. There could be lots of areas for differences.

On the surface it sounds like by putting recovery on top of this kind of analysis it would not be unreasonable to end up with plants under the 10 to the minus 4 area, but I would have my doubts as to whether all the plants were in the 10 to the minus 4 area. That is sort of my gut reaction.

MR. WARD: Any other questions?

MR. DAVIS: I have a quick one, Karl. I need some guidance on how to handle the data on these problems. I took a look at your paper and decided to do an independent assessment of the common cause analysis of the discharge valves failing to open.

I used the beta factor model. One of the problems with the beta factor model has, and I think all these common cause factor models have this same problem, they need as input the independent failure rate plus some measure of the common cause contribution. And in the beta factor model, those two numbers are multiplied together.

MR. FLEMING: Almost.

MR. DAVIS: The point is that you really compound any variations in both of these parameters when you apply these models. Just on the valves alone, in the literature, I found variations in the independent valve failure rates and variations in the beta factor that would cause two orders of magnitude variation in the common cause contribution of the four valves failing.

And I can tell you where all these numbers come from, but that's not the point.

MR. FLEMING: It doesn't surprise me.

MR. DAVIS: They're in the literature. And, in your example, that was the dominant contributor; almost

half was because of those four valves failing.

This is troublesome to me because I can make the number anything I want by selecting the data from these sources.

MR. FLEMING: I know exactly what you're saying. I have taken a lot of grief personally because people have lifted numbers that I have generated for specific applications, literally lifted them and plugged them into some kind of model.

That's the very reason why we urge very strongly that it be placed on the responsibility of the systems analyst to reconcile a document, his intrepretation of each one of these events and how it does or not apply, and the reasons why, and put that on the responsibility of the industry.

I would not recommend that anybody lift a numerical value beta factor and plug it into a model, to do anything more than maybe a private sensitivity study, or whatever.

MR. DAVIS: But you can't always get your hands on the data. The Seabrook data base, for example, is proprietary.

MR. FLEMING: All of the events that went into the Seabrook report are available to the public in every EPRI-sponsored document; I can provide you with references

to that. The NRC has it. We can get copies to anybody who needs it.

But all the Seabrook events that went into the Seabrook PRA came from 2,300 LER's that were searched and evaluated. We came up with something like 425 dependent events, and we screened those and we screened out functional dependencies, and things like that. But every one of those dependent events is documented.

There's a nice little cause and effect logic diagram in this EPRI report, which is one of the data bases that we have at our disposal. There's no reason why. It doesn't take very long for an analyst to take those events that belong to the component group in his system and do a thoughtful evaluation of each event.

For example, there's only 22 diesel generator events. You know, you can. There's a limit as to how much insight you can get from those 22 reports. You read them. You either understand them or you don't. You go back over them a second time. It doesn't really take a lot of manhours to ask the systems analyst to take those, document his impact for those events and the reasons why. He threw it out, included it, or weighted it differently, or whatever. I think that's the secret to that problem, is to put the responsibility of documentation on the analyst and don't allow the analyst to lift beta factors or failure

rates.

The other problem you alluded to, and that is that we've gone to the process of careful event by event type screening for these common cause factors. It's unfortunate that we haven't been able to do a comparable level of effort for the failure rates.

There's only a few components that I've ever seen supported by a careful event by event screening of the data. Most of our failure rates are based on judgment. They're based on IEEE-500 and WASH-1400 and other synthesized distributions.

Unfortunately, we don't have as much confidence in what's behind those numbers as we now have I think on the common cause factors. But whenever you can consistently screen all the events and all the analysis, that should be done.

But the resources to handle the independent events are like an order of magnitude greater; that's the problem. They might be on the order of hundreds of common case events and there'll be thousands of independent events that have to be evaluated.

MR. EBOERSOLE: What comments could you make on the merits of the bleed/feed adjunct to the problem of cooldown?

MR. FLEMING: Well, I listened to the comments

DAV/bc

earlier about bleed and feed. I'm not an expert on that subject, but I do know that in the PRA's that we've done, we go through a process of asking our utility clients to provide some information to support the capability of the PORV's to sustain that environment.

In some cases, we have not been able to get such documentation and that capability has not been in the PRA. In other cases where our analysts are satisfied that something like 24 hours worth of cooling can be maintained in that mode, then they take both.

I can't really speak to what the specific criteria are. But, again, some of the other comments I heard about the PRA today is that I think we have to distinguish between what may be regarded as sort of the collective practice of a given group of analyses and the responsibilities of the analyzers.

I think the PRA's, like anything else done in supportive reactor safety and engineering, is an analytical activity that should be documented and it's subject to the same principles of documentation as a stress calculation, or whatever.

I don't think that just because we put a PRA label on it gives these people an escape clause not to have to either state what their assumptions were or provide, you know, the backup calculation to support it.

MR. MICHELSON: In considering the possible contribution to risk, say, from a seismic disturbance, how do you handle the failure of the nonseismically qualified equipment in terms of what it might do to the ability of the seismic equipment to function? It's a potential common mode challenge.

For instance, if the fire protection system would actuate as a consequence of a seismic event, it will spray several trains, several different systems, and so forth. How do you come to grips with that kind of a question?

MR. FLEMING: That's a very good question. In fact, I recall that specific scenario mentioned at the Seabrook ACRS meetings that preceded the low power letter. In fact, I have to admit, when that particular scenario -- the earthquake taking out the nonseismically qualified sprays on top of these generators, that, in fact, was not identified in the PRA at that particular point in time.

Of course, it caused us to go back and take a look at it in that specific instance. It was determined, or it was determined after the fact that that system was not normally energized. It was normally valved out of service. So we calculated and retrospectively put that back in the model.

And it didn't seem to be important. But that's a real problem. It stems from the fact that the PRA analysts

have to base their analysis on their level of information and knowledge about the plant. I think the PRA's have been very successful in being able to get the basic functional characteristics of the plant modeled.

There's pretty good accountability of what the intersystem dependencies are, what supports what and accounting for all the components, and things like that. The only recommendation I have is that I don't feel that PRA's in general have spent enough time looking at the data in a qualitative way.

There's no reason why some kind of a checklist approach couldn't be taken to at least make sure that you have accounted for what you have observed. And what ad hoc approaches have theorized in meetings such as this.

But that's all I would have to say.

MR. MICHELSON: I'm not sure you answered my question. If it did, it went by a little too fast. You say of course that the analyst is supposed to model. I guess what you're saying is the analyst is really supposed to model the nonseismically qualified system to the extent that he can ascertain if there are interaction capabilities.

MR. FLEMING: Absolutely.

MR. MICHELSON: Is this commonly done?

MR. FLEMING: I think it is. I think, in the current PRA's that we're doing now, we are not just

confining our seismic analysis to seismically qualified components. And what that translates into, it basically translates into not having as warm a feeling about the fragility curves that you're using.

Fragility curves are based more on generic data and they can't really link the fragility curve calculation into the safety factors built into the design process.

MR. MICHELSON: These are all good words. I think I agree with you.

MR. FLEMING: I guess what I'm saying is that we include them and we end up with larger uncertainties.

MR. MICHELSON: Well, how do you come to grips with, for instance, relay and instrument contact chatter in nonqualified systems where you may have rather limited experience with such devices, if any? Since they weren't normally seismically qualified anyhow?

How do you speculate in doing this modeling, how these kinds of systems are going to behave? Or, do you make all worst case assumptions?

MR. FLEMING: This is a little bit out of my field. I'll address it as much as I can. In the relay and contact chatter area, the current work we're doing, we're going through some kind of process to classify these components as to what their physical characteristics are.

Are they normally energized? Normally

de-energized? We make basically global assumptions. If they're one type, they will fail in a certain way. If they're another type and energized, they'll perform differently.

We do assume that this chatter phenomenon will occur and model that into our plant in what we think is a conservative way.

But the real problem there is it's very difficult to cope with the number of possible states that one could hypothesize. And I can't state with great confidence that we're adequately addressing the issue right now. We have thought about it and are trying to take some reasonable approaches to take into account that relay chatter phenomenon.

I assume that relay chatter will in fact occur and we'll try to map that into the behavior on the plant based on the characteristics of the relays.

MR. MICHELSON: A more complex issue arises when you allow ventilation systems to fail during seismic events, which a nonqualified might very well do, particularly fans. And then you start worrying about the solid state control systems that might be thereby affected due to elevated temperatures, and then how they all feed back.

And it gets pretty wild after a while.

MR. FLEMING: It is wild. It's very difficult

what we're trying to tackle in these PRA's.

MR. MICHELSON: You do attempt to some extent to address such issues from what you're saying, I believe.

MR. FLEMING: We are attempting to tackle those. In fact, the room heatup question in general, including those with and without earthquakes, I think is one of the most challenging problems we're facing in our current PRA's. There are three or four inhouse PRA's where your final core melt frequency results might be anywhere from 10 to the minus 2 to 10 to the minus 4, depending on how you treat the behavior of the equipment in the degraded environment.

MR. MICHELSON: I understand, in some cases on solid state controls, it's unpredictable, it could go either way.

MR. FLEMING: It's very difficult to figure out what the failure mode will be. We are addressing those questions and we'll have to get some actual analyses out on the street and get them reviewed to see how well we're going.

MR. WARD: Okay, Mr. Fleming, we appreciate your talk and your responses. Let's go to the next speaker now, who is going to be someone from the staff.

MR. EL-BASSIONI: My name is El-Bassioni. I am a Senior Reliability and Risk Analyst of the Reliability and

Risk Assessment Branch, in the Division of Safety Technology of NRR.

(Slide.)

I'll start by talking about the highlights of the report co-authored by Karl. I hope I quoted him right and he'll speak up if I've misquoted any of his conclusions.

The first one that Karl and his co-author recognized, that the treatment of common cause failures in published PRA's are inconsistent and nonsystematic. Different methods are used, different boundary conditions, and usually we get different conclusions because also of different data that were used.

His report has claimed that random independent failures contributed less than 1 percent of the overall system unavailability. For a two-motor-driven train, if we add a third redundant motor-driven train, we're going to have an improvement of about 1.5.

And in case that third train is substituted by a diverse turbine-driven train, this factor of 1.5 will increase to about 1.7, which means that the net effect of diversity is about 10 percent increased from the case where we had just pure redundancy.

And the last one is that for a typical three-train auxilliary feedwater system, we get a typical value for unavailability of one 10 to the minus 3 per

DAV/bc

demand.

MR. WARD: Again, the last number is without any recovery?

DR. EL-BASSIONI: I'm coming to that.

(Slide.)

The methodology that is provided by Pickard, Lowe and Garrick appears to be attractive, and it is systematic; however, in our view, it has a number of limitations. The first is that that report treated only common cause failures, as far as similar components are concerned, but when we get to common cause, the effects that would impact dissimilar components, the methodology cannot be easily extrapolated to include that, and if it is extrapolated to include the dissimilar components, it will be very complex.

Carl has indicated also that failure dependency experienced data is still sparse. As we have seen in his impact vectors, those vectors are highly subjective. It relies on the analyst's interpretation of the data and whether the data is applicable to the particular system under analysis or not.

MR. EBERSOLE: May I ask a question?

In particular, the first bullet, and to some extent, the others, don't each of them indicate that he underestimated the common cause failure potential?

DR. EL-BASSIONI: It could go both ways. When I go to all of the limitations, some of them will contribute

this way and some others will contribute that way; however, the main contributor, in our view, is the subjectivity in the interpretation of the data.

The biggest contributor would be the definition of the impact vectors. And that was seen in the regulatory letter, when we get to estimate high water parameters, the gamma and delta parameters. We have very large uncertainties.

This might be where the largest contribution to our effort is.

MR. EBERSOLE: What you're saying is, that in itself is an influence on the common cause factors.

DR. EL-BASSIONI: Yes.

MR. EBERSOLE: And there lies -- I once had a fellow who asked me, and it's a common thing. He say, "How do you want the answer to come out? I have such a range of assumptions here I could put into it. They could go from black to white."

That then brings up the common cause influence of highest interests in the outcome.

DR. EL-BASSIONI: However, I want to give credit to that report.

Carl has taken a very systematic view to reviewing dependent data, experience data. There is some difference between dependency data, dependency experience

DAVbw

data and random independent failure data.

In most cases, when we look at incidents that involve dependent failures, usually we have some corrective action taking place that follows that. So we cannot rely on experience as much as we rely on independent failure data.

We have to emphasize good engineering judgment, in terms of, is this piece of information applicable to the system that we have, or is it not applicable?

MR. EBERSOLE: One of the cases we can't seem to quite get away from is the Palo Verde case, where there is a claim with a rather deficient aux feedwater system that they've got 10 to the minus 4 per demand.

I guess you're acquainted with that. They have no PORVs.

DR. EL-BASSIONI: In this case study also, they did not model any of the support systems and recovery was not included in their model. Carl pointed out that recovery is sequence-dependent. This is why it was not included in the model; however, there are some very routine recovery actions like, in case we have automatic initiation, automatic actuation failure, the operator can initiate manual actuation.

MR. EBERSOLE: Would you follow Davis-Besse recovery routing?

DR. EL-BASSIONI: In my judgment that was a

routine.

MR. WARD: Would you expand a little bit on the importance of leaving out the support systems in the aux field study?

DR. EL-BASSIONI: What I was trying to point out, out of the Pickard, Lowe and Garrick report was very sketchy and whether they had included support systems or not, I couldn't judge from the fault trees that they had in the report. In some cases that I have seen, they looked at auxiliary feedwater systems and assumed that all the support systems are available. Some did not. Out of the report, I couldn't make a judgment on whether they had included that or not.

This points out one very important thing. Since we are looking for a systematic methodology, we should have a very well-defined boundary for the auxiliary feedwater system, so when we say "auxiliary feedwater system," we'd know what we're talking about.

MR. THADANI: Dave, let me give you a specific example.

Let's take a plant with two diesel generators, two motor-driven pumps, and that's all it's got. The unavailability of the auxiliary feedwater system may, in fact, now be limited by the unavailability of the diesel generators. Now let me take three motor-driven pumps,

three diesel generators, and let me employ Carl's methodology on common cause failures.

I may, in fact, conclude that three water-driven trains in an aux feed system are not much better than two motor-driven trains in an aux feed. Again, if use Carl's approach, I say, let me replace the third motor-driven pump by a turbine-driven pump, and using this approach, I might then conclude that the turbine-driven aux feed train buys me a lot more than a third multidriven train of aux feed.

The reason I come to a totally different conclusion than the one that Carl came to in his analysis is, by having included it in another support state, which is availability of electric power or nonavailability of electric power. That's very important, because I suspect -- at least it's my own personal view that the unability of diesels is probably going to show unavailability of two motor-driven aux feed pumps, having taken care of certain key vulnerabilities, especially in terms of nonrecoverable thoughts.

That's really what Dr. El-Bassioni is saying, in terms of support states, that one ought to carefully consider those. But then analysis becomes very completed.

MR. WARD: That was my next question. If they are considered, is it practical to consider this approach?

MR. THADANI: That's exactly the question that

Adel is addressing in his next one or two slides on the complexity of the analysis.

MR. WARD: Carl?

MR. FLEMING: I think right off the bat here, I think it's worthwhile to distinguish between the limitations of the methodology and the scope of the paper. I chose in my paper to address a certain narrow aspect of what we have to consider the PRA, and there is certainly nothing inherent in the method that would preclude it from looking at support states.

DR. EL-BASSIONI: I didn't say otherwise, Carl.

MR. FLEMING: I'll help you find the sentence in the paper where it clearly states that this analysis is done over the assumption that all boundary conditions are available.

MR. WARD: Unless it makes it so complicated that it's not a practical method of analysis, that's the question.

MR. FLEMING: You see, the point is, there is no real difficulty in PRAs in dealing with functional dependencies. Everybody's doing a pretty good job of that, so I didn't want to complicate the paper by addressing that.

DR. EL-BASSIONI: The only thing that I spoke about is the state of the support system. We tend to

concentrate on the figure, which is 10 to the minus 3, without knowing what goes under that.

(Slide.)

The next limitation is the increase of the number of minimum cut sets by a factor of about 5, by including these sub-basic events. I think this problem will be more chronic once we go beyond similar components to dissimilar components. This might not be a problem for a small-sized system with a small typical fault tree of 17 or 18 gates, but when we get to a full-scope PRA, this might be a big problem, and it might overburden the analysis.

My last thing is about methodology. It seems to highlight quantitative aspects of common cause failure rather than qualitative, and we emphasize qualitative analysis to draw insights and look at vulnerabilities in the design.

Carl mentioned something about two separate approaches. One of them is called system familiarization that he used, and the other one the Europeans use is the FMEA, and I wish he would have talked more about that.

(Slide.)

I want to say that the Staff has always called for a well-disciplined, consistent treatment of dependent failures. Staff has several programs that provide improvement in the state of the art and common cause

failure, one of them in the systems interaction program, the RMIEP program. There is a cooperative effort with EPRI, and this effort, we are supposed to provide a procedures guide for treatment of dependent failures. Carl Fleming is one of the major authors or participants in that effort.

MR. EBERSOLE: As I recall, at the last subcommittee meeting on subsystem interaction, I was impressed with the low level of support and the budget.

How many people are working on that in the Staff? I think it was two, wasn't it?

DR. EL-BASSIONI: I'll ask Ashok to answer this question.

MR. THADANI: I don't know the answer as to the number of people right now. Certainly, the level of effort has come down from what it was years ago. I think the Staff has a proposal in hand to try to resolve the unresolved safety issue, A-17. What Dr. El-Bassioni is addressing is not in the context of a resolution of the USI, but rather all the effort that has gone into trying to identify and capture those interactions. The effort that was conducted at Brookhaven, Lawrence Livermore Laboratories that I think you're familiar with. The particular attention there was, in terms of functional interactions.

MR. EBERSOLE: I was just commenting on the fact that it says that they have the full support of the Staff.

MR. THADANI: I think this should be read as follows, that we're certainly in support in the PRA world of trying to address all the common cause failures, to the best of our ability.

Dr. El-Bassioni is pointing out various programs, the outcome of which would help, in terms of methods to be applied to identify these interactions, dependencies or common cause failures, and in fact, if he were to go on, he could tell you about some of the guides he's working on, writing procedures and how to go about treating these common cause failures.

MR. EBERSOLE: Mr. Thadani, that statement would hold water, it would be perfectly accurate, if there was only one man working on system interaction, and he was enthusiastically supportive of common cause failure analysis.

That's all I'm saying.

DR. EL-BASSIONI: Sir, I just pointed out that the call for careful, well-disciplined, consistent treatment has the support of the Staff. We recognize that this is a problem, as Carl pointed out, and we are working on it. This is what I wanted to say.

MR. WARD: They're in favor of doing good PRAs.

MR. THADANI: That's how it should be interpreted.

(Laughter.)

MR. MICHELSON: From time to time, the people in the environmental qualification world find instruments and controls, and so forth, don't really behave in adverse environments like they had thought they would behave. So they have to go back and make certain modifications and fixes, and whatever, which then makes them behave properly.

Do you people go back now and pick up those instruments that were not so modified, since they were not in safety-related equipment and systems and think about them, in terms of creating common cause problems for balance of plant equipment, which is safety-related? It's a similar question that I asked earlier, but another aspect of it.

We seem to ignore the fact that these pieces of equipment are known to fail under adverse conditions, but we fixed it for those pieces that had to be fixed.

How do we pick that up on the rest of the world? And how do we factor that back into possible system interaction effects, and so forth? Do we really try to do that, or do we just give lip service?

MR. THADANI: I think the toughest ones, somewhere, at least at this stage, I think there is a very limited amount of work done on the nonseismically qualified equipment mounted in such a location, failing under seismic

events of a certain magnitude and the consequential failure of some other systems, at least as far as I understand, that is not done particularly well. In fact, it's probably done very poorly today.

Another example might be fire in a specific room. I think today, fire analyses may have large uncertainties, but at least people seem to be taking into account not just fire growth, but also what temperatures the rooms might get to, flame directions, and so on, the ability of certain cables to withstand temperatures at certain levels, and so on.

There seems to be some work being done in that area.

MR. MICHELSON: But even in that area, they're still focusing on assuring the protection of safety-related equipment in the vicinity and ignoring the nonsafety-related equipment, which is seeing the same fire environment which can, in turn, cause unwanted actions. We just don't chase this potential for unwanted actions too well, because it's a very difficult thing to chase.

DAVbur

MR. RUBINSTEIN: I have two comments. The first is the identification of the vulnerability or deficiency. In the deterministic world engineers can fix that. As to whether or not they ultimately pick it up in the analysis, that is preventive, or having originally been known to be vulnerable is another story.

But one has to go to the philosophy on fire, which is very similar to safeguards, which is to bring the plant to a safe shutdown mode, and when one looks at fire in these kind of dependent system vulnerabilities we ask the ultimate question: will a sufficient set of instruments and components survive which will allow you to get to safe shutdown? And that would assure a great degree of reliability.

That doesn't assure that the balance of the plant is going to survive.

MR. MICHELSON: Don't forget the basic assumption in doing that analysis, if I understand it correctly, is that you are not going to address the potential for unwanted actions from all this other equipment. You just pick out the set you need, make sure it is protected environmentally, and so forth. But you assume it is not being adversely interacted by the failure of other equipment in the fire area that was not related.

MR. RUBINSTEIN: To a limited degree, we do look

at independence and associated circuits, particularly through the electrical.

Jerry could probably expand on this.

MR. MICHELSON: I don't think we want a debate. That isn't my point.

MR. RUBINSTEIN: I just want to say that I don't want to leave it on the record that they are aspects that we don't look at.

MR. WARD: Go ahead, Doctor.

(Slide.)

DR. EL-BASSIONI: My last conclusion that we have is that if we take the numbers in the report literally and assume that it presents a typical system, then we think that the impact of common cause failure, which is dominating the unavailability of the auxiliary feedwater system and was giving credit of more than 99 percent contribution to the unavailability, we do not agree with that and we think that we can get more credit using diversity.

I think we had some discussions with Karl. Karl agrees that with certain plant specific features that we show independence between the trains. We can achieve greater values compared to the values that were mentioned in the report.

As Mr. Rubinstein has just indicated, we recognize that independence is the main factor for

improvement of the auxiliary feedwater system rather than throwing blindly redundant trains or having diversity just for the sake of diversity, and we won't allow things like common suction valves like the one in the example. This would be a very undesirable feature.

This concludes my comments.

MR. WARD: Okay. Thank you very much.

Karl?

MR. FLEMING: I wondered if I could just make a couple of comments about some of the conclusions just to maybe form somewhat of a rebuttal to some of the things you have said.

I am very appreciative of getting this feedback. I think it will have an impact on how we think about these things, but there is a couple of points I want to make.

The concern you have about the impact vectors and the subjective elements associated with that, I maintain that that is an unavoidable situation that an analyst faces.

I will further assert that all I have done is that I have invented a diagram on which to display what is going on in the analyst's head and trying to get away from having those necessary subjective value judgments be buried and how maybe Corey Atwood classified them as a lethal

shock.

DR. EL-BASSIONI: Can I respond to that?

(Laughter.)

MR. WARD: Go ahead.

DR. EL-BASSIONI: All what you are saying is that there is subjectivity there. You say it is unavoidable. But implicitly we are introducing another element of uncertainty, which is variability from one analyst to another, unless we provide some general rules or criteria that we have to follow, that we get to almost agreement on the generalization of these impact vectors. One of the elements was .9 and one was .1 and there is nothing in between. If it was my judgment, I would have a distribution.

You see what I mean? Unless we have some guidelines of how to generate this. This can be worked.

MR. WARD: But I don't think he really dealt with yours.

MR. FLEMING: I still won't agree that I have introduced this analyst variability.

MR. WARD: He says he is attempting to display something that is inherent in anybody's analysis.

MR. FLEMING: It does not introduce an uncertainty. After all, the analyst variability we have right now is dominated by whether common cause events are

DAVbur

even included in the analysis. That is certainly an analyst's subjective assumption.

All I am saying is it is an inherent uncertainty associated with doing the analysis, and whether you put it in the diagram or not I don't think is the question.

DR. EL-BASSIONI: Can I respond?

Implicit in that, if I play with these numbers and instead of .9 I use .99 and instead of .4 I use .01, then all of its impacts will not be shown and it will not be as significant.

MR. FLEMING: We have done sensitivity studies on that, and we have checked to see what kind of answers you would get if you throw out all these subjective events and assume they don't exist. It has very little impact on the results because the vast majority of the impact vectors are minor.

The other thing, I didn't see any real engineering reason why you would expect -- why you believe that the common cause failures have been overstated. But I would expect if such reasons could be presented that they could be boiled down to different interpretations of the data, and I think that further could basically be resolved in how well the analysts can document their analysis.

So I assert that it is not really a limitation of the method. It is maybe an issue of whether the given

1 DAVbur

interpretation of the data is correct or not.

I do agree that we need better procedures for coming up with these impact vectors. I think it is better to get them out on the table.

The business about the corrective actions, the thought that common cause failures we have corrective actions for with the implication that independent of that we don't, I don't think that is the way plants are really run. I think in any equipment failure some conscientious effort is made to try to prevent the reoccurrence of that event because if it is not a safety concern it is an economic concern to continue having to procure additional equipment, repair equipment, have the tech specs shut down, and so on and so forth. There is always an attempt, based on the utilities I have been involved with, to recover from the events, whether they be independent or common cause events.

As far as overburdening the analysis is concerned, I think that the basis -- the baseline from which we are judging the straw that broke the camel's back is based on a burden of analysis which, in my view, are based on the analysis of noncontributors.

So I think if there were some way to reduce the burden of all these independent events maybe we would have more room in our budgets to have staff working on it.

And as far as the comment on diversity, the

DAVbur

conclusions I reached on diversity were based on, admittedly, a human's interpretation of the data. But it was data from diverse systems that didn't really involve any subjectivity in terms of postulating something that is not out there.

And I think we should be able to resolve those kinds of differences just by getting the individual events out and discussing them.

That is all I have to say.

MR. WARD: Okay, thank you.

MR. RUBINSTEIN: My name is Les Rubinstein. I am the project director of the project director to the Westinghouse Division. I come to you under my own aegis as Assistant Director for Core and Plant Systems.

Basically, I am going to briefly review three items dealing with the staff's actions to upgrade the AFW reliability.

The first one is where in NRR --

MR. MICHELSON: Before you get started, are you going to be the one that tells me about how you are going to improve acquiring the reliability data, a question raised much earlier today?

And I have patiently waited through all these speeches and I haven't heard it yet. But the guys are fast disappearing now.

DAVbur

MR. RUBINSTEIN: I wasn't privy to your question. But before they disappear, I was not going to talk about changes in LER gathering or data acquisition.

MR. MICHELSON: I got the impression earlier today that before the end of the day I was going to hear what the staff thought about the quality of the reliability data available and perhaps I was going to hear what they were going to do about it. But maybe I just misread.

MR. RUBINSTEIN: Insofar as NRR, I can deal with the latter right now.

MR. MICHELSON: Did I misread what I heard earlier?

MR. WARD: Yes. We only -- you are really asking what AEOD is going to do, and then you want to know what NRR is going to demand that AEOD do.

MR. MICHELSON: When Dennig was giving his presentation, we were bemoaning the problem that the data was not all that good, he couldn't get information. We kind of inquired as to, well, how is this going to be corrected or what is the plan of action or what is going to happen. I kind of got the answer, I thought, well, wait until later today, we are going to hear all about it from the staff.

This is later today, and I haven't heard a word about what the staff is going to do, but I may have just thought I was supposed to hear it.

MR. RUBINSTEIN: Before you respond to that, let me say I would have talked more directly in the licensing arena what we had in mind than I am currently contemplating to do about upgrading the feedwater system. This would encompass a little beyond perhaps an analysis.

MR. MICHELSON: That won't answer my question.

MR. RUBINSTEIN: I understand that. However, what I tell you may transcend the question.

MR. THADANI: Les, I don't recall the specific question, but I think I am personally not aware if there are real problems with current reporting systems, whether we are getting quality data or not.

In my communication with Research staff, I am led to believe that the best source of information for PRAs would probably come from IPRDS and that there is a substantial amount of detail there. So you could actually assign a cause and determine whether that was a legitimate failure or not.

MR. MICHELSON: How many plants is that going to be done on?

MR. THADANI: As I understand, it is a voluntary program, and I think only a handful of plants are participating, as I have been told.

MR. MICHELSON: Maybe for the full committee meeting they could just give us a brief idea unless there is

a comment over here.

MR. HERNON: I would like to comment. If I recall, I asked you to repeat your question because I wasn't sure where it was directing us in this area and what is going to be done to improve the quality of the LERs.

MR. MICHELSON: I didn't say LER because I didn't mean just LER.

MR. HERNON: That is one source of data, is actual operating experience.

The other thing that reliability data could mean is some of these plants that we have no evidence would meet our present SRP criteria -- you know, do we have the latest information on those plants, because there are some hardware improvements. After they do that, of course, they should go back and review their reliability study.

This is new and better reliability data and new and better systems.

MR. MICHELSON: Are they using their own data or -- but I am looking for the real data.

MR. WARD: Carl, I got the impression that what you are asking about was really kind of an AEOD question. We are talking about aux feed systems here, and I guess we have seemed to come to the conclusion early on or I got the impression that the staff is struggling to get any useful information on aux feed reliability out of the AEOD

analysis of LERs.

MR. MICHEL.'ON: And they are struggling with just LERs, which in the first place doesn't tell you the number of demands, for instance.

MR. WARD: So it seems to me we have to address -- that is another subject.

MR. MICHELSON: I asked the question of AEOD, and I got the answer that staff was going to tell us later in the day. Perhaps I was dreaming at the time. I thought I heard the answer.

MR. HERNON: Danny did mention the fact that LER performance and the quality of the material in the LERs has been factored into the SALP process.

MR. MICHELSON: He mentioned that.

MR. HERNON: That was the only thing that is happening.

MR. MICHELSON: Apparently nothing additional is done to try to improve the quality of your reliability data. You know, you can do all kinds of calculations, but if the base numbers aren't too good, then the answers aren't too good.

I was wondering, is there anything going to be done to improve it because Dennig -- I thought he was saying that it isn't too good, we don't have good numbers, this is the best I could do from LERs.

DAVbur

In my mind, I said, well, there must be a better way. Is the staff trying to figure out if there is a better way, and what are they doing about it?

MR. HERNON: I did have a specific discussion with Jack Heltemes, and there is no intention at this time to change the LER rule.

MR. MICHELSON: I suspect that is right. Maybe the LER rule isn't the right way to tackle the problem either. I was hoping that you would tell me the best way to do this and what was being done. I wouldn't want to tell you because I haven't given it much thought.

I was mostly looking to see is there something in the program trying to come up with better numbers because I think they are very important numbers, so we can begin to believe them a little.

MR. THADANI: That is really where I was headed, and you are quite right. Even with IPRDS there are limitations, but we haven't got the results of the program yet as to the number of participants. If they are 50 percent participants, if you will, there may be some level of confidence it is not too bad.

The first word I got, which was quite sometime ago, was that it was maybe about 10, 15 percent participation in this program. It may have improved. At the time, I was told it will probably get better. But I

1 DAVbur

don't the answer to that.

We have a request out to Research. My own view would be that if you really want to hear it directly you ought to get Research staff here and ask them what they are doing because we go to Research to give us better data. They are the ones. They participate, by the way, in IPRDS, also, Research staff.

MR. MICHELSON: We're coming up to the program budget next month, so I was hoping to hear whether this was an area where we had a recommendation. Clearly, we've got to have good numbers. We've got to have better numbers at least than we have been dealing with.

So I was searching to see what was underway.

MR. WARD: I don't think this subcommittee or this meeting is the right window on it.

MR. MICHELSON: It's the only place we hear about it. We won't hear about it in the research program plan. They give you the one high-level big picture. This is lost down there.

MR. WARD: We might see enough. If you think there's a problem, you can recognize there's a problem. But I think you've got to get a handle on that somewhere else.

MR. MICHELSON: I don't know where else, Dave.

MR. WARD: But we're talking about aux feed systems.

MR. MICHELSON: That's all I'm asking as an example, aux feed.

MR. WARD: But is it only an example of general.

MR. MICHELSON: It's a very important system. It's a very important number that we should have. Dennig gave us the best of what he had. People didn't sound too happy with it, and I was wondering what are we going to do

to make it better.

MR. WARD: Okay. But if we have the meeting on scram breaker reliability, we're probably going to get the same impression about the quality of the data from that. It seems to be a problem, an evaluation of operational data.

MR. MICHELSON: I hope it's in better shape than this one is. That one has a different function. It is a safety-related function and it's been looked at much more carefully over time.

MR. WARD: Well, we'd better go on.

MR. MICHELSON: I'm sorry to have interrupted.

MR. RUBINSTEIN: It's quite all right. I'm coming at this from an entirely different aspect of your concerns today. The licensing staff has had for quite a while a number of considerations on how to upgrade the AFWS. First of all, I'd like to just as a bookkeeping item clearly identify in the transition that has gone from the Division of Systems Integration and the branch reporting to the Auxilliary Systems Branch to the Division ESRO, which is the division on Safety Review and Oversight. And the cognizant individual is Warren Minners, who is the chief of the Reactor Safety Issues Branch.

I don't believe anything is going to fall through the crack because we've been working both with Dennig and Minners in their old branches. They've been deeply involved

DAV/bc

in one of the aspects of the upgraded requirement.

The second thing is I'll talk a little about the status of the CRGR package and then those considerations which are prominent in our thinking on how we view the CRGR package. And to do that, I'll need just a little time to go back in history and to place in a different perspective what's in the SRP. And then in the context that I keep hearing it in the terms of what's in the SRP, Section 10-4-9.

The unavailability study, as Ashok said very well before, was used as an enhancement, as Jerry said, supplemented with the short and long-term guidelines of 0737 when we looked at the operating plants.

What it does is it nestles with the deterministic analysis. In and of itself, it is not an absolutely reliability analysis. It is a reliability analysis, as Jerry said, which allows you to compare one Westinghouse plant to another by the very nature of the data which it is derived from. The WASH-1400 data base, and the rules of the analysis and the methodologyit was designed to do that.

So when we talk in terms of low, medium and high ranges, 10 to the minus 3, 10 to the minus 4, 10 to the minus 5, one cannot take and put in it a frequency or a challenge frequency and recovery numbers and come up with some sort of a risk, because it excludes external events.

It doesn't deal with them at all. It deals with three rather limited initiating events which were prominent in the TMI accident and, in and of itself, we used it to gain some regularity on what I would describe in a minute or two on our narrow view of the auxilliary feedwater system as opposed to the broader view.

So with that as a preamble and building on what Wermiel said, what we have is, after the TMI accident, we have a set of analyses, which, clearly, we should have said yes in the case of B&W, they were found to be acceptable because they were guidelines and they were not put in 0737 as requirements.

However, the staff recognized that there were deficiencies in what was sitting out in the plants there at that time, and we were to address them in what I'll call the first CRGR package.

That was again trying to extend as a requirement that the operating reactors which had not met the unavailability numbers with the calculation as expressed in 06-11, for example, and say to them, okay, we've met with you. You've told me you're going to give me automatic start on 2E12, but you're sitting over here with two trains. Maybe you ought to do a little more. Maybe you ought to do a little more of this.

And they said, Well, here's where I am. This is

DAV/bc

my system as I so define it. Most reactors...pardon, most utilities were responsive. It turned out that some honestly felt that they had sufficiently reliable and well enough to find and met all the regulations systems, that they didn't want to do much work. And we're going to deal with that at the CRGR package.

At that time, we put it out to other divisions for review, and it became clear that it ought to be placed in the context with A45 and that it needed a better regulatory analysis. So we went back to the drawing board and then came Davis-Besse.

We were under some pressure to develop a more modern version of that. And we felt at the time that we would deal with this in a narrow sense of the word. We would deal with it isolating it, to say let us fix the hardware of the auxilliary feedwater system. We won't deal with it in the context of A45 and all these others.

The three things we had in what I will call the narrow view version post-Davis-Besse were make all PWR's demonstrate, using either the old 737 methodology and specific data, and it had not become finalized through analysis that they met the unavailability criteria of 10 to the minus 4, 10 to the minus 5, require that they meet power divergency criteria.

At the time, we wrote it immediately after Davis-

Besse. This was not true. Since then, they've fallen into line and, believe it or not, define your configuration because, in dealing with some of the utilities, it became clear -- and I'll give you an example in a moment -- that we really didn't know the post-TMI configurations as they had actually put them into the plants.

It was clear also that the analyses which were done prior to those changes, some had included the changes in the analyses and some had not. And some had voluntarily gone much further, that we found out in subsequent discussions, and had upgraded the startup feedwater pumps and had done other things in upgrading the power or the auto-start capabilities of some of the trains.

So one of the things we required is: Tell us what your feedwater system really is?

And we had one utility, which I'll try not to embarrass, who had a turbine-driven pump and two electrical pumps, and absolutely refused to accept that the turbine-driven pump was 100 percent capacity, was part of the feedwater system, the emergency feedwater system. They said it was part of their AFW.

We said, Well, then you don't need the power diversity requirement. They said, Well, we have the pump. We said that the pump isn't tech spec in terms of availability. Anyway, we settled that. But I wanted to

DAV/bc

give you a feel for the context of where we were.

Well, a little while ago, we sent our CRGR package to the divisions for review, and it came back that it was clear that we were not ready. One thing, the regulatory analysis. And I think you saw from Fleming's discussion and from many others' discussions with the staff, the benefit probably wouldn't cut it to get a third train in CRGR's. We had it constituted. Minners and Harold Vandermolen went back to work on that, and they've done some excellent work on that. That was coming along.

Some of the comments and some of the factors which I'm going to call the broadened view really dealt with the issue:

Can you deal with the feedwater system in this narrow view? And some of the comments today are very pertinent to this. Or, do you deal with the feedwater system in what I'll call the broadened view?

By that, I mean many of the owners' groups, and particularly B&W, have taken very strong steps to stop trips and are looking at the challenges from the loss of main feedwater. Our original CRGR package did not take this kind of thing into account.

Then, from the other end of the train came strong staff objections, which said:

How can you look narrowly at the feedwater system

without taking into account the benefits of an appropriate bleed and feed configuration and what it can do for you in decay heat removal?

We said, that is true, that is something that can't be done immediately.

So we got a comment that said, Gee, you've got to make it compatible with A-45, which was sort of like a deja vu of where we had been previously. And it was also clearly pointed out that you have to deal with common cause effects and do a little better job.

So, in a sense, what we've got is a package which was relatively narrowly scoped, wherein the final decisions have not been made as to how to broaden them, as to whether to broaden them. It is in the SRO. I think Spies and Minners are going to come to grips with it. It has to take into account the Davis-Besse short-term generic issues, the Davis-Besse long-term generic issues, A-45, other staff ongoing efforts.

For example, it wasn't clear to us when you looked at B&W plants the significance of the uprgrades that they had made in putting in the feed only good generators. Some of these have almost totally been insulated from some of the causes which caused main feedwater failure.

For example, the kind of thing that happened in Davis-Besse on some of the other plants is extremely low

DAV/bc

probability. The ICS and NNI are completely buffered from being an actor in causing the demand.

So we're in a situation now, and I can't give you a date, where the jury's still out. How to deal with it? I think it's going to go abroad. I, myself, was a proponent because I saw the opportunity after a couple of years to upgrade in a narrow sense the hardware on the feedwater system that didn't have much to do with the human factors or feed and bleed issues.

But I think it's in good hands now. And I can only say that there is no final NRR policy which says this is the way we're going to go, and we're going to systematically deal with these consideratins and come up with a policy, which we're going to pump back to CRGR.

I would hope it's on the order of months, a few months, rather than six. I'll take questions on it, but I hope I've cleared it up.

MR. EBERSOLE: In the aux feedwater spectrum of possibilities, and of course Palo Verde is invoked, you can get qualified grade secondary PORV's down to whatever pressure you want to, and pump in water from the sewage system, I guess, or whatever.

MR. RUBINSTEIN: I was here for the Palo Verde meeting.

MR. EBERSOLE: Does this augment the reliability

of the system? Is it considered as an adjunct method to improving the reliability?

MR. RUBINSTEIN: There's a school on the staff that definitely believes you should give credit for feed and bleed capability. In the case of Palo Verde --

MR. EBERSOLE: I'm talking just about the secondary.

MR. RUBINSTEIN: I understand. That's a narrow view if you talk only the secondary. If you talk only the secondary, then you darned well better deal with the AFW and make sure that it's reliable.

MR. EBERSOLE: We also found at that meeting, you may recall, that that didn't do much good to depressurize the primary.

MR. RUBINSTEIN: Yes, I do remember. But, for those plants which have modest feedwater unavailabilities, which are maybe borderline, on one or two times 10 to the minus 4, where they have an excellent feed and bleed, philosophically, we have never given directly credit for feed and bleed in the analysis.

When you start to deal with the staff or be in core performance people, we've never sat down and said you've got it. That's always been part of the defense indepth philosophy, that enhancement.

Now, in a sense, we may have to come to grips

with the question: Should I give credit for feed and bleed? How do I quantify it? And does it compensate for the feedwater system of slightly lower availability?

MR. EBERSOLE: It's interesting to observe, I think, how we work in different camps and we don't look across the borders in that the boilers of course use that method as one of the methods to go on. Now they're even invoking open boiling to atmosphere.

MR. RUBINSTEIN: Boilers have 13 ways of delivering water to the core. My buddies in General Electric always point out to me.

MR. EBERSOLE: At a variety of pressures.

MR. RUBINSTEIN: I think the staff's position is that the preferred heat removal capability be relied on through the secondary side, through the steam generators. This is how the plant was designed. This is how I saw it. This is why I press and I think the staff in general presses for an upgrading of the AFWS.

MR. EBERSOLE: It leaves the coupling mechanism from primary to secondary, which involves the delta V and delta T, and there's lots of ways of losing that.

MR. RUBINSTEIN: But then in the real world, if you are looking at the back end of the decay heat removal system, you may then start to rely on feed and bleed.

But also, I think the industry, through their owner's group -- and it shouldn't be ignored -- are making a large effort to reduce the number of main feedwater failures.

I would add that even A-44 is going to contribute to it. One of the main sequences we looked at is the loss of offsite power, and anything you can do in that regard, including B-56, which hopefully can upgrade the diesel generator a lot.

So we are looking at the subject a little more totally. We are interested in comments. If you feel strongly that the narrow view should prevail or the broad view --

MR. EBERSOLE: This challenge frequency bit is also important from an economic viewpoint.

MR. RUBINSTEIN: Oh, yes, they love it.

MR. EBERSOLE: So that is one incentive that the other doesn't have.

I recall an old philosophy that if you call a

1 DAVbur

safety system a safety system and it really is, it should never have to do its thing.

MR. RUBINSTEIN: That would be nice.

MR. WARD: Okay. Any other questions for Mr. Rubinstein?

(No response.)

MR. WARD: Thank you, Les.

We have one more topic, Mr. Hernon, about overseas practices.

MR. HERNON: Not really. What I am going to tell you is that Dr. Spies, who is probably the best prepared one to address this subject, prefers to wait for a couple of months and come down and talk about this area in general and in particular.

MR. WARD: Who is this?

MR. HERNON: Dr. Spies, and he wants to work this in with a planned presentation to the committee on his visit to the plant in France.

MR. WARD: Okay. Any questions for Mr. Hernon?

(Laughter.)

MR. HERNON: One other comment I did want to make. I gave Paul Boehnert a while ago several copies of an October 29th letter from Florida Power on Crystal River. This letter, I feel, is a very well-done submittal in that it summarizes the overall aux feedwater system reliability

problem at Crystal River.

It summarizes the NRC requirements that have emerged since TMI and very specifically indicates what Crystal River has done, including a reassessment of their system reliability study with the fixes on further reliability, and they also talk about a number of other things that have come up today, like their involvement with the owner's group and their effort to reduce trip frequency.

They talked about the environmental qualification aspects, and that answered Mr. Michelson's questions.

I think Paul has distributed this to you.

MR. DAVIS: Excuse me. On the last page of that letter, it indicates that by November of '85 they are going to have a system reliability assessment completed.

MR. HERNON: A reassessment.

MR. DAVIS: Has that been completed?

MR. HERNON: If you look on the second page of the letter, it is very close to completion. They draw out a number in this letter of 1.7 times 10 to the minus 4. I understand that has been inched up a little bit to 1.9. They are very close. But as far as I know, they haven't completed it yet.

MR. DAVIS: You haven't seen their facility?

MR. HERNON: I haven't.

MR. THADANI: It is not in yet.

MR. HERNON: I think realistically we are probably looking for it in January.

MR. EBERSOLE: Dave, one of the themes that I have heard here from time to time is the subject of environmental qualification of the combined steam-electric systems where the steam system has some potential of leaking seals, burst casing, or for whatever, to cause the common environments to be saturated with steam, which contain both the electric motor pumps as well as the steam pumps, that cause the problem.

I have been somewhat dismayed to find no particular rigidity and discipline or anything else to protect the electrical apparatus from this submerging in a steam atmosphere wherein the equipment must be initially somewhat subcooled from the condition it is going to and thus have quite general surface condensation over all the terminal boards and equipment, wherever electrical apparatus exists, which is critical to safety.

When this problem comes up, I see a run off to qualify in a partial way the environmental capability of the equipment by doing studies on leakage currents, how much functional electricity is left after part of it leaks to ground or leaks phase to phase, and in no way do I find a real attempt to enclose this apparatus and make it

independent of this environment that it is subject to.

I take it the staff is accepting these sort of half-shot methods of getting environmental capability this way on a more or less individual plant-by-plant basis and individual equipment-by-equipment basis.

Am I wrong?

MR. HERNON: I can point out what Crystal River has done. If you look at the very bottom of the next to the last page in this letter, they either have qualified the equipment for a harsh environment or replaced it.

MR. EBERSOLE: But when they qualify, they do it by these methods of attempting to measure the quantity being boiled and the degree of leakage current, and they attempt to make judgmental conclusions about whether there is enough working current without short circuits to survive the environmental conditions. They don't haul off and enclose the apparatus, as I think is the reasonably conservative practice.

MR. HERNON: I have no idea specifically.

MR. EBERSOLE: I think the staff needs to have some sort of equipment test conducted where a saturation environment is applied to common ordinary electrical apparatus and the dirty conditions that exist after 20 to 30 years of service, when the leakage current problem is a great deal different from what it is when it is washed

down.

I don't know of anybody that is going around scrubbing the electrical contacts on a monthly or yearly basis to provide this laboratory type of state in which the environmental qualifications were measured.

MR. WARD: Okay. I think that applies to several things. It is not particularly unique to the aux feed reliability issue.

MR. EBERSOLE: That is true.

MR. WARD: Let's see. Our intent here with this meeting was to begin to find out what the staff was doing in this area. There have been a number of events which have been a stimulus to some sort of regulatory activity toward understanding or improving aux feedwater systems.

I guess I have been a little disappointed that more real information isn't available from the operating experience data base, if there is a data base.

Most of the responses seem to be still at kind of the anecdotal responses to events rather than a comprehensive body of experience.

But be that as it may, staff does seem to have a program. It hasn't jelled, as Mr. Rubinstein told us. They still haven't decided on the narrow view or the broad view. He has indicated they are going to come back -- well, that they will be ready with a package proposal from NRR in

DAVbur

several months, less than six, and I guess I would like some subcommittee comments on what they think of the status of the issue.

I don't really -- we didn't plan to take anything to the full committee on it other than a five or 10-minute report. I don't think it is at the stage yet where the committee needs to hear something or where the committee will be making some recommendations.

But if you think there are some recommendations the committee ought to be making, I would like to hear about it.

MR. EBERSOLE: Dave, I notice one theme through this whole presentation is the notion that water should be got into the secondaries only by means of the main and auxiliary feed supplies, and I kept thinking about the benefits of the boiler having access to 13 or 14 sources of water by the process of depressurization and thus conditioning the secondary to receive water from whatever source is available, like the fire pumps.

I didn't hear any mention of this sort of thing, but I would certainly endorse the degree of flexibility that would permit getting water from anywhere, from the primary to the secondary. I would rather have a wet secondary, and I would find it anywhere I could get it.

MR. WARD: I guess there was an absence of that

1 DAVbur

sort of thing. I recall that in the analysis Combustion Engineering Owners Group credited getting condenser cooling.

MR. EBERSOLE: Even if I have to go up and crank open the PORVs and the safeties, I have got to get water to the secondary. That has to be an infallible process as far as I see it. Gravity feed if I could find it.

MR. WARD: Any other comments?

Harold?

MR. ETHERINGTON: I am afraid all I found out is how little I know about the subject.

MR. WARD: Carl?

MR. MICHELSON: I already knew how little I think I knew that.

I do have a problem on this question, of course, of how reliable is the present feedwater arrangement in the given plant. That will determine in part how much I really worry about fixing it.

It gets back to the questions which I think remain unaddressed, and that is: what is the staff going to do, if anything, about improving its knowledge of the reliability of the existing systems?

I sense the answer is nothing they aren't already doing. There is no additional program or no additional effort except perhaps through the IREP route of trying to

come up with better numbers.

MR. WARD: You mean the ORNL?

MR. MICHELSON: That is right. It is not IREP. It is going into the given plant and going into the details of all the operations and trying to find utilities that will let them go in and do it.

The point was that maybe 15 percent of the utilities will volunteer. Maybe they won't.

That seems to be the only source of new information on the reliability of these systems as far as I can tell, the only potential source.

MR. WARD: Why isn't more coming out of the AEOD analysis?

MR. MICHELSON: AEOD is dealing with LERs, which are not reliability oriented to begin with. They are just simply reporting that an event occurred and telling you about the event, but it doesn't tell you the number of challenges to the systems that occurred before the event, that sort of thing.

It is a one data point, and without other information it is of limited value because you don't, for instance, know the number of demands or the nature of the other demands.

You have to have quite a bit more information than just an LER, and not all the LERs have to be reported,

particularly if these people think that it is a nonsafety-related system. Then you don't have to report it at all.

DR. CATTON: AEOD is not limited just to LERs.

MR. MICHELSON: That is why I asked them did they use NPRDS in the study. The answer is no.

Now, they could go in and dig there, but you won't get the demands number out of the NPRDS system either.

You have to do some thinking about what do you really want to know and how do you go about getting it.

MR. WARD: What are we getting out of AEOD?

MR. MICHELSON: Just a detailed analysis of whatever LERs were submitted.

MR. WARD: But to what end?

MR. MICHELSON: It is very limited because it isn't suitable for LERs. It is a good deterministic tool. It tells you the kinds of failures that are occurring.

So it is helpful to the PRA people to be sure to include those kinds of scenarios in their analysis. But the PRA people have to have good reliability numbers on the components and/or the systems.

It is the same problem we have got with valves. We don't have good reliability numbers on valves either. We have got numbers that people are using, but their goodness

is somewhat in question.

MR. EBERSOLE: The main reason for that is the valves are rarely, if ever, tested under true duress.

MR. MICHELSON: Now, I would like to hear more about, you know, how good are the reliability numbers, how could they be improved, how do we presently test the systems, what is wrong with those tests in terms of counting them as real challenges, real demands.

I think it can be done. I don't believe it is a big undertaking. But I think we ought to feel that it is being done. I think we ought to feel the staff is searching for better numbers with which to judge these systems because I don't know how reliable they are presently.

But if I took Dennig's numbers somewhat literally, they don't look all that reliable. But that is limited; it is a one-year study. Statistically, the number of counts are so small that they are hard to use.

MR. WARD: I don't know.

Does there seem to be a consensus from the subcommittee that there is a problem with aux feed systems? Are we just reacting to press clippings, or can we agree that there really is some sort of a problem for which the staff should be addressing programs?

If so, does it look like the program we have heard about is going in the right direction?

2 DAVbur

MR. MICHELSON: Speaking for myself, I think the answer is yes. Read the LERs, and individually there are some serious events occurring to these auxiliary feedwater systems, and I think we have to react to those events with appropriate corrective actions.

Now, how those corrective actions will improve the reliability is a little bit of a question because I don't see good reliability. You know, I don't see a good analysis of the reliability of the present system. Therefore, it is hard to judge what changes would be useful to make.

Clearly, I think there's a problem, unless I'm misreading the LERs,

MR. WARD: Ivan, do you have some comments?

DR. CATTON: I have several comments.

I thought that the summary on operating experience was rather poor.

I think AEOD needs more analysis to supplement the numbers. A more inquisitive pursuit of reasons behind the numbers would be very helpful, and I think maybe necessary to make them meaningful. To just put the numbers up there doesn't serve much purpose.

The auxiliary feedwater testing was mentioned, and from what Carl tells me, this was only done in a research mode. That's only a partial test. It misses the kind of things that Jesse was referring to. I don't understand why they can't test it completely. If thermal shock is a problem, test it during refueling. That area needs to be looked into a little bit.

One wonders what is an ESF and what is not, and who decides. That never did become clear.

It seems to me that NRC ought to require that all of the auxiliary feedwater systems be classified as ESFs and be done with it. I don't know why some were and some were not.

MR. EBERSOLE: In the ESF category, if you're

DAVbw

looking at the FSARs and all the old classical literature, there's a very limited number of pieces in there that are called ESF items or equipment items. All of it relevant to LOCAs. That's all it is. That was the whole safety picture for 20 years.

DR. CATTON: Maybe they ought to upgrade some of them. I didn't understand the discussion of safety grade and safety-related. It seems to me the difference is clear. In one case, you make it safety grade. And I didn't understand whether a safety-related system has to be safety-related, or does it have to be safety grade. I didn't understand it at all.

There seem to be two views about whether auxiliary feedwater systems were ESFs or not. Jerry's presentation implied that they all were, as well as Dennig's presentation. A part of the arguments for not having complete information was that they were not.

MR. EBERSOLE: Let me ask Staff, is there a possibility that one could take a hard line and just come along and forcibly say what are engineering safety features, ESFs, and clear up this muddy business about categorization of equipment?

MR. HERNAN: I suspect we already have that information in FSARs or SERs.

MR. MICHELSON: If it isn't, what can you do

about it?

VOICE: So what, if it is or is not an ESF?

MR. EBERSOLE: I guess that's true, as long as it has the same material qualifications.

VOICE: That's safety-related.

MR. WARD: I think they told us that before '75 aux field systems were not safety grade, safety related. Those two terms means the same thing.

Post-'75, they are safety grade. Now there is some questions about to what extent they have really upgraded the older systems to be the equivalent of safety grade.

DR. CATTON: Some have tech specs, some don't.

MR. WARD: They all have tech specs, but we don't know what that means. We don't know whether that means the equivalent.

DR. CATTON: Dennig said some didn't, but were going to.

MR. EBERSOLE: There was a statement made that safety-related was easier to understand as a description of something than safety grade. I would take the reverse view.

MR. WARD: Jesse, let's not talk about that. That's an old argument.

MR. EBERSOLE: Safety grade is rather clear.

DR. CATTON: I think so too. Coming from a more deterministic side of the fence, I was somehow very comforted by Carl's presentation. I liked the sort of thing he was doing. I was very disappointed to see that only PL&G is involved in the European benchmark exercise, and I think these benchmrk exercises are very good, and they bring a bunch of people together, and one technique gets tested against another.

I would think that NRC would sponsor one of their contractors. PL&G is basically a PRA manufacturer for the utilities, not for the NRC, yet NRC is sponsoring them. I think they would sponsor one of the national labs or somebody who does their PRAs.

Also, I really liked the recommendation that Carl made about the analyst and his documentation and rationalization for what he does. It seems to me that doing so would give the PRA numbers much more credibility than they presently have.

MR. WARD: Thank you. Pete?

MR. DAVIS: Just a couple of brief things.

I think, Dave, maybe we should consider having INPO come in and give us an assessment of what they found on auxiliary feedwater. I know they've done quite an extensive look at the problems and have talked to most of the utilities and have investigated several plants. In addition

DAVbw

to INPO, I know EPRI and NSAC have both been doing some things on decay heat removal.

In fact, last month, our report was published on the Brunswick plant and its decay heat removal capability, so I think there are some other things going on and other sources of data that people are gathering, other than what the NRC has.

I am somewhat comforted by NRC's approach to look for the outliers. That's always been my concern. Since there isn't strict design criteria for auxiliary feedwater system, you can expect to find a rather broad spectrum of reliability, and I think we ought to be looking for the bad ones, and I think a lot has been done to identify those and make some fixes.

One final comment. It's my belief that the utility has got to be the place where these system reliabilities are really concentrated. If the utility is not aware of the significance of aux feed and doesn't understand how their systems operate, I don't think anything NRC does is going to make them reliable.

I really think the utility needs to be made aware that they have a system that's very important, and they need to pay attention to it.

It's not clear to me that's being done. I don't think it should depend on the NRC to take care of all these

problems and watch all the data and make sure all the modifications are not destroying reliability.

Thank you.

MR. WARD: Thank you, Pete.

We'll discuss what we've heard here today with the full committee later this week.

I think that out of that discussion we'll decide on some course of action for this subcommittee, as far as further review of the issue.

MR. HERNAN: Could I briefly respond to one of Dr. Catton's comments on the recirc flow versus the full test flow.

If you look at the last page of the Crystal River document I gave you --

DR. CATTON: I just got it.

MR. HERNAN: One of the items is that we made them commit to a full flow for the aux feedwater system after each cold shutdown.

That was quite an issue, and they fought it, but the reason they fought it was not internal stress or anything, it was because it gave them a fairly good opportunity to put corrosion products in their steam generators, which they didn't want. They wanted to try to keep their feedwater very clean.

MR. MICHELSON: What are they going to use for

steam?

MR. HERNAN: Corrosion products.

MR. MICHELSON: What do they intend to use for steam to get a full flow test? Is this going to be after their return to power?

MR. HERNAN: Yes. On the power.

MR. MICHELSON: They've still got a thermal problem.

MR. HERNAN: But their issue was geting crap in their steam generators.

MR. MICHELSON: Where was it coming from?

MR. HERNAN: The condensate storage tank.

MR. MICHELSON: Yes.

MR. HERNAN: The water sits there and stagnates.

MR. MICHELSON: It sounds fine.

MR. WARD: We'll recess the meeting, reconvening tomorrow morning at 8:30 on another subject.

(Whereupon, at 6:30 p.m., the subcommittee meeting was adjourned, to reconvene at 8:30 a.m., Tuesday, December 3, 1985.)

CERTIFICATE OF OFFICIAL REPORTER

This is to certify that the attached proceedings before the UNITED STATES NUCLEAR REGULATORY COMMISSION in the matter of:

NAME OF PROCEEDING: ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON DECAY HEAT REMOVAL SYSTEMS

DOCKET NO.:

PLACE: WASHINGTON, D. C.

DATE: MONDAY, DECEMBER 2, 1985

were held as herein appears, and that this is the original transcript thereof for the file of the United States Nuclear Regulatory Commission.

(sigt) David L. Hoffman

(TYPED)

DAVID L. HOFFMAN

Official Reporter

ACE-FEDERAL REPORTERS, INC.

Reporter's Affiliation

1984 AUXILIARY FEEDWATER SYSTEM
OPERATING EXPERIENCE

PRESENTATION TO THE
ACRS SUBCOMMITTEE ON DECAY
HEAT REMOVAL SYSTEMS

OFFICE FOR ANALYSIS AND EVALUATION
OF OPERATIONAL DATA

DECEMBER 2, 1985

OPERATING DEMAND ESTIMATE

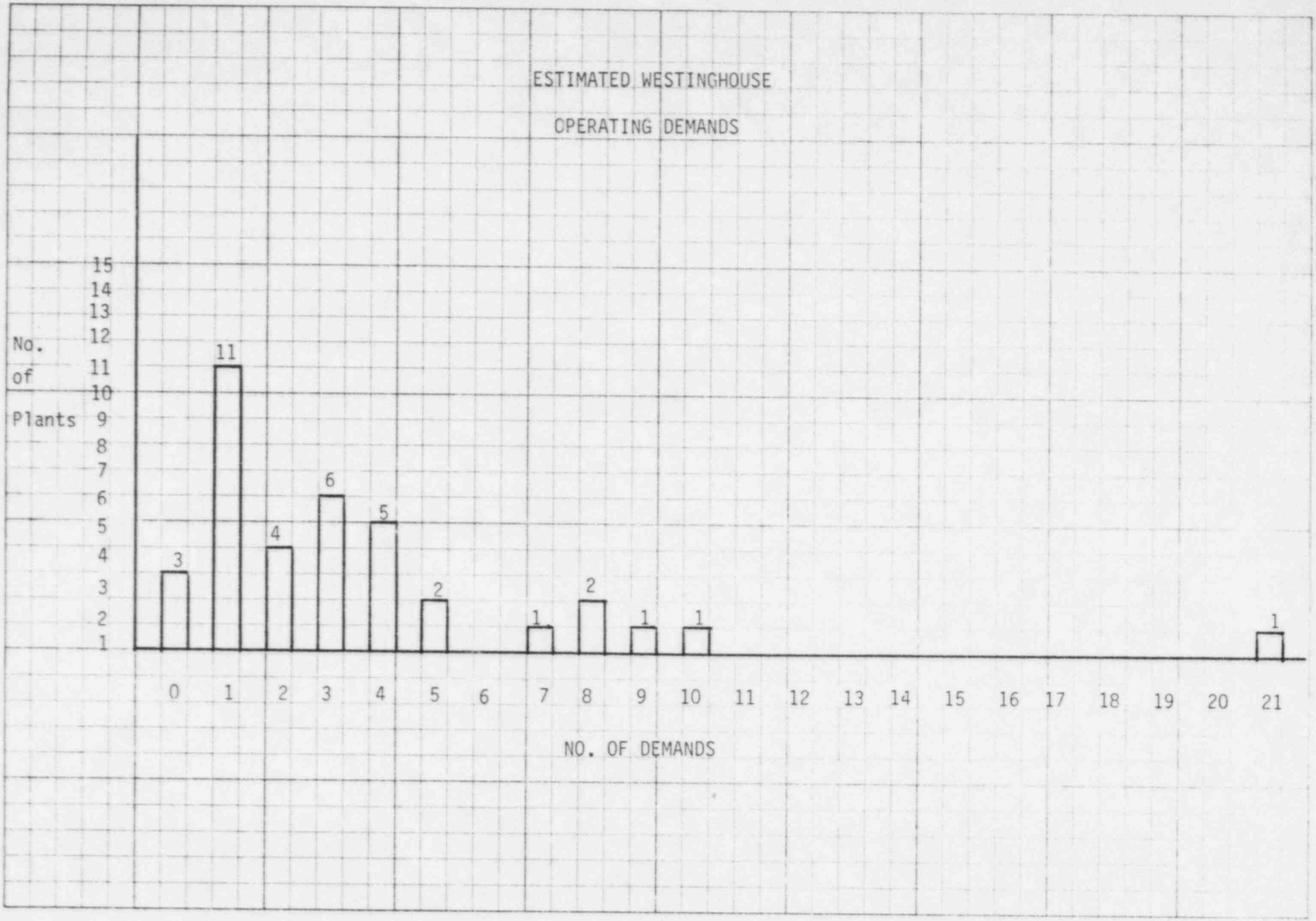
- 10 CFR 50.73(A)(2)(IV) REQUIRES REPORTS OF ALL ESF ACTUATIONS, BUT
  - AUXILIARY FEEDWATER SYSTEM NOT CONSISTENTLY CLASSIFIED AS AN ESF
  - MAY ACTUATE AS PART OF ANOTHER REPORTABLE EVENT, I.E. REACTOR TRIP, AND NOT STATED EXPLICITLY
- USED SYSTEM START SIGNALS + REACTOR TRIP SIGNALS, ESF ACTUATIONS TO ESTIMATE LOWER BOUND ON ACTUAL DEMANDS
  - PLANT TO PLANT VARIATIONS
  - VARIATIONS FOR TURBINE DRIVEN VS MOTOR DRIVEN

WESTINGHOUSE PWRS

- SYSTEM START SIGNALS
    - LO LO STEAM GENERATOR LEVEL
    - SAFETY INJECTION

- ESTIMATE OF DEMANDS
    - REACTOR TRIPS FROM LO LO SG LEVEL
    - SYSTEM STARTS REPORTED AS ESF ACTUATIONS
    - SAFETY INJECTION SIGNALS REPORTED AS ESF ACTUATIONS
    - ELIMINATED OVERLAP

- 130 DEMANDS FROM 34 OF 37 PLANTS LICENSED IN 1984



ESTIMATED WESTINGHOUSE
OPERATING DEMANDS
No. of Plants
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
11
6
5
4
3
2
1
2
1
1
1
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
NO. OF DEMANDS

COMBUSTION ENGINEERING

- START ON LO STEAM GENERATOR LEVEL
- ESTIMATE OF DEMANDS
  - REACTOR TRIPS FROM LO STEAM GENERATOR LEVEL
  - SYSTEM STARTS REPORTED AS ESF ACTUATIONS
  - ELIMINATED OVERLAP
- 22 DEMANDS FROM 8 OF 12 PLANTS LICENSED IN 1984
  - HIGH VALUE OF 6
  - AVERAGE OF APPROXIMATELY 2 PER PLANT PER YEAR

BABCOCK AND WILCOX

- START ON LOSS OF BOTH MAIN FEED PUMPS, VARIOUS OTHER

- DEMAND ESTIMATE BASED ON ESF ACTUATION REPORTS ONLY
  - 3 STARTS AT 2 OF 7 UNITS LICENSED IN 1984

REPORTED OPERATING PRORLEMS

- PARAGRAPH 50.73(A)(2)(v) REQUIRES REPORTING OF:

  "(v) ANY EVENT OR CONDITION THAT ALONE COULD HAVE PREVENTED THE FULFILLMENT OF THE SAFETY FUNCTION OF STRUCTURES OR SYSTEMS THAT ARE NEEDED TO:

  (A) SHUT DOWN THE REACTOR AND MAINTAIN IT IN A SAFE SHUTDOWN CONDITION;

  (B) REMOVE RESIDUAL HEAT;

  (C) CONTROL THE RELEASE OR RADIOACTIVE MATERIAL; OR

  (D) MITIGATE THE CONSEQUENCES OF AN ACCIDENT.

- AUXILIARY FEEDWATER PROBLEMS FOUND IN REPORTS FOR:
  - ESF ACTUATIONS [50.73(A)(2)(IV)]
  - TECH SPEC VIOLATIONS [50.73(A)(2)(I)]
  - COMMON CAUSE [50.73(A)(2)(VII)]
  - DEGRADED CONDITION [50.73(A)(2)(II)]
  - SYSTEM FAULT [50.73(A)(2)(V)]

REPORTED OPERATING PROBLEMS

- WESTINGHOUSE
  - 1 SYSTEM (ALL TRAINS) FAILURE ON DEMAND
  - 1 MD SUBSYSTEM FAILURE DURING SG FILL
  - 2 TRAIN LEVEL FAILURE ON TEST
  - 9 ALL OR PART UNAVAILABLE FOR POTENTIAL DEMAND
    - DOES NOT MEET DESIGN SPECIFICATIONS, INCLUDING SEISMIC

- COMBUSTION ENGINEERING
  - 2 TRAIN LEVEL FAILURE ON DEMAND
  - 2 TRAIN LEVEL FAILURE ON TEST
  - 3 ALL OR PART UNAVAILABLE FOR POTENTIAL DEMAND

- BABCOCK AND WILCOX
  - 1 SYSTEM FAILURE ON DEMAND
  - 2 TRAIN LEVEL PARTIAL FAILURE ON DEMAND
  - 1 UNAVAILABLE FOR POTENTIAL DEMAND

EVOLUTION OF STAFF REVIEW OF THE
AUXILIARY FEEDWATER SYSTEM (AFWS)

° STAFF CRITERIA FOR AFWS DESIGN PRIOR TO ISSUANCE OF THE SRP (1975) SPECIFIED GOOD ENGINEERING PRACTICE

° PLANTS REVIEWED AGAINST THE SRP (1975 TO PRESENT) HAVE PROVIDED A "SAFETY-RELATED" SYSTEM

° A REVIEW OF THE AFWS IN PLANTS LICENSED PRIOR TO THE TMI-2 ACCIDENT (1979) WAS UNDERTAKEN BY THE B&O TASK FORCE

  ° BOTH A DETERMINISTC AND PROBABILISTIC EVALUATION OF RELIABILITY WAS PERFORMED BY THE STAFF

  ° RESULTS WERE PUBLISHED IN NUREG-0611 AND NUREG-0635 FOR WESTINGHOUSE AND COMBUSTION ENGINEERING PLANTS RESPECTIVELY

  ° B&W PLANTS PERFORMED THEIR OWN AFWS RELIABILITY STUDIES (BAW-1584) WHICH WERE REVIEWED BY THE STAFF

° ALL PLANTS WERE REVIEWED AGAINST THE CRITERIA OF NUREG-0737, ITEMS II.E.1.1 AND II.E.1.2 IN ORDER TO IMPROVE AFWS AVAILABILITY AND FOUND ACCEPTABLE

- ALL PLANTS WERE REVIEWED AGAINST CRITERIA OF GENERIC LETTER 81-14 TO IMPROVE AFWS SEISMIC RESISTANCE AND FOUND ACCEPTABLE WITH EXCEPTION OF OCONEE

- SRP SECTION 10.4.9 WAS REVISED JULY 1981 TO INCORPORATE NUMERICAL RELIABILITY CRITERION, 10^{-4} TO 10^{-5} /DEMAND BASED ON KNOWLEDGE GAINED DURING B&O TASK FORCE REVIEWS

  - ALL PWRS NOT REVIEWED IN NUREG-0611 AND NUREG-0635 AND LICENSED AFTER THE TMI-2 ACCIDENT SUBMITTED A RELIABILITY STUDY UTILIZING A COMPARABLE APPROACH

    - THESE PLANTS (12 TOTAL) COMPLY WITH THE SRP RELIABILITY GOAL

  - CURRENT NTOLS COMPLY WITH THE SRP RELIABILITY GOAL

- STAFF REVIEW OF AFWS RELIABILITY IN OPERATING PLANTS HAS CONTINUED SINCE COMPLETION OF THE ABOVE ACTIONS

  - CRGR PACKAGE UNDER DEVELOPMENT - STATUS ADDRESSED IN SUBSEQUENT DISCUSSION

PWRS LICENSED AFTER THE TMI-2 ACCIDENT
WHICH SATISFY THE AFWS RELIABILITY GOAL

DIABLO CANYON 1 & 2

BYRON 1 & 2

CALLAWAY

CATAWBA 1 & 2

ST. LUCIE 2

McGUIRE 1 & 2

PALO VERDE 1, 2, 3

SAN ONOFRE 2 & 3

SEQUOYAH 1 & 2

SUMMER

WATERFORD

WOLF CREEK

NRR STAFF PRESENTATION TO THE
ACRS

SUBJECT: APPLICATION OF AFW RELIABILITY REQUIREMENTS

DATE: DECEMBER 2, 1985

PRESENTER: RONALD K. FRAHM

PRESENTER'S TITLE/BRANCH/DIV: SECTION LEADER
RELIABILITY AND RISK ASSESSMENT BRANCH
DIVISION OF SAFETY TECHNOLOGY

PRESENTER'S NRC TEL. NO.: 492-7112

SUBCOMMITTEE: DECAY HEAT REMOVAL SYSTEMS

I. METHODOLOGY (NUREG 0611)

- SRP 10.4.9 REQUIRES AFWS UNAVAILABILITY RANGE OF 10^{-5} TO 10^{-4} FAILURE PROB/DEMAND. HOWEVER CAN USE OTHER MEANS OF DECAY HEAT REMOVAL.

- NUREG 0611 REQUIREMENTS
  - ASSESS RELATIVE RELIABILITY COMPARISONS OF VARIOUS AFWS DESIGN (PURPOSE)
  - NO SPECIFIC COMMON CAUSE EVALUATION
  - USE EVENT TREES (INDUCTIVE LOGIC)
  - FAULT TREES (DEDUCTIVE LOGIC)
  - 0611 DATA BASE TO QUANTIFY TREES
  - ANALYZE LOFW, LOOP, LOAC

- 0611 HAS RESULTS FOR OPERATING PLANTS

- AFWS EVALUATION INCLUDES HARDWARE FROM THE WATER SOURCE TO THE AFW NOZZLE ON THE SG. SUPPORT SYSTEMS ANALYZED QUALITATIVELY NO HIGH ENERGY LINE BREAK OR EXTERNAL EVENTS

- STAFF REVIEW (ASSISTED BY BNL & SNL)
  - DOMINANT CONTRIBUTORS FOR EACH INITIATOR (MAINTENANCE, AND HARDWARE FAILURE OF PUMPS, VALVES, ACTUATION LOGIC)
  - SINGLE/COMMON MODE FAILURES

- 0611 RESULTS ARE POINT ESTIMATES WITH LARGE UNCERTAINTY
- IMPROVEMENTS IDENTIFIED (AUTO SWITCHOVER, ACTUATION LOGIC, ALTERNATE WATER SOURCES)

II. STAFF REVIEW OF RECENT OL APPLICATIONS

- REVIEWED 17 PLANTS
  - 2 TRAIN AFWS (I. E., ANO-1, CR-3, DB-1, RANCHO SECO)
  - 3 TRAIN AFWS (I. E., CATAWBA, SEABROOK, MIDLAND, WATERFORD, SUMMER)
  - 2 TRAIN AFWS UNAVAILABILITY

    LMFW ABOUT 10^{-3} TO 10^{-4} RANGE

    LOOP ABOUT 10^{-3} TO 10^{-4} RANGE

    LOAC ABOUT 10^{-1} TO 10^{-2} RANGE

  - 3 TRAIN AFWS UNAVAILABILITY

    LMFW IN 10^{-4} TO 10^{-5} RANGE

    LOOP IN 10^{-4} TO 10^{-5} RANGE

    LOAC IN 10^{-1} TO 10^{-2} RANGE

III. 1969 - 1981 PRECURSOR STUDY

- STUDY REVIEWS LERs TO IDENTIFY AND CATEGORIZE PRECURSORS TO POTENTIAL CORE DAMAGE ACCIDENTS

- LER SCREENING PROCESS FOR SEQUENCE PRECURSOR
  - REVIEW ACCIDENT SEQUENCE
  - REVIEW SYSTEM DESIGN
  - REVIEW PLANT ACCIDENT ANALYSIS TO DETERMINE WHICH AFFECTED SYSTEMS ARE REQUIRED TO FUNCTION

- SELECT LER ACCIDENT PRECURSOR
  - ESTIMATE AVERAGE FREQUENCY AND FAILURE PROBABILITY FOR INITIATING EVENTS AND FUNCTION FAILURES

  - INITIATING FREQUENCY AND FUNCTION FAILURE ESTIMATES USED IN CONJUNCTION WITH EVENT TREES TO ESTIMATE CONDITIONAL CORE DAMAGE PROBABILITY

  - CONDITIONAL PROBABILITY ASSOCIATED WITH EACH PRECURSOR USED TO RANK PRECURSOR, IDENTIFY DOMINANT SEQUENCES, RANK SAFETY FUNCTIONS AND ESTIMATE INDUSTRY AVERAGE CORE DAMAGE FREQUENCY

- RESULTS
  - PRECURSORS INVOLVING COUPLED FAILURES STILL OBSERVED: PRIMARILY CAUSED BY ELECTRICAL FAULTS
  - IN 1980 - 1981: NUMBER OF PWR INITIATING EVENTS AND FUNCTION FAILURES (RECOVERY CONSIDERED) WAS LESS THAN 1969-79 PRECURSOR STUDY

- ADDITIONAL RISK REDUCTION PWRs: FEED AND BLEED
  BWRs: LONG TERM CORE COOLING

- DOMINANT SEQUENCES

  PWR

  - SLOCA WITH RECIRCULATION FAILURE
  - DC BUS FAILURE NON-RESTORATION AND AFW
  - LOFW AND F&B FAILURE

  BWR

  - LOFW WITH FAILED L.T. CORE COOLING
  - LOFW WITH HPCI/RCIC FAILED
  - LOFW WITH SCRAM AND SBLC FAILURE

- AFW UNAVAILABILITY APPROXIMATELY 10^{-3}
  - MOST FAILURES RECOVERABLE

A SYSTEMATIC PROCEDURE FOR THE INCORPORATION OF COMMON CAUSE EVENTS INTO RISK AND RELIABILITY MODELS

by
KARL N. FLEMING
ALI MOSLEH
R.KENNETH DEREMER

Presented at
INTERNATIONAL POST-CONFERENCE SEMINAR
8th INTERNATIONAL CONFERENCE ON
STRUCTURAL MECHANICS IN REACTOR TECHNOLOGY (SMiRT-8)
Brussels, Belgium
August 26-27, 1985

Pickard, Lowe and Garrick, Inc.
Engineers • Applied Scientists • Management Consultants
Newport Beach, CA   Washington, DC

COMPONENT LEVEL MINIMAL CUTSETS FOR EXAMPLE SYSTEM – NORMAL ALIGNMENT

Number of Minimal Cutsets	Symbol*	Cutset Description
1	C	Common Suction Path
4	V^3	Three Valves
1	P^3	Three Pumps
1	TP^2	One Turbine and Two Pumps
2	MP^2	One Motor and Two Pumps
2	MTP	One Motor, One Turbine, One Pump
1	M^2P	Two Motors, One Pump
1	M^2T	Two Motors, One Turbine
4	VP^2	One Valve, Two Pumps
4	VTP	One Valve, One Turbine, One Pump
4	VPM	One Valve, One Pump, One Motor
4	VTM	One Valve, One Turbine, One Motor

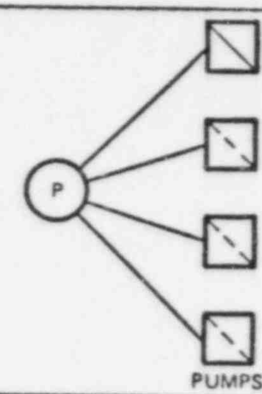
29 TOTAL

ALGEBRAIC EQUIVALENT OF THE MINIMAL CUTSETS FOR NORMAL ALIGNMENT (A_1)

Independent Terms [covering 29 minimal cutsets]	Common Cause Terms [covering 100 minimal cutsets]
C	V_4
$+ 4V_1^3$	$+ P_3$
$+ (P_1 + T)(P_1 + M_1)(P_1 + M_1)$	$+ 4V_3$
$+ 4V_1 (P_1 + T)(P_1 + M_1)$	$+ 12V_2V_1$
	$+ 15V_2^2$
	$+ 10P_1V_2(P_1 + T)$
	$+ 10P_1V_2M_1$
	$+ 10V_2P_2$
	$+ 10V_2M_1T$
	$+ 3P_1P_2$
	$+ 3P_2^2$
	$+ 2P_2M_1$
	$+ 2P_2M_2$
	$+ 4P_2V_1$
	$+ P_2T$
	$+ M_2P_1$
	$+ M_2T$

Approaches to look at data at the cause level and evaluate design specific implications via the impact of the cause

ANALYSIS OF A SINGLE COMMON CAUSE EVENT PRIOR TO PARAMETER ESTIMATION

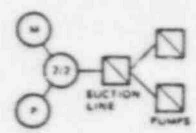
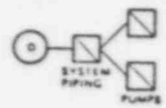
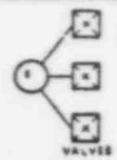
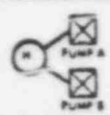
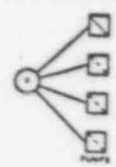
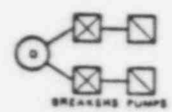
Plant (Date)	Status	Event Description	Cause-Effect Diagram
Point Beach 1 and 2 (April 1974)	Power	Preoperation strainers left in suction line plugged, making motor-driven AFW pump A on Unit 1 inoperable. Similar strainers were found in Unit 1 motor-driven AFW pump B and Units 1 and 2 turbine-driven AFW pumps.	

EVENT CLASSIFICATION

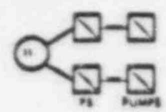
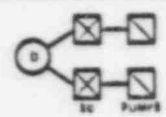
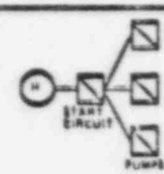
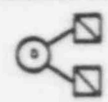
DATA is sparse and FUZZY
Can't APPEND to partition IT.

Plant	P_0	P_1	P_2	P_3	P_4	N/A	Shock Type	Fault Mode
Point Beach	0	.9	0	0	.1	0	Lethal (L)	Fail To Start (S)
Example System	0	.9	0	.1	0	0		
Plant Y	0	0	0	0	0	1		

CLASSIFICATION AND IMPACT ASSESSMENT OF EVENTS INVOLVING DEPENDENT FAILURES AND UNAVAILABILITIES OF AUXILIARY FEEDWATER PUMPS

Plant (date)	Status	Event Description	Cause-Effect Diagram	Application	P_0	P_1	P_2	P_3	P_4	N/A
Ginna (December 1973)	Critical	Two motor-driven auxiliary feedwater pumps inoperable due to air in common suction line.		Ginna	0	0	1	0	0	0
				Grohnde	0	0	0	0	0	1
Zion 2 (February 1974)	Power Escalation Test	Two motor-driven auxiliary feedwater pumps inoperable due to air in suction lines.		Zion 2	0	0	1	0	0	0
				Grohnde	0	0	0	0	0	1
Kewaunee (November 1975)	Shutdown	Resin clogged auxiliary feedwater pump strainers causing reduced flow.		Kewaunee	0.9	0	0	0.1	0	0
				Grohnde	0.9	0	0	0	0.1	0
Turkey Point 3 (May 1974) (two events)	98% Power	Auxiliary feedwater pumps A and B failed to start due to tight packing. Pump C started, but tripped due to governor failure.		Turkey Point 3	0	0	1	0	0	0
				Grohnde	0	0	0	0	0	1
Point Beach 1 and 2 (April 1974)	Power	Preoperation strainers left in suction line plugged, making motor-driven auxiliary feedwater pump A on Unit 1 inoperable. Similar strainers were found in Unit 1 motor-driven auxiliary feedwater pump B and Units 1 and 2 turbine-driven auxiliary feedwater pumps.		Point Beach 1	0	0.9	0	0	0.1	0
				Grohnde	0	0.9	0	0	0.1	0
Zion 2 (September 1981)	Shutdown	All three auxiliary feedwater pumps failed to start. Pumps 2B and 2C failed due to a backfeed circuit that resulted from pump control switch modification. Failure of pump 2A was due to a pressure switch drift.		Zion 2	0	0	1	0	0	0
				Grohnde	0	0	0	0	0	1

CLASSIFICATION AND IMPACT ASSESSMENT OF EVENTS INVOLVING DEPENDENT FAILURES AND UNAVAILABILITIES OF AUXILIARY FEEDWATER PUMPS (CONTINUED)

Plant (date)	Status	Event Description	Cause-Effect Diagram	Application	P_0	P_1	P_2	P_3	P_4	N/A
Zion 2 (November 1979)	Power	Auxiliary feedwater pumps 2B and 2C failed to start due to miscalibrated pressure gauges.		Zion 2	0	0	1	0	0	0
				Grohnde	0	0	0	0	0	1
Zion 2 (December 1979)	Power	Auxiliary feedwater pumps 2B and 2C failed to start due to start circuitry design problem.		Zion 2	0	0	1	0	0	0
				Grohnde	0	0	0	0	0	1
Turkey Point 4 (June 1973)	Prior to Initial Power Testing	All three auxiliary feedwater pumps failed to start automatically due to missing fuses in pump autostart circuit.		Turkey Point 4	0	0	0	0	0	1
				Grohnde	0	0	0	0	0	1
Arkansas One 2 (April 1980)	0% Power	Two emergency feedwater pumps lost suction due to steam flushing; system design problem.		ANO 2	0	0	1	0	0	0
				Grohnde	0	0	0.9	0	0.1	0
				Total	0.9	0.9	0.9	0	0.3	7

LEGEND:

Cause-Effect Diagram:

M - Maintenance
P - Procedural Error
D - Design Error
E - Environmental
I - Internal Failure
H - Human Error

COMMON CAUSE DATA SUMMARY WORK SHEET FOR DIESEL-DRIVEN AUXILIARY FEEDWATER PUMPS

COMPONENT: EFW PUMP AND DIESEL BLOCK

FAILURE MODE: ALL

GROUP SIZE: 4

IMPACT VECTOR:

n_0	n_1	n_2	n_3	n_4	n_5	n_6	N/A*
5.4	3.6	4.4	1.4	10.2	—	—	7

OTHER INDEPENDENT EVENTS = 628.1

MGL MEAN VALUES:

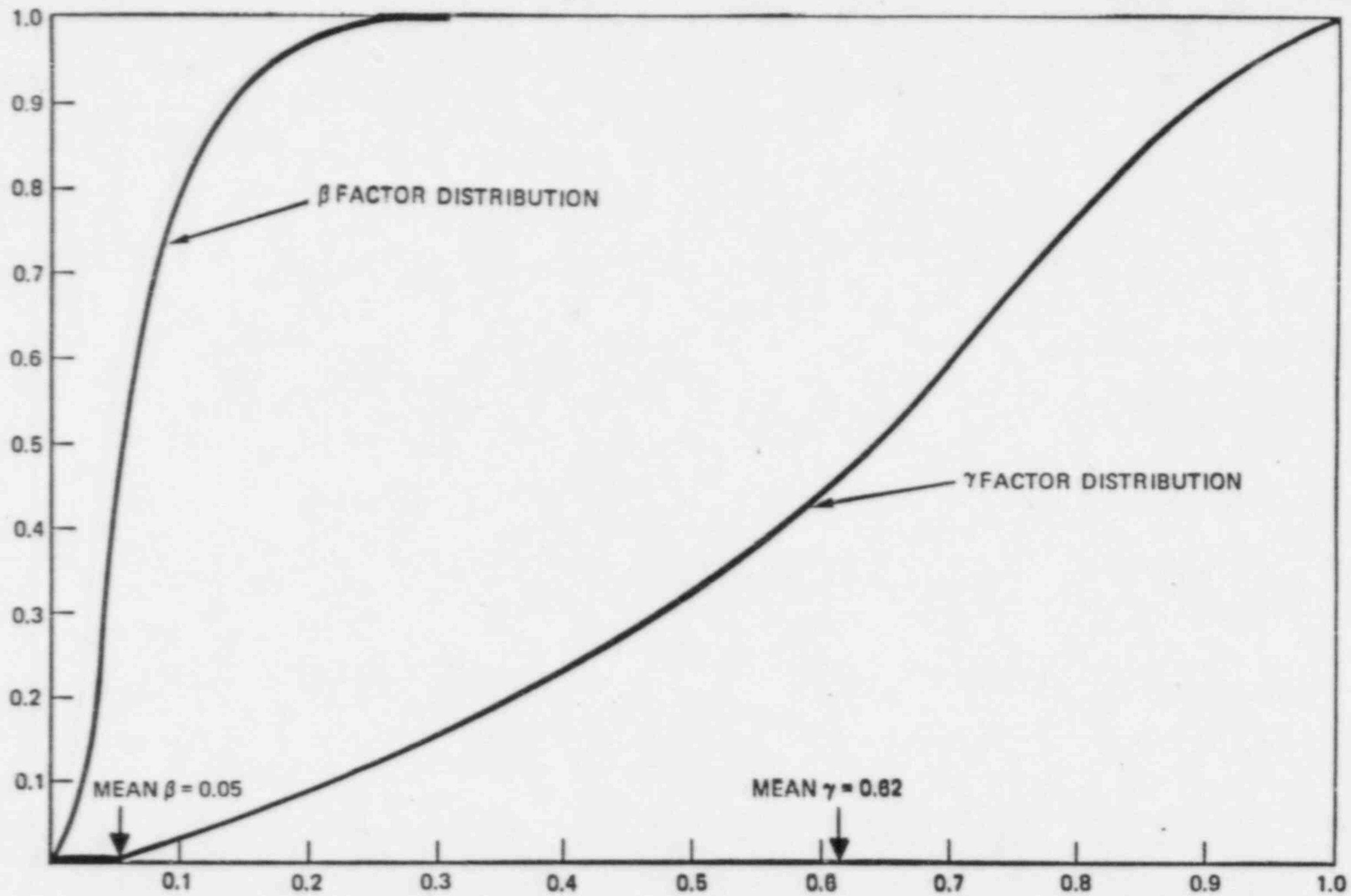
$$\beta = \frac{2n_2 + 3n_3 + 4n_4 + 1}{n_1 + 2n_2 + 3n_3 + 4n_4 + 2} = \frac{54.8}{687.5} = 0.08$$

$$\gamma = \frac{3n_3 + 4n_4 + 1}{2n_2 + 3n_3 + 4n_4 + 2} = \frac{46.0}{55.8} = 0.82$$

$$\delta = \frac{4n_4 + 1}{3n_3 + 4n_4 + 2} = \frac{41.8}{47.0} = 0.89$$

*N/A = NOT APPLICABLE

THE DISTRIBUTION OF MGL PARAMETERS FOR THE EFW PUMP (EXCLUDING DRIVER)



CAUSE TABLE FOR EXAMPLE AUXILIARY FEEDWATER SYSTEM FOR THREE ALIGNMENTS EVALUATED USING MGL MODEL

Normal Alignment		Motor-Driven Pump in Maintenance		Turbine-Driven Pump in Maintenance	
Cause	Frequency	Cause	Frequency	Cause	Frequency
P_3	4.2(-4)	P_3	4.2(-4)	P_3	4.2(-4)
V_4	3.6(-4)	$2TV_1$	4.2(-4)	V_4	3.6(-4)
$4V_3$	2.5(-5)	V_4	3.6(-4)	M_2	1.9(-4)
$M_2(P_1 + T)$	1.1(-5)	P_2	1.9(-4)	P_2	1.9(-4)
$4V_1(P_1 + T)(P_1 + M_1)$	2.7(-6)	$(P_1 + M_1)(P_1 + T)$	1.8(-4)	$4V_1(P_1 + M_1)$	4.7(-5)
C	2.3(-6)	$4V_3$	2.5(-5)	$4V_3$	2.5(-5)
$12V_2V_1$	1.9(-6)	$5V_2(P_1+T)$	1.2(-5)	$4M_2V_1$	2.9(-6)
Others	~ 2.0(-6)	Others	~ 4.0(-5)	Others	~ 2.0(-5)
Subtotal	8.2(-4)	Subtotal	1.6(-3)	Subtotal	1.3(-3)
Alignment Probability	~ 1	Alignment Probability	3.6(-3)	Alignment Probability	4.6(-3)
Total Contribution	8.2(-4)	Total Contribution	5.8(-6)	Total Contribution	6.0(-6)

SYSTEM QUANTIFICATION RESULTS BASED ON THREE PARAMETRIC MODELS

Algebraic Term	Basic Parameter Model	Multiple Greek Letter Model	Binomial Failure Rate Model
P_3	5.5-4	4.2-4	6.8-4
V_4	3.8-4	3.6-4	3.8-4
$4V_3$	4.1-5	2.5-5	4.9-5
$M_2(P_1 + T)$	1.9-5	1.1-5	1.9-5
$4V_1(P_1 + T)(P_1 + M_1)$	2.7-6	2.7-6	3.1-6
C	2.3-6	2.3-6	2.3-6
$12V_2V_1$	2.0-6	1.9-6	1.9-6
Others	~ 2.0-6	~ 2.0-6	~ 2.0-6
Total	1.0-3	8.2-4	1.1-3

COMPARISON OF CAUSE TABLES FOR THREE AUXILIARY FEEDWATER SYSTEMS IN NORMAL ALIGNMENT EVALUATED USING MGL MODEL

Two Motor-Driven; One Turbine-Driven (example system)		Three Motor-Driven		Two Motor-Driven (two steam generators per train)	
Cause	Frequency	Cause	Frequency	Cause	Frequency
P_3	4.2(-4)	P_3	4.2(-4)	P_2	8.0(-4)
V_4	3.6(-4)	V_4	3.6(-4)	V_4	3.6(-4)
$4V_3$	2.5(-5)	M_3	9.5(-5)	M_2	1.9(-4)
$M_2(P_1 + T)$	1.1(-5)	$4V_3$	2.5(-5)	$4V_1(P_1 + M_1)$	4.7(-5)
$4V_1(P_1 + T)(P_1 + M_1)$	2.7(-6)	$4P_2V_1$	2.8(-6)	$(P_1 + M_1)(P_1 + M_1)$	9.8(-6)
C	2.3(-6)	C	2.3(-6)	C	2.3(-6)
$12V_2V_1$	1.9(-6)	$12V_2V_1$	1.9(-6)	$12V_2V_1$	1.9(-6)
Others	~ 2.0(-6)	Others	~ 4.0(-6)	Others	~ 1.0(-6)
Total	8.2(-4)	Total	9.1(-4)	Total	1.4(-3)
Common Cause/ Total	.996	Common Cause/ Total	.997	Common Cause/ Total	.958

CONCLUSIONS ABOUT METHODOLOGY

- SYSTEMATIC APPROACH TO CCF ANALYSIS DEMONSTRATED
- CHOICE OF PARAMETRIC MODEL NOT AS CRITICAL AS HOW ITS INTEGRATED
- DATA ARE AVAILABLE; IT NEEDS TO BE ANALYZED
- IMPORTANT JUDGEMENTS AND UNCERTAINTIES STILL REMAIN
  - HOW TO DEFINE COMPONENT GROUPS
  - ASSESSMENT OF IMPACT VECTORS
  - SPACITY OF DATA FOR HIGHER ORDER PARAMETERS
- REALISTIC RELIABILITY PREDICTIONS NO LONGER HINGE ON UNPROVEN ASSUMPTIONS ABOUT INDEPENDENT EVENTS

CONCLUSIONS ABOUT SYSTEM RELIABILITY

- CURRENT TWO AND THREE TRAIN AUXILIARY FEEDWATER SYSTEMS (AFWS) HAVE SYSTEM UNAVAILABILITIES ON THE ORDER OF 10^{-3}/DEMAND

  Spread of PLANT TO PLANT VARIABILITY ± FACTOR OF 10

- AFWS UNAVAILABILITY DOMINATED BY COMMON CAUSE EVENTS — ANY system ANALYSIS THAT IGNORES CCF - A WASTE OF TIME

- PRINCIPAL BENEFIT OF STEAM DRIVEN PUMP IS INDEPENDENCE OF ELECTRIC POWER VERSUS ADDED DIVERSITY

- NEED TO RETHINK THE USE OF REDUNDANCY AND DIVERSITY AS A DEFENSE AGAINST COMMON CAUSE FAILURES

Pickard, Lowe and Garrick, Inc.

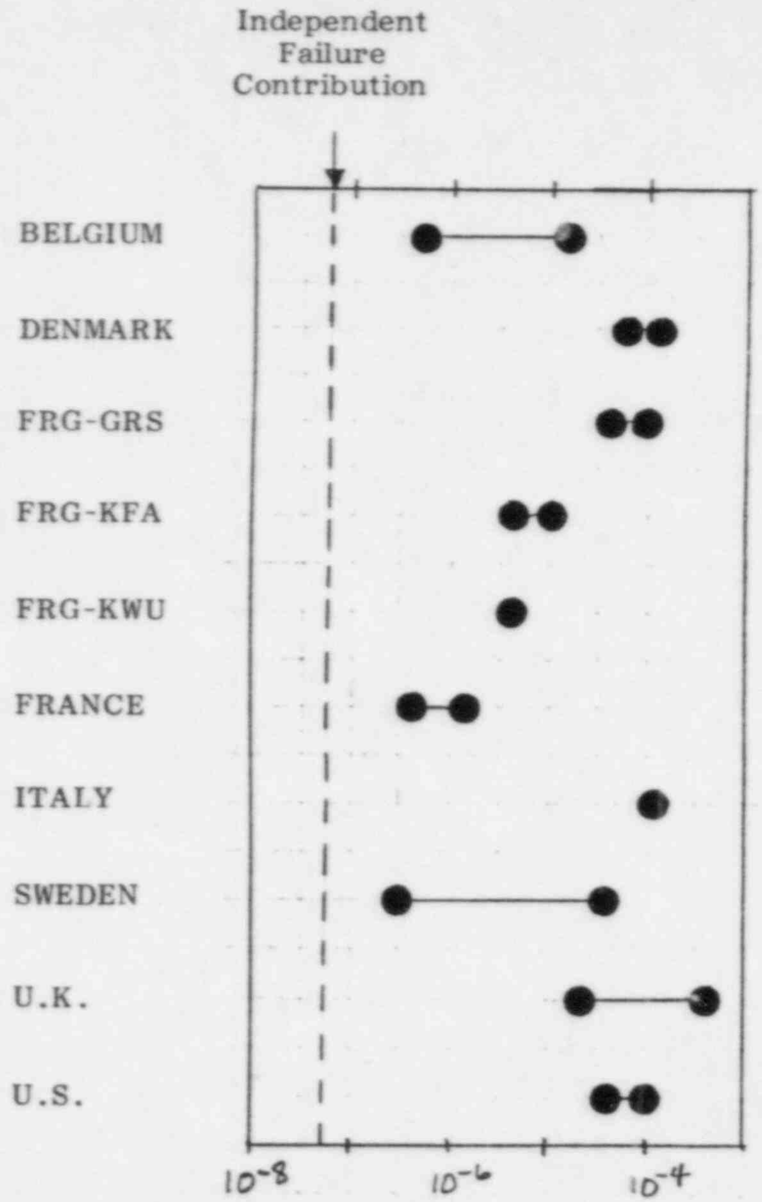
COMMON CAUSE FAILURE RELIABILITY BENCHMARK EXERCISE

- PURPOSE IS TO DEVELOP CONSENSUS CCF ANALYSIS PROCEDURES
- COORDINATED BY JOINT RESEARCH CENTER, ISPRA, ITALY
- TEN TEAMS FROM EUROPE AND U.S. ANALYZING SAME PROBLEM
- PLG REPRESENTING U.S. UNDER EPRI/NRC SPONSORSHIP
- PARALLEL EFFORTS AT EPRI AND NRC TO DEVELOP PROCEDURES
- PROBLEM IS LOSS OF FW AT KWU PLANT - SIX-TRAIN SYSTEM
- INDEPENDENT FAILURE ANALYSIS FIXED
- FIRST OF TWO ANALYSIS PHASES COMPLETED
- SCHEDULED FOR COMPLETION, MARCH 1986

PRELIMINARY RESULTS OF THE CCF-RBE BENCHMARK – TECHNICAL APPROACH

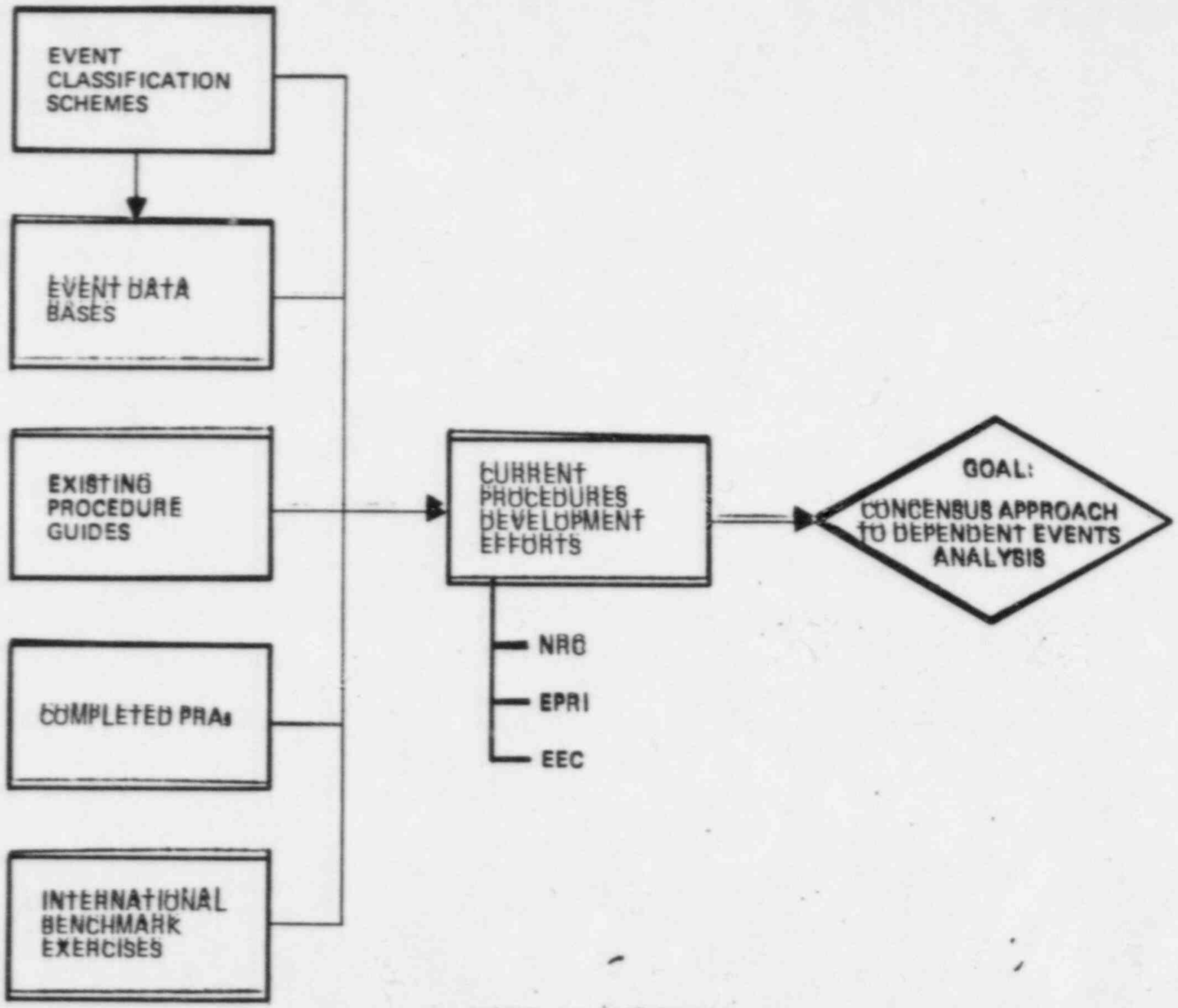
TEAM	QUALITATIVE	QUANTITATIVE
A. BELGIUM	FMEA	BETA FACTOR
B. DENMARK	SYSTEM FAMILIARIZATION	BINOMIAL FAILURE RATE
C. FEDERAL REPUBLIC OF GERMANY-1 (GRS)	SYSTEM FAMILIARIZATION	BETA FACTOR, MARSHALL-OLKIN
D. FEDERAL REPUBLIC OF GERMANY-2 (KFA)	SENSITIVITY ANALYSIS	MARSHALL-OLKIN
E. FEDERAL REPUBLIC OF GERMANY-3 (KWU)	SYSTEM FAMILIARIZATION	MULTIPLE GREEK LETTER
F. FRANCE	GENERIC CAUSE ANALYSIS	MULTIPLE GREEK LETTER
G. ITALY	SYSTEM FAMILIARIZATION	BINOMIAL FAILURE RATE
H. SWEDEN	SYSTEM FAMILIARIZATION	MULTIPLE GREEK LETTER
I. UNITED KINGDOM	FMEA/CHECKLIST	MODIFIED BETA FACTOR, CUTOFF
J. UNITED STATES	SYSTEM FAMILIARIZATION	MULTIPLE GREEK LETTER

CCF-RBE BENCHMARK
PRELIMINARY POINT ESTIMATE RESULTS

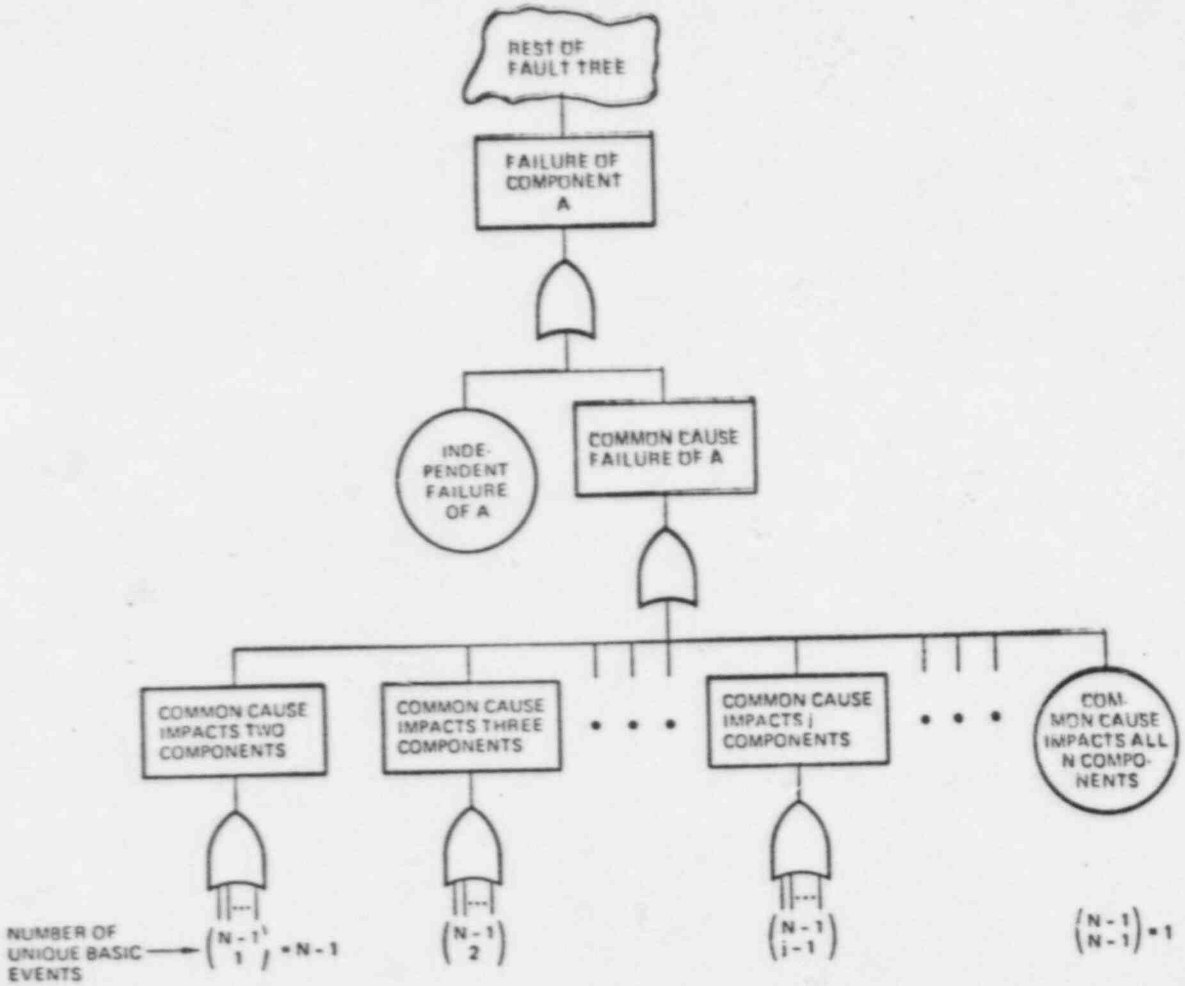


Pickard, Lowe and Garrick, Inc.

DEVELOPMENT OF CONSENSUS APPROACH TO DEPENDENT EVENTS ANALYSIS



GENERAL COMMON CAUSE FAULT TREE SUBTREE FOR COMPONENT A IN A COMMON CAUSE GROUP OF N COMPONENTS



NRR STAFF PRESENTATION TO THE ACRS

SUBJECT:	STAFF COMMENTS ON PLG REPORT
DATE:	DECEMBER 2, 1985
PRESENTER:	ADEL EL-BASSIONI
PRESENTER'S TITLE/BRANCH/DIV:	SENIOR RELIABILITY & RISK ANALYST RELIABILITY AND RISK ASSESSMENT BRANCH DIVISION OF SAFETY TECHNOLOGY
PRESENTER'S NRC TEL. NO.:	492-7646
SUBCOMMITTEE	DECAY HEAT REMOVAL SYSTEMS

HIGHLIGHTS OF THE PLG STUDY

- TREATMENT OF CCF IN PUBLISHED PRA STUDIES IS INCONSISTENT AND NONSYSTEMATIC
- RANDOM INDEPENDENT FAILURES CONTRIBUTED LESS THAN 1% OF THE POINT ESTIMATE OF AFWS UNAVAILABILITY
- INCREASING THE REDUNDANCE OF A 2 TR AFWS BY ADDING A THIRD TRAIN IMPROVED THE PER DEMAND UNAVAILABILITY BY A FACTOR OF ABOUT 1.5
- ADDITION OF A THIRD DIVERSE TRAIN SLIGHTLY INCREASED THIS FACTOR TO ABOUT 1.7
  (NET EFFECT OF DIVERSITY IS UNAVAILABILITY REDUCTION OF ABOUT 10%)
- A TYPICAL 3 TR AFWS CONFIGURATION UNAVAILABILITY IS ABOUT 1.0E-3 PER DEMAND

STAFF EVALUATION

METHODOLOGY: ATTRACTIVE AND SYSTEMATIC
HAS A NUMBER OF LIMITATIONS

- CCF COVERAGE IS LIMITED TO TREATMENT OF DEPENDENCY AMONG SIMILAR COMPONENTS

  EXTENSION TO DISSIMILAR COMPONENTS WILL DEPRIVE IT OF SIMPLICITY

- FAILURE DEPENDENCY EXPERIENCE DATA IS STILL SPARSE

  METHODOLOGY RELIES ON SUBJECTIVE INTERPRETATION OF DATA AND ITS APPLICABILITY

- CASE STUDY EVALUATION DID NOT ACCOUNT FOR AFWS SUPPORT SYSTEMS, AND FOR RECOVERY ACTIONS THAT MIGHT HAVE IMPROVED AFWS UNAVAILABILITY

STAFF EVALUATION (CONTD.)

- DEVELOPING FTs BEYOND BASIC EVENT LEVEL (TO SUB-BASIC EVENT) RESULTED IN AN INCREASE IN THE NUMBER OF CUTSETS BY A FACTOR OF 5

  SUCH AN INCREASE CAN OVERBURDEN THE ANALYSIS

- METHODOLOGY EMPHASIZES THE QUANTITATIVE ASPECTS OF THE ANALYSIS AS COMPARED TO QUALITATIVE ASPECTS (INSIGHTS, VULNERABILITIES)

STAFF EFFORTS

THE CALL FOR CAREFUL, WELL DISCIPLINED, AND CONSISTENT TREATMENT OF DEPENDENT FAILURES HAS THE FULL SUPPORT OF THE STAFF

- CCF HAS HIGH PRIORITY IN SEVERAL RES AND NRR PROGRAMS
  - SYSTEMS INTERACTION
  - RMIEP
  - COOPERATIVE EFFORT WITH EPRI
  - EUROPEAN CCF RELIABILITY BENCHMARK EXERCISE (JRC ISPRA)

CONCLUSIONS

- IMPACT OF CCF ON AFWS UNAVAILABILITY MAY HAVE BEEN OVERSTATED
- WE DO NOT AGREE WITH THE REPORT CONCLUSIONS ABOUT IMPACT OF DIVERSITY ON SYSTEM UNAVAILABILITY
- STAFF RECOGNIZES THAT ASSURANCE OF INDEPENDENCE AMONG REDUNDANT AND DIVERSE TRAINS IS THE REAL KEY TO AFWS UNAVAILABILITY IMPROVEMENT

PRESENTATION OUTLINE

- COMMON CAUSE ANALYSIS PROCEDURES
- EXAMPLE "GENERIC" ANALYSIS OF THREE-TRAIN AFWS
- CONCLUSIONS AND INSIGHTS
- INTERNATIONAL BENCHMARK EXERCISE

MUTUALLY EXCLUSIVE PROPOSITIONS (About Dependent Events)

A. WE DON'T KNOW HOW TO DEFINE IT, MODEL IT, QUANTIFY IT, OR KNOW EXACTLY WHAT CAUSES IT.

B. WE KNOW HOW TO DEFEND AGAINST IT.

MADE MUCH PROGRESS ⇒ Still a lot of CONFUSION AND INCONSISTENCY

⇒ Biggest area of inconsistency is in what I call system level common cause failure analysis in the applied risk and reliability evaluations of the past several years the treatment of these events has ranged from total omission to inclusion as the dominant contributors

⇒ This inspired EPRI to sponsor a project on PRA procedures for dependent events analysis

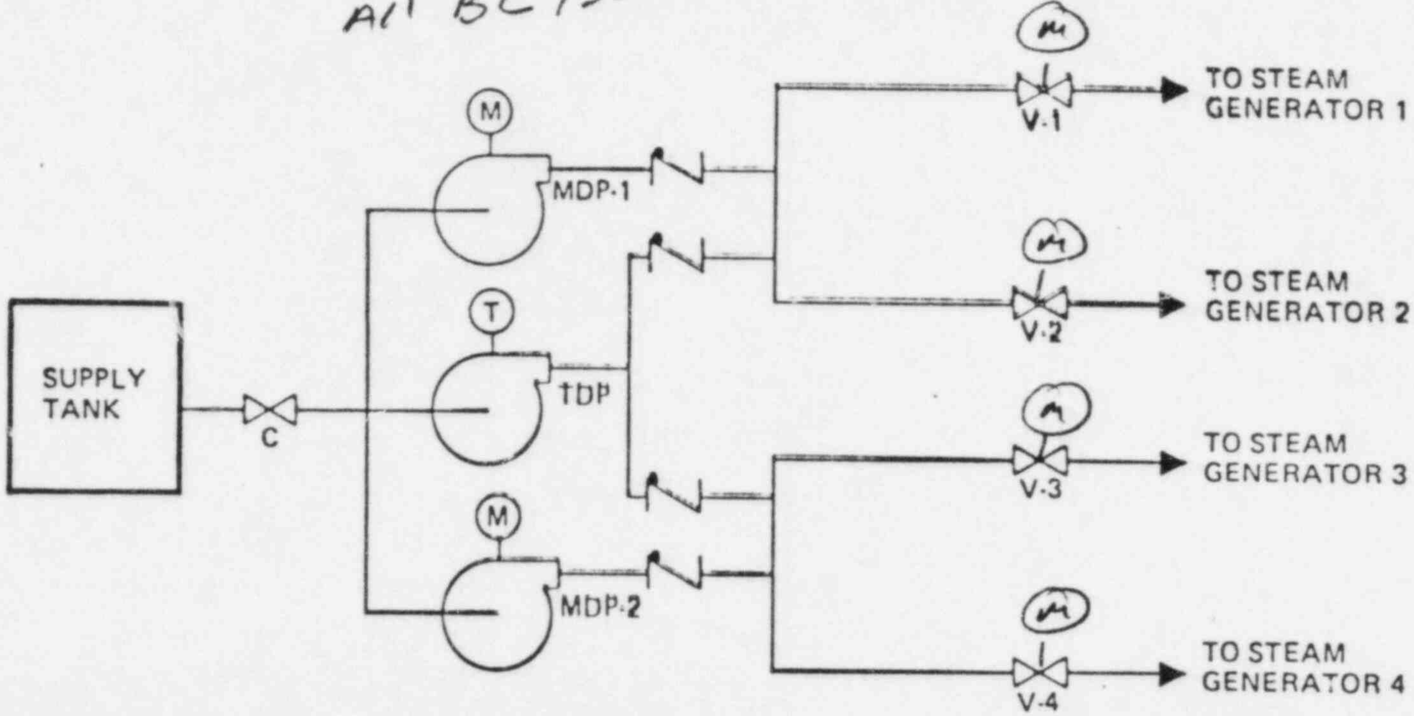
SYSTEMATIC PROCEDURE FOR SYSTEMS ANALYSIS

* 1. SYSTEM FAMILIARIZATION => common cause groups
* 2. LOGIC MODEL DEVELOPMENT => extension for CCE
* 3. BOOLEAN ANALYSIS => more cutsets
* 4. ALGEBRAIC MODEL DEVELOPMENT => alternative parametric models
* 5. PARAMETER ESTIMATION => lots of extra work
* 6. SYSTEM QUANTIFICATION
* 7. RESULTS INTERPRETATION

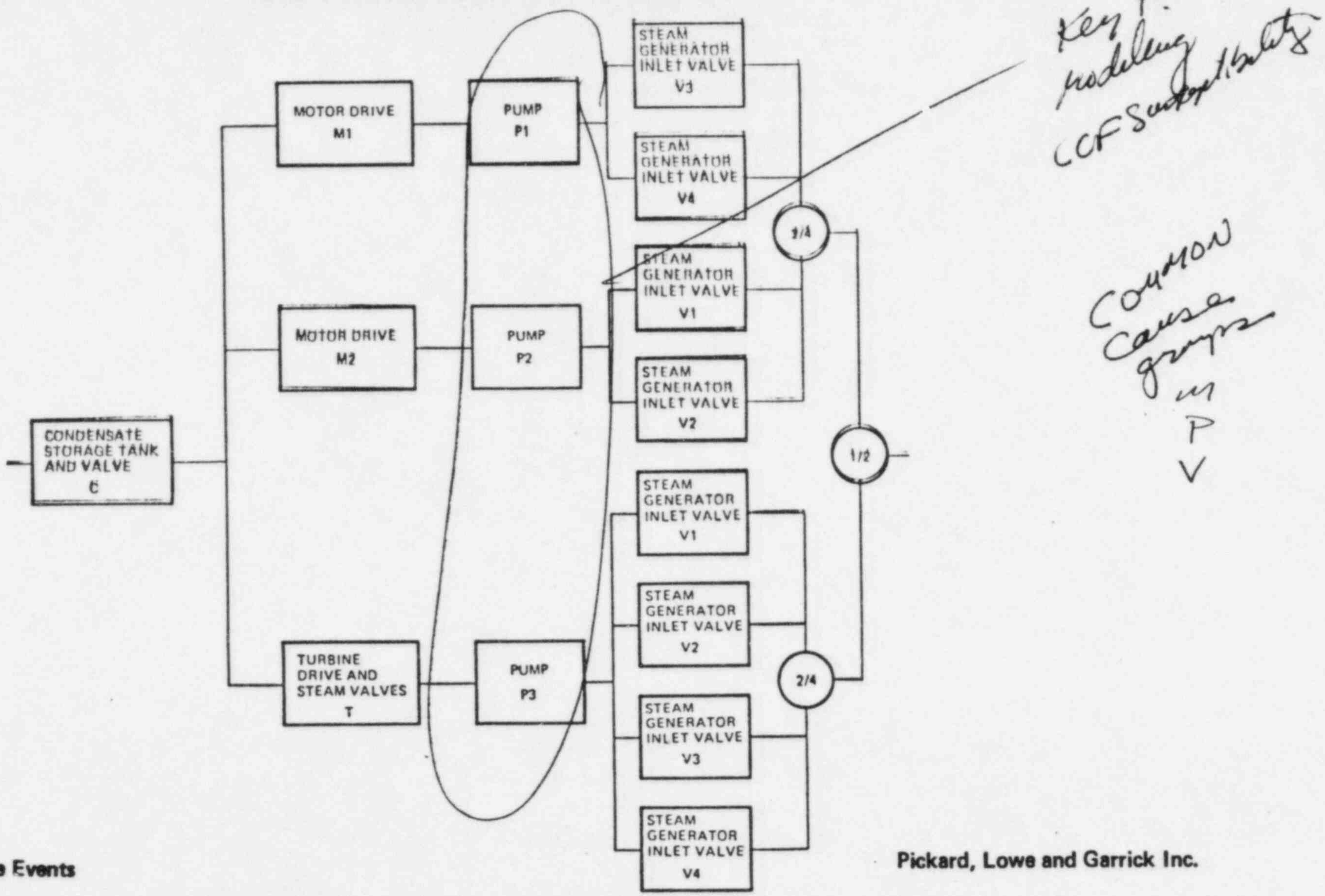
* CRITICAL STEPS FOR COMMON CAUSE ANALYSIS

SIMPLIFIED SCHEMATIC OF MAJOR COMPONENTS IN AN EXAMPLE AUXILIARY FEEDWATER SYSTEM

LOOKING AT
All BC ISS AVAILABLE



RELIABILITY BLOCK DIAGRAM OF AUXILIARY FEEDWATER SYSTEM — NORMAL ALIGNMENT



COMMON CAUSE EVENT SUBTREE FOR MOV V1